



Bypassing the DIA RBL



InstaGate and ThreatWall

COPYRIGHT NOTICES

©eSoft Inc. 2008. eSoft, InstaGate, 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 this 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 this 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 this 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/>).”

INTRODUCTION

eSoft's Web and Email ThreatPaks allow customers to receive real-time updates of existing and emerging threats that exist on the Internet. These real-time updates are provided by eSoft's Distributed Intelligence Architecture (DIA). One component is the DIA reputation and blacklist checks for email. These checks are performed by the Spam Filter portion of the Email ThreatPak. DIA provides valuable feedback and protection against email threats based on the sending mail servers IP address. However sometimes a customer may still want to allow email from a DIA blacklisted IP address. This article gives a brief overview on how to allow DIA blacklisted IP addresses through the email server on an eSoft device.

PART ONE –FINDING A DIA BLACKLISTED IP ADDRESS

In order to allow an IP address that has been blacklisted through the mail server on an eSoft product, it is necessary to white list that IP address. The first step in this process is to find the IP address that is blacklisted by using the ThreatMonitor or email server logs.

The easiest way to find a DIA blacklisted IP address is to search in the ThreatMonitor. Within the ThreatMonitor, click on the *Email* tab and then click the *Details* link under *Recent Activity*. On the Recent Activity page, enter the email address of the sender and click *Refresh*. This will display the IP address of the sender, which is the IP address that needs to be entered into the Spam Filter Whitelist to bypass the DIA Reject block.

The screenshot shows the ThreatMonitor interface with the 'Email' tab selected. The 'Recent Activity' section displays a table with the following data:

Time	Type	Message ID	IP Address	From	To	Score	Size	Action
April 14, 2008 1:34:39pm	DIA Rejected		80.98.213.165	otimxm@nel.it	-	0	0 B	White Black

The search term 'otimxm' in the search box and the IP address '80.98.213.165' in the table are circled in red. The 'Type' column also shows 'DIA Rejected' circled in red. The 'Total Results: 1' is shown at the bottom left, and a 'Done' button is at the bottom right.

The other method of obtaining the IP address being blocked is through the email server logs. In order to view the email logs click on *Support & Diagnostics* then *System Logs* in the InstaGate user interface. On ThreatWall, click *Reports & Logs*, then *System Logs*. From the drop down list make sure *Email Server/Relay* is selected. To open the log, click on the blue “exim_mainlog” text for the desired day.

Select	Log	Date	Size
<input checked="" type="radio"/>	exim_mainlog	04/14/2008	45.06 kB
<input type="radio"/>	exim_mainlog.1	04/13/2008	70.69 kB
<input type="radio"/>	exim_mainlog.2	04/12/2008	66.72 kB
<input type="radio"/>	exim_mainlog.3	04/11/2008	66.11 kB
<input type="radio"/>	exim_mainlog.4	04/11/2008	70.95 kB
<input type="radio"/>	exim_mainlog.5	04/09/2008	72.26 kB
<input type="radio"/>	exim_mainlog.6	04/08/2008	65.66 kB

Once the log has opened it is easiest to use the keyboard shortcut CTRL-F to open a Find dialog box. In this dialog box enter the email address of the sender. In the log example below ‘fake@bogus.net’ would have been entered into the search field.

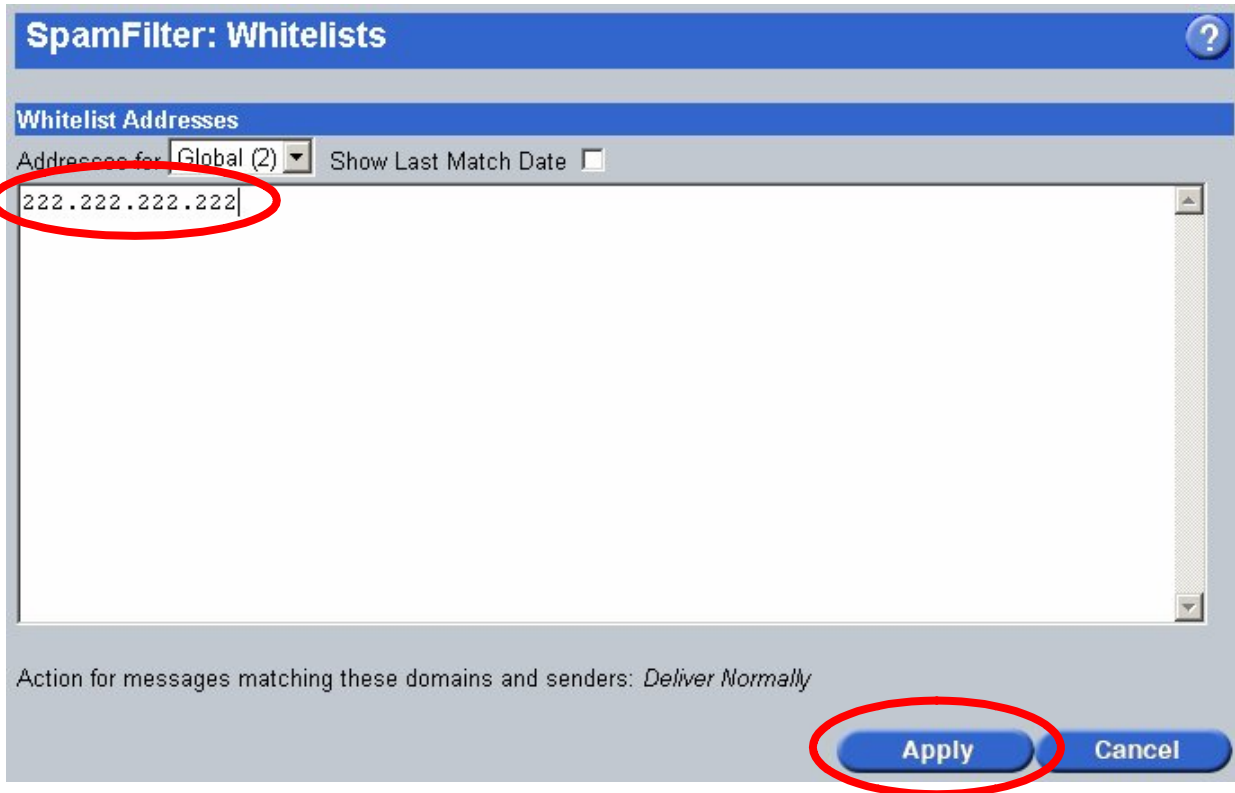
```
2008-04-14 02:28:09 H=([222.222.222.222]) [222.222.222.222]
F=<fake@bogus.net> rejected RCPT <support@esoft.com>: DIA Real-Time Black Listed
```

The log entry above shows a source IP address of 222.222.222.222. This is the IP address that would be needed to bypass the DIA Blacklist.

PART TWO –ALLOWING A DIA BLACKLISTED IP ADDRESS

In order to allow an email address through the email server, the sending IP address must be added to the white list. Adding an email address or domain will not bypass the DIA blacklist.

To white list an IP, click on *Spam Filter* then *Whitelists*. Once the page loads, simply enter the IP address found in the ThreatMonitor or email logs. Click *Apply* to save your changes.



Once applied this change will allow email from this IP address through the mail server. Please keep in mind that by adding this IP address you are bypassing all spam and malware checks for any email from this IP address.

TROUBLESHOOTING

If, after adding the IP address to the white list, emails are still being blocked by DIA's real time blacklist, verify the senders IP address. Some domains have multiple mail servers and therefore emails may be sent from multiple IP addresses.

eSoft's DIA server only hold records for three days. If an IP address sends zero spam three days in a row that IP is automatically removed from DIA's real-time blacklist. It should also be noted, only emails that receive a SpamFilter score will be reported to DIA. Whitelist and Blacklist entries are never scanned by SpamFilter and are therefore not reported to DIA.

For other issues not covered within this document please contact eSoft Technical Support at 877-754-2986 or online at <http://support.esoft.com>.