Migrating to PreciseMail from SpamAssassin

Introduction

The freeware package SpamAssassin is one of the most popular anti-spam filters in use today, but it does have limitations that make it unsuitable for use with some sites. PreciseMail Anti-Spam Gateway is a versatile high-performance filter designed to overcome those limitations. Some of the reasons your site may consider upgrading to PreciseMail include:

- Better filtering accuracy
- More advanced per-user configuration
- Detailed statistical reporting
- Automated filter and virus scanner updating
- Greater administrative control of users and filtering
- Significantly higher message scanning throughput
- Intuitive web-based user interface
- Ability to scale across multiple email server systems
- Available 24/7 phone and email support

This white paper explains the simple steps required to migrate your site's spam filtering from SpamAssassin to PreciseMail.

Installing & Integrating PreciseMail

PreciseMail is distributed as a native software package for your platform (i.e., RPM for Linux, VMSINSTALL package for OpenVMS, etc.). The installation process is covered in detail in the *PreciseMail Installation Guide* for your platform, but it fundamentally consists of running the installation process and choosing the directory you wish to install PreciseMail in. A typical installation takes less than 5 minutes to complete. You don't need to shut down SpamAssassin while you're installing and configuring PreciseMail, so email system downtime can be kept to a minimum.

Because of the wide variety of email server architectures in use today, PreciseMail is made available in several different forms. If your site runs PMDF or Sun's Messaging Server, PreciseMail can be installed as a mail channel. PreciseMail can also be run as a pass-through SMTP proxy in front of any email server, so spam and virus messages never even touch your actual email server.

Configuration

PreciseMail can be configured through either a web-based administration interface or by directly editing the configuration files.

Like SpamAssassion, PreciseMail assigns a numerical score to every incoming email message. The higher the score, the spammier the message. Unlike SpamAssassin, PreciseMail allows you to perform different actions on a message, depending on its score. Messages can be rejected, discarded,

quarantined, tagged, or delivered. Different numerical thresholds can be set for each action, so more several actions can be performed on spammier messages.

For example, a site may wish to insert a [SPAM] tag in the Subject line of all messages that score higher than 3, quarantine all messages that score higher than 5, discard all messages that score higher than 20, and reject all messages that score higher than 100. Another site may wish to quarantine all messages that score higher than 8 and reject all messages that score higher than 50. You can mix and match any combination of actions to fit your site's needs. Users may set their own actions and thresholds for their account, if the system administrator enables them to do so. Users can preview and then release for delivery or delete their quarantined messages through the web interface. The same can be done for discarded messages, if the system administrator allows users to do so. The system administrator can view any user's quarantined or discarded messages, as well as every quarantined or discarded message on the system.

If you've written your own custom rules for use with SpamAssassin, they may also be used under PreciseMail. SpamAssassin rules usually consist of three parts: the rule itself, a short description of the rule, and a score. For example, a simple rule that looks for the word "viagra" in the body of a message would look like:

```
body     VIAGRA      /viagra/i
describe VIAGRA      Message contains the word viagra
score    VIAGRA      5.0
```

If you wanted to have PreciseMail apply this rule to incoming messages, you would place it in the file `/pmas/data/00_local_tests.cf`.

SpamAssassin provides the capability to whitelist or blacklist senders for the entire system. PreciseMail also provides system-wide allowlists and blocklists, although it allows greater flexibility in defining which addresses are allowed or blocked. SpamAssassin whitelist/blacklist entries look like:

```
whitelist_from bigboss@example.com
blacklist_from *@spammer.com
```

The corresponding PreciseMail entries would look like:

```
Allow_From bigboss@example.com
Block_From *@spammer.com
```

PreciseMail allows the use of full-fledged regular expressions in allow and block lists, in addition to simple * and ? wildcard matching. Any header field may be used in a regular expression-based entry. For example, if you wanted to allow every message that contained the name of one of your company's products in the Subject line, you might add an allowlist entry like:

```
Allow_RegEx    Subject: .*Product_Name.*
```

Both PreciseMail and SpamAssassin provide a Bayesian filtering module. PreciseMail's Bayesian filter uses a high-performance tokenizer that is incompatible with the token databases generated by SpamAssassin, but it does provide autotraining functionality so it can quickly become effective at your site. If you're using SpamAssassin's Bayesian filter, simply enable PreciseMail's Bayesian filter and autotraining to gain the same functionality.

User Configuration

PreciseMail users can manage their personal filter settings through an intuitive web-based interface. There's no need for them to log into the actual system or directly manipulate files. PreciseMail automatically creates user accounts as needed - the administrator isn't required to spend time creating and managing individual accounts. Users can be authenticated against an LDAP directory, backend POP and IMAP servers, the system password database, or an internal PreciseMail database. There's no need for users to remember yet another password. Users can also be arranged into groups with different configuration settings either manually or through an LDAP directory.

Per-user allowlists and blocklists in PreciseMail work essentially the same as whitelists and blacklists in SpamAssassin. A user's whitelist and blacklist entries are usually stored in their `user_prefs` file

under SpamAssassin. Under PreciseMail, a user's allowlist and blocklist entries are stored in a file based on their email address in the `/pmas/user_rules/` directory. For example, allowlist and blocklist entries for `jdoe@example.com` would be stored in `/pmas/user_rules/JDOE.EXAMPLE_COM`.

The format of the user allowlist and blocklist entries is essentially the same, except for the entry types. The whitelist/blacklist section of a SpamAssassin `user_prefs` file might look like:
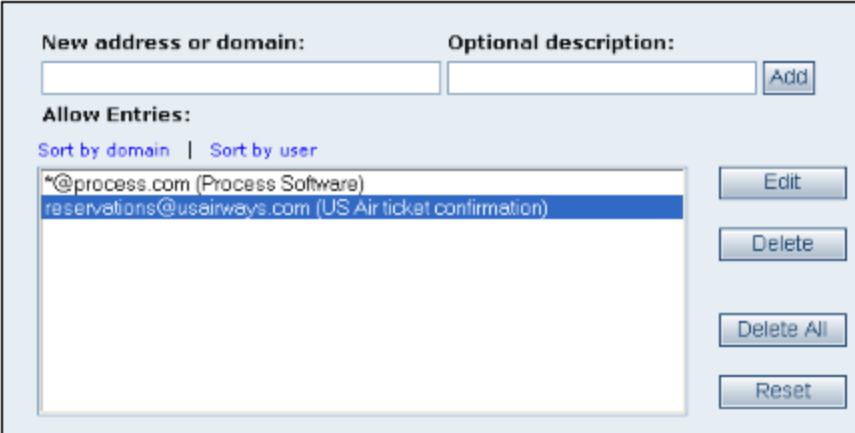
```
whitelist_from *@process.com
whitelist_from reservations@aa.com
blacklist_from *@spammer.com
```

The corresponding PreciseMail user rules file would look like:

```
Allow_From *@process.com
Allow_From reservations@aa.com
Block_From *@spammer.com
```

Note that both SpamAssassin and PreciseMail support the use of the * and ? wildcard characters in per-user allow and block lists.

PreciseMail users can maintain their personal allowlist and blocklist through either an email-based interface or the web-based user interface. Unlike SpamAssassin, PreciseMail also allows users to create advanced filtering rules based on any message attribute (such as the Subject line, body content, etc.).

If allowed by the system administrator, users can set the sensitivity of the PreciseMail filter for their email account through the web-based user interface. They can choose which actions they wish to have performed on mail identified as spam, and choose the message score above which those actions are taken. Granting users the ability to change their personal filter settings is

granular - the system administrator can choose to let users control their tag and quarantine settings but not discard settings, for example.

Statistics

PreciseMail provides detailed statistics about message filtering through its web-based reporting interface. Hourly, daily, monthly, and yearly statistics are available for each category, as well as statistical trends. The statistical data can also be imported as comma-separated value (CSV) files into an external graphing package, such as Microsoft Excel.
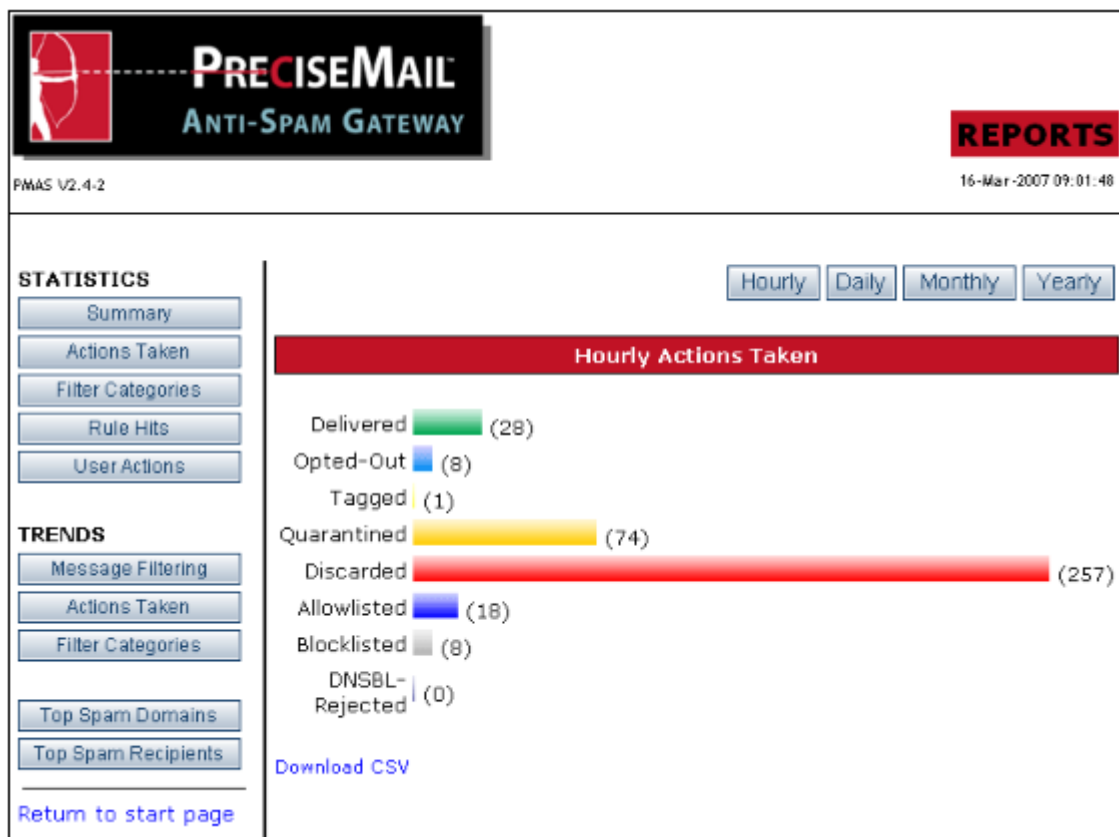
Updates

PreciseMail automatically updates its filtering rules and virus definition files, so there's no need to manually download and install rule updates on a regular basis. Automated updating also ensures that your system always has the best protection against the most recent spam attacks. Updates are pulled from a secure data center and integrity checked before they're applied to your system, so there's no need to worry about possibly corrupted updates from an untrusted source.

Automated updating is enabled by default, so there's no need to setup or configure the update process. If you wish to manually install updates, just disable the automated update process. You (and anyone else you designate at your site) will receive a notification email every time an update is released, along with detailed access information.

Large-Scale Filtering

If your site has more than one email server, PreciseMail can treat multiple systems as one logical filtering system through its Data Synchronization Cluster (DSC) technology. Although email messages can be scanned by any of the systems in the cluster, all quarantined and discarded email will be stored in a central repository. In addition, system-wide or per-user configuration changes

made to one system in the cluster will automatically be propagated to every other system. Systems can be added to or removed from the cluster as incoming email load requires.

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/