

eSoft

Simply better network security.™

®

ThreatWall™

Quarantine

Copyright Notices

© eSoft, Inc. 2004. eSoft and ThreatWall are registered trademarks, and ThreatWall, SoftPak and SoftPak Director are trademarks of eSoft, Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation. Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation. Adobe, the Adobe logo, and Acrobat are registered trademarks of Adobe Systems Inc. UNIX is a registered trademark of UNIX Systems Laboratories, Inc. All other brand and/or product names are the property of their respective holders.

Portions of ThreatWall's software are covered under the GNU General Public License. You may freely obtain source code versions of the software covered by the GNU General Public License through the Internet at <http://www.redhat.com>. However, some applications remain the property of their owners, and require their permission to redistribute. For more information, access the eSoft web site at <http://www.esoft.com>.

Portions of ThreatWall's software are Copyright © The Regents of the University of California. A complete copy of the copyright notice follows:

Copyright © The Regents of the University of California.

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. Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistribution 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 University of California, Berkeley and its contributors."
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “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 REGENTS 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.

Portions of ThreatWall’s software are Copyright © The Apache Group. A complete copy of the copyright notice follows:

Copyright © 1995-1997 The Apache Group. 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 Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).”

4. The names “Apache Server” and “Apache Group” must not be used to endorse or promote products derived from this software without prior written permission.

5. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).”





ThreatWall Email Quarantine

The Email Quarantine holds messages that you would like to review before releasing or deleting them. The Quarantine Options allow you to give users access to their own quarantined messages, send notifications to users about their quarantine and delete messages that have been in the quarantine for too long.

Managing the Email Quarantine

To manage messages in the Email Quarantine, use one of the following:

- Select *Quarantine* from the *SpamFilter* menu.
- Go to the URL: https://<ip_address>/EmailQuarantine with your browser.

If you have more than 2500 messages, you'll see a drop-down list of dates to view. Select the date of the messages you wish to view from the Show Messages For drop-down list. If you have less than 2500 messages in Quarantine, you will see the All option to view the entire Quarantine.

1. To sort the messages, simply click the appropriate column heading (Hits, From, To, or Subject).
2. To view a message, click the associated blue-highlighted text. The message appears in a separate window.
3. To delete a message, select the message and click Delete.
4. To delete other messages in the Email Quarantine with the same From, To, or Subject header as the selected message, select the appropriate check boxes at the bottom of the page, and click Delete. This deletes all applicable messages for the selected date. To apply the delete to all dates, you must select the All Days check box.
5. To delete all messages in the Email Quarantine, click Purge.
6. To release a message to the intended recipient, select the message and click Release.

Note Note: When you release a message in the Email Quarantine, SpamFilter analyzes the message and provides suggestions you may wish to add to the White List. Simply review the suggestions listed, remove any addresses you do not wish to add, and click Apply.

Viewing Messages in the Email Quarantine

When you click the blue-highlighted text associated with a message in the Email Quarantine, the View Message page appears in a separate window, displaying the email message. Inside the message, headers of interest, such as To, From, and Subject appear in bold. Message are cut short if they're very long. Messages are played in plain text to protect against "web bug" images and scripts.

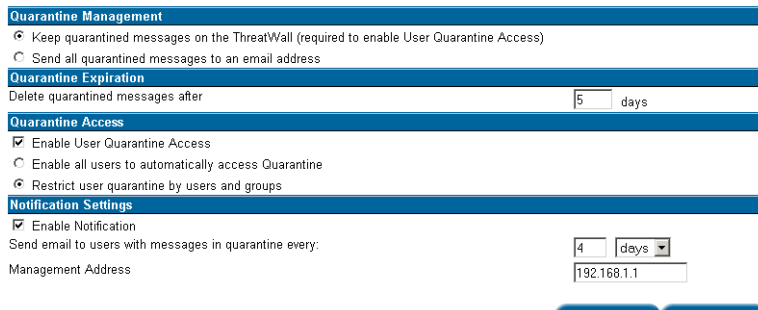
To exit the View Message page and return to the Quarantine interface, click *Close*.

Quarantine Options

The Quarantine Options allow you to adjust how long messages may stay in the Email Quarantine before being deleted automatically and control user access to the Email Quarantine.

To configure the Email Quarantine Options:

1. Click *Quarantine* from the *SpamFilter* menu.
2. Click the *Options* button.



The screenshot shows the 'Quarantine Management' configuration page. It is divided into four sections: 'Quarantine Management', 'Quarantine Expiration', 'Quarantine Access', and 'Notification Settings'. Under 'Quarantine Management', there are two radio buttons: 'Keep quarantined messages on the ThreatWall (required to enable User Quarantine Access)' (selected) and 'Send all quarantined messages to an email address'. Under 'Quarantine Expiration', there is a text input field with '5' and a dropdown menu set to 'days'. Under 'Quarantine Access', there are three radio buttons: 'Enable User Quarantine Access' (checked), 'Enable all users to automatically access Quarantine', and 'Restrict user quarantine by users and groups'. Under 'Notification Settings', there is a checked checkbox for 'Enable Notification', a text input field with '4' and a dropdown menu set to 'days', and a text input field for 'Management Address' containing '192.168.1.1'. At the bottom, there are 'Apply' and 'Cancel' buttons.

3. If you selected Quarantine as the action to perform for any of the spam levels, specify how to manage messages identified as spam:
 - **Keep quarantined messages on the ThreatWall** — Messages marked as spam are saved locally and can be viewed, deleted, and released using the Quarantine interface. This is the recommended option.

-
- **Send all quarantined messages to an email address** — Messages marked as spam are forwarded to the specified email address. The address must be valid and have sufficient disk space available.
4. Enter a Quarantine Expiration interval in days. Every night, the Email Quarantine will be analyzed. Any messages that are older than the number of days in the Quarantine Expiration setting will be deleted automatically.
 5. Select the *Enable User Quarantine Access* check box to enable users to access their messages in the User Email Quarantine.
 6. Select a password option for User Quarantine Access:
 - **Enable all users to automatically access Quarantine** — Choose this option if you want users to receive a password as part of the notification message. This automatic password does not need to be entered by a user; all the user needs to do is click on the link in the notification message. The password is different for each user and will change every time that a notification message is sent. This choice is good for an ThreatWall used as a mail relay.
 - **Restrict user quarantine by users and groups** — Choose this option if you have user accounts on the ThreatWall and you want the users to use their ThreatWall passwords. With this option, you control which users may access the Email Quarantine by using the User Quarantine Management group permission.
 7. Select the *Enable Notification* check box To have the ThreatWall send a Notification Message to every user with email in the Email Quarantine.
 8. Enter a number of hours or days for the *Send email to users with messages in quarantine every* option. This ranges from 1 hour to 30 days.
 9. Enter the *Management Address*. This is the IP address or host name that will be embedded in the notification message. When a user clicks on a link in the notification message, this is the address their web browser will connect to.
 10. Click *Apply* to save your changes or *Cancel* to abandon them.

Quarantine Notification Message

The notification message is an email sent to each user with mail in the Email Quarantine. This notification message contains a list of quarantined mail. Each line of the list has two links to click: *Deliver* and *Delete*.

When *Deliver* is clicked, a small web browser window should pop up with the results of the delivery action. The message should be delivered and if Bayesian Spam Filtering is enabled, the delivered message will be used as an example of a good email that should not be recognized as spam.

When *Delete* is clicked, a small browser window should pop up with the results. The message will be deleted and used as an example of bad spam email, if Bayesian Spam Filtering is enabled.

The notification message has one more link at the bottom of the message: View your quarantined email in more detail. This link opens a web browser window giving access to the User Email Quarantine.

User Email Quarantine

To access the User Email Quarantine, use one of the following:

- Click the *View your quarantined email in more detail* link in the Notification Message.
- Go to the URL: `https://<ip_address>/user/EmailQuarantine.php` with your browser.

If you have more than 2500 messages, you'll see a drop-down list of dates to view. Select the date of the messages you wish to view from the Show Messages For drop-down list. If you have less than 2500 messages in Quarantine, you will see the All option to view the entire Quarantine.

- To sort the messages, simply click the appropriate column heading (Hits, From, To, or Subject).
- To view a message, click the associated blue-highlighted text. The message appears in a separate window.
- To delete a message, select the message and click *Delete*.
- To release a message, select the message and click *Release*.





