



Integrating the AXIGEN Messaging Solution with AMAVIS

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: 3/13/2007

Introduction

This document describes the steps required to perform an integration of the AXIGEN Mail Server with Amavis, in order to insure antivirus protection and functionality. Amavis is a generic interface used to connect a mail server to a number of antivirus products.

Prerequisites

Operating systems

The integration was successfully tested on the following operating systems:

- Fedora Core 5
- Mandriva 2006
- Debian 3.1
- Ubuntu Server 6.06

Amavis

Amavisd-new version 2.4.2 must be used in this setup.

Antivirus products

One of the following antivirus products can be used:

- BitDefender
- Kaspersky Kav4Mailservers-linux

<p>Note: Though tests were only performed with the products listed above, the integration should function with any of the antivirus products Amavis supports (Sophos, DrWeb, F-Secure, Symantec AV engine, F-PROT, Nod32, etc).</p>
--

Setting-up Amavis

For the AXIGEN Mail Server and the desired antivirus product, please follow the installation procedure described in the user's manual.

Dependencies

Amavisd-new requires the following software packages in order to run properly:

- PERL v5.8.2 or newer
- PERL modules
 - Archive::Tar
 - Archive::Zip ver. 1.14 or newer
 - Compress::Zlib ver. 1.35 or newer
 - Convert::TNEF
 - Convert::UUlib ver. 1.05 or newer
 - MIME::Base64
 - MIME::Parser ver. 5.420 or newer
 - Mail::Internet ver. 1.58 or newer
 - Net::Server ver. 0.88 or newer



- o Net::SMTP ver. 1.16 or newer
- o Digest::MD5 ver. 2.22 or newer
- o IO::Stringy
- o Time::HiRes ver. 1.49 or newer
- o Unix::Syslog
- o BerkeleyDB ver. 4.2 or newer

If you have all the dependencies properly installed, Amavis will run correctly.

Below you will find a list of distribution-specific instructions on how to make sure all the dependencies are installed. Make sure you have the specific package management tools (yum, apt-get, etc) installed and properly configured before continuing.

- Fedora Core 5

Run the following commands:

```
# yum -y install amavisd-new
# yum -y remove amavisd-new
```

- Mandriva 2006

Run the following commands:

```
# urpmi amavisd-new
# rpme -e amavisd-new
```

- Debian 3.1

Run the following commands:

```
# apt-get update
# apt-get -y install amavisd-new
# apt-get --purge -y remove amavisd-new
```

Download the 1.42 version of the Compress::Zlib perl module (from [this link](#)), uninstall the old version and install the new one:

```
# dpkg -r --force-all libcompress-zlib-perl
# dpkg -i --force-all libcompress-zlib-perl_1.42-1_i386.deb
```

Note: Forcing the uninstall steps and the installation of a package is not a standard procedure and may result in dependency problems. Please use with care.

- Ubuntu Server 6.06

Run the following commands:

```
# apt-get update
# apt-get install amavisd-new
# apt-get remove amavisd-new
```

Download the 5.420 version of MIME-Tools perl module ([from this link](#)) and install it:

```
# dpkg -i libmime-perl_5.420-0.1_all.deb
```

Installation

All the installation process must be performed while logged-in as the 'root' user.

1. Download and unpack amavis:

- Create temporary directory:

```
# mkdir /tmp/amavis/
```



- Go to the temporary directory
`# cd /tmp/amavis/`
- Download amavisd-new version 2.4.2:
`# wget http://www.ijs.si/software/amavisd/amavisd-new-2.4.2.tar.gz`
- Unpack the archive:
`# tar -zxf amavisd-new-2.4.2.tar.gz`

2. Set-up the Amavis environment

- Create a working dir for Amavis:
`# mkdir /var/amavis /var/amavis/tmp /var/amavis/var /var/amavis/home`
- Set permission for the Amavis working dirs:
`# chown -R axigen:axigen /var/amavis`
`# chmod -R 750 /var/amavis`
- Copy the amavisd binary to its new location:
`# cp /tmp/amavis/amavisd-new-2.4.2/amavisd /usr/local/sbin/`
- Set the ownership and permissions for /amavisd:
`# chown root /usr/local/sbin/amavisd`
`# chmod 755 /usr/local/sbin/amavisd`
- Copy the default config file to: /etc/amavisd.conf:
`# cp /tmp/amavis/amavisd-new-2.4.2/amavisd.conf /etc/amavisd.conf`
- Set the ownership and permissions for /etc/amavisd.conf:
`# chown root /etc/amavisd.conf`
`# chmod 644 /etc/amavisd.conf`
- Create the quarantine folder: /var/virusmails
`# mkdir /var/virusmails`
- Set the ownership and permissions for the quarantine directory:
`# chown axigen:axigen /var/virusmails`
`# chmod 750 /var/virusmails`
- Copy the amavis package contents to /usr/share/
`# mkdir /usr/share/`
`# cp -Rp /tmp/amavis/amavisd-new-2.4.2 /usr/share/`

3. Modify the amavis configuration

Locate the following variables and modify them as below:

```
$daemon_user = 'axigen';  
$daemon_group = 'axigen';  
$TEMPBASE = "/var/opt/axigen/queue";  
$enable_db = 0;  
$enable_global_cache = 0;  
$final_virus_destiny = D_DISCARD;
```



```
$final_banned_destiny = D_DISCARD;  
$final_spam_destiny = D_DISCARD;  
$final_bad_header_destiny = D_PASS;
```

Please remember to uncomment (remove the leading hash '#') the 'final*_destiny' configuration variables before setting them to the values specified above.

Note: the 'D_BOUNCE' option is not supported by Axigen.

Locate the following configuration variable and enable it by removing the leading hash (#):

```
@bypass_spam_checks_maps = (1);
```

Locate the following configuration variable and enable it by removing the leading hash (#):

```
$myhostname = 'host.example.com';
```

Replace 'host.example.com' with your specific hostname.

Under the line:

```
$policy_bank{'AM.PDP-SOCK'} = { protocol=>'AM.PDP' };
```

insert:

```
$protocol='AM.PDP';
```

Under the line:

```
$virus_admin = "virusalert@$mydomain";
```

insert:

```
undef $virus_admin;
```

Antivirus configuration

In order to install the desired antivirus, the procedure described in the user's manual should be followed.

For the Kaspersky Kav4Mailservers, the following additional steps should be taken:

- Change the ownership on the Kaspersky directory

```
# chown -R axigen:axigen /opt/kav/
```
- In the Amavis configuration file (/etc/amavisd.conf) modify the path to Kav4Mailservers
 - Look for the 'kav4mailservers' section
 - Change '/opt/kav/bin/aveclient' to
'/opt/kav/5.5/kav4mailservers/bin/aveclient'

AXIGEN configuration

A filter must be defined in order to instruct AXIGEN to send email messages to Amavis for scanning.

- Log into Webadmin using the "admin" account;
- Go to the 'Server' section;

1. Define the Amavis filter

- Click on the "Filters" page.



- Select the "AV/AS Filters" sub-page.
- Click the "Add new filter" button.
- Fill-in the following filter parameters:
`name: amavis`
`address: inet://127.0.0.1:10024`
`protocolFile: /var/opt/axigen/filters/amavis.afsl`
`idleTimeout: 60`
`actionOnMatch: reject`
`maxConnections: 10`
- Click the "Add" button.
- Click the "Commit" button.

2. Activate the Amavis filter

- Select the "Filters" tab again and
- Click the "Add new filter"
- Fill-in the following parameters:
`priority: 100 or below,`
`filter type: "Socket"`
`filter name: "Amavis"`
`apply on relay: "no".`
- Click the "Add" button
- Click the "Commit" button

3. Save configuration changes

- Go to the "Commands" section
- Click the "Save config" button.

Starting-up

Antivirus

Follow the procedure in the specific antivirus manual to start the service. Normally, the antivirus is automatically started after installation.

Amavis

Run the following command:

```
# amavisd start
```

AXIGEN

The AXIGEN Mail Server is started with the command:

```
# /etc/init.d/axigen start
```

Testing the solution

1. Create a test user (or use an existing one) and logon using the Webmail interface. Alternatively you can use an email client such as Outlook or Thunderbird.
2. Compose an e-mail and send it to the inbox of the same user.
3. Compose another email and attach the EICAR test file (download from [here](#)).



4. You should not receive the second e-mail. The EICAR test file is a 'fake virus' created as a general test to see if your antivirus software is working correctly. This is NOT a live virus.

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.

