



Simply better network security.™

**ThreatWall™**

**Content Filter**



# Copyright Notices

©eSoft, Inc. 2004. eSoft and ThreatWall are registered trademarks, and 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:

Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

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.

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."

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.

## ThreatWall Content Filter

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

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

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.

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/>).”

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

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/>).”

# Content Filter

## Quarantine Options

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

### SpamFilter: Content Quarantine: Options

[Need More Help?](#) 

#### Quarantine Expiration

*Quarantine Expiration changes made here will also affect Spam Quarantine Expiration settings.*

Number of days to retain  days

Maximum allowable disk space  GB *Currently 5.64 MB / 6.93 GB*

#### Notification Recipients

Deliver notification to address list  
*Enter one email address per line. A notification email will be delivered to each address.*

jbriggs@esoft.com  
zlynx@acm.org

Deliver notification to user groups with Content Filter permission

#### Quarantine Access

*The ThreatWall will automatically create passwords and include them in the notification email. This lets you click on links in the email to use the quarantine without needing to enter a password. For security, these passwords change after being used.*

Restrict access by notification email

Restrict access to user groups with Content Filter permission

#### Notification Interval

Send notification email every:  days

Send notification email immediately

#### Management Address

*The Management Address is the IP address or name of your ThreatWall. This is used for the links in the notification email. You may need to change the Management Address if your ThreatWall has different addresses on your LAN and the Internet.*

Management Address

Unlike the Spam Email Quarantine, the Content Quarantine does not notify email recipients that the message has been quarantined, or give them access to release and delete their own messages. Instead, it gives notification and access to a person or group of people who can review the filtered email and decide how to handle it.

To access the Quarantine Options, click the *Options* button in the [Content Quarantine](#) page.

## Quarantine Expiration

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.

## Notification Recipients

These options control who gets email messages notifying them about email in the Content Quarantine.

- Choose *Deliver notification to address list* and provide a list of email addresses to send notifications to. Enter one address per line.  
This is the only choice when you are using a Relay mail server.
- Choose *Deliver notification to user groups with Content Filter permission* if you would like to use the product group permissions to define the notification recipients.

## Quarantine Access

Select a password option:

- Choose *Restrict access by notification email* if you want 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 after being used.
- Choose *Restrict access to user groups with Content Filter permission* if you have user accounts on the product. With this option, you control which users may access the Content Quarantine by using the Content Filter Management group permission.

## Notification Interval

You may choose to have notification email delivered on a schedule, or immediately as filtered messages are received. If you choose to have a schedule, enter a number of hours or days for the *Send notification email every* option. This ranges from 1 hour to 30 days.

## Management Address

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.

After configuring the Quarantine Options, click *Apply* to save your changes or *Cancel* to abandon them.

# Enabling Email Content Filtering

The product can scan incoming or outgoing email messages for undesirable content. Simply specify the words or phrases you wish to filter, and the product identifies messages containing the keywords and redirects them to the [Content Filter Quarantine](#) for review.

Use content filtering to block messages containing offensive words or to keep messages containing proprietary information confidential.

To configure email content filtering:

1. Select *Content Filtering* from the *SpamFilter* menu.

## SpamFilter: Content Filtering

Need More Help? 

### Content Filtering Settings

- Enabled
- Filter incoming email.
- Filter outgoing email.

### Keywords to filter

*SpamFilter uses pattern-matching to find and filter messages containing words and phrases you specify. Please refer to the Help if you are unfamiliar with using regular expressions, as ambiguous entries can result in undesired filtering results.*

```
badword
foul
offensive
Super Product
```

Apply

Cancel

2. Select the *Enabled* check box.
3. Select the *Filter incoming email* check box to scan all incoming messages for the specified content.
4. Select the *Filter outgoing email* check box to scan all outgoing messages for the specified content.
5. Enter the *Keywords to filter*. Keywords can consist of individual words or multiple word phrases. Content filtering matches the words or phrases regardless of case (*aaa* matches *AAA*, *Aaa*, *aAa*, etc.). Each line of text in the text box represents a separate keyword. Press the *Enter* key on your keyboard to access a new text line.

A line in the text box can also contain "regular expressions." Regular expressions are a way to provide more powerful text matching abilities. Searching online can discover many resources for regular expressions, from tutorials, to user friendly programs to help write them.

Here are some basic elements of regular expressions and some examples to get you started:

test	<p>This is the simplest kind of regular expression. Each character matches a character in the text. This expression will match "test", but will not match "tester", "contest", "tes" or "best".</p> <p>Note: The Content Filter keyword entries are automatically modified to only match at the beginning and ending of words. The next example will</p>
------	--


ThreatWall Content Filter

	show you how to match partial words.
.test.*	A "dot", also known as a period or full stop, will match any character. The asterisk, or "star" will match any number of the previous character, or none at all. This expression will match "test", "tester" and "contest", as well as "The test was given and all students passed."
[0-9]{3}-[0-9]{2}-[0-9]{4}	This expression matches a U.S. Social Security number. The "[0-9]" is a character class. It will match anything from 0 to 9. The "{3}" means to match the previous character or character class 3 times. The dash following "{3}" is just a dash to match a dash. This example will match 111-222-3333, but not 1112223333.
[0-9]{3}.?[0-9]{2}.?[0-9]{4}	This expression is similar to the expression above, except it does not require a dash between parts of the U.S. Social Security number. The "." will match any character and the "?" matches the previous character zero or one time. This example will match 111-222-3333, 111.222.3333, 111*222*3333 and 1112223333
(Fred Joe Mary).*Herbert	The parenthesis start a group. The "vertical bar" character between the names Fred, Joe and Mary will match one of the choices. This expression will match any line that contains Fred, Joe or Mary, followed by Herbert on the same line.

6. Click *Apply* to save your settings, or *Cancel* to exit without saving.

## Managing the Content Filter Quarantine

Email messages that match a Content Filter keyword are saved here.

**SpamFilter: Content Quarantine** *Need More Help?* 

Show Messages For  2 / 2 messages

From	To	Subject	Filter
<input type="checkbox"/> Zan Lynx	zlynx	And again with the test	(?i)\btest\b
<input type="checkbox"/> baenringo Listmanager	zlynx	Another test	(?i)\btest\b

On Delete also remove similiar messages with selected  From  To  Subject,  All Days

To manage messages via the Content Filter Quarantine:

1. Select *Content Quarantine* from the *SpamFilter* menu.
2. To sort the messages, simply click the appropriate column heading (*From*, *To*, *Subject*, or *Keyword*).
3. To view a message, click the associated blue-highlighted text. The message in its entirety appears in a separate window. Inside the message, headers of interest, such as *To*, *From*, and *Subject* appear in bold. The keywords that were matched will be bold and highlighted in yellow.
4. To delete a message, select the message and click *Delete*.

To delete other messages in the Local 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 release a message to the intended recipient, select the message and click *Release*.
6. To delete all the messages, click *Purge*.
7. To configure Options about the Content Quarantine, such as Expiration and Notification, click *Options*.

## Quarantine Notification Message

The 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 will be delivered.

When *Delete* is clicked, a small browser window should pop up with the results. The message will be deleted.

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 [Content Quarantine](#).