

WatchGuard[®] SpamScreen[™] Guide

SpamScreen for WatchGuard System Manager



Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

Copyright© 1998 - 2007 WatchGuard Technologies, Inc. All rights reserved.

Complete copyright, trademark, patent, and licensing information can be found in the *WatchGuard System Manager User Guide*.

All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Software: WFS v7.5

Document: SpamScreen-7.5-1

Contents

SpamScreen Options	1
Customizing SpamScreen using Multiple Proxies	2
Installing SpamScreen	3
<i>SpamScreen License expiration</i>	4
Starting SpamScreen	4
Configuring how the Firebox routes spam	4
<i>About SpamScreen headers and tags</i>	5
<i>Tagging messages</i>	7
<i>Denying spam</i>	8
<i>Allowing spam</i>	8
<i>Logging spam</i>	8
Determining How SpamScreen Identifies Spam	9
Configuring RBL/DNS Servers	10
<i>Adding RBL Servers</i>	11
Configuring Spam Rules	12
<i>Adding spam rules</i>	13
<i>Restoring default rules</i>	14
<i>Importing rules</i>	14
<i>Defining spam threshold weight</i>	14
Configuring Exceptions to the Spam List	15
<i>Blocking addresses not on the spam list</i>	16

Monitoring SpamScreen Activity	17
<i>Viewing message header notifications</i>	17
<i>Interpreting log messages</i>	18

WatchGuard SpamScreen Guide

Unwanted e-mail, also known as spam, fills the average inbox at an astonishing rate. Some experts predict that the total number of spam e-mail messages sent each day will increase from 10 billion in 2003 to 30 billion by 2006. This large volume of spam decreases bandwidth, degrades employee productivity, and wastes network resources.

The WatchGuard® SpamScreen™ option increases your capacity to catch spam at the edge of your network when it tries to come into your system. You can use the SMTP Proxy of your WatchGuard firewall to strip or tag incoming spam. With SpamScreen enabled, the WatchGuard SMTP Proxy examines the header content of each message and decides if the message is spam.

NOTE

In this User Guide, the word Firebox refers to a Firebox® III or a Firebox® X hardware device unless we tell you differently.

SpamScreen Options

You can configure SpamScreen™ to customize how the Firebox® identifies e-mail as spam and routes the messages it identifies as spam.

SpamScreen has two methods to identify an e-mail message as spam. With the first method, SpamScreen uses the IP address of the sender of the e-mail. It makes sure that the sender is not on one or more Real-

Time Blackhole List (RBL) servers. If the sender is on an RBL server, then the Firebox identifies the message as spam. An RBL server is a DNS server which keeps the IP addresses of known sources of spam. It also keeps the IP addresses of computers that might be vulnerable to spam attacks. For example, mail relays are frequently vulnerable to a spam attack. SpamScreen also makes sure that the domain name of the source is correct. An RBL server can not be used as a standard DNS server.

The second method SpamScreen uses to identify spam is to apply a list of rules to e-mail message headers. Each rule has a positive or negative weight. The sum of the weight values of rule matches are recorded for each message. If the sum is more than a limit you set, the Firebox identifies the message as spam. For more information, see “Configuring Spam Rules” on page 12.

You can also configure what the Firebox does with a message after it identifies it as spam. The SMTP Proxy can allow the message, deny it, or tag it as spam before it sends it to the recipient.

For more information on features of SpamScreen, see the online support resources at:

<https://www.watchguard.com/archive/showhtml.asp?pack=5985>

Customizing SpamScreen using Multiple Proxies

You can configure more than one SMTP Proxy service to use SpamScreen™. This lets you create custom rules for different groups in an organization. For example, you can use the RBL server method to identify spam for your IT department while at the same time you allow all e-mail to your management and use a spam tag for the marketing team.

When you make more than one SMTP Proxy service, the Rules Lists and RBL Lists apply to all of the services. You can not use different lists for different SMTP Proxy services.

If you want to use more than one SMTP Proxy service with SpamScreen, your network must be set up with one of these configurations:

- Give each user group a different e-mail server; or
- Set the external source or sources which can send e-mail for each user group.

For more information on using more than one SMTP Proxy services with SpamScreen, see the FAQ at:

www.watchguard.com/support/advancedfaqs/spam_multproxies.asp

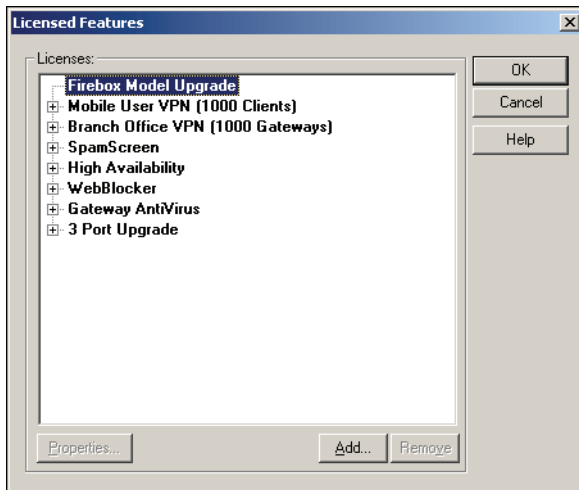
Installing SpamScreen

Before you install SpamScreen™, you must have:

- A SpamScreen license key certificate
 - An e-mail server behind the Firebox®
 - A SMTP Proxy service
- For information on the SMTP Proxy service, see the WatchGuard System Manager User Guide.

To install SpamScreen:

- 1 From Policy Manager, select **Setup > Licensed Features**.
The Licensed Features dialog box appears.



- 2 Click **Add**.
- 3 In the **Add/Import License Keys** dialog box, type your license key. You can also click **Browse** to find a text file with the license key values. Click **OK**.
The new license appears in the Licensed Features dialog box.

SpamScreen License expiration

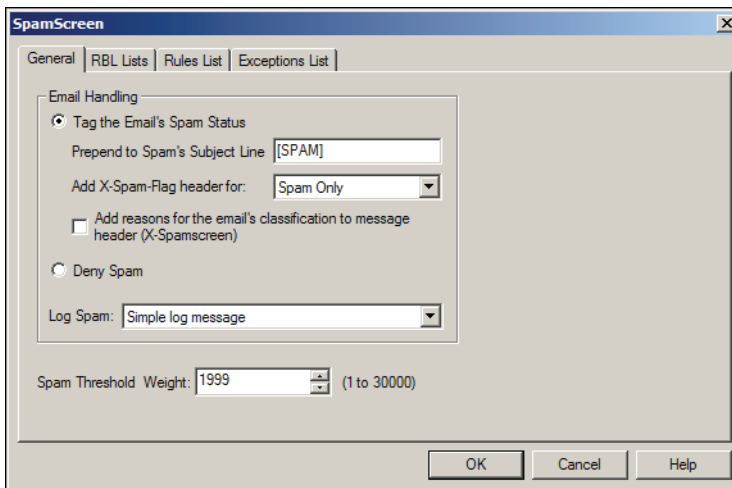
When a SpamScreen license expires, all SpamScreen features stop working. You must add a new or upgrade license to resume SpamScreen protection.

Starting SpamScreen

From the WatchGuard Policy Manager, select **Setup > SpamScreen**. The SpamScreen™ dialog box appears. You use this dialog box to configure:

- The method the Firebox uses to identify spam; and
- The action the Firebox takes after it identifies a message as spam.

You also use the SpamScreen dialog box to configure the RBL server IP addresses, spam rules, log message type, and exceptions to spam rules.



Configuring how the Firebox routes spam

The Firebox® uses SpamScreen™ rules to route e-mail messages. It can:

- **Deny** – Block the spam message without a reply.

- **Tag** – Identify the message as spam or not spam and allow spam messages to go to the recipient.
- **Allow** – Deliver spam messages without a tag.

We recommend that initially you do not use the Deny option. Use the Tag option and monitor the results for a period of time before you enable the Deny option.

About SpamScreen headers and tags

The Firebox can add SpamScreen messages to message headers and to the e-mail subject. You use the SpamScreen dialog box to configure the tag feature to do this.

X-SpamScreen header

The Firebox adds an X-Spamscreen header to each e-mail message it examines. This is an example:

```
X-Spamscreen: Protected by WatchGuard (WGTI) SpamScreen (TM)
v7.3.B1823 Copyright (C) 1996-2004 WGTI
```

You can also configure SpamScreen to show a description of the method the Firebox used to examine the e-mail message. In this example, the X-Spamscreen header has more information including: the message spam score and the spam limit you set. For more information on weight, see “Configuring Spam Rules” on page 12.

```
X-Spamscreen: Protected by WatchGuard (WGTI) SpamScreen (TM)
v7.3.B1823 Copyright (C) 1996-2004 WGTI
Results of SpamScreen: 2000 From contains advertising fingerprint
Score : 2000
Required: 1999
```

X-Spam-Flag header

The Firebox can tag each message it examines with an “X-Spam-Flag” header. This header gives more information about the e-mail message. If the value of X-Spam-Flag is “YES”, then the Firebox identifies the message as spam. If the value of the X-Spam-Flag is “NO”, the Firebox does not identify the message as spam. You can use this header to sort spam e-mail into different folders than regular e-mail.

This example shows a message header with the X-Spamscreen and X-Spam-Flag information with the Firebox configured to tag all e-mail and to include SpamScreen information.

X-Spam-Flag: NO
X-Spamscreen: Protected by watchGuard (WGTI) SpamScreen (TM)
v7.3.B1825 Copyright (C) 1996-2004 WGTI
Results of spamscreen:
701 Subject contains "FREE" in CAPS
Score : 701
Required: 1999

Spam subject line

You can configure SpamScreen to add text to the subject of e-mail messages the Firebox identifies as spam. You can also customize the text that appears. This example uses the text [SPAM]:

Subject: [SPAM] Free auto insurance quote

Example message header

Note that the X-Spam-Flag header appears because SpamScreen has been configured to tag e-mail messages. SpamScreen has also been configured to include processing information in the X-SpamScreen header and to prepend the subject line with a specific string, in this case [SPAM]:

A full e-mail message header includes information about the source, the destination, and the route of the message. When the Firebox adds the SpamScreen information, a typical e-mail message appears like the following example. For this message, the Firebox is configured to add the X-Spam-Flag and X-Spamscreen headers and to add [SPAM] to the subject.

Return-Path: <johndoe@sparta.iceberg2.watchguard.com>
Delivered-To: johndoe@thebes.iceberg.watchguard.com
Received: from iceberg.watchguard.com (unknown [60.100.253.9])
by thebes.iceberg.watchguard.com (Postfix) with ESMTPE7B0918C1F
for <johndoe@thebes.iceberg.watchguard.com>; wed, 2 Jul
2003 08:33:07 -0700 (PDT)
MIME-Version: 1.0
Message-Id: <9402060055.AA06427@iceberg.watchguard.com>
To: johndoe@thebes.iceberg.watchguard.com
From: dude@berrypatch.com
Subject: [SPAM] You've got mail and you've been approved!
X-Spam-Flag: YES
X-Spamscreen: Protected by watchGuard (WGTI) SpamScreen (TM)
v7.0.B1346 Copyright (C) 1996-2003 WGTI
Results of spamscreen:

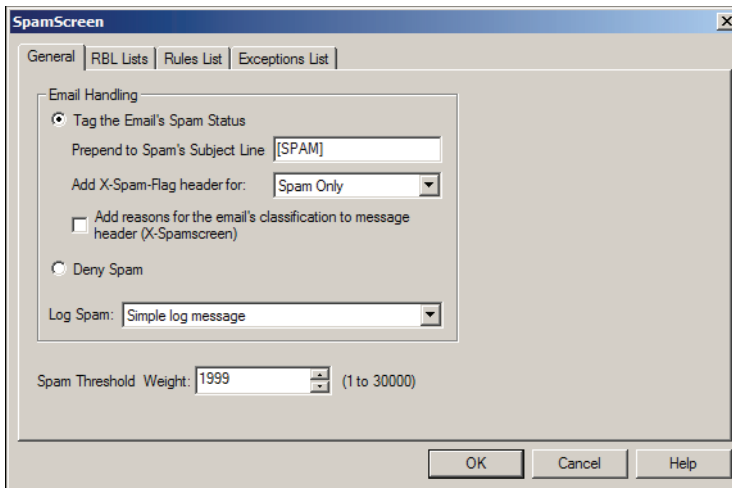
2630 Subject talks about being approved
Score : 2630
Required: 1999
Date: wed, 2 Jul 2003 15:33:08 +0000 (UTC)
Today is your lucky day! you've been approved to get a free e-mail account from our deluxe service.

For information on how to view full message headers, see “Viewing message header notifications” on page 17.

Tagging messages

To tag an e-mail message is to examine the contents and identify the message as unwanted or valuable. Unwanted e-mail is known as spam. Valuable e-mail is frequently known as ham. When you configure SpamScreen to tag e-mail, the Firebox identifies spam messages and then sends them to the recipient.

- 1 From Policy Manager, select **Setup > SpamScreen**.
The SpamScreen dialog box appears.



- 2 To add the X-Spam-Flag header to each e-mail message, select **Tag the e-mail's Spam Status** checkbox.
- 3 To add text to the subject of each spam message, type the word in the **Prepend to Spam's Subject Line** field.
The default value is [SPAM].

-
- 4 Use the **Add X-Spam-Flag header for** drop-down list to select if the Firebox adds the X-Spam-Flag header to all e-mail messages or only to spam messages.
 - 5 To include a description of the method used to examine the message in the X-Spamscreen header, select the **Add reasons for the e-mail's classification to message header (X-Spamscreen)** checkbox.
 - 6 Click **OK**.

Denying spam

The Firebox can block all messages it identifies as spam. This is a good method to prevent spam, but it also adds risk that the Firebox will block an important message that is not spam. We recommend that you initially use the tag option. Only use the Deny option if you find the tag option correctly identifies the spam and ham for your users.

- 1 From Policy Manager, select **Setup > SpamScreen**.
- 2 On the General tab, select the **Deny Spam** option.

Allowing spam

To allow all e-mail messages, including spam, leave both options on the SMTP proxy disabled, as described in the next section “Determining how SpamScreen Identifies Spam.” SpamScreen allows spam e-mail messages and tags them with only the default X-SpamScreen header, as described in “X-SpamScreen header” on page 5.

Logging spam

You can configure the Firebox to record a log message when it identifies an e-mail as spam. There are three **Log Spam** options:

- **No log message** – The Firebox does not record a log message when it identifies an e-mail as spam.
- **Simple log message** – The Firebox records one log message with the sender and recipient.
- **Verbose log message** – The Firebox records the contents of the X-Spamscreen header in the log file.

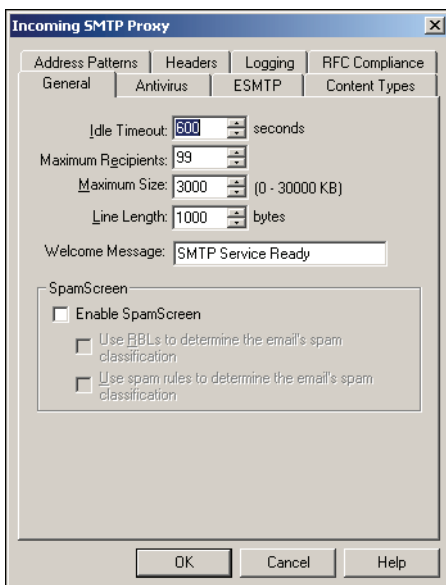
Determining How SpamScreen Identifies Spam

SpamScreen™ includes two methods to identify spam message. The first method makes sure that the IP address of the sender is not on a list of known sources of spam. There are many open source and subscription servers which keep such lists. The Realtime Blackhole List (RBL) servers are one example. The Firebox can also use an MX record lookup to make sure that the e-mail server is at the location of the sender.

The second method that SpamScreen uses to identify a spam message is to examine the message against a group of rules. Spam messages frequently have the same components, such as the sender name or a “bulk mail” header. For more information on rules, see “Configuring Spam Rules” on page 12.

- 1 From the Policy Manager, double-click the **SMTP Proxy** icon. The SMTP Proxy Properties dialog box opens.
- 2 Click the **Properties** tab.
- 3 Click **Incoming**.

The Incoming SMTP Proxy dialog box appears displaying the General tab.



-
- 4 Select the **Enable SpamScreen** check box to enable SpamScreen.
 - 5 To use the RBL servers, select the **Use RBLs to determine the e-mail's spam classification** checkbox.
For information on how to configure the RBL server IP addresses, see "Configuring RBL/DNS Servers," on page 10.
 - 6 To use rules that identify known spam characteristics, select the **Use spam rules to determine the e-mail's spam classification**.
For more information on how to configure spam rules, see "Configuring Spam Rules" on page 12.
 - 7 If it is necessary to temporarily disable the SpamScreen feature, clear the RBL and spam rules checkboxes. The Firebox allows all e-mail messages.

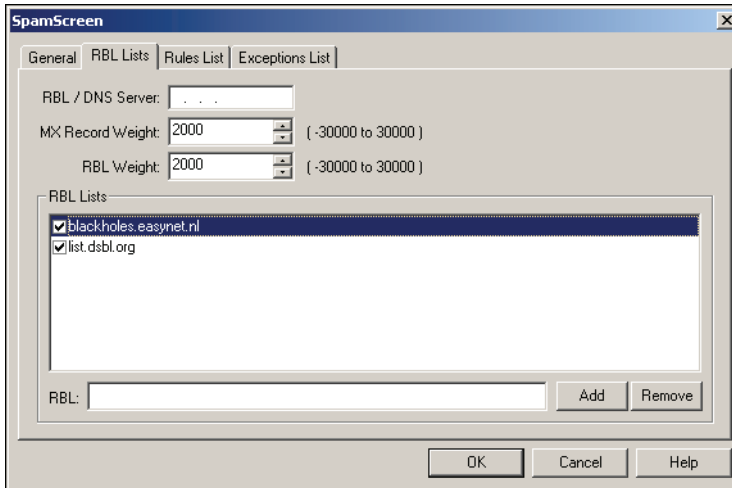
Configuring RBL/DNS Servers

A RealTime BlackHole List (RBL) is a name server that has DNS information for IP addresses that are thought to be the source of spam, a spam relay, or Internet Service Providers that allow or support spam. If the message comes from an address on an RBL, the Firebox identifies the message as spam.

To be a host for an RBL server can be a risk. The network host is frequently the recipient of a legal action. As a result, the list of available RBLs changes for each SpamScreen™ software version. We recommend that you do regular maintenance on the list of RBL servers which your Firebox uses. You can find more information on Web sites which have information about the risks and inappropriate use of e-mail.

Use this procedure to specify the RBL values used by SpamScreen:

- 1 From the Policy Manager, select **Setup > SpamScreen**. Click the **RBL Lists** tab.



- 2 In the **RBL/DNS Server** field, type the IP address of the server. This is frequently the IP address of your DNS server. It can also be the DNS server of your Internet Service Provider. The Firebox uses this server to do an MX record lookup on the sender of each e-mail message.
- 3 When the Firebox does an MX record lookup and can not confirm that the domain name of the sender is real, it adds the **MX Record Weight** to the total Spam Weight. While the default value of 2000 is sufficient in most conditions, you can change this value.
- 4 When the Firebox confirms that the sender IP address matches an address on one or more RBL lists, it adds the **RBL Weight** to the total Spam Weight. While the default value of 2000 is sufficient in most conditions, you can change this value.

Adding RBL Servers

A list of RBL servers appears on the **RBL Lists** tab. To enable an RBL server on the list, select its checkbox. You can also use the **Add** and **Remove** buttons to add or remove other RBL servers.

The IP addresses you add to the RBL List must refer to a DNS server that is specially configured as an RBL server. A standard DNS server does not operate correctly for this function.

You can find more RBL servers at these Web sites:

- <http://www.mail-abuse.org>
- <http://www.abuse.net>

Configuring Spam Rules

You can configure SpamScreen™ to use rules about mail header information to identify spam. The Firebox examines the e-mail message and finds the probability that an e-mail message is spam. Each rule has a weight. The Firebox adds all the rules together and gives the message a score. If the total Spam Weight is larger than a limit you set, the Firebox identifies the message as spam.

The Firebox only examines the e-mail message header. It does not examine the content of the message. A message header is the component of an e-mail that includes: subject, date, sender, recipient. Each header has a title followed by a “:” and then a value. For example, you can find the date a message is sent in the “Date:” header. A message header appears at the top of a message. SpamScreen rules are special expressions that examine e-mail headers to find pattern matches.

WatchGuard customers frequently make SpamScreen rules to help them find and tag spam. An example of a rule is to examine the e-mail header for the text string “free”. If the message has a header with the word “free”, the total Spam Weight increases. You can also make rules about incorrect dates, empty fields, or MIME types.

You assign a weight to each rule. If a message matches more than one rule, it is more likely the Firebox will identify it as spam. You can also assign a negative weight to a rule. This helps the Firebox to not identify good e-mail as spam.

For example, you can set up rules with positive weights for messages with the word “sale.” At the same time, you can set up rules with negative weights for e-mail sent by vendors you regularly do business with. An e-mail from your vendor about “SALE!” in the subject matches two rules: a positive weight for the word “sale” and a negative weight for the sender. When the Firebox adds the two weights, it does not identify the message as spam.

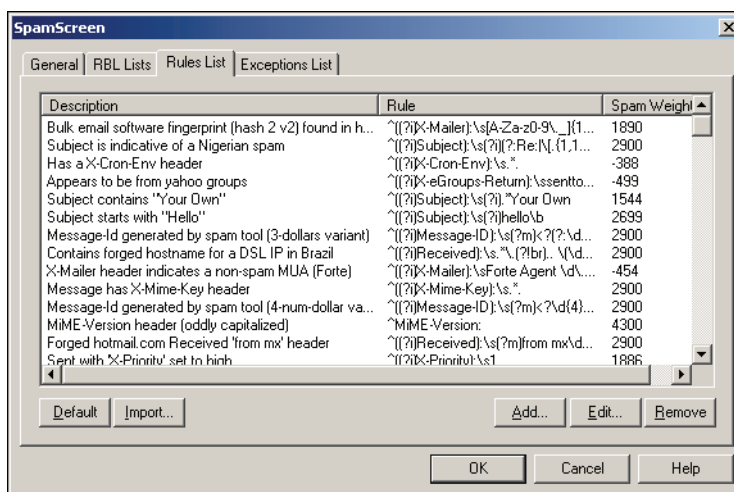
NOTE

Rules apply only to e-mail headers and not to e-mail content. SpamScreen does not examine the text of e-mail messages.

The default SpamScreen configuration includes many rules which are sufficient for most installations. If you are an advanced user, you can add new rules or remove or change the default rules.

Adding spam rules

- 1 From the Policy Manager, select **Setup > SpamScreen**. Click the **Rules List** tab.



- 2 To remove a rule, highlight the rule in the **Rules List**. Click **Remove**.
- 3 To add a new rule, click **Add**. The Spam Rule dialog box appears.



- 4 In the **Description** text box, type a description for the rule. This text appears in the Rules List and helps you find a rule. An example is "Subject starts with "Sale:""

-
- 5 In the **Rule** text box, type the spam rule. Rules use Perl compatible regular expression syntax. For more information on Perl compatible regular expressions, browse to:
<http://www.pcre.org/pcre.txt>
 - 6 Type a weight for the rule in the **Spam Weight** field. You can type a value from -30,000 to 30,000. Positive numbers are for rules that identify spam. Negative numbers are for rules that identify ham.

Restoring default rules

To restore the default configuration for spam rules, on the **Rules List** tab, click the **Default** button.

Importing rules

You can import rules from a file. This can save you time. The rules must be in the same format as the configuration file. The syntax is:

weight "description" rule

Examples:

1886 "Sent with 'X-Priority' set to high" ^((?)X-Priority):\s+1

1594 "Message has X-Library header" ^((?)X-Library):\s+.*

-388 "Has a X-Cron-Env header" ^((?)X-Cron-Env):\s+.*

4300 "Message has X-x header" ^((?)X-x):\s+.*

-192 "Has a Resent-To header" ^((?)Resent-To):\s+.*

- 1 From the **Rules List** tab of the **SpamScreen** dialog box in **Policy Manager**, click **Import**.
- 2 Browse to locate the file. Select the file, and click **Open**.

For more information on **SpamScreen** rules, see the **LiveSecurity** archive at:

www.watchguard.com/archive/showhtml.asp?pack=7131

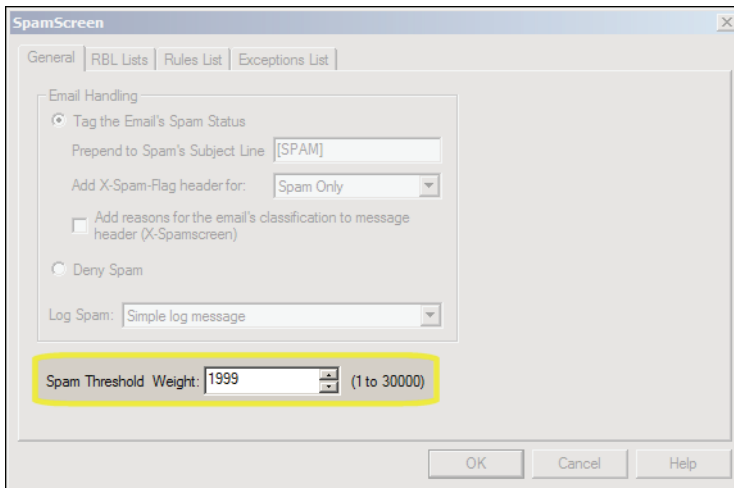
www.watchguard.com/archive/showhtml.asp?pack=7372

Defining spam threshold weight

E-mail must be more than a **Spam Weight** limit that you set before the **Firebox** can identify it as spam. To change the **Spam Threshold Weight** value, open the **SpamScreen** dialog box.

When you increase the **Spam Threshold Weight**, you make it harder for the **Firebox** to identify a message as spam. When you decrease

the Spam Threshold Weight, you make it easier for the Firebox to identify a message as spam.

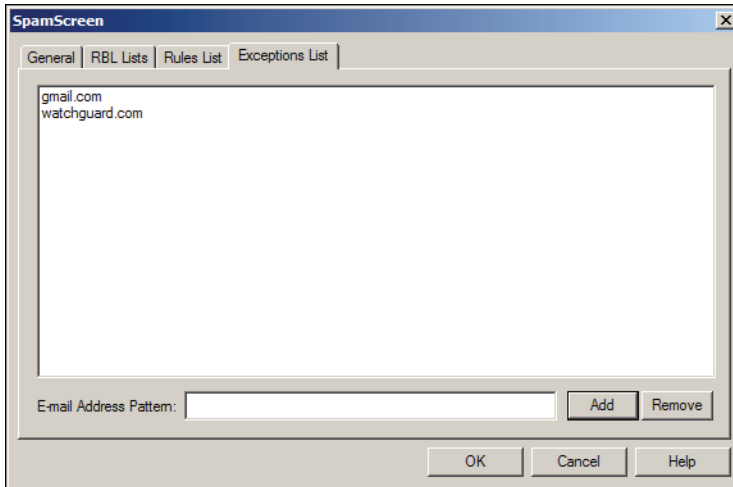


Configuring Exceptions to the Spam List

At times, the Firebox identifies a message as spam when it is not spam. If you know the address of the sender, you can configure the

Firebox with an exception after which it does not examine the messages from that source.

- 1 From the Policy Manager, select **Setup > SpamScreen**. Click the **Exceptions** tab.



- 2 In the **E-mail Address Pattern** text box, type the domain name or e-mail address of the sender. Click **Add**.

The host name or e-mail address appears in the Exceptions to Spam list. SpamScreen does not examine messages from that address.

Blocking addresses not on the spam list

If you are attacked by a spam source that is not on an RBL list, you can use the SMTP Proxy to block all messages from that source.

NOTE

When you use the SMTP Proxy to block an address pattern, you prevent all e-mail from that source. Use caution when using this feature.

- 1 From the Policy Manager, double-click the **SMTP Proxy** icon. The Properties dialog box opens.
- 2 Click the **Properties** tab.
- 3 Click **Incoming**. The Incoming SMTP Proxy dialog box appears displaying the General tab.
- 4 Click the **Address Patterns** tab.
- 5 Use the **Category** drop-down list to select **Denied From**.

- 6 Type the address pattern in the text box to the left of the **Add** button.
- 7 Click **Add**.
The address pattern appears in the pattern list. Repeat for the address pattern of each spammer not blocked automatically by SpamScreen.
- 8 Click **OK**.

Monitoring SpamScreen Activity

You can use a number of methods to monitor SpamScreen™. The WatchGuard System Manager includes reports and real-time log message monitors. You can also use your e-mail software.

Viewing message header notifications

Most e-mail systems use special instructions to show full message headers. The instructions that follow are the procedures for the most frequently used e-mail systems. Use your e-mail system documentation if your software is not in this list.

Microsoft Outlook 97 and Microsoft Outlook Express

- 1 Open the message.
- 2 Select **File > Properties**.
- 3 Click the **Details** tab.

Microsoft Outlook 98 and later

- 1 Open the message.
- 2 Select **View > Options**.
The Internet headers field displays the entire message header.

Netscape Messenger

- 1 Open the message.
- 2 Select **View > Headers > All**.

Pine

- 1 Enable full header command mode. From the Main Menu, type S to enter Setup menu. Type C to enter the configuration screen.
- 2 Use the space or down arrow key to scroll down until you locate:
[] enable-full-header-cmd

-
- 3 Type X to enable full header command. Type E to exit. Type Y to confirm changes.
 - 4 Open the message.
 - 5 Type H to display full headers.

Interpreting log messages

When SpamScreen identifies a message as spam, it records a log message in the log file. Usually, these log messages give a cause for the identification as spam.

These are example SpamScreen log messages in the Simple Log format:

Message	Description
Found spam from server-IP (reason) from user@domain Where <i>server-ip</i> is the IP address of the sending SMTP server, <i>reason</i> explains why SpamScreen marked the message as spam and <i>user@domain</i> is the sender of the message.	The Firebox identified the message as spam based on the SpamScreen rules.
<i>user@domain</i> overrides spam list Where <i>user@domain</i> is the sender of the message	The sender address was found on the Exceptions list. The Firebox did not examine the message.

The example below is of a Verbose Log. In addition to the fields on the previous table, it lists the rules hit, the total score, and the threshold.

```
05/31/03 16:06 smtp-proxy[143]: (spamscreen) e-mail received from
<od@yahoo.com>, marked as spam
05/31/03 16:06 smtp-proxy[143]:      Results of spamscreen:
05/31/03 16:06 smtp-proxy[143]:      2900    Message has X-Mime-Key header
05/31/03 16:06 smtp-proxy[143]:      4300    Message has X-VMP-Text header
05/31/03 16:06 smtp-proxy[143]:      2900    Message has X-PMFLAGS header
05/31/03 16:06 smtp-proxy[143]:      Score   : 10100
05/31/03 16:06 smtp-proxy[143]:      Required: 5000
05/31/03 16:06 smtp-proxy[143]:
```