

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 - 2004 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.

WFS Software Number v7.2

Contents

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

Monitoring SpamScreen Activity	16
<i>Viewing message header notifications</i>	16
<i>Interpreting log messages</i>	17

WatchGuard SpamScreen™ Guide

Unwanted junk email, also known as spam, floods the typical user's inbox at an astounding rate. Some experts predict that the total number of spam email messages sent daily will increase from 10 billion in 2003 to 30 billion by 2006. This deluge of spam degrades bandwidth, saps productivity, and wastes network resources.

SpamScreen considerably enhances your ability to capture spam at the point where it attempts to enter your system: the SMTP proxy service of your firewall. With SpamScreen enabled, the WatchGuard SMTP proxy evaluates the header content of each message and determines whether or not the message is spam.

SpamScreen Options

You can configure SpamScreen in a number of ways to customize how SpamScreen classifies email as spam and what it does to spam once it is detected.

SpamScreen can identify spam in two ways. The first option is to allow SpamScreen to check the IP address of the server sending potential spam against one or more RBL (realtime blackhole list) servers. These are special-purpose DNS servers

that store IP addresses of known spammers and other hosts that may be vulnerable to spam attacks (such as mail relays). In addition to the RBL server lookup, SpamScreen verifies the existence of an email server (DNS MX record lookup) for the sender's domain.

The second way SpamScreen can identify spam is by applying a set of rules to email message headers. Each rule has a positive or negative weight, and the weight values for rule matches are summed for each message. If the message exceeds a certain threshold, it is classified as spam. (For more information on weighting spam, see "Configuring Spam Rules" on page 12.)

You can also configure the actions taken by SpamScreen after a message is determined to be spam. The SMTP proxy can either allow the message, refuse it, or tag it as spam before delivering 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 multiple SMTP proxies so that spam is handled differently for different groups within an organization. For example, you might identify spam by the Rules Lists only for your HR department, identify spam by RBL Lists only for your Engineering group, and allow all email (no SpamScreen processing) for your sales department.

NOTE

Even if you configure multiple SMTP proxies, the Rules Lists, the RBL Lists, or both are applied globally for all SMTP proxies that enable them. You cannot apply different Rules Lists or different RBL Lists to different proxies. For example, you cannot create a RBL Lists-Sales and RBL Lists-HR that are applied to different proxies.

In this respect, you can customize SpamScreen on a "per service" basis. This capability applies only to the two checkbox controls within the SMTP proxy (as described in "Determining

How SpamScreen Identifies Spam” on page 9) and does not apply to other SpamScreen properties.

If you want to use multiple proxies with SpamScreen, your network must be set up in either of the following configurations:

- Multiple internal email servers for each department
- Define what external source can send email for each SMTP proxy

For more information on how to set up your network to use multiple proxies with SpamScreen, see the online support resources at:

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

Installing SpamScreen

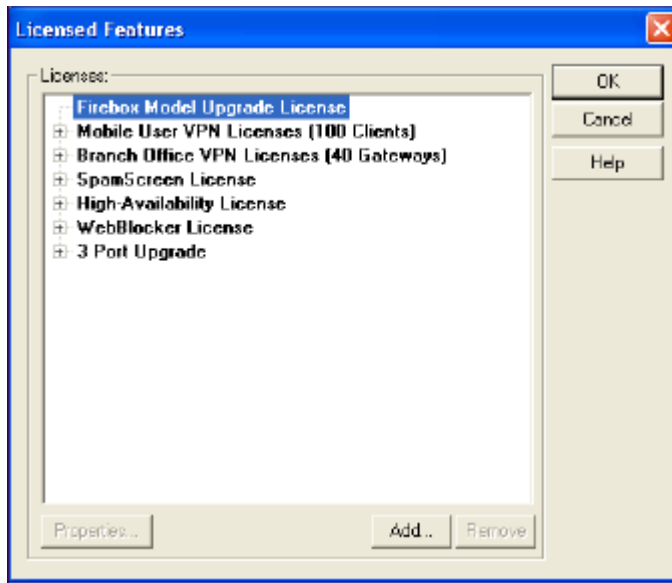
Before installing SpamScreen, you need the following:

- SpamScreen license key certificate.
- Email server behind the Firebox.
- SMTP proxy service. For information on adding the SMTP proxy service, see the WatchGuard Firebox System 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, either type your license key or click **Browse** and find it on your network. Click **OK**.

The new license now appears on the Licensed Features dialog box.

NOTE

The term "Firebox" refers to either the Firebox III or the Firebox X unless specifically stated. Illustrations of Fireboxes are interchangeable unless specifically stated.

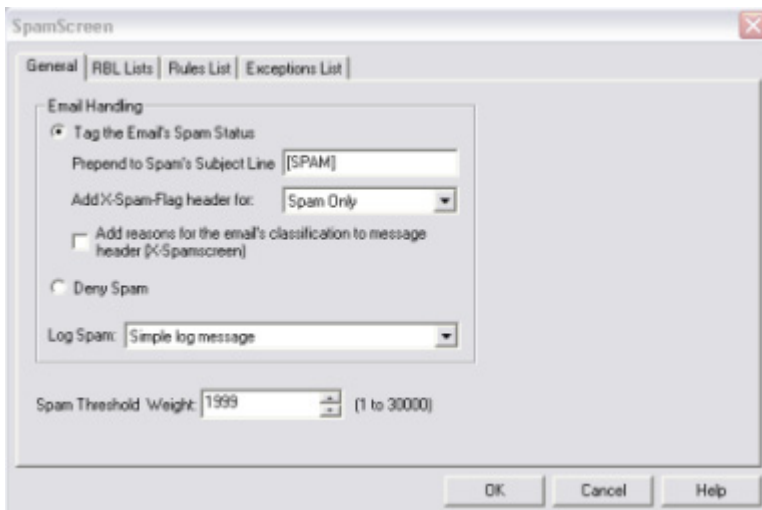
Starting SpamScreen

From Policy Manager, select **Setup** ⇒ **SpamScreen**. The **SpamScreen** dialog box appears, as shown in the following figure. You use the **SpamScreen** dialog box to configure:

- The action SpamScreen takes after identifying spam
- How SpamScreen identifies spam

You also use the **SpamScreen** dialog box to configure RBL and DNS/RBL server IP address lists and spam rules, define the type

of message logged when spam is received, and define exceptions to spam lists.



Configuring Whether Spam is Denied, Tagged, or Logged

SpamScreen can handle a spam message in one of three ways:

- **Deny** – Blocks spam messages.
- **Tag** – Tags messages (either all messages or spam only) and allows spam messages.
- **Allow** – Allows spam messages.

WatchGuard recommends that you not use the **Deny** option initially. Use the **Tag** option and monitor the results for a period of time before using the **Deny** option.

About SpamScreen headers and tags

SpamScreen can add content to message headers or subject lines, depending on how you configure tagging in the **SpamScreen** dialog box.

X-SpamScreen header

SpamScreen adds an “X-Spamscreen” header, by default, to every email message it processes, whether it is spam or not. The following is an example of the default X-SpamScreen header:

```
X-Spamscreen: Protected by WatchGuard (WGTI) Spam-
Screen (TM)
                v7.0.B1000 Copyright (C) 1996-2003 WGTI
```

You can also configure SpamScreen to display a description of how SpamScreen processed the message. The following example shows the X-SpamScreen header with additional processing information, including the message’s weight and the threshold weight. (For more information on weight, see “Configuring Spam Rules” on page 12.)

```
X-Spamscreen: Protected by WatchGuard (WGTI) Spam-
Screen (TM)
                v7.0.B1000 Copyright (C) 1996-2003 WGTI
                Results of SpamScreen:
                2000      From contains advertising finger-
print
                Score    : 2000
                Required: 1999
```

X-Spam-Flag header

You can configure SpamScreen to tag email with the “X-Spam-Flag” header in addition to the default X-SpamScreen header. You can also choose whether SpamScreen displays X-Spam-Flag for all email messages or just for those designated as spam. If a message is designated as spam, the header reads “X-Spam-Flag: YES.” If you have selected to tag all email (not just spam) and the message is not spam, the header reads “X-Spam-Flag: NO.” If you want to be able to read spam email but don’t want it to appear in your inbox, you can use X-Spam-Flag to filter spam and redirect it to a folder.

The following is an example of how a message header might appear when SpamScreen displays both the X-SpamScreen header and the X-Spam-Flag header. In this example, SpamScreen is configured to tag all email and to include SpamScreen processing information in the X-SpamScreen header.

```
X-Spam-Flag: NO
```

```
X-SpamScreen: Protected by WatchGuard (WGTI) Spam-
Screen (TM)
    v7.0.B1346 Copyright (C) 1996-2003 WGTI
    Results of spamscreen:
        701    Subject contains "FREE" in CAPS
    Score    : 701
    Required: 1999
```

Spam subject line

You can configure SpamScreen to tag the subject line of spam messages with a string of your own choosing. The following is an example of a subject line that includes a tag ([SPAM]):

```
Subject: [SPAM] Free auto insurance quote
```

Example message header

The following is an example of a spam email's full message header. Note that the X-Spam-Flag header appears because SpamScreen has been configured to tag email 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]:

```
Return-Path: <johndoe@sparta.iceberg2.watch-
guard.com>
Delivered-To: johndoe@thebes.iceberg.watch-
guard.com
Received: from iceberg.watchguard.com (unknown
[60.100.253.9])
    by thebes.iceberg.watchguard.com (Postfix)
with ESMTP id E7B0918C1F
    for <johndoe@thebes.iceberg.watch-
guard.com>; Wed, 2 Jul 2003 08:33:07 -0700 (PDT)
MIME-Version: 1.0
Message-Id: <9402060055.AA06427@iceberg.watch-
guard.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) Spam-
Screen (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 email account from our deluxe service.

For information on how to view full message headers, see
“Viewing message header notifications” on page 16.

Tagging messages

For further information on the options for tagging email, see
the previous section, “About SpamScreen headers and tags” on
page 5.

From Policy Manager:

- 1 Select **Setup** ⇒ **SpamScreen**.
The SpamScreen dialog box appears.
- 2 If you want to tag email with the X-Spam-Flag header in
addition to the default X-SpamScreen header, select **Tag
the Email's Spam Status**.
SpamScreen adds an X-Spam-Flag header to either all email
messages or just spam email messages, depending on which option
you choose in step 4.
- 3 If you want to add a tag word or phrase, such as [SPAM], to
a spam email message's subject line, enter the word or
phrase in the **Prepend to Spam's Subject Line** field.
- 4 Next to **Add X-Spam-Flag header for**, specify whether you
want the X-Spam-Flag header to appear for spam only or
for all email.
- 5 If you want to include, in the X-Spamscreen header, a
description of how SpamScreen processed the message,
select **Add reasons for the email's classification to
message header (X-Spamscreen)**.
- 6 Click **OK**.

Denying spam

If you simply want to deny spam, in the SpamScreen dialog box, select **Deny Spam**.

Allowing spam

To allow all email 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 email messages and tags them with only the default X-SpamScreen header, as described in “X-SpamScreen header” on page 6.

Logging spam

If you want to log spam, specify how you want the receipt of spam logged:

- Simple log message
- Verbose log message

If you don't want spam to be logged, use the default option **No log message**.

Determining How SpamScreen Identifies Spam

SpamScreen offers two ways to determine how to classify email. The first option is to allow SpamScreen to check the IP address of the server against several public RBL (realtime blackhole list) servers. SpamScreen also verifies the existence of an email server (MX record lookup) at the sender's location.

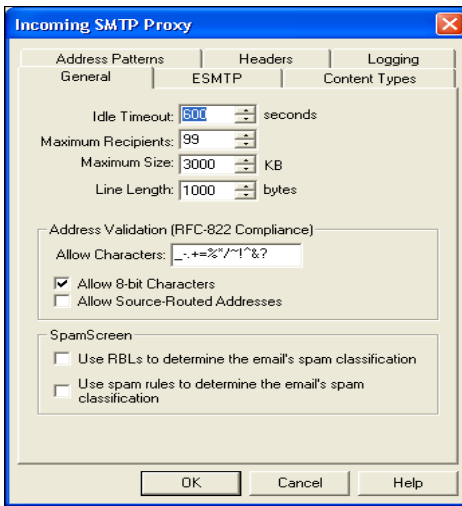
Using the second option, SpamScreen uses rules to identify spam. For more information on rules, see “Configuring Spam Rules” on page 12. You can choose either option, or both options to configure how spam is identified.

- 1 In the Services Arena, double-click the **SMTP Proxy** icon. The service Properties dialog box opens.
- 2 Click the **Properties** tab.
- 3 Click **Incoming**. The Incoming SMTP Proxy dialog box appears displaying the General tab.
- 4 To check email against RBL servers, select **Use RBLs to determine the email's spam classification**. You can now

configure the RBL/DNS servers, as described in the next section.

- 5 To check email header content against rules, select **Use spam rules to determine the email's spam classification**. You can now configure spam rules, as described in “Configuring Spam Rules” on page 12.
- 6 To allow spam, as described in “Allowing spam” on page 9, leave both options unselected.

You can configure multiple SMTP proxies so that spam is handled differently for different groups within your organization. For more information, see “Customizing SpamScreen using Multiple Proxies” on page 2.



Configuring RBL/DNS Servers

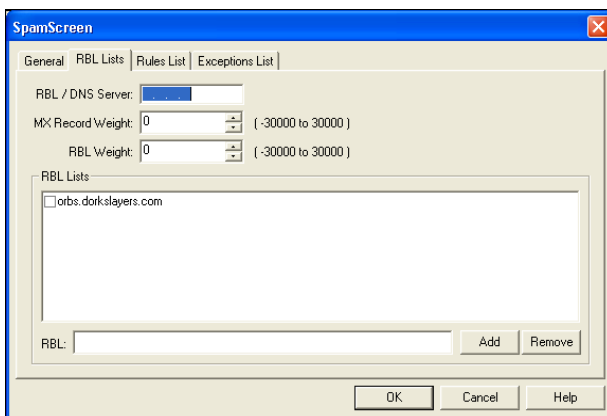
The RealTime BlackHole List (RBL) is a name server that has DNS records for sites considered to be spammers, spam relays, or spam-friendly service providers. If the message originates from an address on the RBL, SpamScreen marks the message as spam.

- 1 To specify the RBL/DNS server used by SpamScreen, from the **SpamScreen** dialog box, click the **RBL Lists** tab.

- 2 In the **RBL/DNS Server** field, type the IP address of the server.
This is generally the IP address of your (or your Internet provider's) DNS server.
- 3 The default weight (2000) in the **MX record weight** field is adequate in most cases. However, if you want to change it, enter the weight added to an MX record lookup email with a non-existent domain name. This weight is added to the spam weight as described in “Configuring Spam Rules” on page 12.
- 4 The default weight (2000) in the **RBL weight** field is adequate in most cases. However, if you want to change it, enter the weight added to an email from a host listed at an RBL in the list. This weight is added to the spam weight as described in “Configuring Spam Rules” on page 12.

Configuring RBL lists

A list of RBL servers appears on the **RBL Lists** tab.



You can enable use of an RBL server by selecting the checkbox to the left of its name. You can also use the **Add** and **Remove** buttons to add or delete other RBL servers.

NOTE

Providing real-time blackhole lists is risky because these organizations are often subject to lawsuits. Because these providers often come and go between our product release

cycles, WatchGuard recommends that you stay current by checking sites dedicated to email abuse.

Addresses you enter in the RBL list must reference a special-purpose DNS server that is specifically designated as an RBL server. A normal DNS server will not function correctly.

You can find additional RBL servers at the following Web sites:

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

Configuring Spam Rules

If you have chosen rules to identify spam (as described in “Determining How SpamScreen Identifies Spam” on page 9), a set of rules determines the probability that an email message is spam. Each rule has a weight, and the “hits” are tallied for a given email message. If the message’s header exceeds a certain threshold, it is classified as spam.

SpamScreen rules act on message headers, not on the content of the messages. Headers define particular aspects of an email message. For example, the “Subject:” header defines the subject line of a message, while the “Date:” header tells when an email message was sent. Headers appear at the top of a message and consist of one or more words followed by a colon. SpamScreen rules consist of special expressions that parse email headers, looking for specific pattern matches.

For example, you might set up rules such that all email headers are examined for the strings “free,” “approved,” or “100%.” You might also set up rules such as those that check for invalid dates, contain an empty Reply-To field, or have an X-Mime-Key header. Each rule is assigned a certain weight such that a message header containing two or three of the strings is definitely tagged as spam. Those messages containing just one string might not be tagged as spam.

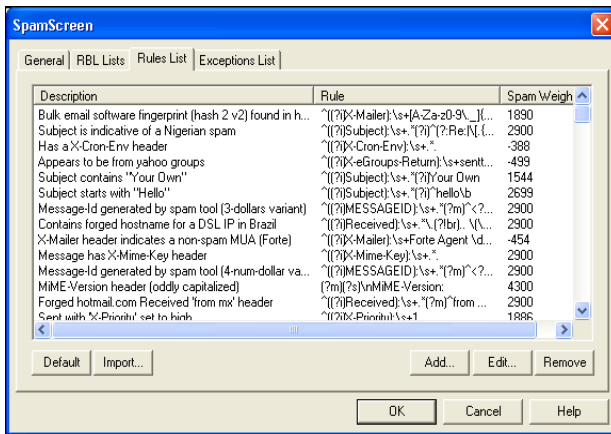
You can assign negative weights to rules as well to prevent legitimate email from being marked as spam. For example, you can set up rules with positive weights for messages dealing with sales and free offers, but assign negative weights for email sent by vendors you regularly do business with. Those email mes-

sages are given a high “spam” weight because of their sales content, but the negative weights applied to them prevent them from exceeding the spam weight threshold.

NOTE

Rules apply only to email headers and not to email content. SpamScreen does not evaluate the text of email messages.

SpamScreen is preconfigured with a number of rules which are adequate for most installations. However, if you are an experienced user, you can add new rules or delete or modify the existing ones. To configure spam rules, click the **Rules List** tab. The default SpamScreen rules appear, as shown in the following figure.



Defining spam threshold weight

As described in the previous section, email must exceed a certain threshold to be classified as spam. In the **Spam Threshold Weight** field (on the **General** tab), enter the weight a message must achieve before being marked as spam.

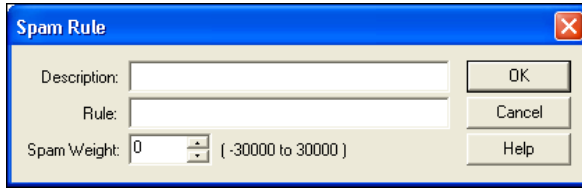
Adding rules

You can add your own rules to SpamScreen; however, WatchGuard recommends this only for expert users.

To add rules:

- 1 From the **SpamScreen** dialog box, click the **Rules List** tab.

- 2 Click **Add**.
The Spam Rule dialog box appears.



- 3 In the **Description** field, enter a description for the rule, such as **Subject starts with "Sale"**.
- 4 In the **Rule** field, enter the spam rule, such as:
^Subject:.*Sale
Rules use Perl-compatible regular expression syntax. For more information on Perl-compatible regular expressions, go to:
<http://www.pcre.org/pcre.txt>
- 5 Enter a weight for the rule in the **Spam Weight** field (-30000 - 30000).

Restoring default rules

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

Importing rules

You can import rules from a file rather than defining them manually. From the **Rules List** tab:

- 1 Click **Import**.
- 2 Browse to locate the file. Double-click it, or select it and click **Open**.

The rules must be in the same format as the configuration file, as shown in the following examples. The format of rules is:
weight "description" rule.

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

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

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

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

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

For more information on reading SpamScreen Rules, see the online resource at:

<https://www.watchguard.com/archive/showhtml.asp?pack=7131>

For more information on writing SpamScreen rules, see the online resources at:

<https://www.watchguard.com/archive/showhtml.asp?pack=7372>

Configuring Exceptions to the Spam List

Occasionally a message will be mistakenly determined to be spam. If you know the sender's address, you can configure exceptions so that address will not be checked by SpamScreen, and subsequently designated as spam.

- 1 From the **SpamScreen** dialog box, click the **Exceptions** tab.
- 2 In the **Email Address Pattern** field, enter the domain name or email address in the text box to the left of the **Add** button.
- 3 Click **Add**.
The host name or email address appears in the Exceptions to Spam list. SpamScreen will no longer check any messages originating from that address.

Blocking addresses not on the spam list

If you are the target of a spammer that has not been detected by SpamScreen, you can block incoming messages from an address pattern using the **Incoming SMTP Proxy** dialog box.

- 1 In the Services Arena, double-click the **SMTP Proxy** icon.
The service 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**.

NOTE

Blocking an address at the SMTP Proxy blocks all users on that domain, and not just the single user you are attempting to block. Use caution when using this feature.

Addresses you enter in the RBL list must reference a special-purpose DNS server that is specifically designated as an RBL server. A normal DNS server will not function correctly.

Monitoring SpamScreen Activity

You can use several methods to monitor SpamScreen activity using both WatchGuard Firebox System monitoring and logging tools as well as your email application.

Viewing message header notifications

Most mail systems require special instructions to display full message headers. The following are instructions for the most commonly used mail systems. Consult your mail system documentation if your application is not listed here.

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 generates a message in the logdb file. Typically, these log entries explain why SpamScreen identified the message as spam.

SpamScreen generates the following log messages when spam is detected or overridden. The following information is included in a simple log.

Message	Meaning
Found spam from <i>server-IP</i> (<i>reason</i>) from <i>user@domain</i> 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 message was determined to be 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, and spam checks were skipped.

The following is an example of a verbose log as seen on the **Traffic Monitor** tab of System Manager. 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) Email
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]:	