PreciseMail Technical Overview

PROCESS™ SOFTWARE

PreciseMail Overview - The Email Threat

Spam, viruses, and other malware are a converging email threat that produce more sophisticated attacks which can result in significant damage to an organization's email infrastructure and its users. For example, a virus containing malware can be used to turn your computer into a zombie, which is responsible for sending out millions of spam messages. This not only consumes network and system resources, but also can tarnish the organization's image and expose it to legal liability.

The emergence of more sophisticated spammer tricks is accelerating. The intent of many spammers is to steal a user's identity (called phishing) for financial gain. Many spammers have been successful at gaining access to email user's bank account numbers, social security number and other personal information.

It is difficult to quantify both the personal and organizational cost of this email threat. One study conducted by the University of Maryland indicated that time wasted deleting junk e-mail costs American businesses nearly $22 billion a year. This doesn't take into account the fraudulent, legal or system resource costs associated with spam.

There are many email security products on the market today that claim to be effective at combating spam and viruses. In reality, they are not designed to address these evolving email threats.

To add to the complexity of finding an effective email filter is that not all email users define spam the same way. For example some users may consider receiving email about an upcoming sale from their favorite retail outlet to be spam, while others may not. Many solutions cannot accommodate the various definitions users apply to spam.

PreciseMail Anti-Spam Gateway is an enterprise email security solution that eliminates spam, phishing and virus threats at the Internet gateway or mail server. It meets the diverse needs of many different organizations' email environments and users because of its highly adaptive architecture and functional design. This overview details how PreciseMail Anti-Spam Gateway works and describes features available in the latest version.

Multiple Filtering Techniques

PreciseMail Anti-Spam Gateway uses multiple email filtering technologies, which make it difficult for spammers to circumvent. The filtering engine achieves a balance of using different, highly effective spam filtering methods in parallel with one another. At the same time, it doesn't use too many filtering methods which prevent any noticeable effect on email server performance. PreciseMail Anti-Spam Gateway has a flexible design allowing each filtering method to be enabled or disabled. The following filtering techniques are included:

Heuristics

Large numbers of spam messages tend to share the same set of characteristics. Heuristic filtering applies a set of rules to each incoming message to detect these spam-like features. Each of the rules

has a value associated with it. To determine if a message is spam or not, the values for all the rules the message matches are added together. If the total value is greater than a threshold set by the user or system administrator, the message will be filtered as spam. PreciseMail Anti-Spam Gateway comes with a comprehensive set of heuristic rules, which have been proven to be 98% accurate at detecting spam. Administrators can tune or add their own rules. Process Software provides customers with timely automatic updates of filtering rules so that PreciseMail Anti-Spam Gateway's accuracy is sustained over time.

Bayesian Artificial Intelligence

PreciseMail Anti-Spam Gateway's Bayesian artificial intelligence filter learns the difference between spam and non-spam messages automatically by examining large collections of each. It continuously updates its knowledge to stay current with new spam messages. It learns about new tricks that spammers develop almost as fast as the spammers can come up with them. There is an autotrain feature that allows administrators to teach the engine spam vs. non-spam words prior to putting it into a production environment.

DNS Blacklisting

Several services maintain lists of IP addresses known to be sources of spam. With PreciseMail Anti-Spam Gateway, administrators can use these services to filter out undesirable traffic. During the SMTP transaction, PreciseMail queries a DNS server provided by the DNS blacklisting service. Based on the information returned from the query, PreciseMail will either reject the incoming message, or accept it for further analysis. DNS blacklisting can remove around 30% of spam without performing heavyweight filter operations.

Verify Mail From Address (VMF)

The VMF module dynamically checks the sender's address for incoming email to make sure it's valid. This address, also known as the envelope MAIL FROM: address, is often forged in spam messages and frequently specifies bogus email address (i.e, you can't actually send mail to the address). VMF works by sending the sender address for each message to a Process Software server, which verifies the validity of the address by initiating an SMTP session with the purported sender's mail server.

URL Reputation Filtering

Process Software actively analyzes several million web sites for over 20 indicators that are used by spammers and phishers. Sites are also analyzed for adult content. Each analyzed web site is given a reputation score, based on how "bad" it is. PreciseMail Anti-Spam Gateway obtains reputation scores for URLs contained in incoming email messages, and uses the reputation data to help determine if a message is spam.

Sender Policy Framework (SPF)

The purpose of SPF (RFC 4408) is to prevent email senders from forging email addresses thereby reducing phishing attempts. It allows the owner of a domain to specify their mail sending policy, e.g., which mail servers they use to send mail from their domain.

Tarpitting

Tarpitting is the practice of slowing the transmission of e-mail messages sent in bulk as a means of thwarting spammers. The intent is to maintain a high quality of service for legitimate users while making the sending process impractical for spammers, who -because of low response rates -- must be able to send vast volumes of messages quickly and inexpensively. PreciseMail allows administrators to specify the number of invalid RCPT TO: commands per session that are allowed before tarpitting is active and the number of seconds that each RCPT TO: response should be delayed.

Received: header DNSBL

Integrated (as opposed to SMTP standalone) installations of PreciseMail may check remote senders against DNS blacklists. The Received: headers are analyzed for IP addresses, which are then checked against the configured DNS blacklists.

URI DNSBL

Domains from URIs located in message bodies are checked against the configured DNS blacklists. PreciseMail confirms that the domain is associated with a spammer via one or more block lists.

Reverse DNS Lookups

Reverse DNS Lookups on domains specified in URI in the message bodies. Spam domains often do not have reverse DNS domains defined.

Anti-Relay Plugin

The Anti-Relay option prevents third parties from sending or receiving email messages that are not for or from the local host. PreciseMail will verify the MAIL FROM: addresses purporting to be from a domain for which local addresses are defined. This will prevent forged email addresses from those systems from being accepted. Sites can supply a shareable image for customized address verification against third-party sources, such as an LDAP server.

Block and Allow List

PreciseMail Anti-Spam Gateway also provides administrators and users with the capability to block senders regardless of the messages content. This list can be defined by a sender's email address or a group of addresses coming from the same domain.

Users generally have a list of email addresses from known business partners and colleagues that they communicate with on a regular basis. Filtering messages from these trusted senders is not needed, regardless of the message content. PreciseMail Anti-Spam Gateway provides system administrators and users with the ability to create a list of trusted senders that always bypass the filters. This feature, called the allow list, can be defined by a sender's email address or a group of addresses coming from the same domain. It is easy to generate this list using the intuitive web interface. Users can also build their allow list without having to manually type in addresses. When messages are retrieved from quarantine, an option is automatically displayed asking users if they want to add the sender's email address to the allow list so that all future communication with this person will bypass the filters. Also, users can import their existing address book entries to their PreciseMail allow list quickly and easily

through the web interface. Maintaining an allow list has proven to be an effective way of preventing false positives (or the filtering of legitimate email). Block and allow lists can be created system wide or on a per user basis.

Virus Filtering Options

To provide a complete secure email filtering solution, PreciseMail Anti-Spam Gateway includes bundled anti-virus options.

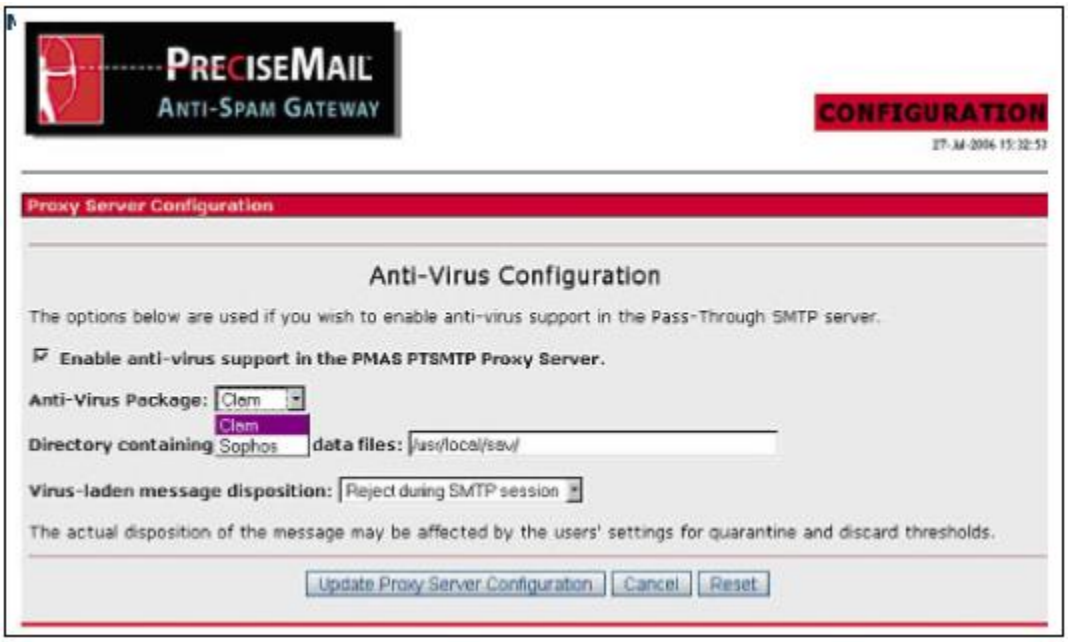
Clam AntiVirus

PreciseMail Anti-Spam Gateway's web administration interface makes it easy to enable Clam Anti-Virus, the leading open-source anti-virus software. According to research published on www.clamAV.net, Clam AntiVirus has over 6 million users worldwide and a good reputation for being updated frequently. Process Software provides automatic updates of new virus definition files from ClamAV along with PreciseMail Anti-Spam filter updates. Clam Anti-Virus is supported on Linux and UNIX platforms in the standalone SMTP proxy configuration.

Sophos Anti-Virus

Because viruses, worms, Trojan horses and spyware pose a substantial threat to organizations, PreciseMail Anti-Spam Gateway includes a second optional anti-virus module with industry-leading Sophos anti-virus software. It includes a unified centralized web interface and automatic virus

definition updates for easy administration. Sophos Anti-Virus is supported on Linux, UNIX, and OpenVMS platforms in the standalone SMTP proxy configuration.



Customized Filtering

Although PreciseMail Anti-Spam Gateway is an effective out-of-the-box solution, organizations can customize it to meet site-specific requirements. PreciseMail Anti-Spam Gateway analyzes messages using several proven methods, which work together to classify messages as spam. System administrators can adjust the aggressiveness of each filter method or the whole filtering engine.

Users and administrators can use the graphical web interface to create their own message filtering rules that can allow, block, tag, or quarantine a message based on any part of the message body or headers.

Deployment Architecture

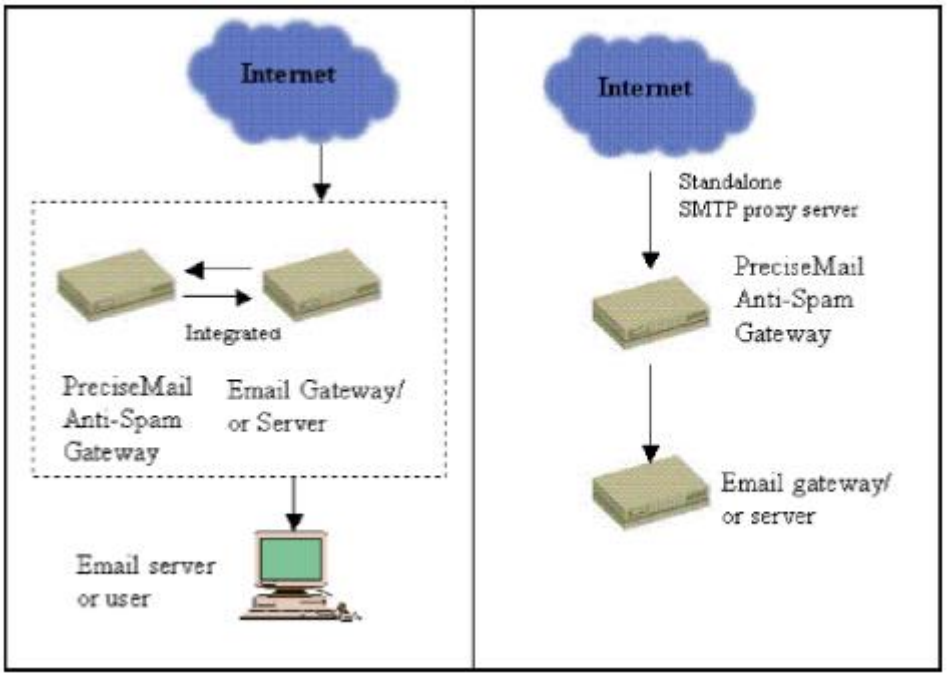
You can deploy PreciseMail Anti-Spam Gateway as an integrated or standalone solution.

Integrated

PreciseMail Anti-Spam Gateway can be integrated with your existing email server or gateway if you are using PMDF (on Linux or OpenVMS). This deployment option allows you to take full advantage of the features provided by your existing MTA. You can simply install PMAS on your existing email server or gateway, without being required to purchase any additional hardware.

Standalone SMTP Proxy

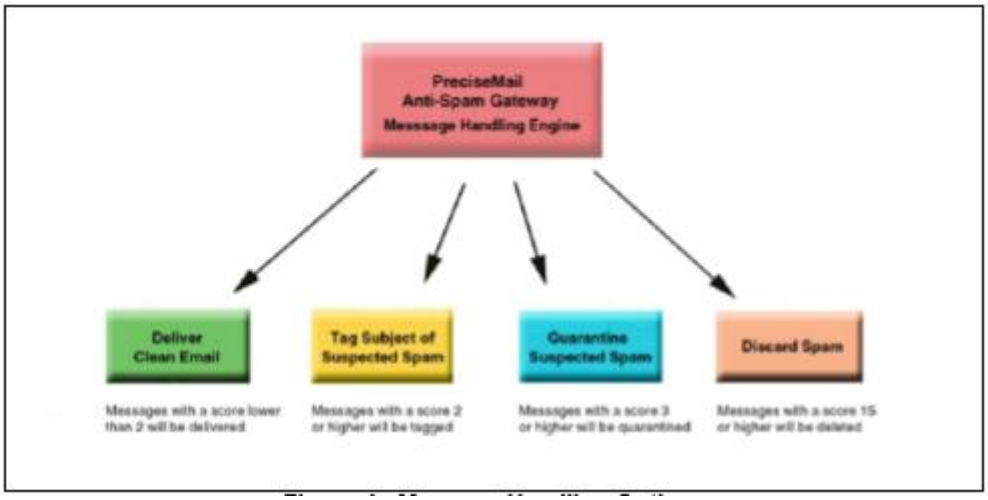
Running PreciseMail Anti-Spam Gateway as a proxy allows it to work with any email server or gateway. The PreciseMail Anti-Spam Gateway SMTP proxy server has the ability to receive email from the Internet or another email server, filter out spam, and then relay filtered email to the destination email server. Filtering email for spam before it is received by the email server reduces the email server's load and improves its performance. The standalone version of PreciseMail Anti-Spam supports Linux and OpenVMS.



Message Handling

PreciseMail Anti-Spam Gateway's message scoring system permits a range of actions to be taken based on a message's final score. Messages that are definitely spam can be discarded or rejected. Messages that are probably spam can be quarantined or tagged, eliminating the loss of legitimate email.

System administrators can establish defaults for these message-handling options. They can also provide users with the ability to adjust some or all of these defaults. This allows organizations and users to decide how to best handle spam in their environment.



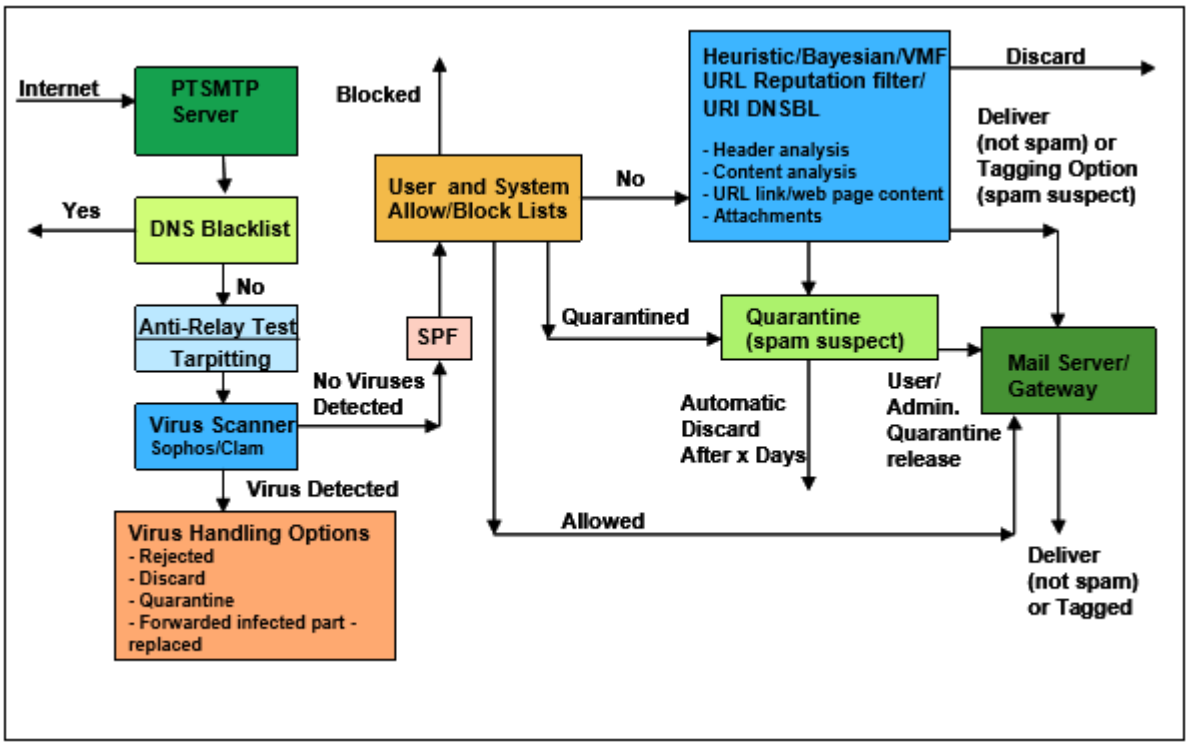
How It Works

PreciseMail Anti-Spam Gateway architecture is flexible and can be configured in many different ways. The below diagram provides an example of a typical SMTP standalone proxy deployment. Each message passes through multiple filtering layers before it reaches an end user's inbox. Overlapping methods increases filter accuracy and make it virtually impossible for spammers to circumvent the system. This diagram shows the default order of the filtering layers - the system administrator can apply the filters in any order appropriate for their email architecture.

The first filtering layer is one or more DNS blacklists. DNS blacklists make a good first layer because they have very low system resource requirements, and can eliminate a sizeable portion of incoming spam (usually around 30%) very quickly. Optional filtering such as tarpitting and anti-relay analysis follow. Virus scanning should usually be performed before any message has an opportunity to be placed into a user's inbox or quarantine.

User and system block and allow lists are processed next. User block and allow lists take precedence over the system allow and block lists to ensure personal spam filtering preferences are met first. If a message matches an allow list entry, then the mail doesn't need any further analysis and bypasses the rest of the filtering engine. If a message matches a blocklist entry, then it's discarded without any further analysis.

Heuristic analysis, Bayesian filtering, VMF, reputation filtering, and URI DNSBL all contribute to the main filtering engine's message scoring system. Each method can be tuned according to an organization's requirements. All filtering modules can be easily enabled or disabled through the web administration interface. After the analysis is complete, messages are quarantined, tagged, discarded, or rejected.



Security

To help system administrators cope with complex email architectures, PreciseMail includes a number of authentication methods that can be mixed-and-matched together to fit a site's needs. The ability to simultaneously support multiple authentication methods is unique to PreciseMail.

Supported authentication methods include:

- LDAP
- POP3
- IMAP4
- Local system password
- PreciseMail's user database

The authentication system provided by PreciseMail is designed to let multiple authentication mechanisms co-exist in as simple an environment as possible. The system administrator doesn't have to maintain a database that explicitly lists which authentication methods must be used for which user, and users aren't required to know anything about their site's authentication mechanisms.

When PreciseMail Anti-Spam Gateway is installed, the system administrator chooses which authentication methods should be used at the site, the order they should be used in, and options related to those methods. When a user authenticates themselves to PreciseMail, each authentication method is tried in the order specified by the system administrator. If the user's authentication

credentials are rejected by the first authentication method, the other methods are tried in order until either a successful authentication occurs or the list is exhausted.

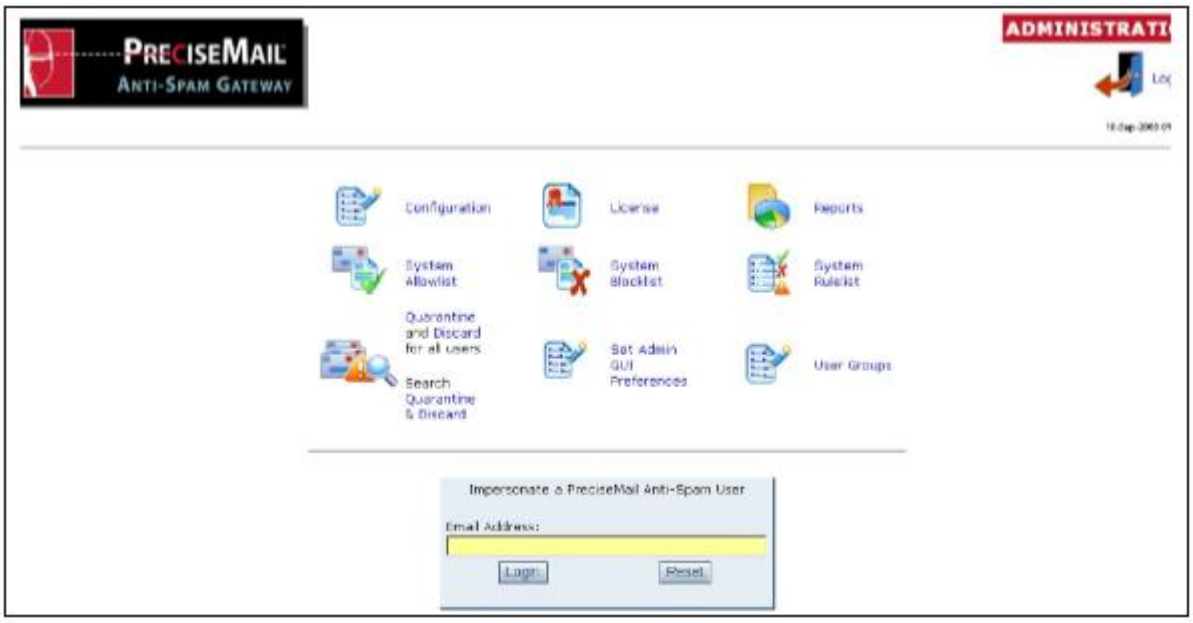
The PreciseMail SMTP proxy natively supports TLS so an organization can send and receive confidential email through the proxy.

Centralized Administration

Web Configuration

PreciseMail Anti-Spam Gateway requires minimal administration to filter spam effectively. Administrators may either use their own full-featured web server (Apache) or may opt for the simplicity of using the integrated HTTP server (Linux versions only). The web-based administration interface centralizes all configuration and management tasks. PreciseMail Anti-Spam Gateway's default configuration is effective out of the box, but it also provides system administrators the ability to customize the product to their site's requirements. Web-based administration options include:

- Setting default filtering policies and message handling options for users or groups of users
- Generating graphical reports
- Tuning filter thresholds
- Modifying settings for all users or an individual user
- Enabling end user web features
- Selecting authentication methods and web server configuration
- Creating allow lists and block lists
- Writing content filters
- Controlling logging and debugging
- Editing all configuration files



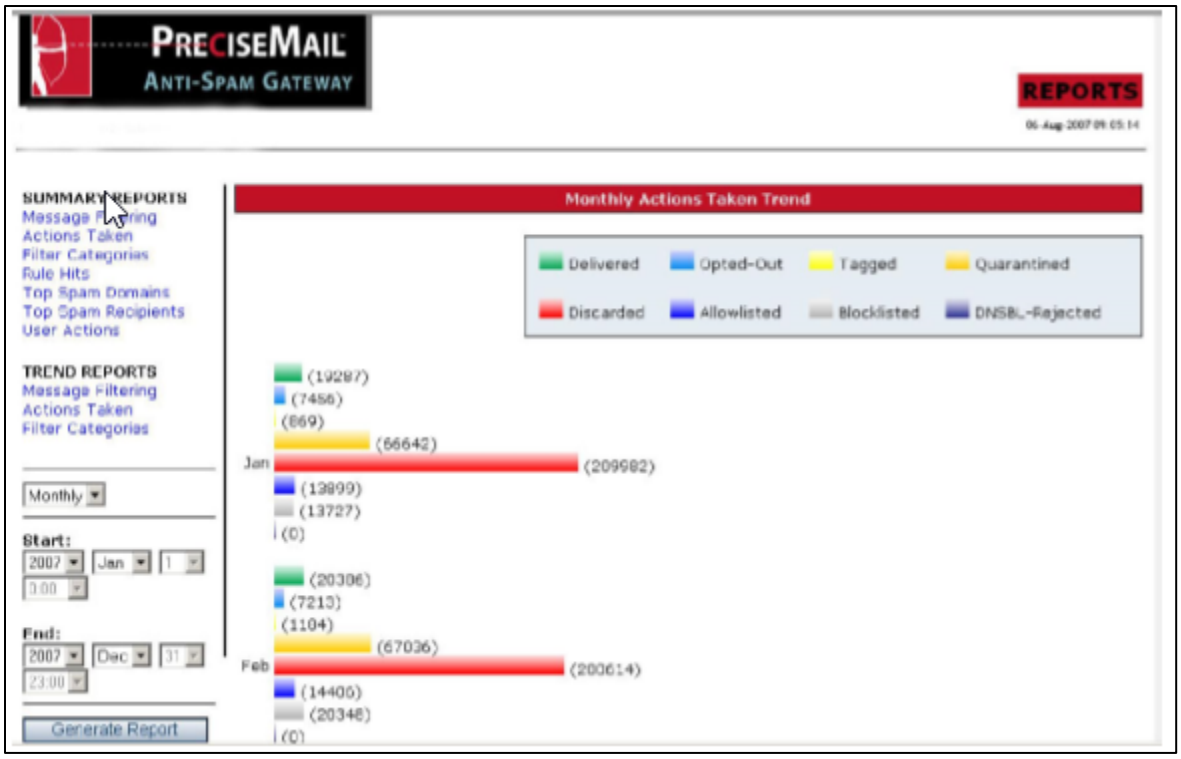
Reporting

The on-demand reporting capabilities provide administrators the ability to generate graphical trend reports at any date or time interval. Administrators can quickly access a greater level of detail on their message environment. These reports provide useful information on the messaging environment. Statistics and trends that are reported include:

- Number of messages processed
- Number of messages filtered
- Number of messages quarantined
- Number of messages allowed and blocked
- Top spam sending domains
- Top spam recipients
- Number of times spam or virus filter rules were triggered
- User actions such as web interface logins, quarantine views, allow/block list updates, released messages, previewed messages, and deleted messages

Reports can also be downloaded as CSV files that can be imported by most popular spreadsheet and graphing software for additional data analysis. The information obtained from these reports allows you to monitor your return on investment by showing how much spam is filtered and no longer affecting your users or system and network resources.

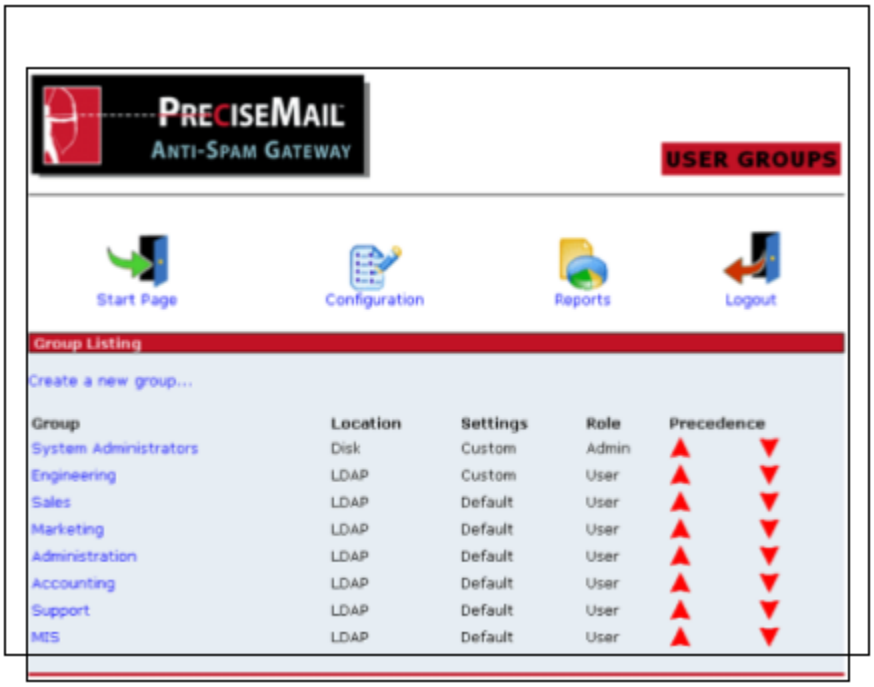
PreciseMail Anti-Spam Gateway's extensive logging and reporting capabilities allow system administrators to quickly determine why an email message was classified as spam. This information is useful for determining if a rule or threshold should be modified.



User or Group Settings

Various departments in an organization often have different filtering requirements. PreciseMail Anti-Spam Gateway allows administrators to create different filtering policies for groups of users. Group policies can include settings for filter thresholds and actions taken if a message is identified as spam. Groups can be created in an LDAP directory or inside PreciseMail using the graphical web interface.

For example, the technical support department does not want to quarantine suspected spam messages to insure that customer problems are seen and responded to in a timely fashion. As a result, this department only wants to tag suspected spam messages as a default setting. The accounting department may not be so open to viewing any potential spam email, so the administrator will create a default setting to quarantine all messages at a lower threshold than the system-wide default.



Advanced Infrastructure (AI)

The Advanced Infrastructure (AI) module provides a scalable backbone for organizations that have deployed multiple high traffic email systems. It allows organizations to easily manage filtering distributed among multiple MTAs. Sharing data among many systems simplifies both management and end-user access. Currently, AI allows sites to consolidate configuration and filtering statistics. Administrators can run AI in simple mode, which is a basic client/server system with one master server, and one or more clients who depend on it. Advanced mode allows cluster tasks to be distributed across multiple systems.

In order to provide the reliability and high performance required in this environment, AI includes:

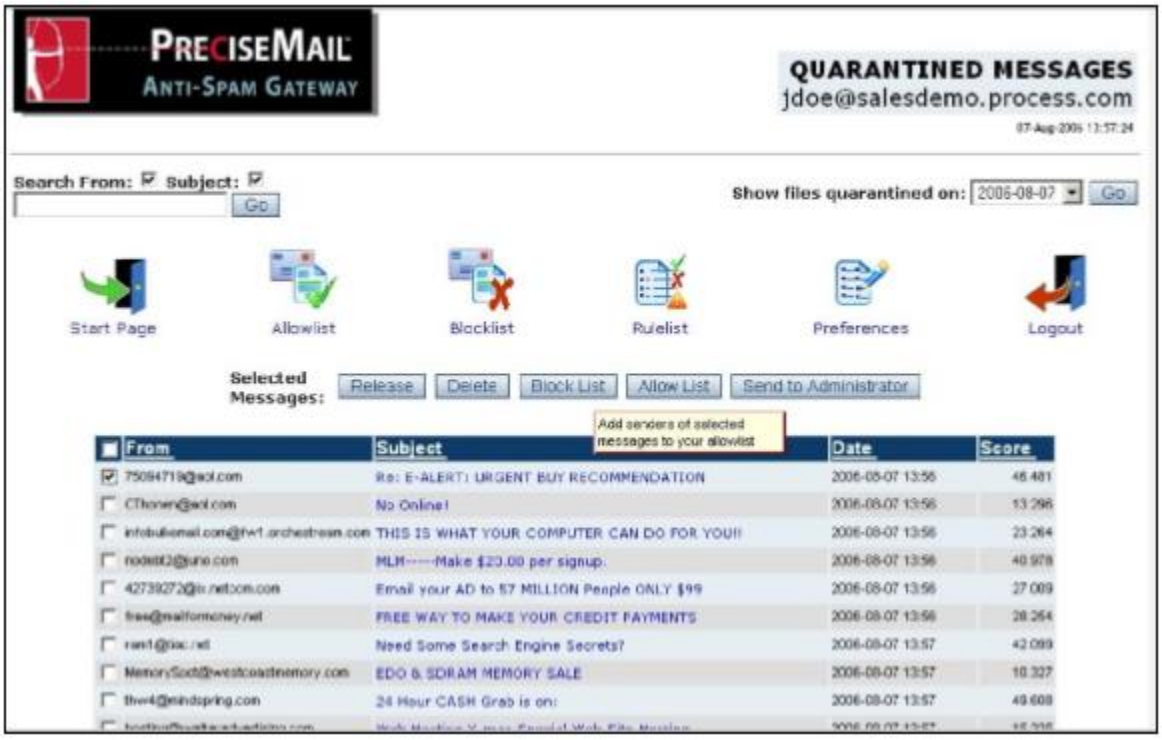
- Compression of data prior to transmitting it between systems. This reduces bandwidth usage for large transfers.
- Automated network error detection and correction. If one or more clustered systems are attached to a network segment that suddenly becomes saturated or otherwise unusable, PreciseMail will alert the administrator and hold data until the network link regains functionality. In addition, when a new system is inserted into a cluster, PreciseMail performs a bandwidth and performance check and alerts an administrator if they are insufficient.
- Integrated strong cryptography for all data transmission.
- Advanced role processing. This allows administrators to designate one or more systems to perform a single spam-filtering function such as message scanning or quarantined message storage.
- Quarantined and discarded messages from one or more systems running PreciseMail may be coalesced onto a quarantine server and/or discard server.

End User Spam Controls

PreciseMail Anti-Spam Gateway includes an extensive set of user options compared to other products. Users control their personal anti-spam settings through a web interface, so no additional software is required on users' desktop systems. User options include:

- Setting spam-handling preferences including any combination of tagging, quarantining, and/or discarding.
- Previewing, deleting, and releasing quarantined messages
- Receiving a summary of quarantined messages by email twice daily
- Adjusting filter sensitivity
- Creating and modifying per-user allow and block lists
- Opting out of filtering
- Forwarding incorrectly classified messages to an account where the system administrator can review them or send them to Process Software for analysis

PreciseMail Anti-Spam Gateway's user interface is designed to provide extensive user flexibility intuitively so that no training is required. Users can participate in defining spam as much or as little as they wish. Giving end users control over their spam allows them to contribute to the solution. The result is higher user satisfaction and acceptance and a greater return on investment.



Conclusion

PreciseMail Anti-Spam Gateway is a powerful tool for stopping spam and viruses at the gateway or mail server. Its adaptive architecture and flexible design lets each organization and every user determine how best to filter email in their environment. Process Software provides secure networking and messaging solutions to mission critical environments for over twenty years. We were early innovators of email software and anti-spam technology. With twenty years in business and over 3,000 customers, Process Software has a proven track record of success.

About PreciseMail Anti-Spam Gateway

PreciseMail Anti-Spam Gateway is an enterprise software solution that eliminates spam, phishing and virus threats at the Internet gateway or mail server. It has a proven 98% spam detection accuracy rate out-of-the-box without filtering legitimate messages. PreciseMail Anti-Spam Gateway has a highly sophisticated filtering engine is based on a combination of proven heuristic, DNS blacklisting, and Bayesian artificial intelligence technologies, which automatically learn how to separate spam messages from legitimate email. As a result, PreciseMail Anti-Spam Gateway can determine whether email is spam instead of passively reacting to known spammers by creating rules that block them after a spam attack occurs.

About Process Software

Process Software has been a premier supplier of communications software solutions to mission critical environments for twenty years. We were early innovators of email software and anti-spam technology. Process Software has a proven track record of success with thousands of customers, including many Global 2000 and Fortune 1000 companies.

U.S.A.: (800) 722-7770 • International: (508 879-6994 • Fax: (508) 879-0042
E-mail: info@process.com • Web: http://www.process.com/