PreciseMail Anti-Spam Gateway User's Guide

July 2010

This manual describes the PreciseMail Anti-Spam Gateway user interface.

Operating System and Version:	OpenVMS VAX V6.1 or later
	OpenVMS Alpha V6.1 or later
	OpenVMS I64 V8.2 or later
	Solaris 8 or later
	Tru64 UNIX V4.0D or later
	RedHat Linux V7.2 or later
PMDF Version:	PMDF V6.1 or later
Software Version:	PreciseMail Anti-Spam Gateway V3.2

Process Software

20 July 2010

Process Software, LLC
959 Concord Street
Framingham, MA 01701-4682 USA
Voice: +1 508 879 6994; FAX: +1 508 879 0042
info@process.com

Contents

Preface

This guide describes how to release quarantined messages, how to set up allow and block lists, and how to interpret X-PMAS headers.

Intended Audience

This manual is intended for anyone who is using the PreciseMail Anti-Spam Gateway product.

What PreciseMail Anti-Spam Gateway Does

PreciseMail Anti-Spam Gateway is a high-performance anti-spam solution that eliminates spam at the Internet gateway without filtering critical legitimate messages.

Document Structure

This guide consists of three chapters.

Chapter 1	Describes PreciseMail Anti-Spam Gateway quarantine notices and releasing messages.
Chapter 2	Describes PreciseMail Anti-Spam Gateway allow and block rules.
Chapter 3	Describes how to interpret PreciseMail Anti-Spam Gateway X-PMAS headers.

Related Documents

You can find additional information in the following documents:

- *PreciseMail Anti-Spam Gateway Installation Guide* describes the PreciseMail Anti-Spam Gateway installation procedure.
- *PreciseMail Anti-Spam Gateway Management Guide* describes how to manage PreciseMail Anti-Spam Gateway.
- *PreciseMail Anti-Spam Gateway Release Notes* contain information and updates not included in this manual. The release notes are part of the software distribution kit.

Getting Help on Using PreciseMail Anti-Spam Gateway

For more information on using PreciseMail Anti-Spam Gateway, go to the "Support" page at http://www.process.com.

What Happens to Spam Messages

The way that PreciseMail Anti-Spam Gateway handles spam messages depends on how your system administrator has configured the product to run on your network. For example, some sites will not use quarantining, but will modify the Subject: lines of mail messages before sending them to the recipients. Other sites will quarantine messages, requiring recipients to either retrieve the messages or delete them.

PreciseMail Anti-Spam Gateway can do any of the following things with a message it determines to be spam:

- The message can be discarded
- The message can be quarantined
- The message can have X-PMAS headers added to it
- The message can have its subject line modified and be delivered

1 About Quarantined Messages

This chapter describes PreciseMail Anti-Spam Gateway quarantined mail messages and how to release them.

1.1 What Happens to Quarantined Messages

When a message is identified as spam, it is quarantined until further review by the recipient. At a set interval (usually twice a day), users are automatically notified by email with a summary of their quarantined messages. At this point, recipients can choose to release quarantined messages that they wish to receive. Email recipients can also use this automated process to set up individual allow and block lists. Since users control their own quarantined messages, there is no need for system administrators to spend time reviewing thousands of quarantined emails to identify potentially legitimate mail.

By default, PreciseMail Anti-Spam Gateway will "quarantine" messages that have a score above a certain threshold (5.0, by default). When a message is quarantined, it is written to the PreciseMail Anti-Spam Gateway quarantine directory and an entry for the message is logged to a quarantine index file.

1.2 How to Retrieve Quarantined Messages

When PreciseMail Anti-Spam Gateway designates a message to be quarantined, a confirmation message is sent to the recipient. In order to retrieve the message, the recipient must:

- Open the quarantined message notification in your "Inbox" folder.
- Depending on your client, click the "Reply" button, select the "Reply" link, or type REPLY.
- When you are in the message composition window that appears after you enter "Reply", select "Send" after modifying the contents of the message. Delete everything except entries for messages that you want to retrieve.
- Two messages are sent: one message confirming that the quarantined message is being released, and the other message contains the actual quarantined message text.
- A header (X-PMAS-QUARANTINE) is added to the quarantined message, indicating that it has been released to the recipient.

1.2.1 Sample Quarantined Message Text

Following is an example of the standard text that is used in a quarantined message notice.

```
PreciseMail Anti-Spam has quarantined the following incoming messages
for you.  To retrieve a message from the quarantine area, delete all
of the text except the "Message:" lines you want retrieved. For
help on using PreciseMail Anti-Spam, send the command HELP in the body
of a mail message to "PreciseMail".

At the time of the notification, these messages will
be retrievable for 14 days (until 26-August-2003).
```

2 Setting up Allow and Block Lists

This chapter describes how to set up and customize allow and block lists using PreciseMail Anti-Spam Gateway.

2.1 What are Allow and Block Lists?

- An **allow list** is a list of all addresses that should be accepted without being scanned by PreciseMail Anti-Spam Gateway. This list can include subscriber lists and public mailing lists, as well as personal and business email addresses.
- A **block list** is a list of known spam offenders that should not be delivered to the user's email account. Any incoming mail messages from blocked addresses will automatically be deleted by the system.

Note: Allow and block lists are case-insensitive.

2.2 PreciseMail Anti-Spam Gateway Graphical User Interface

PreciseMail Anti-Spam Gateway includes a web-based graphical user interface that you can use to control your allowlist, blocklist, quarantined messages, and personal spam filtering preferences. Ask your system administrator for more information.

2.3 How the PreciseMail Anti-Spam Gateway Processor Works

The PreciseMail Anti-Spam Gateway Processor can be used to release messages from the PreciseMail quarantine directory. If an incoming message is from one of your allowed addresses, it is automatically forwarded to you without being checked for spam content. If an incoming message is from a blocked address, it is immediately discarded.

2.4 Adding to Allow and Block Lists

PreciseMail Anti-Spam Gateway allows users to specify rules by using an ALLOW: command for messages that should always be accepted and by using a BLOCK: command for messages that should always be blocked. Multiple allow or block addresses can be added at the same time.

2.5 Using List Commands

In order for the PreciseMail Anti-Spam Gateway Processor to know how to process your request, you need to use a specific command (called a list command) in the text or body part of the reply messages that you send to the PreciseMail Anti-Spam Gateway Processor.

The following list commands are supported by the PreciseMail Processor:

- HELP—Sends this help message
- REVIEW—Sends your allow and block rules
- MESSAGE:—Releases a message from the quarantine directory
- ALLOW:—Adds an allow rule
- BLOCK:—Adds a block rule
- UNALLOW:—Removes an allow rule
- UNBLOCK:—Removes a block rule

Some commands use a colon (":"), others do not.

The following list commands use a colon:

- ALLOW:
- BLOCK:
- MESSAGE:
- UNALLOW:
- UNBLOCK:

The following list commands do not use a colon:

- HELP
- REVIEW

Make sure that a colon is included if it is part of a list command. The specified address used in the allow or block can contain wildcards. A question mark ("?") will match any single character, whereas an asterisk ("*") will match any number of characters.

2.5.1 Sample List Command Format

The following example shows the list command format used when adding an allow rule and a block rule:

```
ALLOW: user@domain
BLOCK: naughtyspammer@example.com
```

2.5.2 Sample List Command Format for Wildcards

The following example shows the command format used for wildcards:

```
ALLOW: *@process.com
ALLOW: caesar@example.com
ALLOW: number?@example.com
BLOCK: *teen*@*
BLOCK: *offers*@*
```

2.5.3 How to Add an Allow Rule

Follow these steps to add an allow rule:

- Send an ALLOW: command to PreciseMail Anti-Spam Gateway.
- PreciseMail Anti-Spam Gateway Processor returns a confirmation message to the user.
- Send the confirmation message back, in its entirety, to PreciseMail Anti-Spam Gateway. To do this from PMDF Mail, simply REPLY/EXTRACT/NOEDIT. For all other email programs, press "Reply".
- The PreciseMail Anti-Spam Gateway Processor verifies the existence of the CONFIRM: tag and its validity before applying the ALLOW: command.

Note: Allow rules are applied to the message before block rules, which means that the allow list has precedence over the block list. If the same pattern is specified in both an allow rule and a block rule, the allow rule will be used.

2.5.4 How to Add a Block Rule

Follow these steps to add a block rule:

- Send a BLOCK: command to PreciseMail Anti-Spam Gateway.
- PreciseMail Anti-Spam Gateway Processor sends back a confirmation message to the user.
- Send the confirmation message back, in its entirety, to PreciseMail Anti-Spam Gateway. To do this from PMDF Mail, simply REPLY/EXTRACT/NOEDIT. For all other email programs, press "Reply".
- The PreciseMail Anti-Spam Gateway Processor verifies the existence of the CONFIRM: tag and its validity before applying the BLOCK: command.

2.6 When to Use Allow Lists

Allow rules should be used to ensure that you receive all messages from particular addresses. Obvious examples of allow rules include business and personal mail addresses, subscriber lists, and public mailing lists.

If you use your email account for electronic transactions, messages from commercial companies are more likely to display the characteristics of a spam message, even when it is a legitimate piece of email. For example, confirmations of orders or reservations are usually sent as autoreplies, which may cause the messages to be flagged as spam. Adding the originator's address to an allow rule will ensure that all messages from that address will be delivered to your account.

2.7 When to Use Block Lists

While block rules are not very effective as a generic spam-filtering tool, there are special situations where using a block rule is effective. For example, if you receive continous unwanted messages from one particular address, setting up a block rule for that address will block all future messages from being delivered to your account.

There are certain instances when block rules are useful for mailing lists. If the volume of messages coming from a mailing list becomes overwhelming, adding the originator's address to a block list will prevent messages from being delivered until you remove that address from the block list. Removal instructions from subscriber and mailing lists don't always work. Creating a block rule for the offending list address ensures that PreciseMail Anti-Spam Gateway will block all future messages.

2.8 Confirmation Messages

When list commands are sent to the PreciseMail Processor, a confirmation message will be mailed back to you for confirmation that you want to make the specified changes.

2.9 Note for Non-PMDF Mail Users

If you are using an email client other than PMDF Mail, when you reply to a confirmation notice, text and HTML versions may be sent. You should ensure that your client is configured to send only plain text messages. If you send a message with both plain and HTML text parts, your confirmation message may show the command line twice, once as you expect it to look, and again with HTML tags following the address. If your confirmation message looks like that, you should delete the second line with the HTML tags present.

The following example shows a confirmation message that contains HTML tags.

```
{CONFIRM: ncvgmipBsvtcfuv2hon}

New List Commands
-----------------

ALLOW: new_user@hotmail.com
ALLOW: new_user@hotmail.com</FONT></SPAN></DIV></BODY></HTML>
```

Using this example, you would delete the second line that contains HTML tags before sending a reply. The reply should only contain the first line of text "ALLOW: new_user@hotmail.com".

2.10 Removing Addresses from Allow and Block Lists

In order to remove addresses from your allow and block lists, you must use either the UNALLOW: or UNBLOCK: command. The address specified in an UNxxxxx command must match one of the defined rules.

The following examples show how to remove an address from an allow list and a block list:

```
UNALLOW: *insurance*@*
UNBLOCK: *offers*@*
```

3 How to Interpret X-PMAS Headers

This chapter describes the various types of spam headers that may appear on your spam messages. By default, the headers added to messages by PreciseMail Anti-Spam Gateway begin with the text “X-PMAS-”. This text is configurable by the system administrator and may be different on your system.

A separate spam folder can be created in your email client so that all spam messages are automatically sorted into that folder.

All messages passing through the PreciseMail Anti-Spam Gateway will receive a header like this:

```
X-PMAS-Software: PreciseMail V3.2
```

If no rules were triggered, the message will have:

```
X-PMAS-Not-Spam: 0.000
```

If rules are triggered, those rules appear, along with a description and a score for each rule, as shown in the following examples:

```
X-PMAS-HDR-VERY_SUSP_RECIPS: To: contains similar usernames at least 5 times (2.000)
X-PMAS-BDY-HOME_EMPLOYMENT: Information on how to work at home (2) (1.652)
X-PMAS-BDY-BAD_CREDIT: Eliminate Bad Credit (0.787)
X-PMAS-META-ORIGINAL_MESSAGE: Looks like a reply to a message (-3.000)
```

which generates a header similar to the following:

```
X-PMAS-Final-Score: 7.550
```

If it was enabled by your system administrator, you may see the following header:

```
X-PMAS-Spam-Level: *******
```

where there is an "*" for each truncated whole score (7 above).

If a final score is negative, this header appears:

```
X-PMAS-Not-Positive: -6.000
```

When a message is quarantined and released, it gets the following header:

```
X-PMAS-Quarantined: PreciseMail
```

Finally, the system admininistrator can have the subject modified, as shown in the following example:

```
Subject: [SPAM] Original subject
```

The "[SPAM]" text is configurable by the system administrator.

Glossary

Allow list: A list of addresses from whom all messages should be accepted, regardless of their spam score.

Block list: A list of known spam offenders from whom all incoming email messages will be deleted. For example, if a user constantly receives spam messages from naughty_spammer@example.com, they might wish to place that address on their block list.

Discarded messages: PreciseMail Anti-Spam Gateway can be configured to discard messages that have a score above a certain site-specific discard level that is set by the system administrator. Discarded messages are automatically deleted from the system after the specified number of days has elapsed. The default value is 14 days.

False negative: A spam message that is incorrectly identified as non-spam by an anti-spam filter.

False positive: A non-spam message that is incorrectly identified as spam by an anti-spam filter.

Ham: Any non-spam email message (an email message that a recipient wishes to receive).

Quarantined messages: Messages that are identified as spam with a score of 5 or higher are quarantined for a defined number of days (14 is the default) until further review by the recipient. Users are automatically notified by email, and can either delete or retrieve quarantined messages.

Spam: An unsolicited commercial email sent to multiple email recipients against their wishes.

Spamicity: Based on the sum of scores for all the matching rules, a message's final score determines its likelihood of being spam, known as its "spamicity".

Index