

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., Vcontoller, 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 (eay@cryptsoft.com). This product includes software written by Tim

Hudson (tjh@cryptsoft.com).

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

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@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 aheared 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: 6.2

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.

WatchGuard SpamScreen™ Guide

Thank you for purchasing WatchGuard SpamScreen. This document describes how to install and configure SpamScreen to immediately reduce the time and effort of controlling junk email on your network.

Installing SpamScreen

Your purchase of the WatchGuard SpamScreen includes a license key certificate. You enter your license key when you install the WatchGuard Firebox System software.

- 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, click the checkbox marked **SpamScreen**.
- 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 poster included with your Firebox.

NOTE

You must have an email server behind the Firebox to be able to use SpamScreen.

Configuring SpamScreen Message Handling

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

- **Deny** — Deletes the message.
- **Allow** — Disables SpamScreen and allows messages to pass to the recipient unchanged.
- **Tag** — Passes the message to the recipient with a tag-phrase in the subject line.

NOTE

SpamScreen requires the SMTP proxy service. If it is not already configured, use Policy Manager to add the SMTP proxy service. For information on adding the SMTP proxy service, see the *WatchGuard Firebox System User Guide*.

SpamScreen offers two levels of checks: normal and advanced. Normal SpamScreen checks headers for known spam sources. It also runs a known characteristics check and screens for bulk mailer tags. (For more information, see “How SpamScreen Identifies Spam” on page 5.)

SpamScreen checks the IP address of the server against several public 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).

With Advanced Spam Mail Filtering enabled, SpamScreen expands the headers evaluated. This option considerably reduces “false negatives”—SpamScreen failing to identify a spam message as spam. The disadvantage is that it makes SpamScreen considerably more sensitive and may increase the number of “false positives”—SpamScreen

identifying a normal message as spam. Advanced Spam Mail Filtering may result in SpamScreen identifying mailing list messages as spam.

From Policy Manager in the Advanced view (to access the advanced view, click View ⇒ Advanced):

- 1 Select **Setup** ⇒ **SpamScreen**.
- 2 Enter the DNS Server IP address.
- 3 In the **Spam Mail Handling** box, select **Allow**, **Tag**, or **Deny**. (See the next section for more information on the **Tag** option.)
- 4 To enable advanced spam mail filtering, enable the checkbox marked **Advanced Spam Mail Filtering**.
- 5 In the RBL List box, select RBL servers if desired.
For more information, see "RealTime BlackHole List" on page 5.
- 6 Click **OK**.

Tagging spam

The Tag spam mail handling option prepends a word or phrase in the Subject line of each message identified as spam. This option lets recipients filter and redirect spam, identified by its prepended message tag, into a folder for later perusal. You define the message tag. Example tags include: [UCE] or [SPAM]. From Policy Manager:

- 1 Select **Setup** ⇒ **SpamScreen**.
The SpamScreen dialog box appears.
- 2 Select the **Tag** option.
- 3 Enter a tag word or phrase.
- 4 Click **OK**.
Consult the documentation for your email application to learn how to filter mail based on Subject line.

Allowing blocked addressees

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 tagged as spam.

From the Policy Manager:

- 1 Click **Setup** ⇒ **SpamScreen**.
The SpamScreen dialog box appears.

-
- 2 Under **Exceptions to Spam List**, 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 spammer that has not been detected by SpamScreen, you can block incoming messages from an IP address 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 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.

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.

Receiving an update via LiveSecurity

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. Follow the directions to install the software update.

How SpamScreen Identifies Spam

SpamScreen considerably enhances your ability to deal with 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 each message and determines whether or not the message is spam. If it concludes the message is spam, the SMTP proxy automatically either refuses the messages or places a tag in the subject line before delivering it to the recipient.

SpamScreen uses several methods to identify spam.

RealTime BlackHole List

SpamScreen first checks the message against the RealTime BlackHole List (RBL). The 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.

As of March 1, 2002, SpamScreen comes pre-configured with the following RBL server:

bl.orbl.org

You can enable use of this RBL server by clicking the checkbox to the left of the particular name. You can also use the Add and Remove buttons to configure 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, we advise you to stay current by reading the Slashdot news site: <http://slashdot.org>

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>

Known characteristics check

Typically, spam messages share one or more characteristics found in the message header. The indicators are frequently a by-product of the spammers' desire to hide their address and avoid a deluge of bounced mail and irritated replies. Examples of known characteristics include:

- From or Reply-To with `noreply@`
- From, To, or CC with `friend[0-9a-zA-Z]@`
- From, To, or CC with `moneymakers@`
- To or CC with blank before the @ sign
- To or CC with "(Recipient list suppressed)"
- To or CC with `to.all.our.friends@`
- Reply-To with Remove in the string

SpamScreen checks the message against an extensive list of known characteristics. If any one of these conditions are true, SpamScreen marks the message as spam.

Commercial bulk mailtags

Most commercial bulk email applications leave some fingerprint on the message header. For example, many include an "X-" header identifying the name of the application. SpamScreen checks the message against a list

of known bulk mailer patterns. If a pattern is found, SpamScreen marks the message as spam.

Valid sender address

To escape complaints, many spammers send email messages from domains that do not exist and are therefore impossible to reply to. To detect this, SpamScreen attempts to validate addresses in the From and Reply-To headers. It does this by querying the configured DNS name server for a Mail Exchanger (MX) record for any domains in those headers. If an MX record does not exist, SpamScreen marks the message as spam.

SpamScreen message header

After processing a message through all three checks, SpamScreen allows it to pass through the firewall. SpamScreen adds an "X-SpamScreen" header to every message. If the message is spam, SpamScreen includes a description of why the message was marked as spam.

```
X-SpamScreen: Protected by WatchGuard SpamScreen (TM)
v5.0.B841 Copyright (C) 1996-2002 WGTI WGTI
Found spam from 131.107.3.126 (no recipients)
```

Monitoring SpamScreen Activity

There are 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

Spam is often readily identifiable by the contents of the message headers. SpamScreen uses these headers to mark spam. In addition, SpamScreen adds an "X-SpamScreen" header to every email message it processes. 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 configuration.
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.

DNS errors

Errors and diagnostic logs relating to DNS queries are of the format:
query #N to Server for Domain: ...

where:

N is the query number assigned by SpamScreen
Server is the DNS server configured to handle SpamScreen
Domain is either the domain of the RBL server or the MX server.

Common errors

DNS Error Message	Meaning
can't connect to DNS socket error in sending query error in receiving response	An error occurred while attempting to send a request or receive a response from the DNS name server. Make sure the Firebox is configured with the address of a working name server.
no server to query	No DNS name server was configured. Make sure the Firebox is configured with the address of a working name server.
nameserver responded with error	The name server received an unexpected error while processing the request.
timed out — resending	The DNS request timed out, and was resent. This may happen if the Firebox is misconfigured, the DNS server is not working, or downstream DNS servers were unable to look up a domain name quickly enough.
too many tries	Several DNS requests were made, and none completed. This may happen if there are misconfigured downstream DNS servers.

Info logs

These are log messages that SpamScreen generates when spam is detected or overridden.

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.

