

ESET Mail Security & Zarafa 7 infrastructure Integration

Whitepaper

20-2-2012 -- version 2.0

Donny Maasland

donny@nod32.nl

Verified

10-2-2012

Remon van Gijn, Zarafa QA

r.vangijn@zarafa.com



we protect your digital worlds

Table of contents

Introduction and scope	3
Download and install	3
Setting up Zarafa integration	5
Web interface	6
Setting up antispam	7

Introduction and scope

ESET Mail Security for Linux/BSD/Solaris offers lightweight yet powerful protection for heavy-duty mail servers based on the Unix platform. This product features ThreatSense®, the industry's most accurate proactive technology for detecting all types of malware. The Zarafa 7 collaboration platform offers mail, calendaring, tasks and notes sharing to its users combined with online meeting options. Zarafa uses an open architecture model for its MTA and distributions allowing a fine-tuned integration with various MTA products like Postfix, sendmail and Exim that can be complimented with other elements like **ESET Mail Security for Linux**.

This document describes the ESET setup on a 64 bit system setup using Zarafa 7 with Postfix and ESET Mail Security for Linux as front end SMTP server, resulting in proper detection and movement of malicious mail to Zarafa mail spam folders for recipients.

ESET Mail Security for Linux/BSD/Solaris: <http://www.eset.com/us/business/products/mail-linux/>
Zarafa 7: <http://www.zarafa.com/>

A business trial license for ESET Mail Security can be acquired via this URL:

<http://www.nod32.nl/freetrial/> (Note: The page is in dutch, but will be translated soon).

A free community edition of Zarafa is enough to perform the functionality described in this whitepaper

Download and install

*Note: please keep your license details ready. You will need them during the install and configuration of ESET Mail Security

Step one is to download the appropriate installation package for your system. All versions can be found [here](#). In this example, we are running Ubuntu Server 10.04.3 LTS, so we will be using esets.amd64.deb.bin:

```
wget http://download.eset.com/download/unix/esets.amd64.deb.bin  
--user=<eav number> --password=<password>
```

(Replace <eav number> with your license username and <password> with your license password)

After the installer finished downloading, run the following, and accept the license agreement:

```
sh esets.amd64.deb.bin
```

Because this is a 64 bit system, the ia32-libs are also needed:

```
aptitude install ia32-libs
```

Install the software:

```
dpkg -i esets-4.0.5.amd64.deb
```

Copy the "nod32.lic" file that came with your license (attached to the license email inside "nod32.zip") to the machine running ESET Mail Security, and import the license file into the product:

```
/opt/eset/esets/sbin/esets_lic --import nod32.lic
```

Edit the ESET configuration file (/etc/opt/eset/esets/esets.cfg) to enable the web interface (optional), and enter the license details.

Web interface:

```
[wwwi]
# Settings for ESETS Web Interface configuration module

# agent_enabled = yes/no
# Enables operation of the esets_wwwi.
agent_enabled = yes

# listen_addr = "address"
# Address (IP or name) where esets_wwwi listens for HTTPS client connections.
# If set to 0.0.0.0 then esets_wwwi listens on all available network interfaces.
listen_addr = "0.0.0.0"

# listen_port = port
# TCP port where esets_wwwi listens for HTTPS client connections.
# You may have to open this port in your firewall.
listen_port = 3537

# username and password needed for accessing the interface (required)
username = "username"
password = "password"
```

Licence details:

```
#
# ESETS Update options.
#
# av_update_server = "server"
# ESET server used to update ESETS anti-virus modules,
# empty string means - autoselect.
#av_update_server = ""

# av_update_username = "username"
# Username used in authentication against ESET server.
av_update_username = "EAV-xxxxxxx"

# av_update_password = "password"
# Password used in authentication against ESET server.
av_update_password = "password"
```

Update the product to ensure the license details are correct, and install the latest modules:

```
/opt/eset/esets/sbin/esets_update --verbose
```

Start the `esets_daemon`

```
/etc/init.d/esets start
```

Setting up Zimbra integration

There are multiple ways to integrate EMSL into Zimbra, depending on your configuration. In this example Zimbra is configured to use LMTP so the EMSL SMTP agent has to be used. The EMSL SMTP agent receives email on port 25, and relays it to your MTA on another port. To change the listening port on postfix, change the following in `/etc/postfix/master.cf`:

```
smtp inet n - n - - smtpd

to

2525 inet n - n - - smtpd
```

Reload the postfix configuration:

```
/etc/init.d/postfix restart
```

Enable the EMSL SMTP agent and setup the relay by editing the configuration

`/etc/opt/eset/esets/esets.cfg`:

```
[smtp]
# Settings for ESETS SMTP filter module.

# agent_enabled = yes/no
# Enables/disables operation of the esets_smtp.
agent_enabled = yes

# listen_addr = "address"
# Address (IP or name) where esets_smtp listens for SMTP client connections.
# If set to 0.0.0.0 then esets_smtp listens on all available network interfaces.
listen_addr = "0.0.0.0"

# listen_port = port
# TCP port where esets_smtp listens for SMTP client connections.
listen_port = 25

# server_addr = "address"
# Address (IP or name) of the SMTP server where esets_smtp connects to.
server_addr = "localhost"

# server_port = port
# TCP port of the SMTP server where esets_smtp connects to.
server_port = 2525
```

Reload the `esets_daemon`

```
/etc/init.d/esets restart
```

ESET Mail Security for Linux is now integrated with Zarafa, and will check all incoming email for malware. The result will be written to the e-mail headers and the message body. This behaviour can be configured through the web interface or the configuration file:

```
X-Virus-Scanner: This message was checked by ESET Mail Security
for Linux/BSD. For more information on ESET Mail Security,
please, visit our website: http://www.eset.com/.
```

```
x-esetresult: clean, is OK
x-esetid: 37BB632351150D6B62F83F
```

Information from ESET Mail Security, version of virus signature database 6853 (20120203)

The message was checked by ESET Mail Security.
<http://www.eset.com>

Web interface

If the WWWI has been enabled in the esets.cfg file, the web interface can be reached at <https://<ip>:<port>/>. Note that the esets.cfg file must have credentials set for the web interface to work:

ESET SERVER SECURITY
FOR LINUX/BSD/SOLARIS

Login

Username:

Password:

All settings regarding ESET Mail Security for Linux can be configured through the web interface. Several things are managed, i.e. licenses, the quarantine (if configured) and statistics:

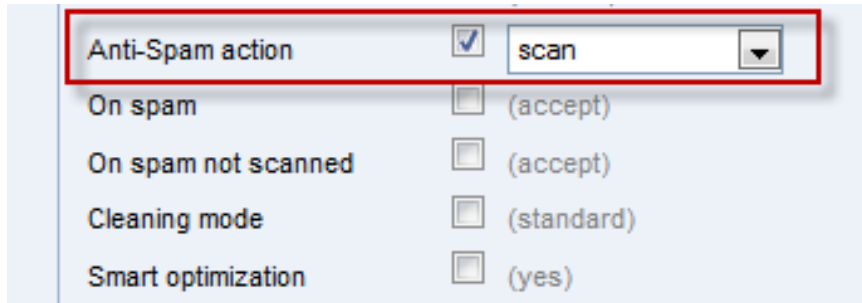
Statistics

Virus scan statistics

	Mail	Mail part	Total
Scanned:	26	-	26
Error:	-	-	-
Infected:	-	-	-
Cleaned:	-	-	-
Accepted:	13	-	13
Deferred:	-	-	-
Discarded:	-	-	-
Rejected:	-	-	-

Setting up antispam

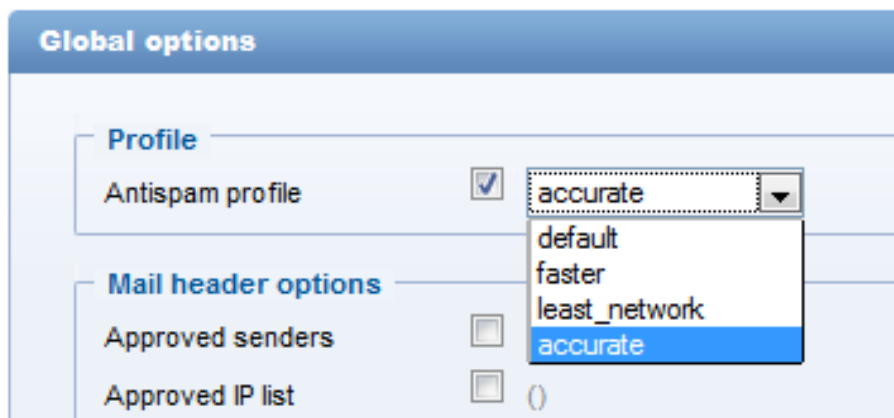
It is also possible to use ESET Mail Security for Linux as an antispam provider for Zarafa. It does this using the mailshell antispam engine. To enable the antispam feature, open the webinterface and navigate to “Configuration -> SMTP”, and set the “Anti-Spam action” to “scan”:



The screenshot shows a configuration panel with the following settings:

Anti-Spam action	<input checked="" type="checkbox"/>	scan
On spam	<input type="checkbox"/>	(accept)
On spam not scanned	<input type="checkbox"/>	(accept)
Cleaning mode	<input type="checkbox"/>	(standard)
Smart optimization	<input type="checkbox"/>	(yes)

Optionally, you can change the antispam profile from the default profile to the “most accurate” profile. This will allow for better spam detection, but will consume more system resources. This can be done by navigating to “Configuration -> Global -> Antispam options -> Antispam profile” in the web interface:

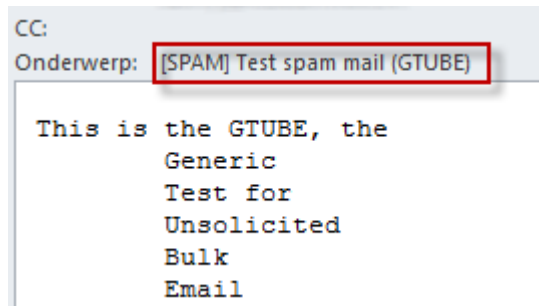


The screenshot shows the “Global options” section with the following settings:

Profile		
Antispam profile	<input checked="" type="checkbox"/>	accurate
Mail header options		
Approved senders	<input type="checkbox"/>	
Approved IP list	<input type="checkbox"/>	()

The “Antispam profile” dropdown menu is open, showing the following options: default, faster, least_network, and accurate (highlighted).

After saving and applying these settings, EMSL will also scan all incoming email for spam, and add a [SPAM] prefix to the subject if the spam score is high enough:



CC:
Onderwerp: [SPAM] Test spam mail (GTUBE)

This is the GTUBE, the
Generic
Test for
Unsolicited
Bulk
Email

X-ESET-AntiSpam: SPAM;98;calc;2012-02-03 11:30:56;1202031130560001;2431

In this configuration the spam will be delivered to the user's inbox. If you want to deliver the spam to the "Junk E-mail", change the following in `/etc/zarafa/dagent.cfg`:

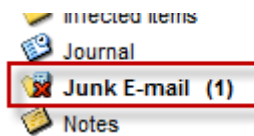
```
spam_header_name = X-Spam-Status  
to  
spam_header_name = X-ESET-AntiSpam
```

```
spam_header_value = Yes,  
to  
spam_header_value = SPAM
```

Restart zarafa-dagent:

```
/etc/init.d/zarafa-dagent restart
```

Zarafa will now place all spam email in the "Junk E-mail" folder:



Mail spam statistics

	Number of mails	%
Ham:	1	11.1
Likely ham:	3	33.3
Likely spam:	0	0.0
Spam:	5	55.6