

ThreatWall Gateway Anti-Spyware SoftPak

Copyright Notices

©eSoft, Inc. 2004. eSoft and ThreatWall are registered trademarks, and ThreatWall, SoftPak and SoftPak Director are trademarks of eSoft, Inc. Sophos is a registered trademark of Sophos Plc. 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 SoftPak Gateway Anti-Spyware

eSoft's Gateway Anti-Spyware SoftPak protects your company network from spyware. It scans HTTP (websites and some types of file downloads) and FTP traffic (another type of file download) for spyware applications and stops them before they enter your company network. The SoftPak includes address blocking which prevents computers from reaching domains and addresses known to distribute spyware and determined to be used as sites where spyware reports data.

Configuring Gateway Anti-Spyware

Gateway Anti-Spyware works around the clock to ensure that virus infections and spyware applications are intercepted before they cause damage. If enabled, the Gateway Anti-Spyware proxy scans all incoming and outgoing HTTP and FTP traffic, intercepting harmful content and replacing it with warnings.

To enable Gateway Anti-Spyware:

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



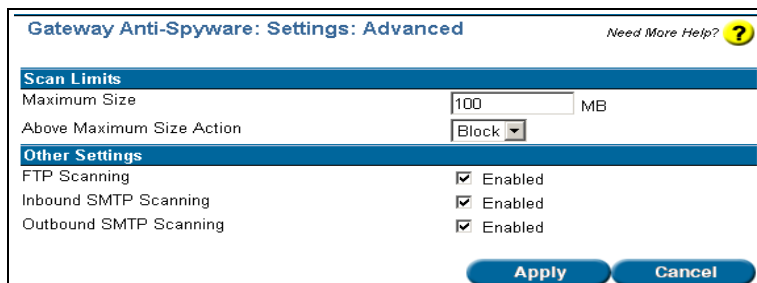
2. Check *Enabled*.
3. Select the interval of time to schedule automatic updates.
4. Click *Apply* to save setting or *Cancel* to exit without saving changes.

-
5. Click the *Update Now* button to immediately check for signature updates.

Configure Advanced Gateway Anti-Spyware Settings

To configure Advanced Gateway Anti-Spyware Settings.

1. Select Settings from the Gateway Anti-Spyware menu.
2. Click *Advanced* to load the Advanced form.



The screenshot shows a configuration window titled "Gateway Anti-Spyware: Settings: Advanced" with a "Need More Help?" link and a question mark icon. The window is divided into two sections: "Scan Limits" and "Other Settings".

Scan Limits	
Maximum Size	100 MB
Above Maximum Size Action	Block

Other Settings	
FTP Scanning	<input checked="" type="checkbox"/> Enabled
Inbound SMTP Scanning	<input checked="" type="checkbox"/> Enabled
Outbound SMTP Scanning	<input checked="" type="checkbox"/> Enabled

At the bottom of the window are two buttons: "Apply" and "Cancel".

3. Enter the Maximum Size of file you would like Gateway Anti-Spyware scan (enter 0 or "unlimited" to scan all files).
4. Select the action to perform when the file size exceeds the maximum set above.
 - a. Allow - Files larger than Maximum Size will not be scanned, but will be passed to requesting client.
 - b. Block - Files larger than Maximum Size will not be passed to the client.

Note Scanning large files can greatly impact system performance. Under normal circumstances it is not recommended to set Maximum Size above the default value of 100MB.

5. Check FTP Scanning to scan ftp traffic for spyware content (default).
6. Check In-bound Scanning to scan incoming email traffic for spyware content (default).
7. Check Out-bound Scanning to scan outgoing email traffic for spyware content (default).
8. Click *Apply* to save your size-limit settings or *Cancel* to return to the previous screen without making changes.

Configuring Threat Levels

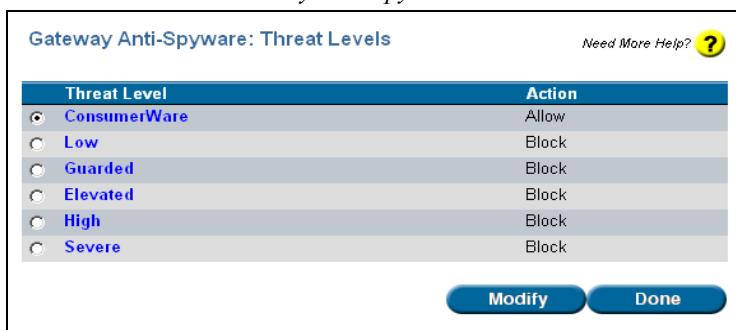
Gateway Anti-Spyware recognizes that some threats are more serious than others and it can handle each of six *Threat Levels* differently.

The different threat levels are:

1. *ConsumerWare* is a term that describes advertising or marketing supported software that meets and exceeds strict guidelines for Spyware. These useful applications, often given away for free, provide value to the end-user, pose no spyware risk, and are easily and completely removed through Add and Remove Programs.
2. *Low* severity indicates minor adware. There are no real tracking issues or system stability issues for low level threats.
3. *Guarded* severity indicates Browser Helper Objects (BHO) and adware. These are some minor aggregate tracking issues. None are over very minimal security concerns, such as causing lock-ups or crashes on isolated workstations or unique environments.
4. *Elevated* severity indicates a high level of Web and usage tracking for aggregate and other purposes. Security risks are increased and include the silent installation of unsafe code
5. *High* severity indicates the possibility of personally identifiable tracking and system compromising security concerns, including code that can crash or expose a browser or system to other risks. High severity spyware may also take advantage of current security exploits, if present.
6. *Severe* threats include keyloggers and remote administration tools. Severe spyware has a very big risk of personal information being captured and compromised, including passwords, credit card numbers and social security numbers.

To change the way a threat level is handled:

1. Select *Threat Levels* from the *Gateway Anti-Spyware* menu



2. Click the radio button next to the category you wish to modify and click *Modify*.

-
3. Select *Allow* or *Block* to apply that action to all of the entries in the category or *Custom* for fine-grained control over each entry in the category.

Gateway Anti-Spyware: Threat Levels: Modify Need More Help? ?

Threat Level Settings

Threat Level: **ConsumerWare**

Default Action: **Custom**

Threat	Categories	Action
AdminMagic1.0	Keylogger, Surveillance Software	Block
WhenU.Weathercast	Consumerware	Block
WhenU.SaveNow	Consumerware	Block
WTDMMMP	Adware	Block
WTVWebDriver	Adware	Block
VSN	Adware	Block
AdminMagic	Keylogger, Surveillance Software	Block
WhenU.WhenUSave	Consumerware	Block
WhenU.SideFinder	Consumerware	Block
WhenU.Searchbar	Consumerware	Block
WhenU.Browserbar	Consumerware	Block

Apply **Cancel**

Note Hover the mouse cursor over an entry in the *Threat* column for a description

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

Setting Up Custom Destination Rules

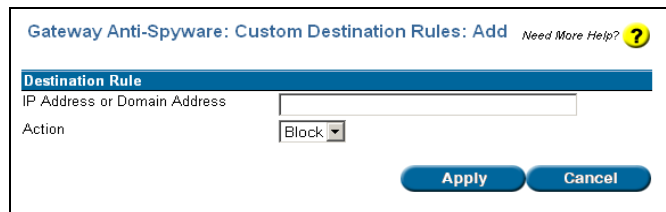
Gateway Anti-Spyware has the ability to block domains and IP addresses. There are already a large number of domains and IP addresses that are blocked because they have consistently carried dangerous content but if there are additional sites you'd like to block you may add them here. You may also use *Custom Destination Rules* to remove the block on predefined domains or IP addresses by entering the site and selecting *Allow*.

To define a custom domain or IP address:

-
1. Select *Custom Destination Rules* from the *Gateway Anti-Spyware* menu.



2. Click Add.



3. In the *IP Address or Domain* field, enter the IP address, domain or sub-domain that you want to control. *Custom Destination Rules* support domain matching. For example, creating a rule with the domain “baddomain.com” will control any URL ending in “baddomain.com”, such “mail.baddomain.com” and “www.baddomain.com”. *Custom Destination Rules* do not do what is called *sub-word matching* meaning that “badgers.com” will not block “brownbadgers.com.” For that, you must create a separate rule..
4. There are three options available for your custom rule:
 - c. *Block* - Blocks access to the site
 - d. *Allow* - Allow permits connections to the site and will scan content for spyware.
 - e. *Trust* - Trust permits connections to the site, but will **not** scan content for spyware.

Note *Custom Destination Rules* process *Allow* and *Trusted* rules first then *Block*. This ordering permits you to *Allow* sub-domain to pass while preventing other sub-domains to be blocked. For example, if you created a *Block* rule for “domain.com” and an *Allow* rule for “mail.domain.com”, access to “mail.domain.com” would be permitted while access to “domain.com” and “www.domain.com” would not.

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

To Delete a Custom Destination Rule

1. Select *Custom Destination Rules* from the *Gateway Anti-Spyware* menu.
2. Select the *Destination Rule* to be modified.
3. Click *Delete*.

Setting Up Custom Source Rules

Gateway Anti-Spyware by default protects every system connected to the LAN from Spyware by scanning HTTP, FTP and DNS. In rare cases there may be a need to allow certain hosts or even networks from being scanned by *ThreatWall*.

To exempt a host or network address from scanning:

1. Select *Custom Source Rules* from the *Gateway Anti-Spyware* menu.



2. Enter the IP address or network address you would like exempt from Gateway Anti-Spyware in the box.

Note You may enter multiple addresses in the box by putting each IP address or network address on a new line.

3. Click *Apply*


Creating Reports

Gateway Anti-Spyware reports contain information about clients on your network that have been protected from spyware and which servers on the Internet have been blocked from providing spyware to your clients. This information is useful to see the benefits to your network from using *Gateway Anti-Spyware*.

These reports can also be used to find clients that may have spyware installed. Spyware may attempt to report data it has collected, or download new advertisements or instructions. Spyware infected clients attempting to “call home” may show on the report as a client that is often blocked from connecting to a spyware site on the Internet.

To generate a report:

1. Select *Reports* from the *Reports and Logs* menu.
2. Select *Spyware* from the *Report Available* section.

Reports & Logs: Reports Need More Help? 

Reports Available	
Web Proxy	(No reports available)
<input type="radio"/> Mail	- Today's Report ▾
<input type="radio"/> SpamFilter	- Today's Report ▾
<input checked="" type="radio"/> Spyware	- Today's Report ▾

Report Detail

Summary

View **Cancel**

3. Click *View* to generate the report.