

## Setting Up Sophos + Amavis for Postfix

Protecting a system with an anti-virus software is an important thing for every system administrator. Although there is no real threat from viruses on UNIX, some users may use Windows OS on their home PCs. Most of the users don't care or don't know how to protect themselves against viruses. They don't check their files and mail messages against viruses. Either they might be infected or infect other people on the internet. I felt responsible for protecting my users' emails. I also felt responsible for protecting the Internet against my users spreading infected emails consciously or unconsciously all over the world.

What I am going to offer you in this article is a somewhat tricky installation of Postfix, Amavis and Sophos. It took me some time to finally run this configuration successfully. I am happy I managed that. I want to help other FreeBSD souls to save their time.

In this article I will cover how to install Sophos and Amavis. It will not cover Postfix installation and configuration. I will help you to configure those three programs in a very common way. It is up to you if you want to install amavis-perl or amavisd. From my experience, amavisd is faster than amavis-perl. It runs as a daemon, so on heavily loaded systems this might be crucial.

Sophos installation:

Get the newest possible Sopor Anti-virus program. When paying the licence, you will be posted a new version of this software every month. On the CD, there are two versions of Sophos for FreeBSD. One is called `freebsd.aout.tar` and is for FreeBSD version 2 and older. The other is `freebsd.elf.tar`, which is for FreeBSD version 3 and higher.

If you have recently obtained FreeBSD, then it will certainly be version 3 or above. Check the system version with `uname -v` command.

Copy one of the files to `/tmp`. Untar it with the command:

```
tahoe# cd /tmp
tahoe# tar -xvf freebsd.elf.tar
sav-install/
sav-install/vdl-3.58.dat
sav-install/install.sh
sav-install/Readunix.txt
sav-install/Install.txt
sav-install/icheckd.1
sav-install/icheckd.conf.5
sav-install/sweep.1
sav-install/icheckd
```

```
sav-install/libsavi.so.2.2.03.098
sav-install/sweep
```

Before the installation, create a user and a group called "sweep". Sophos' InterCheck Server, or sweep will be run with the very low privileges of the sweep user. Adding new users is described in FreeBSD Handbook. The entry in /etc/passwd file should look like:

```
sweep*:1005:1005:AMAVIS USER:/home/vscan:/sbin/nologin
and in /etc/group:
sweep*:1005:
```

To install, run the install script.  
tahoe# cd sav-install

If you ever happen to mount /tmp as "noexec", then as root do:  
# mount -u -o exec /tmp

```
tahoe# ./install.sh
Sophos Anti-Virus installation utility [FreeBSD/Intel]
Copyright (c) 1998,2001 Sophos Plc, Oxford, England
```

You have to be root to do this. This will perform a default installation, placing:

- binaries in /usr/local/bin
- the shared library in /usr/local/lib
- the virus data in /usr/local/sav
- manual pages in /usr/local/man

All defaults can be changed, run: ./install.sh -h for details.

To be sure, the files were installed:

```
tahoe# cd /usr/local/bin
tahoe# find . -cmin -5 -print
```

```
./sweep
./icheckd
```

You can check it for every directory listed above.

To update your virus database run this script:

```
#!/bin/sh -
cd /usr/local/sav
#in one line:
/usr/local/bin/wget -q -N ` /usr/local/bin/sweep -v | /usr/bin/grep "Product version" | /usr/bin/sed -e "s/.*:
\(\.\)\.\(\.\)\$ / http://www.sophos.com/downloads/ide/\1\2_ides.zip/"`
/usr/local/bin/unzip -q -n "??_ides.zip"

/bin/chmod 644 *

/usr/bin/logger -f /var/log/messages -t SOPHOS-IDE -p local0.notice UPDATED
#END
```

To save yourself trouble with amavis and amavisd installation and configuration change user-name "sweep" to "vscan" in /etc/passwd and /etc/group.

Amavis-perl installation:

Re-cvsup your ports collection and:

```
tahoe# cd /usr/ports/security/amavis-perl/  
tahoe# make
```

This will fetch the port, check the checksums and dependencies.

Amavis depends on these ports:

arc-5.21e.8\_1; lha-1.14i; p5-Archive-Tar-0.22; p5-Archive-Zip-1.03; p5-Compress-Zlib-1.16; unarj-2.43\_1; unrar-3.00; [zoo-2.10.1](#); p5-Convert-TNEF-0.17; p5-Convert-UUlib-0.213; p5-MIME-Base64-2.12; p5-File-Spec-0.82; p5-IO-stringy-2.108; p5-MIME-Tools-5.411a\_2; p5-Mail-Tools-1.48; [compat3x-i386-4.4.20011227](#); p5-Net-1.11,1; uvscan\_dat-4220; uvscan-4.16e\_1; p5-Unix-Syslog-0.100

Some time ago, there were some problems with p5-Compress-Zlib-1.16 but not anymore. Default port installs also uvscan, an anti-virus. You may use it for free for about a month and then you need to get the license code. I advise not to install uvscan anyway.

I think the easiest way is to let make run for a while, install all the ports amavis depends on and break it with ^C when it starts the configuration process.

This way, you might be sure all ports were installed corectly and flawlessly.

Now go to:

```
tahoe# cd work/amavis-perl-11
```

(You are in /usr/ports/security/amavis-perl/work/amavis-perl-11) and type in one line:

```
tahoe# ./configure --enable-postfix --enable-smtp --with-smtp-port=10025 --with-amavisuser=vscan  
--with-runtime-dir=/home/vscan/amavis --with-logdir=/home/vscan/amavis  
--withvirusdir=/home/vscan/virusmail --with-sophos-ide=/usr/local/sav
```

At the end you should see:

\*\* Configuration summary for amavis perl-11 2001-04-07:

Install amavis as:	/usr/sbin/amavis
Configured for use with:	postfix
Relay configuration:	no
Enable SMTP:	yes
Use SMTP port:	10025
Use virus scanner(s):	McAfee Virusscan Sophos Sweep
Scanner runs as:	vscan
Logging to syslog:	yes
Quarantine directory:	/home/vscan/virusmail
Max. recursion depth:	20
Add X-Virus-Scanned header:	yes
Display AMaViS credits:	no
Warn sender:	yes

Reports sent to: virusalert  
Reports sent by: postmaster

To accept the above, type "make"

```
tahoe# make  
make all-recursive  
Making all in amavis  
Making all in tests
```

The correctly configured amavis might be found in:  
/usr/ports/security/amavis-perl/work/amavis-perl-11/amavis directory. Copy  
/usr/ports/security/amavis-perl/work/amavis-perl-11/amavis/amavis to /usr/local/sbin/amavis.

Now it's time to configure postfix MTA:  
Create an alias "virusalert" pointing at root. See man 5 aliases. Edit main.cf located in  
/usr/local/etc/postfix and at the end of this file add a line:

```
content_filter = vscan:
```

Save and quit.

Edit master.cf, it is in the same place where main.cf, and add:

```
vscan unix - n n - 10 pipe  
user=vscan argv=/usr/local/sbin/amavis ${sender} ${recipient}  
localhost:10025 inet n - n - - smtpd  
-o content_filter=
```

The only thing left is to run postfix reload and test the configuration.

Everything should be working fine. See headers of your test message. It should contain a line:  
"X-Virus-Scanned: by AMaViS perl-11".

Amavisd installation:

```
tahoe# cd /usr/ports/security/amavisd  
tahoe# make  
Break it as before with ^C;
```

```
tahoe# cd work/amavisd-snapshot-20020531
```

and run the configure with parameters given above. The configuration script should end with a message:

```
** Configuration summary for amavisd snapshot-20020531 2002-05-31:  
Install amavis daemon as: /usr/sbin/amavisd  
Install amavis client as: /usr/sbin/amavis  
Daemon config file: /etc/amavisd.conf  
Path to socket: /home/vscan/amavis/amavisd.sock  
Configured for use with: postfix
```

Configuration type:	SMTP
Use virus scanner(s):	McAfee Virusscan Sophos Sweep
Scanner runs as:	vscan
Logging to syslog:	yes
Run-time directory:	/home/vscan/amavis
Warn sender:	yes
Warn recipient(s):	no
Notify admin:	yes

To accept the above, type "make"

```
tahoe# make
tahoe# cd amavis
(Now you are in /usr/ports/security/amavisd/work/amavisd-snapshot-20020531/amavis
directory)
tahoe# cp amavis amavisd /usr/sbin
tahoe# cp amavisd.conf /etc/
tahoe# cp ../amavisd.sh /usr/local/etc/rc.d
```

As with amavis-perl, create "virusalert" alias; add content\_filter = vscan: to main.cf postfix file; and to master.cf add

```
vscan unix - n n - 10 pipe flags=q user=vscan
  argv=/usr/sbin/amavis ${sender} ${recipient}
localhost:10025 inet n - n - - smtpd
  -o content_filter=
```

Amavisd requires a configuration file, /etc/amavisd.conf. Read this file and change what is appropriate for you.

Amavisd is run as user vscan. To make it work correctly change sweep's user shell from /sbin/nologin to /bin/sh.

Start amavisd and reload postfix with commands:

```
tahoe# /usr/local/etc/rc.d/amamvisd.sh start
tahoe# /usr/local/etc/rc.d/postfix.sh reload
```

Both amavisd and Postfix should be working fine. Check it with ps.

```
tahoe# ps -auxw | grep amavis
vscan 28039 0.0 0.0 8592 0 ?? IWs - 0:00.00 /usr/bin/perl -T /usr/sbin/amavisd
```

In both configurations (Sophos – Amavis-perl, or Sophos – Amavisd) every message entering or leaving the system is scanned against viruses. If a virus is found an error message is generated and sent to the originator of the email. A copy of the error message is also sent to virusalert alias which in our case points to root mailbox. This way virus senders and abusers might be traced and their activity blocked. Remember to update Sophos' virus database on a daily basis or even often.

I hope all BSD users will find this article useful and helpful. Happy anti-virus scanning!