



Simply better network security.™

ThreatWall™

AntiVirus SoftPak

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.

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/>).”

Configuring Anti-Virus Scanning

eSoft's Gateway Anti-Virus SoftPak provides virus protection for the product's users. If enabled, the Gateway Anti-Virus SoftPak works around the clock to ensure that virus infections are intercepted before they cause damage.

Every time the product sends or receives an email message, the message is automatically scanned for viruses.

If no viruses are detected, the email message is passed on to its destination as is.

If a virus is found, the infected component of the message is removed and a notice is appended in its place notifying the user that the message contained a virus. A notification message can also be sent to the original sender of the message, as well as the system administrator.

Note: To immediately remove all attachments of a specified type regardless of whether or not a virus is found, see [Configuring Attachment Stripping](#).

To configure Anti-Virus scanning:

1. Select the *Virus Settings* from the Gateway Anti-Virus menu

The screenshot shows the 'Gateway Anti-Virus: Virus Settings' configuration page. At the top left is the 'ThreatWall with ThreatWise Technology' logo. The page title is 'Gateway Anti-Virus: Virus Settings' with a 'Need More Help?' link and a question mark icon. The settings are organized into two sections: 'Scanning Options' and 'Notification Settings'. Under 'Scanning Options', there are three rows: 'Scan Incoming Mail' with a checked checkbox and 'Enabled' status, 'Scan Outgoing Mail' with an unchecked checkbox and 'Enabled' status, and 'Strip Attachments' with an unchecked checkbox and 'Enabled' status. To the right of these rows are three yellow boxes containing descriptions: 'Scan Incoming addresses', 'Scan for all addresses', and 'Accept the message but remove infected or blocked attachments. Otherwise reject the message. For optimal performance, it is recommended that you do not strip attachments.' Under 'Notification Settings', there are two rows: 'Send Notification Back to Sender' with an unchecked checkbox and 'Enabled' status, and 'Send Notification to System Administrator' with an unchecked checkbox and 'Enabled' status. At the bottom right, there are three buttons: 'Apply', 'Cancel', and 'Notices'.

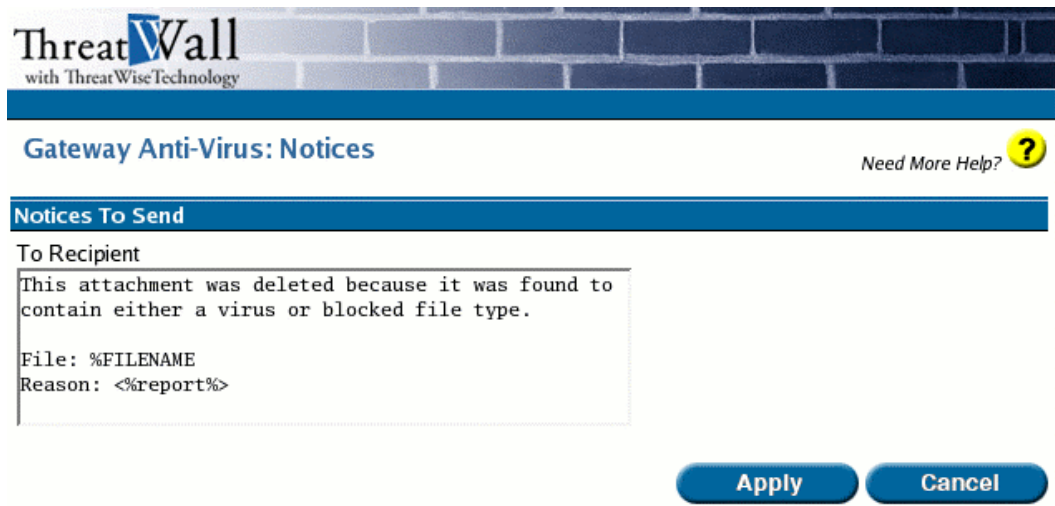
2. Select the *Scan Incoming Mail Enabled* check box to automatically scan all messages received by the product.
3. Select the *Scan Outgoing Mail Enabled* check box to automatically scan all messages sent by the product.
4. Select *Strip Attachments* to accept the message but remove infected or blocked attachments. Otherwise reject the message. For optimal performance, it is recommend that you do not strip attachments.
5. To send a notification message to the original sender of an email message containing a virus, select the *Send Notification Back to Sender Enabled* check box.
6. To send a notification message to the system administrator when an infected email message is discovered, select the *Send Notification to System Administrator Enabled* check box.

7. To customize the notice appended to an infected email message (and optionally the notification message sent to the sender of an infected message and/or the the product system administrators), click [Notices](#).
8. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Customizing Virus Notification Messages


To customize the notices appended to infected email messages:

1. Click *Notices* in the [Anti-Virus configuration](#) page.
2. Enter the warning notice to append to email messages containing a virus in the *To Recipient* text box. If you have attachment stripping enabled, this message is also appended to messages containing an attachment of a forbidden file type.



ThreatWall
with ThreatWiseTechnology

Gateway Anti-Virus: Notices

Need More Help? 

Notices To Send

To Recipient

This attachment was deleted because it was found to contain either a virus or blocked file type.

File: %FILENAME
Reason: <%report%>

Apply Cancel

Note: To include information obtained from the virus scan in the notification message, enter the variable `<%report%>` in the message text box.

3. If *Send Notification Back to Sender* is selected in the Anti-Virus configuration page, enter the warning notice to return to the original sender of an infected email message (and optionally to the sender of a message containing a forbidden file attachment) in the *To Sender* text box. To include the address of the sender in the notification message, enter the variable `<%sender%>` in the message text box.
4. If *Send Notification to System Administrator* is selected in the Anti-Virus configuration page, enter the warning notice to send to the system administrator when an infected email message (and optionally an email message containing a forbidden file attachment) is discovered in the *To System Administrator* text box. To include the address of the recipient in the notification message, enter the variable `<%recipients%>` in the message text box.
5. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Configuring Attachment Stripping

The attachment stripping feature included in the Anti-Virus SoftPak protects the product's users from viruses spread through email attachments.

If enabled, attachment stripping automatically scans all incoming and outgoing email messages for attachments. If an attachment of a forbidden type (specified by the administrator) is found, the attachment is immediately removed from the message, and a user defined warning notice is appended in its place.

Note: To only remove attachments that contain a virus, see [Configuring Anti-Virus Scanning](#).

To configure Attachment Stripping:

1. Click *Attachment Stripping* in the Anti-Virus menu.
2. Select the *Attachment Stripping Enabled* check box.

Gateway Anti-Virus: Attachment Blocking [Need More Help?](#) ?

Attachment Blocking Options

Attachment Blocking Enabled

File Extensions Settings

Email messages with the selected extensions will be blocked with notifications sent to the sending email server.

File Extensions to Block
Use ctrl-click to select multiple extensions.

- .dms
- .doc
- .dvi
- .dxr
- .eps
- .etx
- .exe

Additional File Extensions

.bat, .chm, .cmd, .com, .pif, .scr, .shs, .vbe, .vbs

To block messages with attachments having extension not shown above, enter them here in the following format: .xxx,.aaa,.xyz

Apply **Cancel**

3. To immediately strip attachments of a specified file type from incoming and outgoing email messages, select the *File Extensions to Strip*. Use the *Ctrl* key to select multiple file extensions.
4. To strip file extensions not listed, enter the *Additional File Extensions*. To specify more than one file extension, separate each extension with a comma (for example, *.xxx, .aaa, .bbb*).
5. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Updating Virus Signatures and Software

The virus signatures used by the product to detect infected messages are updated via the Internet with newly discovered viruses. The anti-virus software is also updated. The Updates page allows you to specify the frequency to check for updates, and to download the latest virus definitions and software immediately.

To set up virus signature and anti-virus software updates:

1. Click *Updates* in the Gateway-Anti-Virus menu.

The screenshot shows the 'Gateway Anti-Virus: Updates' configuration page. It features a title bar with a help icon and the text 'Need More Help?'. Below the title bar, there are two main sections: 'Virus Signatures' and 'Update Schedule'. The 'Virus Signatures' section contains a table with two rows of update information and an 'Update Now' button. The 'Update Schedule' section contains a label 'Check for updates every:' followed by a dropdown menu set to '30 Minutes' and 'Apply' and 'Cancel' buttons.

| Virus Signatures | |
|---|---------------------------------|
| Last Successful Update (<i>ThreatPak</i>) | Fri, 09 Jun 2006 16:20:04 -0600 |
| Last Successful Update (<i>Premium</i>) | Fri, 09 Jun 2006 16:10:08 -0600 |

Update Signatures Now Update Now

Update Schedule

Check for updates every: ▼

Apply Cancel

2. To immediately download the latest virus signatures and software, click *Update Now*.
3. Select how often to automatically check for updates from the drop-down list.
4. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Index

A

Anti-Virus

Configuring4

Notification Messages6

Updates8

Anti-Virus4, 6, 8

Attachment Stripping

Configuring7

Notification Messages 6

Attachment Stripping..... 6, 7

F

File Extensions..... 7

N

Notification Messages 6

U

Updating Virus Signatures 8