



Protecting the AXIGEN Messaging Solution with TrendMicro

GECAD Technologies

10A Dimitrie Pompei Blvd., BUCHAREST 2, ROMANIA

Tel.: +40 21 303 20 80

+40 21 303 20 81

<http://www.axigen.com>

Last modified: 1/29/2007

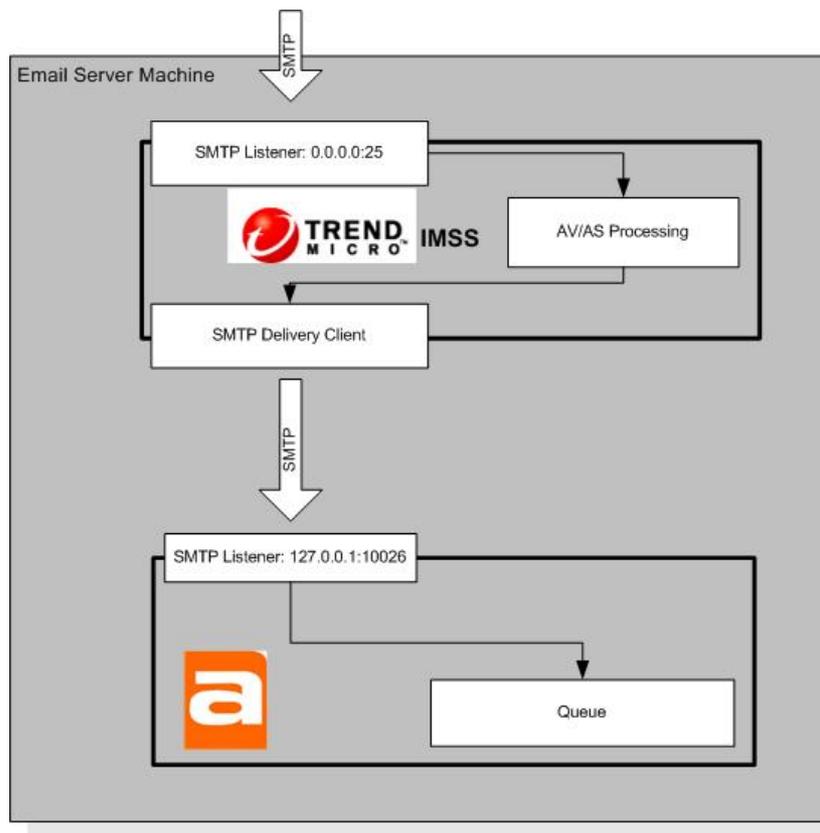
Introduction

This article focuses on the integration of the AXIGEN Mail Server with TrendMicro's Interscan Messaging Security Suite for the purpose of obtaining a cleaner email traffic, virus-safe and without spam. We shall describe how both components must be set-up to ensure proper functionality. In the last section of the article, we will also describe the IMSS tweaking fine tuning to ensure a better performance.

Overview

The integration of AXIGEN with IMSS is performed by replacing the AXIGEN listener on port 25 with IMSS's SMTP listener. IMSS delivers the email, after processing it, to AXIGEN's SMTP listener on a different port (in our example, tcp/10026).

The figure below depicts the message flow through IMSS and AXIGEN.



Email messages pass, from SMTP, through IMSS's filtering engine for antivirus and antispam detection, before being delivered to the AXIGEN Mail Server.



Prerequisites

Software&Licenses

- AXIGEN Mail Server v1.2 license - for the number of mailboxes you would like to host;
- TrendMicro Interscan Messaging Security Suite (IMSS) v5.7 - for the number of mailboxes you would like to protect; it should be the same number of mailboxes as defined in AXIGEN.
- Common available platforms: Linux, the following distributions:
 - Redhat Enterprise Linux 3
 - SuSE Linux 9.0

The AXIGEN Mail Server must be installed on the machine and configured as per your needs. For information on performing the AXIGEN installation, please consult the product manual.

Follow the installation procedure from the manual for setting up IMSS. At the end, check that IMSS is working properly by running a telnet on port 10025 on the local machine. The connection should be established and then be closed immediately (due to the fact that IMSS cannot yet connect to the mail server). Wait half a minute before performing this test so that IMSS can properly startup its services.

```
[root@localhost ~]# telnet localhost 10025
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
421 Internal configuration error
Connection closed by foreign host.
```

If the connection is rejected before being established or a different error is reported, please consult the troubleshooting section of the IMSS manual.

Interconnecting AXIGEN and IMSS

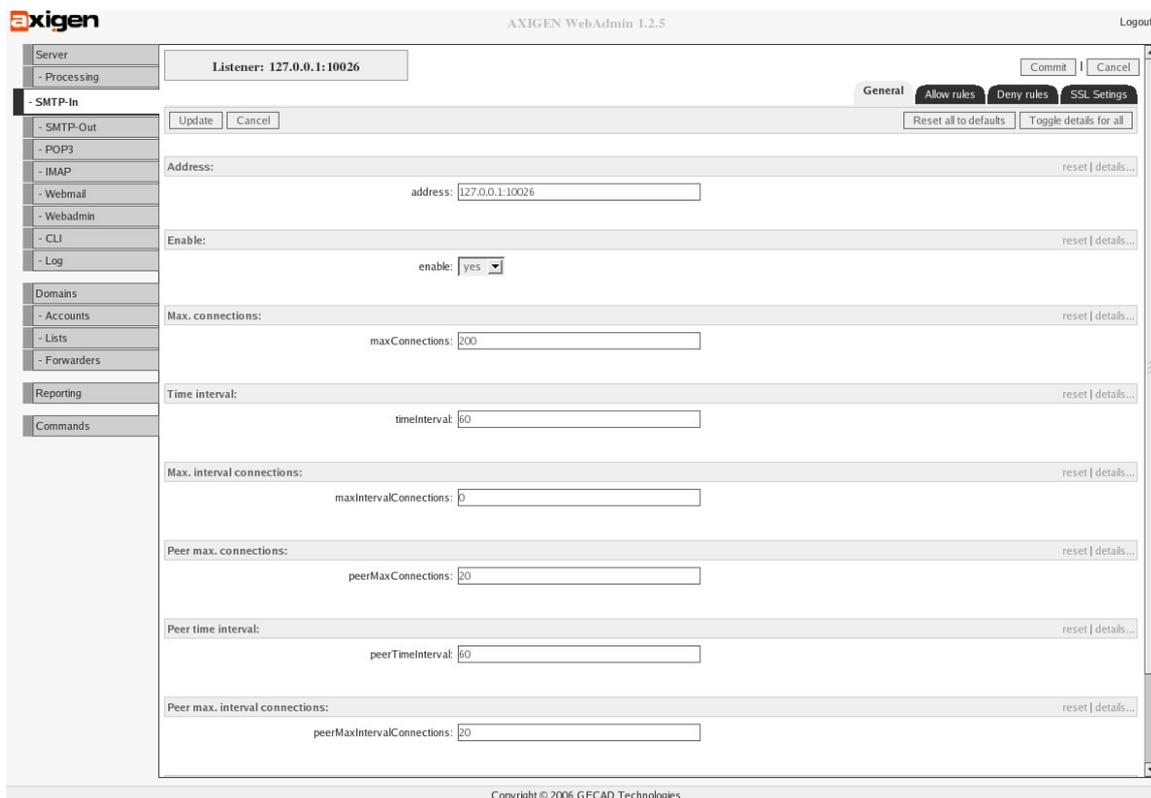
Now that both AXIGEN and IMSS are installed, some configuration steps must be performed to ensure the optimal email flow.

1. Reconfigure AXIGEN's SMTP listener.

- Login to the web administration interface (typically located at <http://localhost:9000>, if you're running the browser from the same machine);
- Go to the 'SMTP-In' section;
- Click on the 'Listeners' property tab;
- Configure one listener with '*address*': "127.0.0.1:10026". Make sure no other listeners exist;
- Set the '*enable*' option to 'yes';
- Set the '*maxIntervalConnections*' parameter to '0' (Unlimited);
- Set the '*peerMaxConnections*' parameter to '200';
- Set the '*peerMaxIntervalConnections*' parameter to '0' (Unlimited);
- Click 'Update', the 'Commit';
- Make sure you save the configuration by going to the 'Commands' administration section and clicking 'Save Config'.



Below is a screenshot of the listener configuration, as described above:



2. Reconfigure IMSS's SMTP listener

- Using a text editor, open the '/opt/trend/imss/config/imss.ini' file (the location may differ if when you have installed IMSS you have chosen a different directory);
- In the '[smtp]' section, comment-out (prefix with hash '#') the 'smtp_allow_client_ip' configuration option. This will disable IP address verification for inbound SMTP;
- Locate the 'proxy_service=SMTP_SERVICE' line. Modify the 'proxy_port' below it to '25' (the default value is 10025). Typically, this parameter is located in the '[socket1]' section of the configuration file;
- Locate the 'proxy_smtp_server_ip' configuration option and modify it from '127.0.0.1' (the default) to '0.0.0.0'. This will instruct IMSS to listen on all server IP addresses;
- In the '[pop3]' section, set the 'pop3_enable_proxy' and 'pop3_virus_scan' options to 'no'. This will disable the POP3 scanning.

3. Restart the IMSS service by running:

```
# /etc/init.d/S99ISIMSS restart
```



4. Verify the connection

- Run a telnet on the local machine, on port 25. The connection should open, and two SMTP banners must appear: one from the IMSS and the other from AXIGEN:

```
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
220-TrendMicro IMSS SMTP proxy
220 localhost.localdomain Axigen SMTP ready
```

- Enter the 'quit' command in order to close the connection

5. Send a mail through

- Using an SMTP email client (Outlook, Mozilla) already configured to use the AXIGEN Mail Server, send an email to a valid recipient;
- The email must reach the destination mailbox and it must contain the IMSS headers (e.g. X-imss-version).

Configuring IMSS policies

This section describes the behavior of your newly configured solution when a virus/spam is detected. At this point the AXIGEN integration with IMSS is operational.

IMSS relies on a series of hierarchical policies that handle, based on the originator or recipients' email addresses, the decisions that are to be taken.

Using a web browser, go to the following URL:

https://<server_ip>:8445/IMSS.html

Replace <server_ip> with your actual email server's IP address. Login (the default is no password) by clicking on Enter.

1. Configure notifications

- Go to the 'Configuration' section;
- Open the 'Event Monitoring' subsection and click on 'Notification Settings';
- Change the administrator's email address to a valid mailbox on the AXIGEN Mail Server;
- Save the configuration, then click on the red 'Apply now' button.

2. Policies

- The policies are located in the 'Policy Manager' section of the IMSS web administration interface;
- Please refer to IMSS manual for information on how to configure the policies.



3. Actions

- When a policy's filter is triggered by the content of an email message, a specific set of actions is performed;
- The administrator can choose out of:
 - Delivery options (original message, modified message)
 - Notifications
 - Archiving
- For information about configuring actions, please refer to the IMSS manual.

Tweaking

1. **In the default configuration, IMSS does not advertise the AUTH ESMTX extension.** In order to allow the SMTP clients to use the SMTP authentication, the IMSS configuration must be altered.
 - Using a text editor, open the '/opt/trend/imss/config/imss.ini' file (the location may differ if when having installed IMSS you have chosen a different directory);
 - Locate the '[smtp]' section and, in it, the 'supported_esmtx_cmds' option;
 - At the end of the line, add the 'AUTH' string, separating it with a comma:
`supported_esmtx_cmds=PIPELINING,SIZE,VERFY,ETRN,XVERP,8BITMIME,AUTH`
 - Restart the IMSS service by running:
`# /etc/init.d/S99ISIMSS restart`
2. **Normally, since outside SMTP clients no longer connect directly to AXIGEN, connection cannot be directly managed. However, the IMSS SMTP connection manager immediately closes the connection if AXIGEN takes this action.** This way, system administrators can manage the maximum number of simultaneous connections and the connection rate directly from AXIGEN.
 - Login to the AXIGEN web administration interface (typically <http://localhost:9000>);
 - Go to the 'SMTP-in' section, then to the 'Listeners' tab;
 - Edit the listener;
 - Configure, as desired, the following parameters:
 - 'maxConnections'
 - 'maxIntervalConnections'
 - 'timeInterval'
 - Do not modify the peer-related options since they no longer make sense in this set-up.

Caveats

Although the configuration guidelines provided in this article cover the needs of most users, there are some aspects that one must keep in mind when using the Axige/IMSS combination:

1. IMSS does not support TLS. Even though AXIGEN advertises the STARTTLS extension, the IMSS SMTP listener will not advertise, nor support it.
2. Emails going in the AXIGEN mail server through channels other than SMTP (e.g. webmail) will not pass through IMSS, thus will not be scanned for viruses or spam.



3. Since all SMTP connections AXIGEN receives are from IMSS, hence originate from IP 127.0.0.1, configuring IP-based rules in the 'Clients' section of the SMTP-In module no longer makes sense.
4. As previously said, all the SMTP connections received by AXIGEN originate from the 127.0.0.1 IP. When running the AXIGEN Configuration Wizard, the following code will be added in the SMTP Policy File, in the onEhlo event definition:

```
if (...iprange (remoteSmtIp, "127.0.0.0/255.0.0.0")...) {  
    set(remoteDelivery, "all");  
}
```

This means that all connections from 127.0.0.1 will allow open relaying which is a crucial security flaw. To correct it, you should remove the specified code lines.

5. For the same reason as described above, setting the 'peerMaxIntervalConnections' parameter for the SMTP-in listener to a value different than 0 is of no use. Use the 'maxIntervalConnections' parameter instead.
6. IMSS does not support the BINARYMIME ESMTP extension therefore, even though AXIGEN advertises it, IMSS will not.

AXIGEN Copyright © 2006 GeCAD Technologies SRL [AXIGEN]. All rights reserved. This material or parts of the information contained herein cannot be reproduced in any form or by any means without the prior written permission of AXIGEN. The product and the documentation that comes with the product are protected by AXIGEN copyright. AXIGEN reserves the right to revise and modify its products and documentation according to its own necessities, as well as this document content. This material describes a status, as it was in the moment this material was written and may not correctly describe the latest developments. For this reason, we recommend you to periodically check our website, <http://www.AXIGEN.com/>.

AXIGEN cannot be held responsible for any special, collateral or accidental damages, related in any way to the use of this document. AXIGEN does not guarantee either implicitly or explicitly the suitability of this material for your specific needs. This material is provided on an "as-is" basis.

