



## *Content Filtering Enhances Monitoring and Control of Email*

The newest enhancement to our Email Security Gateway Powered by SpammerTrap® enables organizations to monitor and control email messages containing client-specified content—helping to prevent sensitive data from being leaked either inadvertently or intentionally.

This additional layer of security facilitates compliance with internal corporate policies as well as government regulations such as SOX, HIPAA, GLBA and others. It helps to safeguard organizations from legal actions that can damage reputations and result in costly penalties.

### **All These Features - Standard**

- Enables Inbound and Outbound email messages to be scanned for content, as specified by client site administrator.
- Allows administrators to whitelist, tag, quarantine or block messages containing the specified content.
- Enables filtering of personally identifiable information (PII), as specified by client, such as:
  - Social Security numbers
  - Tax ID numbers
  - Credit card numbers
  - Account numbers
  - Employee identification numbers
- Filters according to specified keywords, customized expressions, or patterns of content.
- Scans either subject content or email body content, or both—which many filters do not.
- Enables administrators to test new or edited content rules prior to live production.
- Simplifies set-up with intuitive screens, plus 24/7 technical support as needed.
- Offers a variety of useful reports.

### **Benefits of Email Content Filtering**

- Reduces potential for leakage of sensitive data
- Facilitates regulatory compliance with Sarbanes-Oxley, HIPAA, GLBA and others
- Supports compliance with corporate policies
- Deters abuse or misuse by employees or third-party/outsources
- Protects client records, payroll records, and other personally identifiable information
- Helps avoid negative publicity and legal actions resulting from compromised emails
- Provides robust reporting to document results
- Enhances overall email security

Content filtering is available at no charge with all SME, ENT and GEM models, integrated in the email security appliance with no additional hardware purchase required.

### **The Next Generation of Email Security**

SECNAP continues to drive the standard higher for email security—this time, with content filtering that offers unrivaled flexibility, easy configurability, and comprehensive performance reporting.

Contact us to learn more about this and other next-generation features of the Email Security Gateway Powered by SpammerTrap.

***Cybercrime advances relentlessly. Shouldn't your security solutions?***

**877-667-7264**

**www.secnap.com**

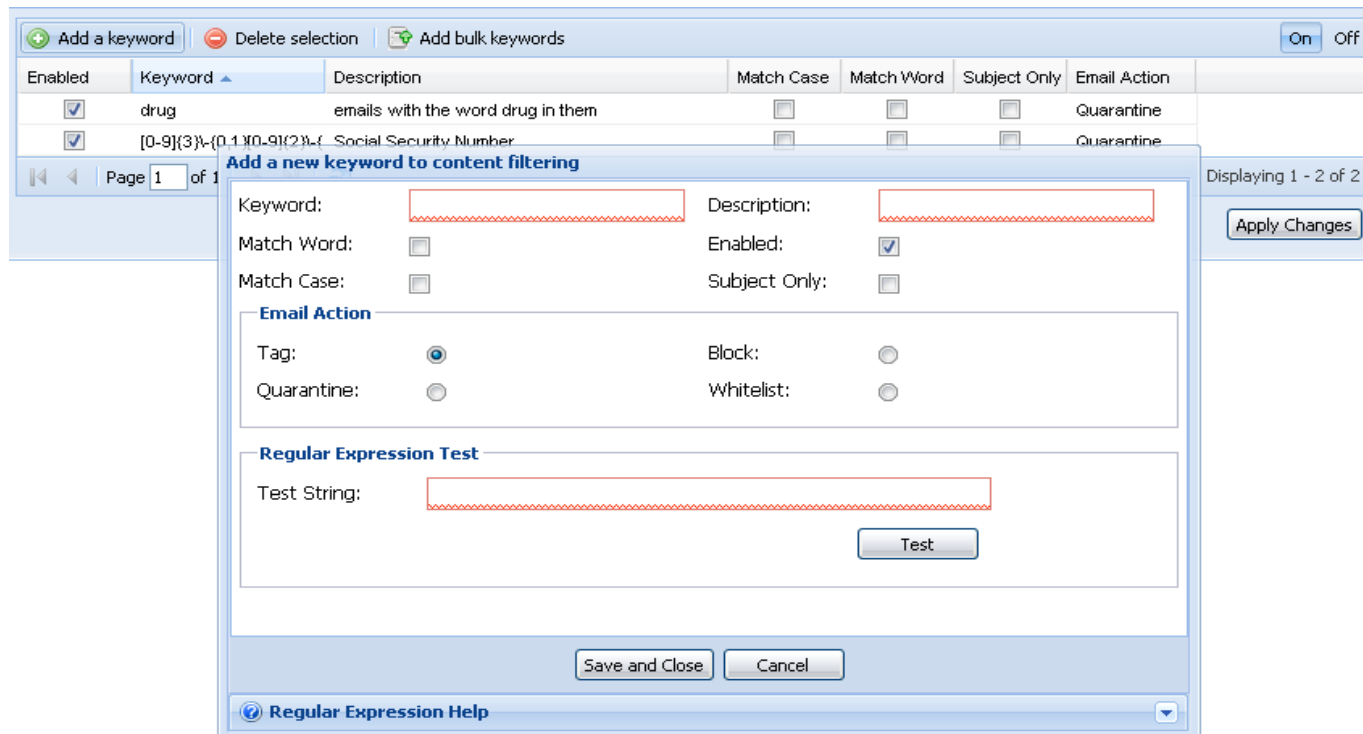
*See reverse side for screen illustrations and feature highlights*



SpammerTrap Content Filtering is accessible through the SpammerTrap maintenance function. To begin set-up, enter a keyword and description of it (see screen below). Then, specify instructions for keyword review and matching, which may include any or all of these options: Match Word, Match Case, Subject Only (default is a review of subject and message body).

This screen also enables selection of Email Actions to be taken for individual emails when specified keywords are found, with options including Tag, Quarantine, Whitelist, or Block.

*Other useful features enable keywords to be tested prior to live production using the "Test String" field, and to be added in bulk as a time-saver.*



**What use is a great feature without great reporting?** SpammerTrap Content Filtering provides highly flexible reporting that enables you to track results and measure performance, sorting by any column of data (see screen below). Searching for data is easy too, using filters available for each column.

