Executive Summary .................................................................................................................. 4

Proventia Mail Filter 2.2 Deployment Scenario ........................................................................ 7
Between MTA and Internet ......................................................................................................... 7

Content Analysis ....................................................................................................................... 8
Integration of CAL with Proventia Mail Filter ........................................................................... 8

Content Analysis in Detail ........................................................................................................... 11
Keyword Search ......................................................................................................................... 11
Important Documents ................................................................................................................ 11
Porn Detector ............................................................................................................................. 12
Media Type ................................................................................................................................ 12
Source Code Detector ................................................................................................................ 12
Text Categories .......................................................................................................................... 13

Spam Detector ........................................................................................................................... 13
Virus Detector ............................................................................................................................. 13
URL Checker ................................................................................................................................ 14
Message Fields Checker ............................................................................................................ 14
Attachment Checker .................................................................................................................. 14

Proventia Mail Filter 2.2 Concept of Filtering .......................................................................... 15
Who, When, What, Action .......................................................................................................... 15
Filtering by E-mail Address Patterns ....................................................................................... 16
Filtering by Users and User Groups ......................................................................................... 16
Filtering Criteria – What Object ................................................................................................ 16
Actions ......................................................................................................................................... 17

Proventia Mail Filter 2.2 Actions ............................................................................................... 18
Modification ................................................................................................................................. 19
Modify .......................................................................................................................................... 19
Remove Attachment ................................................................................................................... 19
Notification ................................................................................................................................. 19
Macros ..............................................................................................................22
System Macros .................................................................................................22
Message Macros ...............................................................................................23
Common Message Fields .................................................................................23

Spam Detection ..................................................................................................24
RBL, Black Lists and White Lists .........................................................................24
E-Mail Header Checking .......................................................................................25
Spam Signature Database ...................................................................................25
Spam Text Categorization ...................................................................................25
Pornographic Images and Spam URLs ...............................................................26
Friendly Sender .................................................................................................26

Management: The Message Store ......................................................................27

Conclusion ..........................................................................................................29

Technical Requirements .....................................................................................30

About Internet Security Systems .......................................................................31
Executive Summary

While e-mail brings speed, convenience and simplicity to modern communication, the negative side of e-mail, misuse and spam, are causing serious problems for businesses, including significant losses in employee productivity.

Internet Security Systems Proventia Mail Filter 2.2 is an e-mail filtering application that allows you to monitor, manage and control inbound and outbound e-mail traffic for your entire organization. With Proventia Mail Filter 2.2, organizations can increase employee productivity, reduce legal liability and improve network performance.

Proventia Mail Filter 2.2 not only detects of unwanted or confidential content, e.g. pornographic images, internal confidential documents, spam and junk mail etc, but also defines user-specific actions regarding outgoing and incoming e-mails. Intelligent blocking of unwanted e-mails protects the company brand and reputation and reduces the potential for resulting financial loss.

E-mail content, including attachments, is analyzed with Internet Security Systems’s premier content filtering technology. Proventia Mail Filter 2.2 recognizes numerous file formats including Office documents, images, archives and multimedia files, irrespective of the file name and extension. Even compressed files are automatically unpacked and analyzed.

Proventia Mail Filter 2.2 is easy to configure for individual users and user-groups from within the Proventia Mail Filter management console. Based on a policy system, the exchange of e-mail content can be denied or allowed for each employee individually. If desired, e-mails can also be sent to the administrator to be examined manually. Further actions such as modifying e-mail content or changing e-mail delivery status are also made possible with the Proventia Mail Filter 2.2.
Proventia Mail Filter 2.2 System Architecture

Proventia Mail Filter 2.2 should be placed between your corporate intranet and the Internet. It will work with an existing Simple Mail Transfer Protocol (SMTP) server. Proventia Mail Filter 2.2 supports various major platforms, including Windows 2000 and Windows XP.

There are 3 major components of Proventia Mail Filter 2.2: Proventia Mail Filter 2.2 Server, Proventia Mail Filter Management Console and the Content Analysis Library (CAL). Each has unique functions and features, and together they perform efficient e-mail message analysis and filtering.

The combinations work in the following way: Proventia Mail Filter 2.2 Server is responsible for implementing the defined policy. It analyzes incoming and outgoing messages that go through the SMTP server and searches for matching messages. The Proventia Mail Filter Management Console provides easy and direct graphical user interface (GUI) to help users in policy configuration. Besides policy configurations, statistics can also be viewed. It serves as a useful tool to configure the Proventia Mail Filter 2.2 Server.
Last but not least is the Content Analysis Library. The CAL provides powerful analysis modules that allow you to detect content from text to archived documents. The use of multiple CAL modules can also be implemented in the same rule to ensure higher efficiency. Further information on this topic is discussed in later sections of this whitepaper.

The Proventia Mail Filter 2.2 Server implements content analysis and filtering based on policy rules. It does not matter if you have a Microsoft Exchange Server or a Linux Sendmail/Postfix Server, Proventia Mail Filter will work with your existing SMTP server as a SMTP relay. With the variety of integration possibilities, you will find one that suits the needs of your corporation.

Proventia Mail Filter 2.2 also integrates itself with your current directory service. Whether it is Microsoft Windows NT Domain or Active Directory, or Lightweight Directory Access Protocol (LDAP), Proventia Mail Filter 2.2 can make use of your current directory service to provide you with lists of users and user groups to be used to define analysis and filtering rules.

The next section covers how Proventia Mail Filter 2.2 can be integrated into your current network.
Proventia Mail Filter 2.2 Deployment Scenario

Internet Security Systems’ Proventia Mail Filter 2.2 is a complete and flexible system that can be easily deployed in most infrastructures. Proventia Mail Filter 2.2 only requires integration with a Mail Transfer Agent (MTA) that supports SMTP. This flexibility provides easy integration within your corporation. Below is a deployment scenario which will explain how the Proventia Mail Filter 2.2 will fit best in different environments.

Between MTA and Internet

The most common scenario is where the Mail Transfer Agent is located between the intranet and the Internet. It could be a Microsoft Exchange server or a Postfix SMTP server. Proventia Mail Filter 2.2 can be deployed as shown below:

With this deployment Proventia Mail Filter server will act as the SMTP relay for your current SMTP server. In this setting, all incoming and outgoing e-mail messages will be analyzed and filtered by Proventia Mail Filter.
Content Analysis

Internet Security Systems’s Content Analysis Library is based on knowledge acquired over the past six years together with customers, engineers and researchers in different industries and universities. Its core technology has been proven in many applications in the past and is continuously being improved.

Different methods support text, images, videos, archive files and virtually any kind of files, documents, data and information, which in short is called content. Core technologies for content analysis are Optical Character Recognition (OCR), face recognition, recognition of logos, trademarks, signs and symbols. Further, it includes image categorization, nudity detection, text categorization, digital fingerprints, etc.

Integration of CAL with Proventia Mail Filter

For each e-mail, the content analysis process is defined by four steps:

Step One: Recognition of File Type

E-mails can be complex in nature with multiple attachments, ZIPs, HTML and other kinds of files. In some cases, it is not even obvious which kind of file is attached in an e-mail, since somebody might just rename the file or its extension. Internet Security Systems’s CAL offers a reliable solution to this problem. Using binary pattern matching, it is possible to recognize almost every type of file or attachment by its content rather than its file extension. Each file format (e.g. a ZIP file or a Word file) has a special signature (some bytes or a typical pattern) stored somewhere within the file that can be used to uniquely identify its type. For security reasons, Proventia Mail Filter can be configured to block e-mails that contain unrecognizable file types.

Step Two: Break Down into Basic Parts

Most files contain more than one piece of content. For example, archive files (.zip and others) contain multiple files, all with different content. Sometimes they store hundreds or different text files, images, Excel sheets etc. Even commonly used Word files may contain images or multiple files as embedded objects.

This second step now breaks each file or attachment down into its unique parts. This sometimes can be a very complex job. Consider a ZIP file which contains a Word file, which itself contains another ZIP file.
The CAL handles these complex operations in the background. Proventia Mail Filter users never have to bother with this.

Figure: Various parts of e-mail are extracted

**Step Three: Content Analysis in Detail**

The content analysis in step three, all comes down to the common media types: text, images, video, sound and others. Each piece of content is analyzed by the following powerful CAL modules which are described in detail later:

- Keyword Search
- Pornography Detector
- Media Type
- Source Code Detector
- Text Categories
- Important Documents
- URL Checker
- Attachment Checker
- Message Field Checker
- Virus Detector
- Spam Detector
Every module can be configured to exactly define what content is important for your organization.

Automated content transformation is another important and powerful feature of the Content Analysis Library. For example, text content can have many different sources. In addition to a text file attachment, Word files, HTML files and more can be handled as text. Images can also contain text information. Using built-in Optical Character Recognition, the CAL automatically extracts all text found within an image and transfers it into text content. This way, the Keyword Search module is able to find keywords within images. This allows you to block any kind of content that contains the word "confidential", no matter if this occurs in the subject line of an e-mail, in a Word file or an image.

**Step Four: Build up the Result**

The final step collects all the data from the previous steps and builds a detailed categorization of the e-mail that is being processed by Proventia Mail Filter. Depending on the categories, rules and actions you have defined, the e-mail can now be correctly handled by Proventia Mail Filter. All results from every analysis module are available in XML format and can further be used in actions for custom e-mail handling, reporting, etc.
Content Analysis in Detail

With CAL, Proventia Mail Filter is capable of analyzing e-mails with the following modules:

Keyword Search

The Keyword Search module is used to search for special keywords in any text content. It also offers keyword combinations and the usage of wildcards (text patterns). Here are some examples:

<table>
<thead>
<tr>
<th>Keyword Combination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Porn, XXX, or adult-related</td>
<td>Identifies content that contains any of the words “porn,” “XXX” or “adult-related.”</td>
</tr>
<tr>
<td>Confidential contract</td>
<td>Identifies content where the word “confidential” appears near the word “contract” within a document.</td>
</tr>
<tr>
<td>Porn*</td>
<td>Identifies content that contains any word that starts with the prefix “porn,” like pornographic, pornsite etc.</td>
</tr>
</tbody>
</table>

Important Documents

With the Important Document module you can prevent special or confidential documents from leaving the organization. To ensure that documents do not leave your company, Proventia Mail Filter provides a special document repository that can be configured individually.

Any kind of confidential data, e.g. contracts, project files, customer data, business reports, banking information and financial data can be protected.

Just inform Proventia Mail Filter where your organization stores important documents, and enter directories of network file shares, file servers etc. Proventia Mail Filter automatically builds a database (repository) of all the documents with all the necessary information to identify this content later in e-mails. This process is called a digital fingerprint. For every document a digital fingerprint will be stored.

Every outgoing e-mail and its attachments will be analyzed and compared with the documents in the repository. If a sufficient piece of information is found within the e-mail it will be identified and reported. Text content and images will be analyzed and identified.
What constitutes a sufficient piece of information that can be identified? For text content, usually two sentences or a few lines out of a text document are enough to identify its origin. With images, the method is quite robust for resizing and format changes, so images can be converted from BMP to JPEG and will still be identified. For all other content types, identical copies will be identified and reported.

Depending on an organization’s security policy, individual actions can be defined to encrypt, block, isolate, delay or simply notify a defined person. All unauthorized transmission of e-mail containing intellectual property or breaches of confidentiality will be prevented.

**Porn Detector**

This module identifies pornographic images by detecting of nudity within an image using multiple algorithms. First, a face detection process locates all faces in the image. This is used to get reliable information about skin tones, skin color and skin texture in the picture. Using this information as reference, the rest of the image will be analyzed for typical distribution of skin tones and texture.

If no faces can be found, the Porn Detector uses a predefined dataset with skin colors and skin textures, built with a large database of sample data.

**Media Type**

Sometimes it is useful to identify certain file types. As mentioned before, file types are recognized intelligently using binary pattern matching. The same technology is applied here. For instance, this module makes it possible to block all PDF files. It does not matter if a PDF file like intro.pdf is renamed into intro.jpg. It can also be packed into a ZIP archive, which will be renamed into word.doc, for instance. The CAL will identify this original file as a PDF file.

The Media Type module offers a selection of all file formats supported by the CAL and helps you control which file formats are allowed for e-mail use in your organization.

**Source Code Detector**

Depending on your organization, programming source code as well as scripts and HTML pages can be valuable assets that you have to protect from external publication and misuse. Using the Source Code Detector, the CAL can identify source code and source code pieces in various flavors like C++, Visual Basic,
Java, Perl, SQL, HTML and others. The Source code Detector works on any text content as mentioned before with other modules.

**Text Categories**

The Text Categories module can be used to analyze the meaning of text. Compared to the Keyword Search module, the Text Categories module does not look just for keywords, it treats the whole text as an entity. Based on semantic and statistical methods, each piece of text will be analyzed and compared with a database of predefined and well-trained categories. The text categories database right now includes categories like Pornographic, Hate, Crime and others. More categories are being added continuously.

Using the Text Categories module you can save your organization from e-mails that contain illegal or unwanted content that does not have the typical keywords in it.

**Spam Detector**

Spam is one of the most common e-mail abuses today. E-mail spam brings in not only unwanted content to your users, but also wastes valuable bandwidth and system resources. The Spam Detector is capable of detecting spam that is found in your e-mail and will notify Proventia Mail Filter to take further action against these spams. The antispam technology provided by the Proventia Mail Filter 2.2 uses multiple methods in order to achieve an excellent detection rate. The following methods are especially designed to detect spam:

- Spam Online Classifier
- Spam Signature Database
- Spam URL Check
- Spam Heuristics

A detailed description of the Spam Detector follows in a special chapter.

**Virus Detector**

Viruses are known for bringing threats to computer systems, and e-mail is one of the possible-propagating agents. With Proventia Mail Filter 2.2, an integrated virus scanner minimizes virus threats from incoming e-mail, and controls the spread of virus-infected documents within your network.
URL Checker

This module compares data with URL entries found on the Internet. It utilizes the Filter Database, a huge collection of URLs. The URL database is divided into 58 categories that allow you to select content to be compared. It is easy to configure, and effective because categories are well-defined and the URL database is constantly updated.

Message Fields Checker

The Message Fields Checker is a customizable header checker that looks into e-mail headers for matching items. The headers are defined as you create a new What object (see description in the Concept of Filtering section) using the Message Fields Checker. By using different macros, you can assign Proventia Mail Filter to examine e-mail headers for desired information.

Attachment Checker

Attachments have made e-mail a more practical and common tool, but have also introduced problems for organizations. Since the size of attachments, especially non-work-related content, can be quite large, attachments will waste company resources if undesired content is constantly distributed.

The Attachment Checker will alleviate this problem. It effectively checks attachments found in messages with the given conditions configured by the Management Console: number of attachments, size of each single attachment and total size of the whole message. With this rule, attachment propagation can now be controlled and monitored. Together with other CAL modules, you can even examine the content of the attachment so that control of attachment content can also be implemented.
Proventia Mail Filter 2.2 Concept of Filtering

Every message that travels through Proventia Mail Filter 2.2 will be analyzed and checked to see if there is a rule defined that matches the content or nature of the message. A rule consists of different entities. It defines the people involved (Who is sending or receiving the message) and the time allowed (When should the message be allowed/blocked). It also tells Proventia Mail Filter 2.2 to look for What sort of content. Finally Actions should be taken to deny or allow the message according to the defined rule.

Who, When, What, Action

The mail policy for Proventia Mail Filter 2.2 is defined by multiple rules. Each rule defines one piece of your policy. In detail, each rule consists of the following elements:

- Who Objects
- When Objects
- What Objects
- Action Objects

A Who Object defines any combination of e-mail address, users and user groups. Using the Proventia Mail Filter Management Console, you can define either individuals, or groups of people using different Who Objects. A When Object defines time ranges (e.g. “lunch-break”). Time ranges are used to define rules...
based on time of day, allowing you to set up different policies for different times, such as main business hours and late hours.

A What Object defines content categories that should be analyzed or detected. It tells Proventia Mail Filter what sort of data is to be noticed and to be taken action on. When it comes to which actions to take, this is the duty of Action Objects. The combination of all four objects creates a rule.

**Filtering by E-mail Address Patterns**

The best way to control e-mail content in your corporation is to define lists of addresses that are allowed. This list could consist of only corporate e-mail addresses, or a list of recognized/known e-mail addresses. This will reduce e-mail misuse. The same lists can also be used to control outgoing message content so that important documents will not be leaked to the outside world.

**Filtering by Users and User Groups**

Filtering by users and user groups is a powerful and easy way to apply corporate Internet access policy. Usually different user groups in a Windows domain or Directory Service correspond to different privileges and needs. As mentioned above, this information can be easily used for mapping users and user groups to Who Objects in respective rules.

Changes in the directory service are continuously monitored and updated in the Proventia Mail Filter Management Console to ensure integrity and to minimize administrative effort.

**Filtering Criteria – What Object**

As mentioned above, What Objects define the message content that should be detected during analysis. What Objects are defined by using the appropriate Content Analysis Library modules. The efficient and powerful CAL modules can be used to create unlimited combinations of criteria that will attempt to detect content that you would like to find in both incoming and outgoing messages.
Actions

Besides the Who, When and What objects, Proventia Mail Filter 2.2 also introduces Action objects that give instructions to the Proventia Mail Filter 2.2 to take appropriate action in policy implementations. These actions will decide what should take place on a message that matches a respective rule.

Actions available are explained in detail in the following chapter.
Proventia Mail Filter 2.2 Actions

Another unique feature of Proventia Mail Filter 2.2 is the variety of Action Objects. They allow you to decide how an e-mail should be handled after analysis. Different situations require different actions to be taken in order to achieve the best result possible. Proventia Mail Filter 2.2 provides you with the following options:

- Allow
- Block
- Delete
- Delay
- BCC
- Report
- Store
- Send Mail
- Daily Report
- Modify
- Remove Attachment

The complete and comprehensive e-mail action procedures are illustrated below:
A message that reaches the Proventia Mail Filter Server will always be analyzed by CAL to find matching rules. When it matches one or more rules, the corresponding Action Objects will be executed. There are basically 3 categories of Action Objects: modification, notification and delivery.

Modification

The modification actions modify the content or nature of the original message. These actions come in handy when you would like to remove unwanted content from messages, or add a standard company disclaimer for every outgoing message. There are two Action Objects:

Modify

Modify will create a copy of the original message and make modifications to the message. With Modify, disclaimer text can be added at the end of the message. The subject title can also be modified if defined. Also, e-mail header fields can be modified or added. For instance, Spam detection scores can be stored in a user-defined mail header field, like "X-Spam-Score". Finally, attachments can be added to the message if required.

Remove Attachment

Analysis can be performed on attachments found in messages. If the attachment matches the Who/When/What condition defined, it can be removed from the original message. With this, important documents can be stopped from leaving your corporation. The chances of sensitive or unwanted attachments entering or leaving your network are also minimized.

Notification

The next category of Actions Object is notification. As the name suggests, notification action objects are implemented to notify designated people, for example they can be used to remind administrators about blocked messages or to send warnings to users who have sent out large attachments. You can also use action objects from this category to make a comprehensive message management log. Below are the detailed descriptions of notification action objects:
Report

This action allows a new entry to be added to the custom log file or report database. You can record desired data into the log file or the report database by using this action object. Then you can keep track of certain content that is defined in the rules using the Report notification.

Store

With the Store action selected, messages can be saved to a MessageStore Folder. This will be useful when you want to monitor certain types of messages or to make duplicates of designated messages in a specific folder. Quarantine can be performed using this Action Object.

Note: We will look in detail at MessageStore in the next chapter

Send Mail

You can request Proventia Mail Filter to reply to the sender of the analyzed message, with different options for message content manipulation. Allowable actions include creating a new message to the sender, attaching the original message or sending a predefined warning e-mail to the original sender.

Daily Report

The Proventia Mail Filter provides Daily Reports that allow your e-mail users to permit the delivery of blocked e-mails. This alleviates the burden on the administrator. The administrator can enable this feature in order to inform e-mail users with a periodic report of blocked e-mails that are defined in rules with a Daily Report action, and users themselves can select e-mails that should be delivered to their mailboxes.

Delivery

Delivery is the final Action Object category. The Delivery action object decides the final action that should be taken for e-mail messages, whether they are modified or not. Below are the available Delivery actions one can choose to perform:
Allow

If an analyzed e-mail is safe to be sent or received, Delivery will permit it to reach the recipients.

Block

E-mails analyzed and set to be blocked will not be delivered to recipients. They will end up in the ‘blocked’ folder.

Delete

You could delete a blocked message. This will permanently erase the blocked message, and is irrecoverable. Delete must be used in conjunction with a Block action.

Delay

Messages can be set aside to be sent at a later time. Using this function, you can set the delay in hourly increments. Delay is particularly useful to create a queue system or priority for your e-mail traffic for higher efficiency.

BCC

This action will send a blind copy of the message to the given recipient. The message sent as the BCC can be modified with other action objects. The BCC action applies to all messages, no matter whether they are allowed or blocked.
Macros

Macros are definable variables that can be incorporated with Action Objects. By using macros you have the flexibility to define actions with custom values that will suit your requirements and needs. Macros allow system variables to be integrated into your policy definition and implementation. On the other hand, macros also allow for the automatic changing of values that vary according to defined fields.

Listed below are the available macros categorized in 3 groups:

**System Macros**

<table>
<thead>
<tr>
<th>Macro</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(ADMINISTRATOR)</td>
<td>Address of administrator</td>
</tr>
<tr>
<td>$(SECURITY)</td>
<td>Address of security service</td>
</tr>
<tr>
<td>$(NEWMSGSENDER)</td>
<td>Specifies the sender address that will be used for newly created messages.</td>
</tr>
<tr>
<td>$(MSGSTORE)</td>
<td>Global message store root directory</td>
</tr>
<tr>
<td>$(DATE)</td>
<td>Current Date</td>
</tr>
<tr>
<td>$(DATE.DAY)</td>
<td>Current Day</td>
</tr>
<tr>
<td>$(DATE.MONTH)</td>
<td>Current Month</td>
</tr>
<tr>
<td>$(DATE.YEAR)</td>
<td>Current Year</td>
</tr>
<tr>
<td>$(DATE.HOUR)</td>
<td>Current Hour</td>
</tr>
<tr>
<td>$(DATE.MINUTE)</td>
<td>Current Minute</td>
</tr>
<tr>
<td>$(MACHINE)</td>
<td>Machine name</td>
</tr>
<tr>
<td>$(ENV.&lt;environment variable&gt;)</td>
<td>Environment Variable</td>
</tr>
<tr>
<td>$(OPTION.&lt;additional settings variable&gt;)</td>
<td>Value from variable defined in additional settings</td>
</tr>
<tr>
<td>$(FILE.&lt;filename&gt;)</td>
<td>Content of file</td>
</tr>
<tr>
<td>$(CR)</td>
<td>New line macro</td>
</tr>
<tr>
<td>$(TAB)</td>
<td>Tabulator macro</td>
</tr>
</tbody>
</table>
Message Macros

<table>
<thead>
<tr>
<th>Macro</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(SENDER)$</td>
<td>Sender of the original message</td>
</tr>
<tr>
<td>$(RECIPIENTS)$</td>
<td>List of all recipients of the original message</td>
</tr>
<tr>
<td>$(RULE)$</td>
<td>Rule objects that matched for message</td>
</tr>
<tr>
<td>$(WHAT)$</td>
<td>All What objects that matched for message</td>
</tr>
<tr>
<td>$(WHATDETAILS)$</td>
<td>Detailed results of Content Analysis as XML</td>
</tr>
<tr>
<td>$(ACTIONS)$</td>
<td>Actions executed for this message</td>
</tr>
<tr>
<td>$(ALLOWEDRCPTS)$</td>
<td>Recipients that were allowed</td>
</tr>
<tr>
<td>$(BLOCKEDRCPTS)$</td>
<td>Recipients that have been blocked</td>
</tr>
<tr>
<td>$(REMOVEDATTS)$</td>
<td>Filenames of removed attachments (by Remove Attachment action)</td>
</tr>
</tbody>
</table>

Common Message Fields

The following table lists common Message Header fields

<table>
<thead>
<tr>
<th>Macro</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(MSG.ID)$</td>
<td>Internal unique identifier of message</td>
</tr>
<tr>
<td>$(MSG.SIZE)$</td>
<td>Total size (in bytes) of message</td>
</tr>
<tr>
<td>$(MSG.&lt;field&gt;)$</td>
<td>Message field</td>
</tr>
<tr>
<td>$(ORIGMSG.ID)$</td>
<td>Internal unique identifier of message</td>
</tr>
<tr>
<td>$(ORIGMSG.SIZE)$</td>
<td>Total size (in bytes) of message</td>
</tr>
<tr>
<td>$(ORIGMSG.&lt;field&gt;)$</td>
<td>Message field</td>
</tr>
</tbody>
</table>
Spam Detection

Proventia Mail Filter 2.2 implements a very comprehensive procedure to detect spam. Below is a simple illustration of Internet Security Systems’ unique Spam detection mechanism:

The procedures are put together to analyze a message in order to determine whether it is spam or not.

RBL, Black Lists and White Lists

Proventia Mail Filter 2.2 supports multiple user definable External Black List servers. Proventia Mail Filter 2.2 determines the source of the e-mail and compares the sender’s address with known spam sources.

Additionally, internal Black Lists and White Lists can be managed through the use of Who objects in the policy system. This can effectively block or allow complete domains or single e-mail addresses based on your configuration.
E-Mail Header Checking

E-mail headers may contain important information that can identify spam. The Spam Heuristics method is based on heuristics that are typical for spam e-mails. Among others, the following e-mail header items are checked:

- Message-ID field check
- Received field invalid or missing
- Checks for "Apparently-To:" or "X-Apparently-To:" fields
- Checks for mailing list fields
- Checks for multiple recipients
- Checks for missing fields like (From, To)

Using an internal scoring system, the e-mail is considered spam if multiple checks are positive.

Spam Signature Database

The Internet Security Systems Spam Signature Database contains signatures (64 bit hash values and checksums) for every known spam. Internet Security Systems operates hundreds of honey pots worldwide (e-mail accounts that attract spammers). These accounts receive thousands of spam e-mails every day. After a defined preprocessing workflow, the e-mail signatures are being calculated and stored in the Internet Security Systems Spam Signature Database, which is an integral part of the Filter Database. The Spam Signature Database will be updated multiple times a day. End-user feedback on unknown spam can be sent to the Internet Security Systems SpamLearn service, which feeds updates into the Spam Signature Database.

Spam Text Categorization

Subsequently, the message will be analyzed with different text classifiers: Spam, Pornography and Criminality. The Spam Online Classifier (Text Category Spam) is a highly effective statistical text classifier based on support vector machines (SVM) technology. Internet Security Systems provides a pre-trained classifier that does not require additional training. The Spam Online Classifier will be updated automatically at frequent intervals to protect against new types of spam. Besides using Text Categories, keyword and keyword pattern analysis is also performed to check for spam-related terms.
Pornographic Images and Spam URLs

For further analysis, the Porn Detector and URL Detector come into play. Using these two methods, spam that contains pornographic images or clickable links that are commonly found in spam will immediately be detected. More than 80 percent of all spam e-mails contain URLs and links to related Web offerings. Along with storing spam signatures in the Filter Database, all relevant URLs that appear in spam e-mails are stored in the Filter Database as well. This is a unique Internet Security Systems advantage. Since Internet Security Systems’ Filter Database has more than 20 million categorized URLs from the World Wide Web, Internet Security Systems is able to identify and categorize relevant URLs for spam offerings.

Friendly Sender

Sometimes, an e-mail from a good friend or business contact gets blocked because it is suspected to be spam. Internet Security Systems’ dynamic sender rating eliminates “false positive” e-mails from friendly senders. Proventia Mail Filter 2.2 internally manages a rating on every e-mail sender. The ranking gets adjusted dynamically with every e-mail. If somebody is sending you an e-mail that is suspected to be spam, but has sent many non-spam e-mails before, the e-mail will not be categorized as spam. Conversely, if the same e-mail came from an unknown sender, it would be categorized as spam.
Management: The Message Store

The Message Store is another powerful, unique feature of Proventia Mail Filter 2.2. It is like a virtual storeroom able to store messages as requested. By default, Message Store will keep blocked or delayed e-mail. Messages that are considered bad or problematic will also be kept in Message Store for further investigation.

Expanding from the default setting, you can keep other types of messages in the Message Store. For example, you can define suspicious messages with certain criteria to be kept in a quarantine folder in the Message Store. These messages can be virus-infected messages, important confidential data or e-mails that contain the company’s logo. Using the Management Console tools, you can view complete information about stored messages in a structured yet simple manner.

Every stored message is displayed with its respective information, including sender, recipient, subject, date, e-mail details, view log and more. You can also implement actions that you would like to carry out on the messages found in the Message Store. For example, quarantined messages are stored and displayed, but you could also choose to send, delete or reprocess these messages. The Message Store can be used as a backup for certain e-mails too, such as “every e-mail from technical support should always be put into a folder in the Message Store as a backup or archive.”
There are unlimited possibilities for using the Message Store application. You can perform any variety of tasks with the right combination of Who, When, What and Action Objects.
Conclusion

Proventia Mail Filter 2.2 delivers many unique features: thorough e-mail filtering and analysis, ease of use, flexible and powerful implementation, simple administration and configuration. Proventia Mail Filter 2.2 is the answer for organizations that want a robust and efficient antispam and e-mail analysis tool.
Technical Requirements

Software:
• Windows 2000 or Windows XP
• Internal Mailserver (Proventia Mail Filter integrates as SMTP relay)

Hardware:
• Intel Pentium III, 800 Mhz or more
• RAM, 1GB or more
• Harddisk 20GB

Supported Directory Service:
• Exchange Server 5.5 and 2000
• Lotus Domino Server
• NT Domains (via LDAP)
• LDAP (depends on deployment)
About Internet Security Systems

Internet Security Systems, Inc. (ISS) is the trusted expert to global enterprises and world governments providing products and services that protect against Internet threats. An established world leader in security since 1994, ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise for more than 11,000 customers worldwide. ISS products and services are based on the proactive security intelligence conducted by ISS’ X-Force® research and development team – the unequivocal world authority in vulnerability and threat research. Headquartered in Atlanta, Internet Security Systems has additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at www.iss.net or call 800-776-2362.