

WatchGuard® SpamScreen™ Guide

SpamScreen™ for WFS



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 - 2003 WatchGuard Technologies, Inc. All rights reserved.

AppLock, AppLock/Web, Designing peace of mind, Firebox, Firebox 1000, Firebox 2500, Firebox 4500, Firebox II, Firebox II Plus, Firebox II FastVPN, Firebox III, Firebox SOHO, Firebox SOHO 6, Firebox SOHO 6tc, Firebox SOHO|tc, Firebox V100, Firebox V80, Firebox V60, Firebox V10, LiveSecurity, LockSolid, RapidStream, RapidCore, ServerLock, WatchGuard, WatchGuard Technologies, Inc., DVCP technology, Enforcer/MUVPN, FireChip, HackAdmin, HostWatch, Make Security Your Strength, RapidCare, SchoolMate, ServiceWatch, Smart Security. Simply Done., Vcontroller, VPNforce, The W-G logo are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries.

© Hi/fn, Inc. 1993, including one or more U.S. Patents: 4701745, 5016009, 5126739, and 5146221 and other patents pending.

Microsoft®, Internet Explorer®, Windows® 95, Windows® 98, Windows NT® and Windows® 2000 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

RC2 Symmetric Block Cipher, RC4 Symmetric Stream Cipher, RC5 Symmetric Block Cipher, BSAFE, TPEM, RSA Public Key Cryptosystem, MD, MD2, MD4, and MD5 are either trademarks or registered trademarks of RSA Data Security, Inc. Certain materials herein are Copyright © 1992-1999 RSA Data Security, Inc. All rights reserved.

RealNetworks, RealAudio, and RealVideo are either a registered trademark or trademark of RealNetworks, Inc. in the United States and/or other countries.

Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All right reserved.

© 1995-1998 Eric Young (eay@cryptsoft). All rights reserved.

© 1998-2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

-
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
 3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
 6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"
THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

© 1995-1998 Eric Young (ey@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,

WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Copyright (c) 1998-2001 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

-
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
 3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
"This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>)."
 4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.
 5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.
 6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,

EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Apache Software License, Version 1.1
Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

"This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

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

Part No:

WFS Software Number: 7.0

WatchGuard Technologies, Inc.
SpamScreen Software
End-User License Agreement

IMPORTANT - READ CAREFULLY BEFORE ACCESSING
WATCHGUARD SOFTWARE:

This SpamScreen End-User License Agreement ("AGREEMENT") is a legal agreement between you (either an individual or a single entity) and WatchGuard Technologies, Inc. ("WATCHGUARD") for the WATCHGUARD optional software product for the WatchGuard Firebox System you have purchased, which includes computer software components (whether installed separately on a computer workstation or on the WATCHGUARD hardware product) and may include associated media, printed materials, and on-line or electronic documentation, and any updates or modifications thereto, including those received through the WatchGuard LiveSecurity Service (or its equivalent), (the "OPTIONAL SOFTWARE PRODUCT"). WATCHGUARD is willing to license the OPTIONAL SOFTWARE PRODUCT to you only on the condition that you accept all of the terms contained in this Agreement. Please read this Agreement carefully. By installing, activating or using the OPTIONAL SOFTWARE PRODUCT you agree to be bound by the terms of this Agreement. If you do not agree to the terms of this AGREEMENT, WATCHGUARD will not license the OPTIONAL SOFTWARE PRODUCT to you, and you will not have any rights in the OPTIONAL SOFTWARE PRODUCT. In that case, promptly return the OPTIONAL SOFTWARE PRODUCT/license key certificate, along with proof of payment, to the authorized dealer from whom you obtained the OPTIONAL SOFTWARE PRODUCT/license key certificate for a full refund of the price you paid.

1. Ownership and License. The OPTIONAL SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This is a license agreement and NOT an agreement for sale. All title and copyrights in and to the OPTIONAL SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and applets incorporated into the OPTIONAL SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the OPTIONAL SOFTWARE PRODUCT are owned by WATCHGUARD or its licensors. Your rights to use the OPTIONAL SOFTWARE PRODUCT are as specified in this AGREEMENT, and WATCHGUARD retains all rights not expressly granted to you in this AGREEMENT. Nothing in this AGREEMENT constitutes a waiver of our rights under U.S. copyright law or any other law or treaty.

2. Permitted Uses. You are granted the following rights to the OPTIONAL SOFTWARE PRODUCT:

(A) You may install and use the OPTIONAL SOFTWARE PRODUCT on that number of WATCHGUARD hardware products (or manage that number of WATCHGUARD hardware products) at any one time as permitted in the license key certificate that you have purchased and may install and use the OPTIONAL SOFTWARE PRODUCT on multiple workstation computers. You must also maintain a current subscription to the WatchGuard LiveSecurity Service (or its equivalent) for each additional WATCHGUARD hardware product on which you will use a copy of an updated or modified

version of the OPTIONAL SOFTWARE PRODUCT received through the WatchGuard LiveSecurity Service (or its equivalent).

(B) To use the OPTIONAL SOFTWARE PRODUCT on more WATCHGUARD hardware products than provided for in Section 2(A), you must license additional copies of the OPTIONAL SOFTWARE PRODUCT as required.

(C) In addition to the copies described in Section 2(A), you may make a single copy of the OPTIONAL SOFTWARE PRODUCT for backup or archival purposes only.

3. Prohibited Uses. You may not, without express written permission from WATCHGUARD:

(A) Use, copy, modify, merge or transfer copies of the OPTIONAL SOFTWARE PRODUCT or printed materials except as provided in this AGREEMENT;

(B) Use any backup or archival copy of the OPTIONAL SOFTWARE PRODUCT (or allow someone else to use such a copy) for any purpose other than to replace the original copy in the event it is destroyed or becomes defective;

(C) Sublicense, lend, lease or rent the OPTIONAL SOFTWARE PRODUCT;

(D) Transfer this license to another party unless

(i) the transfer is permanent,

(ii) the third party recipient agrees to the terms of this AGREEMENT, and

(iii) you do not retain any copies of the OPTIONAL SOFTWARE PRODUCT;
or

(E) Reverse engineer, disassemble or decompile the OPTIONAL SOFTWARE PRODUCT.

4. Limited Warranty. WATCHGUARD makes the following limited warranties for a period of ninety (90) days from the date you obtained the OPTIONAL SOFTWARE PRODUCT from WATCHGUARD or an authorized dealer:

(A) Media. The disks and documentation will be free from defects in materials and workmanship under normal use. If the disks or documentation fail to conform to this warranty, you may, as your sole and exclusive remedy, obtain a replacement free of charge if you return the defective disk or documentation to us with a dated proof of purchase.

(B) OPTIONAL SOFTWARE PRODUCT. The OPTIONAL SOFTWARE PRODUCT will materially conform to the documentation that accompanies it or its license key certificate. If the OPTIONAL SOFTWARE PRODUCT fails to operate in accordance with this warranty, you may, as your sole and exclusive remedy, return all of the OPTIONAL SOFTWARE PRODUCT and the documentation to the authorized dealer from whom you obtained it,

along with a dated proof of purchase, specifying the problems, and they will provide you with a new version of the OPTIONAL SOFTWARE PRODUCT or a full refund, at their election.

Disclaimer and Release. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 4, 4(A) AND 4(B) ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ITS LICENSORS AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD AND ITS LICENSORS, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE OPTIONAL SOFTWARE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY THAT THE OPTIONAL SOFTWARE PRODUCT WILL MEET YOUR REQUIREMENTS, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD AND ITS LICENSORS AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE OPTIONAL SOFTWARE PRODUCT).

Limitation of Liability. WATCHGUARD'S LIABILITY (WHETHER IN CONTRACT, TORT, OR OTHERWISE; AND NOTWITHSTANDING ANY FAULT, NEGLIGENCE, STRICT LIABILITY OR PRODUCT LIABILITY) WITH REGARD TO THE OPTIONAL SOFTWARE PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT), FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE OPTIONAL SOFTWARE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.

5. United States Government Restricted Rights. The OPTIONAL SOFTWARE PRODUCT is provided with Restricted Rights. Use, duplication or disclosure by the U.S. Government or any agency or instrumentality thereof is subject to restrictions as set forth in subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or in subdivision (c)(1) and (2) of the Commercial Computer Software -- Restricted Rights Clause at 48 C.F.R. 52.227-19, as applicable. Manufacturer is WatchGuard Technologies, Inc., 505 5th Ave. South, Suite 500, Seattle, WA 98104.

6. Export Controls. You agree not to directly or indirectly transfer the OPTIONAL SOFTWARE PRODUCT or documentation to any country to which such transfer would be prohibited by the U.S. Export Administration Act and the regulations issued thereunder.

7. Termination. This license and your right to use the SOFTWARE PRODUCT will automatically terminate if you fail to comply with any provisions of this AGREEMENT, destroy all copies of the OPTIONAL SOFTWARE PRODUCT in your possession, or voluntarily return the OPTIONAL SOFTWARE PRODUCT to WATCHGUARD. Upon termination you will destroy all copies of the OPTIONAL SOFTWARE PRODUCT and documentation remaining in your control or possession.

8. Miscellaneous Provisions. This AGREEMENT will be governed by and construed in accordance with the substantive laws of Washington excluding the 1980 United National Convention on Contracts for the International Sale of Goods, as amended. This is the entire AGREEMENT between us relating to the OPTIONAL SOFTWARE PRODUCT, and supersedes any prior purchase order, communications, advertising or representations concerning the OPTIONAL SOFTWARE PRODUCT AND BY USING THE OPTIONAL SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. IF THE SOFTWARE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THIS AGREEMENT ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS AGREEMENT; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS AGREEMENT AND PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT AND; (C) THIS AGREEMENT AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THIS AGREEMENT DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY. No change or modification of this AGREEMENT will be valid unless it is in writing and is signed by WATCHGUARD.

Contents

SpamScreen Options	1
Customizing SpamScreen using Multiple Proxies	2
Installing SpamScreen	3
Starting SpamScreen	3
Configuring Whether Spam is Denied, Tagged, or Logged ..4	
About SpamScreen headers and tags	5
Tagging messages	7
Denying spam	8
Allowing spam	8
Logging spam	8
Determining How SpamScreen Identifies Spam	8
Configuring RBL/DNS Servers	10
Configuring RBL lists	11
Configuring Spam Rules	12
Defining spam threshold weight	13
Adding rules	13
Restoring default rules	14
Importing rules	14
Configuring Exceptions to the Spam List	15
Blocking addresses not on the spam list	15

Keeping SpamScreen Current	16
Monitoring SpamScreen Activity	16
Viewing message header notifications	17
Interpreting log messages	18

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.

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 rules only for your HR department, identify spam by RBL servers only for your Engineering group, and allow all email (no SpamScreen processing) for your sales department. 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 8) and does not apply to other SpamScreen properties.

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:

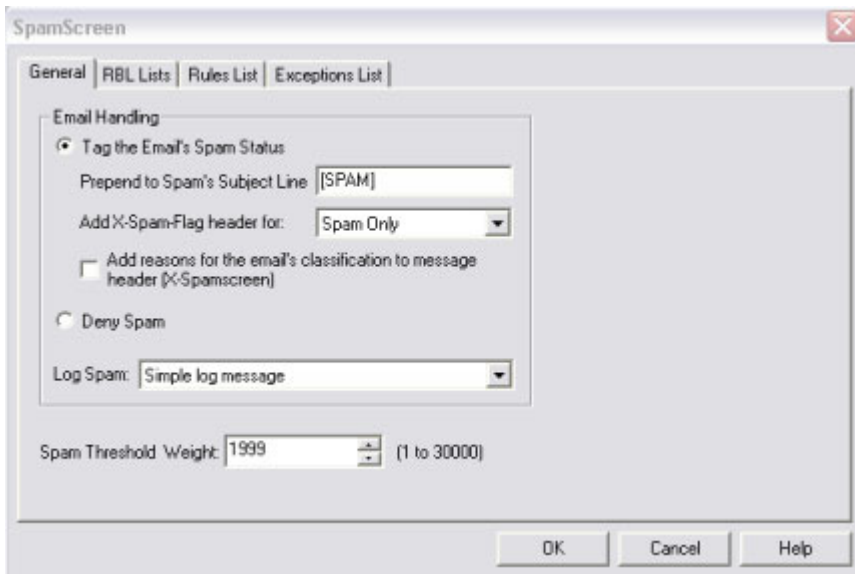
- 1 Insert the WatchGuard Firebox System CD.
If the installation wizard does not start automatically, double-click `install.exe` in the root directory of the CD.
- 2 On the Select Components screen of the installation wizard, select the **SpamScreen** checkbox.
- 3 Enter the SpamScreen license key found on your license key certificate.
- 4 Continue with the installation of the WatchGuard Firebox System, as described on the QuickStart Guide included with your Firebox.

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) SpamScreen (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) SpamScreen (TM)
              v7.0.B1000 Copyright (C) 1996-2003 WGTI
              Results of SpamScreen:
                2000    From contains advertising fingerprint
              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) SpamScreen (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.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 ESMTP id
E7B0918C1F
         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 email account from our deluxe service.

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

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 5.

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

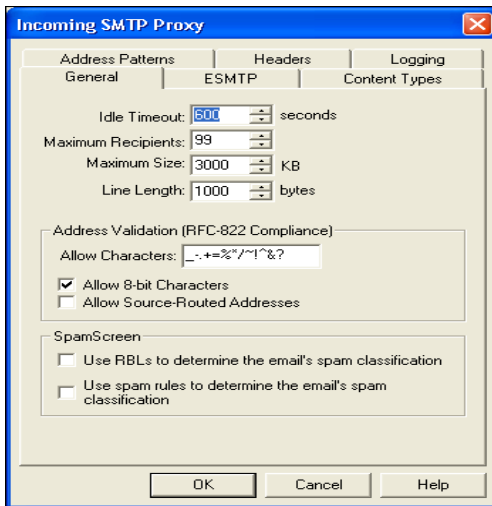
SpamScreen offers two ways to determine how to classify email. The first option is to allow SpamScreen to check the IP address of the server against several public RBL (real-time blackhole list) servers. SpamScreen also verifies the existence of an email server (MX record lookup) at the sender’s location.

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 8, 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.

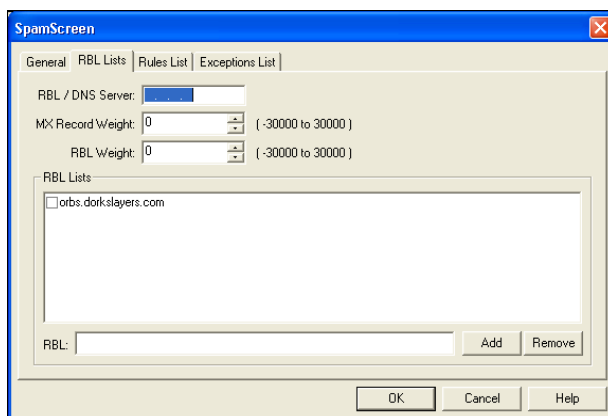
- 1 To specify the RBL/DNS server used by SpamScreen, from the **SpamScreen** dialog box, click the **RBL Lists** tab.
- 2 In the **RBL/DNS Server** field, type the IP address of the server.
This is generally the IP address of your (or your Internet provider's) DNS server.
- 3 The default weight (2000) 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 check-box 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 8), 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 exceeds a certain threshold, it is classified as spam.

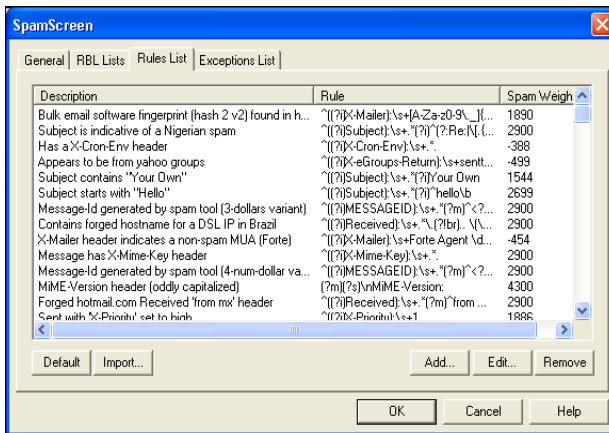
For example, you might set up rules such that all email headers are examined for the strings “free,” “approved,” or “100%.” You might also set up rules such as those that check for invalid dates, contain an empty Reply-To field, or have an X-Mime-Key header. Each rule is assigned a certain weight such that a message 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 messages 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

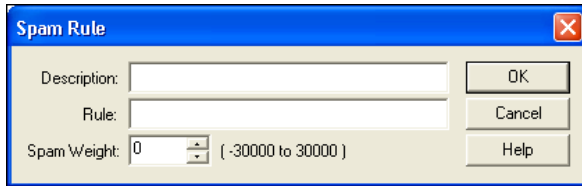
As described in the previous section, email must exceed a certain threshold to be classified as spam. In the **Spam Threshold Weight** field (on the **General** tab), enter the weight a message must achieve before being marked as spam.

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+.*.
```

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.

Keeping SpamScreen Current

Our team at WatchGuard monitors anti-spam newsgroups, mailing lists, and Web sites in order to keep our product current with the latest tactics in the battle against spam.

As a LiveSecurity Service subscriber, you will automatically receive periodic updates to the SpamScreen utility. Like other broadcasts, these software updates are sent to you through your email client.

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 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 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 spam-
screen:
05/31/03 16:06 smtp-proxy[143]:           2900    Mes-
sage has X-Mime-Key header
05/31/03 16:06 smtp-proxy[143]:           4300    Mes-
sage has X-VMP-Text header
05/31/03 16:06 smtp-proxy[143]:           2900    Mes-
sage 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]:
```