SCOUTS®
Creating a Better World
World Organization of the Scout Movement
Organisation Mondiale du Mouvement Scout
Всемирная Организация Скаутского Движения
Organización Mundial del Movimiento Scout
المنظمة العالمية للحركة الكشفية

A free and open source anti-spam and anti-virus solution for a FirstClass system

(Mac OS X version)

Published 24 January 2007

Marcus Ljungblad
Unit Officer, Information Technology
World Scout Bureau

with foreword by

Ray Saunders
Director, Information Technology
World Scout Bureau

Head Office
Rue du Pré-Jérôme 5
1205 Geneva
Switzerland

worldbureau@world.scout.org
www.scout.org

Table of Contents

Foreword

This document describes the process of setting up ASSP (an anti-spam filter) and ClamSMTP (anti-virus filter) to protect a FirstClass Server with FirstClass Internet Services, all running on a single Mac OS X 10.3.9 computer.

In May 2006, the World Scout Bureau adopted a global policy in favour of using open source software:

"The World Scout Bureau will consider open source software solutions alongside proprietary ones in all IT procurements. Where available, an open source default choice will apply but purchases will be made on an overall value for money basis."

Beginning in the summer of that year, we undertook a feasibility study to assess the possibilities of migrating our existing FirstClass Server 8.0 running on a proprietary Mac OS X 10.3.9 system to a FirstClass Server 8.3 running on a free and open source Linux system. Our target was to add better anti-spam measures than those afforded through the default FirstClass Internet Server mail rules solution together with a free, open source anti-virus solution to replace the commercial and proprietary-only offering supported in FirstClass (currently Norton Anti-Spam Engine).

Having succeeded in that mission, we turned our attention to our existing FirstClass Server 8.0 running on Mac OS X 10.3.9. Given that FreeBSD lies at the core of Mac OS X, would it also be possible to apply the same anti-spam and anti-virus combination to our production server sooner rather than delay adding that protection until we finally upgraded to FirstClass Server 8.3? The answer was an emphatic "Yes!"

CREDIT WHERE CREDIT IS DUE

Much of our current work was inspired and guided by a previous discussion in the since-archived "Advanced Connections" forum in FirstClass Online. Back in May 2004, Tom Smith, FirstClass Administrator in Park School, Brookline, MA (USA), published his draft of *"Setting up ASSP to work with FirstClass"*. In the discussion which ensued, Cedric A. Paine, Ian Baker, Fritz from "UNICORN Germany", Robert Bradley, Stefano Costantini, Christopher Butler all variously contributed to increasing our knowledge of how to incorporate ASSP as an anti-spam filter into our FirstClass solution. Their insights have been included in this document in the form of updating the text and illustrations to reflect the many changes that have taken place in ASSP and its interface. Thanks to all for their pioneering work.

WHAT'S NEW HERE

For various reasons during its development, ASSP has included, then dropped and then re-introduced (with limited success, to-date) anti-virus filtering in its mix. At every stage, this has involved the use of the highly regarded ClamAV open source anti-virus engine. We decided to look for an alternative method for achieving the same goal and our research led us to discover Nate Nielsen's ClamSMTP.

"ClamSMTP is an SMTP filter that allows you to check for viruses using the ClamAV anti-virus software. It accepts SMTP connections and forwards the SMTP commands and responses to another SMTP server. The 'DATA' email body is intercepted and scanned before forwarding.

ClamSMTP aims to be lightweight, reliable, and simple rather than have a myriad of options. It's written in C without major dependencies."[1]

It sounded ideal for our purposes and all we had to do was figure out how to include it in the mix with ASSP, which is precisely what this document aims to show you. As Tom Smith wrote in his initial message *"While many different platforms and configurations are possible, this description is specific to our Macintosh computers, though other configurations would be quite similar."*[2]

We believe that by simply adapting the solution as we have presented it here, ASSP coupled with ClamSMTP can also provide a well-supported anti-spam and anti-virus solution in many other mail server configurations. Should you choose to follow such a route, we would be very pleased to hear from you and learn from your experiences. Indeed, any feedback on what we have done would be welcome – even if it is of a critical nature.

---

1 ClamSMTP, http://memberwebs.com/nielsen/software/clamsmtp/

2 Setting up ASSP to work with FirstClass, *Smith, Tom*

Sharing knowledge is a virtue common to both open source software and Scouting. In this year, 2007, Scouting celebrates its first centenary, marking 100 years of community involvement around the world, under the slogan *"One World One Promise"*. We believe that by publishing this guide, we are helping to create a better world for all: one free of spam and virus-laden email attachments.

This document is our small gift to the FirstClass Online community. We hope that by sharing our knowledge about the free software we have used, more system administrators will choose to implement solutions around these valuable open source projects and thereby support and encourage their development communities.

Ray Saunders
Director, Information Technology
World Scout Bureau

"I found it understandable and well written. It actually comes to me at a pretty good time, since I will shortly build a completely fresh FCIS server with a new ASSP installation. I am a few revisions behind on my production ASSP, so your details are welcome.... Well done."

Tom Smith, January 2007
Author of the original "Setting up ASSP to work with FirstClass"

Introduction

SET-UP OVERVIEW

This guide explains how-to set up Anti-Spam SMTP Proxy (ASSP) Server and Clam anti-virus to filter spam and scan incoming mail for viruses to a FirstClass mail system. While there are many different Unix like platforms, this guide is specific to Mac OS X 10.3.9 or later.

The components in this set-up, running on a Mac OS X 10.3.9 machine, with FirstClass Server 8.0 and FirstClass Internet Services 8.0 are the following:

ASSP 1.2.6
ClamSMTP 1.8
Clam anti-virus 0.88.6
Postfix

Our primary goal was to have all services running on the same machine, but modifications can be introduced to spread the services onto several computers.

"ASSP is an open source platform-independent SMTP Proxy server which implements whitelists and Bayesian filtering to rid the planet of the blight of unsolicited e-mail."[3]

"ASSP has no built-in SMTP server, so you need Postfix (or some other SMTP server) to relay mail to the Internet. Since we are using Mac OS X 10.3, the built-in Postfix is an excellent choice. FCIS sends mail through ASSP to the Internet, since that is how ASSP builds its whitelist. All mail addresses that FirstClass users explicitly send mail to are assumed to be not-spam."[4]

Clam anti-virus is an open-source software to scan files for viruses. *"The main purpose of this software [ClamAV] is the integration with mail servers (attachment scanning)."*[5] Additionally, ClamAV comes with a tool for automatically keeping your virus database up-to-date, and even more importantly, the central virus database itself is updated several times a day.

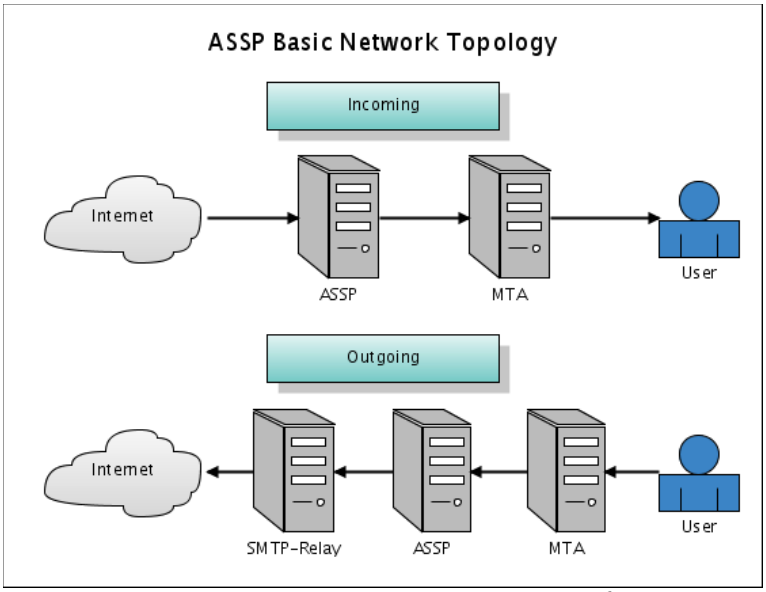

Figure 1: Basic network topology used with ASSP.[6]

OVERVIEW OF COMMUNICATIONS

ASSP is able to connect to ClamAV using a Perl module. At time of writing, this has however proven to be limited in its accuracy and we therefore opted for another route for our production server, using ClamSMTP as an SMTP filter which calls ClamAV to scan incoming e-mails. This way it is possible to use the computer's resources more efficiently and detect viruses more accurately. Nevertheless, better internal support for ClamAV might be integrated in future versions of ASSP.

3 Anti-Spam SMTP Proxy, http://www.asspsmtp.org
4 Setting up ASSP to work with FirstClass, *Smith, Tom*
5 Clam anti-virus, http://www.clamav.net/abstract.html
6 Anti-Spam SMTP Proxy, http://www.asspsmtp.org/wiki/Configuration

To include the virus-scanning functionality we are going to insert ClamSMTP between ASSP and FCIS (which can be thought of as being represented by the MTA box in the above figure). It would be possible to scan outgoing e-mails as well, however, we have chosen not to.

Our communciation paths will therefore look like this:

Incoming e-mails
Internet --> (25) ASSP (10025) --> (10025) ClamSMTP (125) --> (125) FCIS --> FCS --> User

Outgoing e-mails
Internet (25) <-- (25) Postfix (325) <-- (325) ASSP (225) <-- (225) FCIS <-- FCS <-- User

The numbers in the brackets are the port numbers each application will listen and send data on.

REQUIREMENTS
It is assumed that you already have a working FirstClass Server with Internet Services either running on the same machine or on two separate machines. If FCIS is running on a separate machine, you will install ASSP and the other applications used in this solution on that machine also and not on the FirstClass Server.

This guide is detailing how to run ASSP, ClamSMTP and FirstClass on one machine. It is perfectly possible to run ASSP and ClamSMTP on a separate machine, but you will then need to configure the applications differently from what is described in *Part 2: Configuration*.

All applications, except for ASSP, will run as the fcadmin user, which is a requirement of FCS and FCIS.

To follow this guide it will be helpful if you have knowledge about the Terminal, `pico` or `vi`, which are terminal based text-editors, and a basic understanding about the underlying UNIX file structure. Most commands and code snippets in this document are ready to copy and paste. However, some will require your interaction. You will need to work as the super-user, called root, which has full control over everything in your system, therefore don't do anything you don't fully understand, hence be careful.

In order to install ClamSMTP, ClamAV and the required Perl modules to run ASSP it is necessary to install the Xcode Tools provided with your Apple Install CDs or DVD. The developer tools will give you the necessary files to configure and compile the required applications used in this set-up.

Installing Xcode Tools is straightforward. Locate your Mac OS X CD (or DVD) named Xcode Tools and follow the installation instructions provided with it.

When given the option to choose the packages to install, select the default and make sure that the BSD-SDK package, which may have to be chosen manually, is included. When installation is finished you might be asked to restart your computer.

Part 1: Installation

INSTALLING PERL MODULES REQUIRED BY ASSP

When Tom Smith wrote his cookbook for ASSP in 2004, ASSP had a lot less dependencies on Perl modules. Over time, the dependency for specific functions has increased, which ultimately has led to better performance of ASSP, but also made it a little bit more complicated to install.

Perl is a highly modular language and there are modules for almost anything you can imagine. To help users install additional modules Perl provides an interface to the repository where all modules are stored, called Comprehensive Perl Archive Network, abbreviated CPAN.

If you are running Mac OS X 10.4 you may have to install some of the following modules, most of them are might already installed. You can test which modules that are installed on your system by running this command in Terminal:

```
FC-Server-8:~ fcadmin$ perl -MNet::DNS -e 1
```

Notice that there is no space between the argument M and the name of the Perl module. If nothing is returned, everything for that module is OK. If you receive something like "`Can't locate Net/DNS.pm in @INC`" you will have to install that module.

Mac OS X 10.3 on the other hand comes with Perl 5.8.1-RC3 and therefore requires most of the modules listed below to be installed. Here, all modules required or optional to ASSP are installed, that way all functions are available without having to install, or re-install, modules at a later stage, even though it could be decided not to implement them in the configuration. The only exception being the Perl module for ClamAV.

Remember that the optional modules are used to increase ASSP's performance in correctly determining what is spam and what is ham.

Modules required or optional to ASSP

* Digest::MD5 (Digest-MD5-2.36)
* Compress::Zlib (Compress-Zlib-2.003)
Email::Valid (Email-Valid-0.179)
File::Scan::ClamAV (File-Scan-ClamAV-1.8)
File::ReadBackwards (File-ReadBackwards-1.04)
Mail::SPF::Query (Mail-SPF-Query-1.999.1)
Mail::SRS (Mail-SRS-0.31)
* Net::DNS (Net-DNS-0.59)
Net::LDAP (perl-ldap-0.33)
Sys::Syslog (installed by system)
* Time::HiRes (installed by system)

Modules required by one or more of the modules above and will normally be installed as dependencies

IO-Compress-Base-2.001
IO-Compress-Zlib-2.001
Compress-Raw-Zlib-2.001
Digest-SHA1-2.11
Digest-HMAC-1.01
MLDBM-2.01
Net-CIDR-Lite-0.20
URI-1.35
Convert-ASN1-0.20
MailTools-1.74
Net-IP-1.25
Digest-1.15
Sys-Hostname-Long-1.4

*Note: Items marked with an * are required for ASSP to run. The name within brackets is the actual name of the file to download at time of writing.*

The easiest way to install a Perl module is by using CPAN.

```
FC-Server-8:~ fcadmin$ sudo perl -MCPAN -e 'install Net::DNS'
```

Change the module name (`Net::DNS`) accordingly.

CPAN will automatically detect any dependencies and install these for you and if CPAN is successful you will only need to install those required and optional to ASSP. The other modules will be resolved by CPAN.

Note: If this is the first time you run CPAN, the program will ask you a number of questions, the defaults are OK. When it asks for mirrors, you may use any of the following mirrors found on this page: http://www.cpan.org/SITES.html

If CPAN does not work on your system it will be necessary to install each module separately. Download each package from the CPAN website. http://www.cpan.org then do the following for each package.

```
FC-Server-8:~ fcadmin$ tar zxvf Convert-ASN1-0.20.tar.gz
FC-Server-8:~ fcadmin$ cd Convert-ASN1-0.20/
FC-Server-8:~/Convert-ASN1-0.20 fcadmin$ perl Makefile.PL
FC-Server-8:~/Convert-ASN1-0.20 fcadmin$ make
FC-Server-8:~/Convert-ASN1-0.20 fcadmin$ sudo make test
FC-Server-8:~/Convert-ASN1-0.20 fcadmin$ sudo make install
```

Note: You need to change the name of the package accordingly.

If you have problem installing the modules as fcadmin, try running all the commands as root, by using `sudo`. Repeat the process until all modules are installed properly. If you encounter any errors, you may lack necessary dependencies. These are normally printed on the screen, download and install the dependent package and try again.

According to ASSP's website you may install the Perl module ClamAV to handle virus scanning, but as the set-up described here intends to use ClamSMTP, I've deliberately left this module out.

INSTALLING ASSP

Start by downloading the latest ASSP version, in this case version 1.2.6, from http://www.asspsmtp.org/wiki/Downloads

It is essential to use the following commands to extract the compressed zip file. (Do not use the copy which may have been automatically unziped for you depending on your browser's download behaviour.)

```
FC-Server-8:~ fcadmin$ cd /Users/fcadmin
FC-Server-8:~ fcadmin$ unzip ASSP_1.2.6-Install.zip
```

Then change the name of the extracted folder to lower-case characters.

```
FC-Server-8:~ fcadmin$ mv ASSP/ assp/
```

Now copy the necessary `._.DS_Store` file to the ASSP directory as described in ASSP's `Install.txt` file.

```
FC-Server-8:~ fcadmin$ cp __MACOSX/assp_1.2_macosx/._.DS_Store assp/
```

I found that it was easier to run ASSP from the fcadmin's home folder rather than from `/usr/local/assp/` or `/assp/` and the startup scripts provided is constructed with ASSP installed in `/Users/fcadmin/assp`.

Mac OS X defines the nobody user and nobody group with Ids less than zero which prevents ASSP from starting up. To get around this, do the following:

Now try launching ASSP by

```
FC-Server-8:~ fcadmin$ cd assp/
```

```
FC-Server-8:~/assp fcadmin$ sudo perl assp.pl
```
Most probably it will fail, but ASSP has created the configuration file which we will need to edit.

```
FC-Server-8:~/assp fcadmin$ sudo pico -w assp.cfg
```

Change

```
runAsGroup:=nobody
runAsUser:=nobody
```

to

```
runAsGroup:=admin
runAsUser:=
```

Close and save your changes then try starting ASSP again. If all is well it should work this time.

If you encounter any unmet Perl requirements, review the output from ASSP and install the necessary module(s) using CPAN or, if needed, manually. There is no need to worry about the missing ClamAV module as mentioned before.

ASSP is now running and has created a local socket for you to connect to. Try accessing http://127.0.0.1:55555 or http://your-fcserver.com:55555 in a web-browser. Make sure your Mac OS X firewall is not blocking port 55555. Use any username and the default password is 'nospam4me'. We shall configure ASSP later, first we just want to make sure it starts properly.

You may quit ASSP from the terminal by pressing <Ctrl> + c in the Terminal window.

INSTALLING CLAMAV AND CLAMSMTP

First of all we need to download the necessary packages.

We found that the easiest way to install ClamAV is by installing ClamXav which is a port of the application for Mac OS X and relies on the ClamAV bundle.

Download the latest ClamXav DMG file from:
http://www.markallan.co.uk/clamXav/

Note: This guide used ClamXav version 1.0.6. If you are installing on a version of Mac OS X Server, you must carefully follow Mark Allans instructions for that situation.

Start by installing ClamXav, this is done by double-clicking the DMG file and dragging ClamXav to your Applications folder. When finished copied, launch ClamXav to install the engine behind the graphical interface, namely ClamAV. This is done automatically the first time you launch ClamXav and you will be asked for the administrator password. Make sure the installation completes successfully. There is no need to configure anything else in ClamXav, you may safely close it and move on to ClamSMTP.

Note: Alternatively, ClamAV could be installed manually by compiling the source available at http://www.clamav.net

Next download the latest ClamSMTP package from:
http://memberwebs.com/nielsen/software/clamsmtp/

Installing ClamSMTP will require some Terminal effort. If you have never compiled a program from its source code by yourself before, don't be scared. Just follow the steps carefully.

Launch the Terminal and place yourself in the directory where you've downloaded ClamSMTP-1.8.tar.gz, in my case this is:

```
FC-Server-8:~ fcadmin$ cd /Users/fcadmin/
```

Then unpack the compressed tar file:

```
FC-Server-8:~ fcadmin$ tar zxvf clamsmtp-1.8.tar.gz
```

Enter the newly created directory:

```
FC-Server-8:~ fcadmin$ cd clamsmtp-1.8/
```

Then run the following commands one by one to install ClamSMTP. By default ClamSMTP is installed in `/usr/local/sbin/`

```
FC-Server-8:~/clamsmtp-1.8 fcadmin$ ./configure
FC-Server-8:~/clamsmtp-1.8 fcadmin$ make
FC-Server-8:~/clamsmtp-1.8 fcadmin$ make check
FC-Server-8:~/clamsmtp-1.8 fcadmin$ sudo make install
                                     (Provide the fcadmin password)
FC-Server-8:~/clamsmtp-1.8 fcadmin$ make clean
```

If you are returned with an error from any of above commands, make sure you have the developer tools installed correctly.

ClamSMTP is now successfully installed. We will configure ClamSMTP later.

Part 2: Configuration

All components of our set-up is now installed and starting up nicely, let us move on to the fun part, configuration.

CONFIGURING FIRSTCLASS

We cannot have FirstClass Internet Services running when we configure ASSP, and there are a few things we need to change in FirstClass. Let's change this before shutting FCIS down.

Log in as administrator and open your `Internet Services` folder located on your administrator desktop.

Open the `Advanced Mail` form and go the tab `SMTP`. Change `SMTP port` to '`125`'.

Click on the tab `Routing`. Tick the box `Route through one SMTP server` and change `IP Address` to '`127.0.0.1:225`'.

Stop FirstClass Internet Services. This is required for FCIS to bind to the new ports, otherwise you will not pass through ASSP on the way in or out, and for us to configure ASSP properly.

CONFIGURING ASSP

ASSP has a massive configuration interface. There are some essential variables we need to change to adapt it to our set-up. As ASSP has to run on ports below 1024 it has to be started as the super-user.

Start ASSP as root (or use sudo) by executing:

```
FC-Server-8:~ fcadmin$ cd assp/
FC-Server-8:~/assp fcadmin$ sudo perl assp.pl
```

Since ASSP is a Perl application we need Perl to start it for us. If you are unsure whether ASSP is running or not, you could try logging in to its web-interface or running this command in a Terminal window:

```
FC-Server-8:~/assp fcadmin$ ps aux | grep assp
```

You should get an output similar to this:

```
fcadmin     4935  0.0  0.2    4336    628 ?        Ss   13:53   0:00 perl assp.pl &
fcadmin    10124  0.0  0.3    2892    828 pts/0    S+   15:56   0:00 grep assp
```

Log-in to its web-interface on http://127.0.0.1:55555 with any username and the default password 'nospam4me'. You are strongly advised to change this password at once.

Below is a list of the variables that you need to change in order for ASSP to work together with ClamSMTP and FirstClass. A complete list of the configuration I used is attached with this document.

It is important to save changes as you go, otherwise you might lose settings.

Network Setup

```
SMTP-Destination: 127.0.0.1:10025
Tick As a Daemon          (This one is important for the start-up scripts to work)
Listen port: 25
MaxSessionsIP: 5
SMTP Idle Timeout: 999    (In tests we found the default 120 seconds did not give
                          ClamSMTP sufficient time to scan for viruses in larger
                          attachments.)
Tick Session Limit Logging
```

White-listing

```
Whitelisted domains - remove sourceforge.net
```

No-processing Options

```
Expression to Identify No-processing Mail: X-FC-MachineGenerated|X-FC-Autoforward-By
```

Relaying

```
Local Domains: your.maildomain.com|your-other.maildomain.com|spamreport.gov
Relay Host: 127.0.0.1:325
Relay Port: 127.0.0.1:225
```

Virus Control

```
External attachment blocking: 1
Uncheck Use Av Clamd
```

TestModes

```
Prepend Spam Subject: '<SPAM?>'
```

Security

```
Change Web Admin Password
```

Consult the ASSP documentation before deciding which TestModes to activate.

When you have confirmed changes above you will need to restart ASSP.

```
FC-Server-8:~/assp fcadmin$ ps aux | grep assp
FC-Server-8:~/assp fcadmin$ sudo kill `cat pid`
```

You will also want to edit the `spamreport.txt` and `nospamreport.txt` files which are located in the `assp/` folder. These contain the text that ASSP will send to users who forward spam and not-spam messages to ASSP to teach it which mail is or isn't spam.

Of course there are many many more options to ASSP and you should read more about them on ASSP's own website http://www.asspsmtp.org

CONFIGURING CLAMAV

ClamAV's configuration file is located in `/usr/local/clamXav/etc/` and called `clamd.conf`.

```
FC-Server-8:~/assp fcadmin$ sudo pico -w /usr/local/clamXav/etc/clamd.conf
```

The first you need to do is to comment out the line which reads, otherwise your configuration file wont be read properly by clamd.

```
# Comment or remove the line below.
Example
```

to

```
# Comment or remove the line below.
#Example
```

We need to find out which socket ClamAV is listening on. In my case this was `/tmp/clamd`. The socket parameter is found in the `clamd.conf`.

To make sure the `ScanMail` feature is activated remove the # infront of `ScanMail` in `clamd.conf`

Last we need to change the user for which ClamAV is going to run.

Change

```
#User: clamav
```

to

```
User: fcadmin
```

Close and save the file.

Note: If you have activated logging, good for troubleshooting, make sure the fcadmin user can write to the log file. This can be changed by running

```
FC-Server-8:~/assp fcadmin$ sudo touch /var/log/clamd.log
FC-Server-8:~/assp fcadmin$ sudo chown fcadmin /var/log/clamd.log
```

if that is the location of your log file.

Moreover, we want to have our virus database updated automatically at least once a day. This may be scheduled using `Crontab`.

Open `/etc/crontab` in your favorite text-editor and copy the following line. A line like this will execute `freshclam` every night at 02h00.

```
FC-Server-8:~/assp fcadmin$ sudo pico -w /etc/crontab
```

```
0    2    *    *    *    fcadmin    /usr/local/clamXav/bin/freshclam
```

Save the file and exit. We choose to run `freshclam` as fcadmin since this user can handle this process just fine.

Start `clamd` by running

```
FC-Server-8:~/assp fcadmin$ /usr/local/clamXav/sbin/clamd
```

It may take a while to start ClamAV as it performs a self-integrity check on startup to make sure the virus database is intact and up-to-date. The program then automatically forks to the background.

Anytime you change the `clamd.conf` you will need to restart `clamd` for the changes to take effect.

CONFIGURING CLAMSMTP

ClamSMTP requires its configuration file to be located in `/usr/local/etc/` and is simply called `clamsmtpd.conf`. By default on Mac OS X 10.3 and 10.4 there is no such location so we have to create it and then copy the example configuration file to this new location.

```
FC-Server-8:~/assp fcadmin$ sudo mkdir /usr/local/etc
FC-Server-8:~/assp fcadmin$ sudo cp /Users/fcadmin/clamsmtpd-1.8/doc/clamsmtpd.conf
/usr/local/etc
```

This file contain all the directives that may be used with ClamSMTP and there are a few of them we have to change to pass incoming e-mails through ClamSMTP.

Open the configuration file with `nano` (or `pico` if you're running OS X 10.3).

```
FC-Server-8:~/assp fcadmin$ sudo pico -w /usr/local/etc/clamsmtpd.conf
```

Change the following variables (removing the # when necessary):

```
OutAddress: 127.0.0.1:125
     (This is the port FC will listens on)

KeepAlives: 30

XClient: on
     (Not all receiving servers support it, FC does, and therefore we can send some
additional information about the connection by enabling XClient)

Listen: 127.0.0.1:10025
     (This is the port ClamSMTP listens on, hence connection from ASSP)

ClamAddress: /tmp/clamd
```

```
     (This is the socket ClamAV listens on, the value here is found in your
clamd.conf)

Header: X-Virus-Scanned: ClamAV using ClamSMTP
     (This will leave a mark in the header of the e-mail so you can see that is has
been scanned by ClamAV)

User: fcadmin
```

ClamSMTP has to be run as the same user as ClamAV, I chose to run it as fcadmin for convenience. Start it by running:

```
FC-Server-8:~/assp fcadmin$ /usr/local/sbin/clamsmtpd
```

from the Terminal.

To see if ClamAV and ClamSMTP is running you can start the activity monitor. Under the view "My Processes" you should see `clamd` and `clamsmtpd`.

CONFIGURING POSTFIX

Since ASSP cannot deliver mail on its own we need Postfix to do that for us. Postfix is installed by default on Mac OS X 10.3 and 10.4 and is therefore an good choice.

Postfix is controlled by two configuration files and we need to change only three lines.

Open `/etc/postfix/master.cf` and change the following line:

```
FC-Server-8:~/assp fcadmin$ sudo pico -w /etc/postfix/master.cf

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

to

```
325       inet  n       -       n       -       -       smtpd
```

If you intend to listen with another port on Postfix, change `325` to the port of your desire.

In the other configuration file, `/etc/postfix/main.cf` we need to change these lines:

```
FC-Server-8:~/assp fcadmin$ sudo pico -w /etc/postfix/main.cf

myhostname = mailout.mydomain.com
relayhost = smtprelay.your-isp.com
```

Don't use the name of your FirstClass host for the `myhostname` variable, it will break the ability for internal users to send e-mails to your Internet domain. The `relayhost` variable is only needed if you have to use a SMTP-relay. This is normally provided from your ISP, and if you are using it, it would have been in your FirstClass configuration before. All other defaults are fairly reasonable and you do not need to change anything else. It is especially important not to create an open relay which spammers can misuse and you are likely to end up on several RBLs.

If Postfix does not start automatically on your computer you may in in `/etc/hostconfig` change:

```
FC-Server-8:~/assp fcadmin$ sudo pico -w /etc/hostconfig

MAILSERVER=-AUTOMATIC-
```

to

```
MAILSERVER=-YES-
```

STARTING FCIS

You can now go ahead and start FirstClass Internet Services again.

GETTING EVERYTHING TO START AUTOMATICALLY

I've created a small script to start the necessary services for ASSP, so that it starts automatically if you ever need to restart your server.

Create a folder in `/Library/StartupItems/` called `ASSP_Clam`

```
FC-Server-8:~ fcadmin$ sudo mkdir /Library/StartupItems/ASSP_Clam
```

Copy the `ASSP_Clam.tar.gz` to your fcadmin's home folder.

Extract the files

```
FC-Server-8:~/assp fcadmin$ cd /Users/fcadmin
FC-Server-8:~ fcadmin$ tar zxvf ASSP_Scripts.tar.gz
```

If you have installed ClamAV through ClamXav and ClamSMTP with the default configuration there is no need to adjust the `ASSP_Clam` file. Otherwise, open it with `pico` or `vi` and change the file paths according to your set-up.

Copy the startup scripts to the ASSP_Clam folder by entering the following command in a single line:

```
FC-Server-8:~ fcadmin$ sudo cp ASSP_Scripts/ASSP_Clam
ASSP_Scripts/StartupParameters.plist /Library/StartupItems/ASSP_Clam/
```

Copy the ASSP start and stop script to the ASSP folder:

```
FC-Server-8:~ fcadmin$ cp ASSP_Scripts/startassp.sh ASSP_Scripts/stopassp.sh assp/
```

Then make the ASSP start and stop scripts executable

```
FC-Server-8:~ fcadmin$ chmod 0755 assp/startassp.sh assp/stopassp.sh
```

That's it.

Finishing off

TESTING YOUR SERVER

First of all it is important to test whether it works or not. Try sending e-mails out from and to FirstClass. Also try sending messages to from FirstClass to another FirstClass user by using his/her Internet e-mail address.

Then we need to make sure ClamSMTP actually scans the incoming messages. One way could be to monitor the `mail.log` file, note that this is not the same maillog that you will find through ASSP's web administrator interface, while you send an e-mail to a FirstClass user from the outside world. Remember, sending an e-mail internally will not make it pass through ClamSMTP.

```
FC-Server-8:~/assp fcadmin$ sudo tail -f /var/log/mail.log
```

"Using real viruses for testing in the real world is rather like setting fire to the dustbin in your office to see whether the smoke detector is working. Such a test will give meaningful results, but with unappealing, unacceptable risks.

Since it is unacceptable for you to send out real viruses for test or demonstration purposes, you need a file that can safely be passed around and which is obviously non-viral, but which your anti-virus software will react to as if it were a virus."[7]

By sending an EICAR test virus file, downloadable from http://www.eicar.org/anti_virus_test_file.htm, to an FC account you can test ClamSMTP's ability to determine viruses. If it finds it successfully, ClamSMTP will delete the entire message, or take the necessary actions according to the configuration in `clamsmtpd.conf`.

In the `mail.log` file you will see which virus signature it found or if the message was clean and passed on to FCIS.

Here is a sample record of a clean incoming e-mail from the `mail.log` file.

```
Jan 18 11:39:51 FC-dev clamsmtpd: 100000: accepted connection from: 127.0.0.1
Jan 18 11:39:54 FC-dev clamsmtpd: 100000: from=testuser@scout.org,
to=alluser@fc1.scout.org, status=CLEAN
```

Anything else than `status=CLEAN` indicates an error or more likely, the existance of a virus in the incoming e-mail.

TRAINING ASSP

With a new installation of ASSP the Bayesian spam filtering will be relatively weak. By leaving ASSP in test mode it is possible to train it to detect spam. This is something your users may help with.

Make sure you have spamreport.gov in your Local Domains variable in ASSP. *"ASSP sees this as a local domain and therefore routes the mail to its own spam area for inclusion in its Bayesian filtering calculations. It never actually routes the mail to spamreport.gov. You can use any domain that is unlikely your users will actually send mail to."*[8]

Tom Smith went on to suggest creating FirstClass conferences named "Spam" and "Notspam". Create a single receive rule on each conference that re-directs received mail to <spam@spamreport.gov> and <notspam@spamreport.gov> respectively.

Then tell your users to forward undetected spam messages to the Spam conference. Similarly, if a message was mistakenly tagged as spam, forward it to the Notspam conference.

ASSP's intelligence has be updated once in a while and this is done through the `rebuildspamdb.pl` script. Execute it by:

```
FC-Server-8:~/assp fcadmin$ perl rebuildspamdb.pl
```

---

7 EICAR, http://www.eicar.org/anti_virus_test_file.htm
8 Setting up ASSP to work with FirstClass, *Smith, Tom*

Note: We recommend adding this to `/etc/crontab` *in a similar fashion as the* `freshclam` *update.*

"I waited several days while running ASSP in TestModes, and groomed the whitelist, and spam database. After ASSP grew smarter at recognizing spam, I set:

```
Prepend Spam Subject = [SPAM]
```

and left ASSP in "TestModes", which only flags spam without filtering it. This makes it easy for users to see what e-mails ASSP flags as spam.

We very much want to reduce spam, but it is even more important that we keep false positives as near zero as possible. So we will wait probably a week or two until we are comfortable that no good mail is tagged as spam. To tell ASSP that mail it has erroneously tagged good mail as spam, users can either forward it to the "notspam" conference, or simply reply to it (or send a new message to that address) thereby adding that address to the whitelist. When we are happy with ASSP, we will remove the checks from "TestModes" and spam-be-gone!"[9]

While it is quite possible to run ASSP and FC mailRules simultaneously this would be a duplication of effort so, for example, we might recommend disabling RBL lookups in FirstClass Basic Internet Setup. Every site policy will be different and FirstClass admins should review the *"Managing system security"* chapter in the Internet Services documentation provided in their local FirstClass Admin help folder.

9 Setting up ASSP to work with FirstClass, *Smith, Tom*

Bibliography

1. "Setting up ASSP to work with FirstClass"
   "Advanced Connections" forum, FirstClass Online
   Tom Smith, Park School, Brookline, MA (USA)
   Posted: 20 May 2004
2. Anti-Spam SMTP Proxy
   http://www.asspsmtp.org
   Last visited: 17 January 2007
3. ClamSMTP
   http://memberwebs.com/nielsen/software/clamsmtp/
   Last visited: 5 January 2007
4. ClamXav
   http://www.markallan.co.uk/clamXav/
   Last visited: 8 January 2007
5. Comprehensive Perl Archive Network
   http://www.cpan.org
   Last visited: 5 January 2007
6. OSXFAQ – Using StartupItems in Mac OS X
   http://www.osxfaq.com/Tutorials/LearningCenter/HowTo/Startup/index.ws
   Last visited: 5 January 2007
7. EICAR, European Expert Group for IT-Security
   http://www.eicar.org/
   Last visited: 18 January 2007

Appendix A

This is our sample `assp.cfg` configuration file.

```
AVBytes:=100000
AddConfidenceHeader:=
AddCustomHeader:=
AddIntendedForHeader:=
AddRBLHeader:=1
AddRegexHeader:=
AddSPFHeader:=1
AddScoringHeader:=1
AddSpamHeader:=1
AddSpamProbHeader:=
AddSpamReasonHeader:=1
AsADaemon:=1
AsAService:=
AttachmentError:=500 These attachments are not allowed -- Compress before mailing.
AvClamdBufSize:=512
AvClamdLocal:=
AvClamdPort:=3310
AvError:=500 Mail appears infected with '$infection' -- disinfect and resend.
BadAttachL1:=exe|scr|pif|vb[es]|js|jse|ws[fh]|sh[sb]|lnk|bat|cmd|com|ht[ab]
BadAttachL2:=
BadAttachL3:=zip
BlockExes:=1
BlockNPExes:=0
BlockWLExes:=0
BounceSenders:=postmaster|mailer-daemon
ChangeRoot:=
CleanDelayDBInterval:=3600
ConnectionLog:=
DEBUG:=
DebugSPF:=
DelayAddHeader:=1
DelayEmbargoTime:=5
DelayError:=451 4.7.1 Please try again later
DelayExpireOnSpam:=1
DelayExpiryTime:=36
DelayLog:=
DelayNormalizeVERPs:=1
DelaySL:=
DelayUseNetblocks:=1
DelayWL:=
DelayWaitTime:=28
DoBayesian:=1
DoBombHeaderRe:=1
DoBombRe:=1
DoDomainCheck:=0
DoExtremeNP:=
DoExtremeWL:=
DoFakedLocalHelo:=1
DoFakedNP:=
DoFakedWL:=
DoInvalidFormatHelo:=1
DoInvalidPTR:=0
DoLDAP:=
DoNoSpoofing:=
DoNoValidLocalSender:=0
DoPenalty:=0
DoRBLCache:=1
DoRFC822:=1
DoReversed:=0
DoScriptRe:=1
DoTestRe:=
DoValidFormatHelo:=0
EmailAdminReportsTo:=
EmailErrorsModifyWhite:=1
EmailErrorsReply:=1
```

```
EmailErrorsTo:=
EmailFrom:=<spammaster@yourdomain.com>
EmailHam:=asspnotspam
EmailHelp:=assphelp
EmailInterfaceOk:=1
EmailNoNPRemove:=1
EmailNoWhiteToRed:=
EmailRedlistAdd:=asspred
EmailRedlistRemove:=asspnotred
EmailRedlistReply:=1
EmailRedlistTo:=
EmailSenderOK:=
EmailSpam:=asspspam
EmailVirusReportsTo:=
EmailWhitelistAdd:=asspwhite
EmailWhitelistRemove:=asspnotwhite
EmailWhitelistReply:=1
EmailWhitelistTo:=
EnableDelaying:=
EnableFloatingMenu:=1
EnableHTTPCompression:=1
EnableSRS:=
EnforceAuth:=
ExtremeExpiration:=7
ForceRBLCache:=1
GoodAttach:=doc|xls|ppt|pdf|zip|rtf|txt
GreetingWaitTime:=0
HeaderMaxBytes:=100000
HeloMismatch:=
KeepWhitelistedSpam:=
LDAPFail:=
LDAPFilter:=
LDAPHost:=localhost
LDAPLog:=
LDAPLogin:=
LDAPPassword:=
LDAPRoot:=
LocalAddresses_Flat:=
LocalPolicySPF:=v=spf1 a/24 mx/24 ptr ~all
LogRollDays:=7
MaillogTailBytes:=10000
MaillogTailJump:=
MaillogTailWrapColumn:=80
MaintenanceLog:=
MaxBytes:=4000
MaxErrors:=10
MaxFiles:=18009
MaxWhitelistDays:=90
NoExternalSpamProb:=1
NoHaiku:=
NoMaillog:=
NoRelaying:=530 Relaying not allowed (SPAM)
NoValidRecipient:=550 5.1.1 User unknown
NotGreedyWhitelist:=
OrderedTieHashSize:=5000
OutgoingBufSize:=102400
PenaltyDuration:=60
PenaltyError:=
PenaltyExpiration:=360
PenaltyExtreme:=150
PenaltyLimit:=50
PenaltyLog:=1
PenaltyUseNetblocks:=
PopB4SMTPFile:=
PopB4SMTPMerak:=
RBLCacheRefresh:=24
RBLError:=550 5.7.1 Blacklisted by RBLLISTED
RBLFailLog:=3
RBLLog:=
RBLServiceProvider:=zen.spamhaus.org|combined.njabl.org|list.dsbl.org|
dul.dnsbl.sorbs.net
```

```
RBLUseNetblocks:=
RBLWL:=1
RBLmaxhits:=1
RBLmaxreplies:=3
RBLmaxtime:=10
RBLsocktime:=1
RamSaver:=
RegExLength:=20
RestartEvery:=0
SPFFailLog:=3
SPFLog:=
SPFNP:=1
SPFWL:=1
SPFneutral:=
SPFsoftfail:=
SRSAliasDomain:=thisdomain.com
SRSFailLog:=3
SRSHashLength:=4
SRSSecretKey:=
SRSTimestampMaxAge:=21
SRSValidateBounce:=1
SaveStatsEvery:=5
SenderInvalidError:=554 5.7.7 REASON .
SessionLog:=1
SpamError:=500 Mail appears to be unsolicited -- send error reports to
postmaster@yourdomain.com
SpamVirusLog:=5
UpdateWhitelist:=3600
UseAvClamd:=
UseLocalTime:=1
UseSubjectsAsMaillogNames:=
ValidateLog:=
ValidateRBL:=1
ValidateSPF:=1
ValidateSenderLog:=1
WhitelistLocalFromOnly:=1
WhitelistLocalOnly:=
WhitelistOnly:=
acceptAllMail:=
allowAdminConnectionsFrom:=
asspLog:=1
base:=/Users/fcadmin/assp
baysConfidence:=
baysNonSpamLog:=4
baysSpamLog:=3
baysSpamLovers:=
baysTestMode:=1
baysValencePB:=0
blDomainLog:=3
blSpamLovers:=
blTestMode:=1
blValencePB:=5
blackListedDomains:=
blackRe:=http://[\w\.]+@|\w<[a-z0-9]+[abcdfghjklmnpqrstuvwxyz0-9]{4}[a-z0-9]*>|
subject: [^\n]*     \S
blackValencePB:=5
bombError:=550 Your message was rejected because it appears to be part of a spam
bomb -- .
bombErrorReason:=1
bombHeaderRe:=
bombRe:=IMG [^>]*src=['"]cid|<BODY[^>]*>(<[^>]+>|\n|\r)*<IMG[^>]+>(<[^>]+>|\n|
\r)*</BODY>
bombReNP:=
bombReRelay:=
bombReWL:=
bombSpamLovers:=
bombTestMode:=1
bombValencePB:=5
ccAddresses:=
ccAddressesMode:=
ccArchivAddressesRec:=
```

```
ccArchivModeRec:=1
contentOnlyRe:=
correctednotspam:=errors/notspam
correctedspam:=errors/spam
defaultLocalHost:=
delaySpamLovers:=
delaydb:=delaydb
denySMTPConnectionsFrom:=
denySMTPnoLog:=
denySenderRe:=
dnsbl:=
erValencePB:=5
exportExtremeFile:=
extAttachLog:=5
fhTestMode:=1
fhValencePB:=200
fileLogging:=1
flValencePB:=10
flsTestMode:=1
freqNonSpam:=1
freqSpam:=1
greylist:=greylist
heloBlacklistIgnore:=
hlSpamLovers:=
hlTestMode:=1
hlValencePB:=5
ihTestMode:=1
ihValencePB:=15
ilValencePB:=10
incomingOkMail:=
invalidFormatHeloRe:=\d+[_.-]\d+[_.-]|^[^.]+\.?$|dynamic|ddns|dns\.org$
invalidPTRRe:=^\d+\.\d+\.\d+\.\d+$|^[^\.]+\.?$
irValencePB:=5
isSpamLovers:=
ispgreyvalue:=
ispip:=
ldLDAP:=
ldLDAPFilter:=
listenPort:=25
listenPort2:=
localDomains:=fc1.scout.org|spamreport.gov
localDomainsFile:=
logfile:=maillog.txt
maillogExt:=.eml
maxSMTPSessions:=50
maxSMTPipSessions:=5
meValencePB:=15
mxValencePB:=10
mxaTestMode:=1
myName:=ASSP.nospam
myServerRe:=
mydb:=
myhost:=
mypassword:=
myuser:=
noDelay:=file:nodelay.txt
noLog:=
noProcessing:=
noSRS:=
notspamlog:=notspam
npAttachLog:=5
npRe:=X-FC-MachineGenerated|X-FC-Autoforward
pbSpamLovers:=
pbTestMode:=
pbdb:=pb/pbdb
pidfile:=pid
poTestMode:=
processOnlyAddresses:=
proxyserver:=
ptValencePB:=10
ptrTestMode:=1
```

```
rblSpamLovers:=
rblTestMode:=1
rblValencePB:=100
redRe:=file:redre.txt
redlistdb:=redlist
regexLogging:=1
relayHost:=127.0.0.1:325
relayHostFile:=
relayPort:=127.0.0.1:225
rlValencePB:=15
runAsGroup:=admin
runAsUser:=
saValencePB:=25
sbTestMode:=1
scriptError:=550 Your email contains html scripting code -- please resend as plain
text.
scriptLog:=3
scriptRe:=
scriptTestMode:=1
sendAllSpam:=
sendHamRec:=
sendNoopInfo:=
silent:=
smtpAuthServer:=
smtpDestination:=127.0.0.1:225
smtpIdleTimeout:=999
smtpReportServer:=
spamBombLog:=6
spamBucketLog:=3
spamHeloLog:=6
spamISLog:=6
spamLovers:=postmaster
spamPBLog:=6
spamSubject:=<SPAM?>
spamSubjectCC:=1
spamSubjectSL:=
spamaddresses:=put|your@spambucket.com|addresses|@here.org
spamdb:=spamdb
spamlog:=spam
spamtrapaddresses:=put|your@spamtrap.com|addresses|@here.org
spfSpamLovers:=
spfTestMode:=1
spfValencePB:=0
spfnValencePB:=0
spfsValencePB:=0
srsSpamLovers:=
srsTestMode:=1
stValencePB:=25
subjectLogging:=1
sysLog:=
testRe:=
useHeloBlacklist:=0
validFormatHeloRe:=^(([a-z\d][a-z\d\-]*)?[a-z\d]\.)+[a-z]{2,6}$
vdValencePB:=15
viruslog:=
webAdminPassword:=nospam4me
webAdminPort:=55555
whiteListedDomains:=
whiteRe:=
whitelistdb:=whitelist
wlAttachLog:=5
```

Appendix B

Source code of the files distributed with ASSP_Scripts.tar.gz and required to start ClamSMTP, ClamAV and ASSP automatically on a Mac OS X system.

ASSP_CLAM

```
#!/bin/sh

##
# Start ClamAV, ClamSMTP and ASSP
##

# Modify paths if necessary
CLAMD="/usr/local/clamXav/sbin/clamd"
CLAMSMTP="/usr/local/sbin/clamsmtpd"
ASSP="/Users/fcadmin/assp/"

##
# Do not edit after this line
##

. /etc/rc.common

ConsoleMessage "Starting ClamAV"
$CLAMD

ConsoleMessage "Starting ClamSMTP"
$CLAMSMTP

ConsoleMessage "Starting ASSP"
$ASSP/startassp.sh
```

STARTUPPARAMETERS.PLIST

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
      <key>Description</key>
      <string>ClamAV, ClamSMTP and ASSP</string>
      <key>OrderPreference</key>
      <string>None</string>
      <key>Provides</key>
      <array>
            <string>ASSP_Clam</string>
      </array>
      <key>Requires</key>
      <array>
            <string>Resolver</string>
      </array>
</dict>
</plist>
```

STARTASSP.SH

```
#!/bin/sh

if [ "$1" = "" ]
then
     BASE=/Users/fcadmin/assp
else
     BASE=$1
fi

echo Starting ASSP Anti-SPAM Proxy server in $BASE
trap '' 1
LANG=
export LANG
perl $BASE/assp.pl $BASE
```

STOPASSP.SH

```
#!/bin/sh
if [ "$1" = "" ]
then
    BASE=/Users/fcadmin/assp;
else
    BASE=$1;
fi

export BASE
echo Stopping ASSP Anti-SPAM Proxy server in $BASE
pidfile=$BASE/pid
kill `cat $pidfile`
```