

*By Oliver Meyer*

Published: 2007-09-04 17:31

# ASSP With Embedded ClamAV Integrated Into Postfix With Virtual Users And Domains

Version 1.0

Author: Oliver Meyer <o [dot] meyer [at] projektfarm [dot] de>

Last edited 08/27/2007

This document describes how to integrate ASSP (Anti-Spam SMTP Proxy) with embedded ClamAV into a mail server based on Postfix featuring virtual users and domains, i.e. users and domains that are in a MySQL database. It rests upon parts of the howto [Users And Domains With Postfix, Courier And MySQL \(Debian Etch\)](#) from Falko Timme.

The resulting Postfix server is functionally almost identic with the one from the howto above mentioned, but doesn't need Amavisd. ASSP provides a comfortable, considerable web-interface for setup/configuration.

This howto is meant as a practical guide; it does not cover the theoretical backgrounds. They are treated in a lot of other documents in the web.

This document comes without warranty of any kind! I want to say that this is not the only way of setting up such a system. There are many ways of achieving this goal but this is the way I take. I do not issue any guarantee that this will work for you!

## 1 Preparation

Please follow the howto [Users And Domains With Postfix, Courier And MySQL \(Debian Etch\)](#) from Falko Timme from step 1 - 8 + 13 before you proceed.

## 2 Needed Packages

First we have to install a few packages needed by ASSP:



```
apt-get install libcompress-zlib-perl libdigest-md5-perl libemail-valid-perl  
libfile-readbackwards-perl libmail-spf-query-perl libmail-srs-perl libnet-dns-perl  
libsys-syslog-perl libnet-ldap-perl libtime-hires-perl unzip
```

### 3 Get ASSP

Download and unzip ASSP:

```
cd /usr/src/  
  
wget http://mesh.dl.sourceforge.net/sourceforge/assp/ASSP_1.3.3.1-Install.zip  
  
unzip ASSP_1.3.3.1-Install.zip
```

### 4 Install ASSP

Prepare some directories:

```
mkdir -p /usr/share/assp/spam  
  
mkdir /usr/share/assp/notspam  
  
mkdir /usr/share/assp/errors  
  
mkdir /usr/share/assp/errors/spam  
  
mkdir /usr/share/assp/errors/notspam
```

Copy ASSP to the right destination:

```
cd /usr/src/ASSP_1.3.3.1-Install/  
  
cp -R ASSP/* /usr/share/assp/
```

## 5 Create Script

To the considerable use of ASSP we create the following script (thanks to Ivo Schaap) and the runlevel-entries for autostart:

```
vi /etc/init.d/assp
```

```
#!/bin/sh -e  
# Start or stop ASSP  
#  
# Ivo Schaap <ivo@lineau.nl>  
  
PATH=/bin:/usr/bin:/sbin:/usr/sbin  
  
case "$1" in  
  
start)  
    echo -n "Starting the Anti-Spam SMTP Proxy"  
    cd /usr/share/assp
```

```
perl assp.pl
;;

stop)
    echo -n "Stopping the Anti-Spam SMTP Proxy"
    kill -9 `ps ax | grep "perl assp.pl" | grep -v grep | awk '{ print $1 }'^
;;

restart)
    $0 stop || true
    $0 start
;;

*)
    echo "Usage: /etc/init.d/assp {start|stop|restart}"
    exit 1
;;

esac

exit 0
```

Change the permission:

```
chmod 755 /etc/init.d/assp
```

Create the runlevel-entries:

```
update-rc.d assp defaults
```

Start ASSP for the first time:

```
/etc/init.d/assp start
```

## 6 ASSP Basic Configuration

Now it's time for the initial configuration. Open `http://%host%:55555` in your preferred browser. Log in with any name and the password `nospam4me`.

ASSP
ASSP Configuration

Expand All Collapse All

- Main
- Network Setup
- SMTP Session Limits
- SPAM Control
- CC Mail
- SPAM Lower/No Processing
- Whitelisting
- Relaying
- Validate Local Addresses
- Penalty Box
- Validate Sender
- Delaying/Greylisting
- SPF
- SRS Options
- DNSBL
- URBL
- Attachments & Viruses
- Regex Filters / Spambomb
- Bayesian Options
- TestModes
- Email Interface
- File Paths
- Collecting
- Logging
- LDAP Setup
- Server Setup
- WhiteRabbit/Tuplefs
- Maillog Tail
- Mail Analyzer
- Info and Stats
- SMTP Connections
- Shutdown/Restart
- Donations

ASSP v1.3.3 10 / pid=11126  
 Mon Aug 27 00:51:56 2007  
 Changed Defaults  
 Last Rebuild SpamDB

Network Setup
SMTP Session Limits
SPAM Control
CC Mail
SPAM Lower/No Processing
Whitelisting
Relaying
Validate Local Addresses
Penalty Box
Validate Sender
Delaying/Greylisting
SPF
SRS Options
DNSBL
URBL
Attachments & Viruses
Regex Filters / Spambomb
Bayesian Options
TestModes
Email Interface
File Paths
Collecting
Logging
LDAP Setup
Server Setup

\* These fields accept a list separated by | or a file designated as follows (path relative to the ASSP directory): 'file:path/to/file/filename.txt'. Files should have one entry per line, anything on a line following a numbersign (#) is ignored (a comment). Whitespace at the beginning or end of the line is ignored.

\*\* Changes to these settings will not take effect until ASSP is restarted. Alternatively, if you are using the Restart Timeout option, you can wait for the restart timeout and settings will be reloaded at that time.

Now open the tab *Server Setup*. Mark the checkbox *Run ASSP as a daemon* and next enter *nobody* for UID and *nogroup* for GID. Next apply the changes with the corresponding button at the bottom on the right.

The screenshot shows the configuration web interface for ASSP. On the left is a navigation menu with options like 'Expand All', 'Collapse All', and various configuration categories such as 'Mail', 'Network Setup', 'SMTP Session Limits', 'SPAM Control', 'CC Mail', 'SPAM Level/No Processing', 'Whitelisting', 'Relaying', 'Validate Local Addresses', 'Penalty Box', 'Validate Sender', 'Delaying/Queueing', 'SPF', 'DNS', 'Attachments & Viruses', 'Regex Filters / Spambomb', 'Bayesian Options', 'Test Modes', 'Email Interface', 'File Paths', 'Collecting', 'Logging', 'LDAP Setup', 'Server Setup', 'AsAService', 'AsADaemon', 'runAsUser', 'runAsGroup', 'ChangeRoot', 'myName', 'proxyserver', 'OutgoingBufferSize', 'webAdminPort', 'webAdminPassword', 'allowAdminConnectionsFrom', 'HeaderMaxLength', 'HeaderMaxLocal', 'SaveStateEvery', 'totalizeSpamStats', 'RestartEvery', 'OrderedTieHashSize', 'EnableHTTPCompression', 'EnableFloatingMenu', 'EnableInternalNameInDesc', 'MaillogTailJump', 'MaillogTailBytes', 'MaillogTailWrapColumns', 'UseLocalTime', 'noicon WhiteRedies/Templates', 'noicon Maillog Tail', 'noicon Mail Analyzer', 'noicon Info and Stats', 'noicon SMTP Connections', and 'noicon Shutdown/Restart'.

The main content area is titled 'LDAP Setup' and 'Server Setup'. It contains several sections:

- Run ASSP as a Windows Service\*\***: A checkbox that is unchecked. Description: "In Windows NT/2000/XP/2003 ASSP can be installed as a service. This setting tells ASSP that this has been done -- it does not install the Windows service for you. Installing ASSP as a service requires several steps which are detailed in the [Quick Start for Win32](#) wiki page." Internal Name: AsAService.
- Run ASSP as a Daemon\*\***: A checkbox that is checked. Description: "In Linux/BSD/Unix/OSX fork and close file handles. Similar to the command 'perl assp.pl &', but better." Internal Name: AsADaemon.
- Run as UID\*\***: A text input field containing 'nobody'. Description: "The \*nix user name to assume after startup (\*nix only). Examples: assp, nobody." Internal Name: runAsUser.
- Run as GID\*\***: A text input field containing 'nogroup'. Description: "The \*nix group to assume after startup (\*nix only). Examples: assp, nobody." Internal Name: runAsGroup.
- Change Root\*\***: A text input field. Description: "The new root directory to which ASSP should chroot (\*nix only). If blank, no chroot jail will be used. Note! If you use this feature, be sure to copy or link the etc/protocols file in your chroot jail." Internal Name: ChangeRoot.
- My Name**: A text input field containing 'ASSP.nospam'. Description: "ASSP will identify itself by this name in the email 'Received:' header. Usually the fully qualified domain name of the host. Examples: mail.mydomain.com, ASSP.nospam." Internal Name: myName.
- Proxy Server**: A text input field. Description: "The Proxy Server to use when uploading global statistics and downloading the greylist. Examples: 192.168.0.1:8080, 192.168.0.1" Internal Name: proxyserver.

Because the changes to the UID and GID, we have to change the permissions for the ASSP-directory:

```
chown -R nobody:nogroup /usr/share/assp/
```

Afterwards open the tab *Relaying* and add your domain to *Accept All Mail and Local Domains*. Apply the changes.



<p>Expand All Collapse All</p> <ul style="list-style-type: none"> <li>[-] Main</li> <li>[-] Network Setup</li> <li>[-] SMTP Session Limits</li> <li>[-] SPAM Control</li> <li>[-] CC Mail</li> <li>[-] SPAM Lower/No Processing</li> <li>[-] Whitelisting</li> <li>[-] Relaying</li> <li>[-] acceptAllMail</li> <li>[-] localDomains</li> <li>[-] noLocalDomains</li> <li>[-] LDAP</li> <li>[-] ISP</li> <li>[-] ISP/Secondary MX Servers</li> <li>[-] ISP/Secondary MX Grey Value</li> <li>[-] Skip Local Domain Check</li> <li>[-] Do LDAP lookup for local domains</li> <li>[-] Validate Local Addresses</li> <li>[-] Penalty Box</li> <li>[-] Validate Sender</li> <li>[-] Delaying/Graylisting</li> <li>[-] SPF</li> <li>[-] SRS Options</li> <li>[-] DNSBL</li> <li>[-] URIBL</li> <li>[-] Attachments &amp; Viruses</li> <li>[-] Regex Filters / Spambase</li> <li>[-] Bayesian Options</li> <li>[-] Test Modes</li> <li>[-] Email Interface</li> <li>[-] File Paths</li> <li>[-] Collecting</li> <li>[-] Logging</li> <li>[-] LDAP Setup</li> <li>[-] Server Setup</li> <li>[-] WhiteRedist/Tuplets</li> <li>[-] Maillog Tail</li> <li>[-] Mail Analyzer</li> <li>[-] Info and Stats</li> <li>[-] SMTP Connections</li> <li>[-] Shutdown/Restart</li> <li>[-] Donations</li> </ul> <p>ASSP v1.3.3 (0 / gid=11126)                  Mon Aug 27 00:51:09 2007                  Changed Defaults                  Last Rebuild SpamDB</p>	<p style="text-align: center;"><b>SPAM Control</b></p> <p style="text-align: center;"><b>CC Mail</b></p> <p style="text-align: center;"><b>SPAM Lower/No Processing</b></p> <p style="text-align: center;"><b>Whitelisting</b></p> <p style="text-align: center;"><b>Relaying</b></p> <hr/> <p><b>Accept All Mail*</b></p> <p><input type="text" value="example.com"/></p> <p>Relaying is allowed for these IPs. They contribute also to the whitelist. This can take either a directly entered list of IPs separated by pipes or a file 'file:files/acceptall.txt'.                  For example: 127.0.0.1 10.169.254.1 72.16.192.168                  Internal Name: acceptAllMail</p> <hr/> <p><b>Local Domains*</b></p> <p><input type="text" value="example.com"/></p> <p>Check local domains against this addresses. Separate addresses with   or use file 'file:files/localdomains.txt'. Include all subdomains.                  For example: put.YourDomains.com here.org                  Internal Name: localDomains</p> <hr/> <p><input type="checkbox"/> <b>Skip Local Domain Check</b></p> <p><b>*** Updated</b></p> <p>Do not check relaying based on localDomains. Let the mailserver do it.                  Internal Name: noLocalDomains</p> <hr/> <p><input type="checkbox"/> <b>Do LDAP lookup for local domains</b></p> <p><b>*** Updated</b></p> <p>Check local domains against an LDAP database.                  Note: Checking this requires filling in LDAP Domainfilter in The LDAP section.                  This requires an installed <b>NET:LDAP</b> module in PERL.                  Internal Name: ldap</p> <hr/> <p><b>ISP/Secondary MX Servers*</b></p> <p><input type="text" value=""/></p> <p>Enter any addresses that are your ISP or backup MX servers, separated by pipes ( ).                  These addresses will (necessarily) bypass Grplist, IP limiting, Delaying, Penalty Box, SPF, DNSBL &amp; SRS checks. For example: 127.0.0.1 10. You can use here the same file which is used for delay-exceptions: 'file:files/nodelay.txt'                  Internal Name: isp</p> <hr/> <p><b>ISP/Secondary MX Grey Value</b></p> <p><input type="text" value="0.5"/></p> <p>It is recommended that for ISP &amp; Secondary MX servers to bypass their Grplist values                  For eg. 0.5 (Completely GrayIP). If left blank then the Grplist "X" value is used.                  Note: value should be greater than 0 and less than 1, where 0 = never spam &amp; 1 = always spam                  Internal Name: ispgrayvalue</p>
--	---

Now open the tab *Test Modes* and mark all checkboxes. After ASSP has learned 500 - 1000 Mails, detection of spam will be effective, and you can unmark these checkboxes.

The screenshot shows the ASSP configuration interface. On the left is a sidebar with a tree view containing categories like 'Main', 'Network Setup', 'SMTP Session Limits', 'SPAM Control', 'CC Mail', 'SPAM Level/No Processing', 'Whitelisting', 'Relaying', 'Validate Local Addresses', 'Penalty Box', 'Validate Sender', 'Delaying/Graying', 'SPF', 'SRV Options', 'DNSBL', 'URBL', 'Attachments & Viruses', 'Regex Filters / Spambomb', 'Bayesian Options', 'TestModes', 'Email Interface', 'File Paths', 'Collecting', 'Logging', 'LDAP Setup', 'Server Setup', 'WhiteRedlist/Tuplets', 'Maillog Tail', 'Mail Analyzer', 'Info and Stats', 'SMTP Connections', 'Shutdown/Restart', and 'Donations'. The main content area is titled 'Regex Filters / Spambomb' and contains sections for 'Bayesian Options' and 'TestModes'. Under 'TestModes', several options are listed with checkboxes and internal names:

- Prepend Spam Subject** (Internal Name: spamSubject): Setting a filter to testmode will tell ASSP not to reject the mail but rather build up the whitelist and spam and notspam collections. This can go on for some time without disturbing normal operation. After this very important phase testmode can be used to tag the message: if TestMode and message is spam Spam Subject gets prepended to the subject of the email. For example: [SPAM]
- Prepend Spam Tag** (Internal Name: spamTag): The check which caused the spam detection will be prepended to the subject of the email. For example: [RBL]
- Message Scoring Modes** (Internal Name: testScoringMode): Put the filter automatically in "Message Scoring Mode" when **Single Message Mode** is set (instead of stopping spam processing altogether).
- Bayesian Test Mode** (Internal Name: baysTestMode)
- BlackDomain Test Mode** (Internal Name: bTestMode)
- Heio-Blacklist Test Mode** (Internal Name: hTestMode)
- Spam Address Test Mode** (Internal Name: sbTestMode)
- SPF Test Mode** (Internal Name: spfTestMode)
- DNSBL Test Mode** (Internal Name: blTestMode)
- Bad Attachment Test Mode** (Internal Name: attachTestMode)
- URBL Test Mode**

## 7 Install ClamAV

We install ClamAV out of the debian repository:

```
apt-get install clamav clamav-daemon
```

## 8 Install ClamAV Perl Module

The installation of the ClamAV perl module is a bit tricky because the old version of this module. The following perl-test will fail with many errors but is necessary to download the module.

**Note:** When you are asked if you want to configure perl manually, choose *no* ^^ the configuration will be done automatically.

```
perl -MCPAN -e shell

test File::Scan::ClamAV

look File::Scan::ClamAV

vi clamav.conf
```

Change:

```
LocalSocket /root/.cpan/build/File-Scan-ClamAV-1.8/clamsock
Foreground
MaxThreads 1
ScanArchive
ArchiveMaxFileSize 1M
ArchiveMaxRecursion 1
ArchiveMaxFiles 2
```

To:

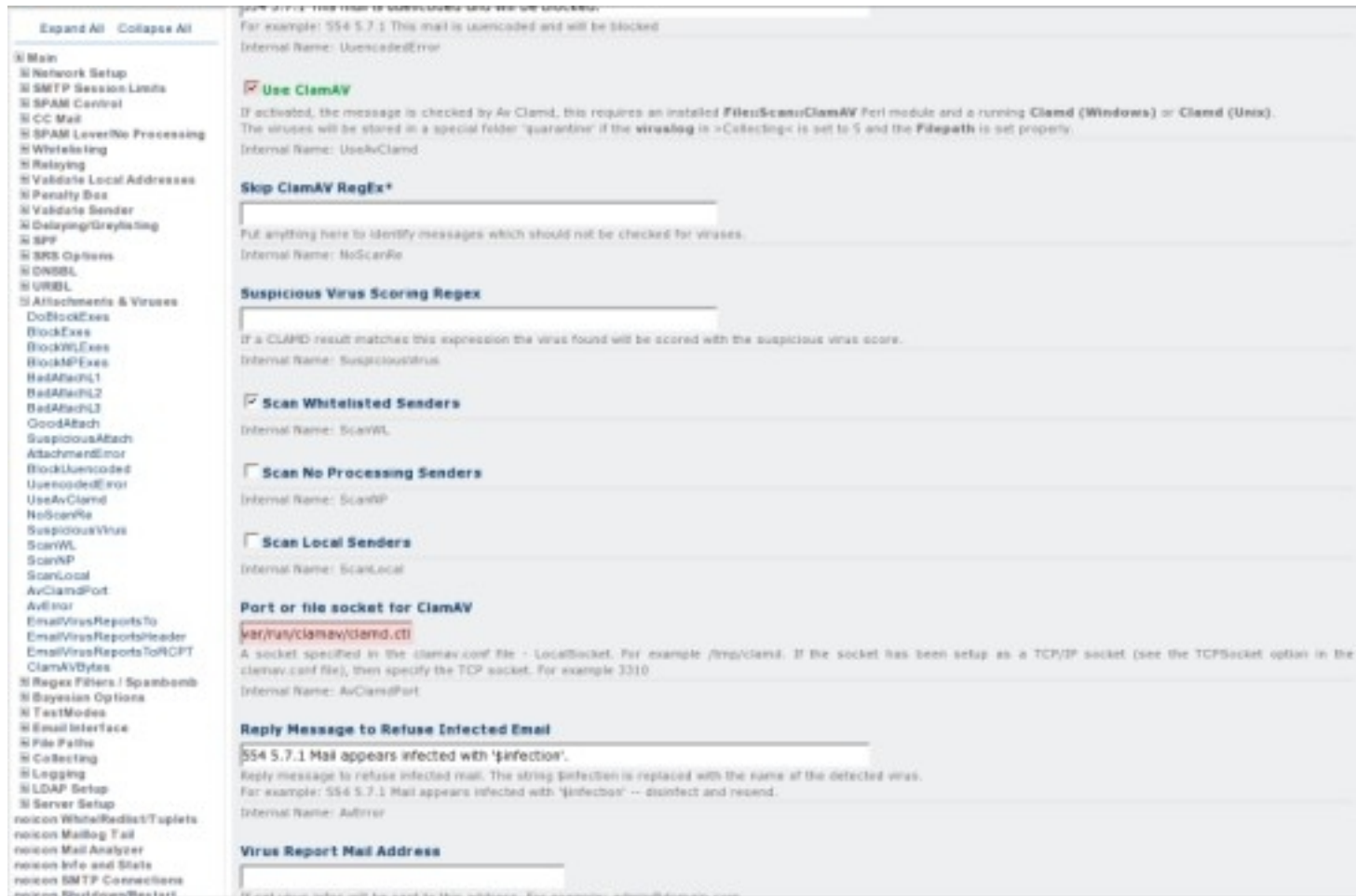
```
LocalSocket /root/.cpan/build/File-Scan-ClamAV-1.8/clamsock
Foreground true
MaxThreads 1
ScanArchive true
ArchiveMaxFileSize 1M
ArchiveMaxRecursion 1
ArchiveMaxFiles 2
```

Afterwards install the module:

```
make install
```

## 9 Integrate ClamAV Into ASSP

After the installation of ClamAV and the related perl module, ClamAV is accessible for ASSP. Switch back to the ASSP web-interface and open the tab *Attachments & Viruses*. Add `/var/run/clamav/clamd.ctl` to *Port or file socket for ClamAV* and apply the changes.



## 10 Integrate ASSP Into Postfix

The easiest part...

```
vi /etc/postfix/master.cf
```

Change:

```
smtp inet n - - - - smtpd
```

To:

```
125 inet n - - - - smtpd
```

Restart Postfix:

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

## 11 Links

- ASSP: <http://assp.sourceforge.net/>
- ASSP Wiki: <http://www.asspsmtp.org/wiki/Welcome>
- ClamAV: <http://www.clamav.org/>
- Postfix: <http://www.postfix.org/>