

## Re: Antispam solutions

**Source:** <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/isp/2005-04/0036.html>

---

**From:** George Georgalis ([george\\_at\\_galis.org](mailto:george_at_galis.org))

**Date:** 04/06/05

Date: Tue, 5 Apr 2005 23:58:01 -0400

To: [freebsd-isp@freebsd.org](mailto:freebsd-isp@freebsd.org)

On Tue, Apr 05, 2005 at 11:00:16AM -0500, Phillip Salzman wrote:

>

>So - my question is what some of you were using for ISP-based antispam, and

>do you know of a user-manageable quarantine for SA? We have roughly 90k

>users and 11k domains.

>

The following system works well for me. Use QMAILQUEUE patch and the following program to queue mail from tcpserver (which has lots of whitelisted subnets from trusted/prefiltered domains). Since you want per user quarantine, I would suggest rather than 'maildir "\${scq}" ...' you extract RCPT from env and qmail-inject it with an envelope from quarantine@you.com, and whitelist that delivery IP.

\* anything that your SA processes as ham will be handed to qmail-queue during smtp, with status returned to sending smtp

\* anything that your SA processes as spam will be rejected in smtp but still delivered to rcpt in a way that they can filter it with their client and that will prevent spam with wrong addressed from being returned to forged from

I've been thinking about extending my system the way you describe for a while, just not done it yet. the script below has worked very well for nearly a year, multiple concurrent mx work fine, and with that many clients you will probably want a spamd cluster network.

(The sleep commands are very effective for emergency throttling of spamd)

```
#!/bin/bash
# exit 31 = permanently refuse
# exit 71 = temporarily refusee
# pwd is /var/qmail
echo $0 # for the logs
scq="spamc-queue" # a maildir with qmaild write perms
tmp="${scq}/safecat "${scq}/tmp" "${scq}" </dev/stdin` \
    || { echo "Error $?"; exit 71; } # put the pipeline to disk, if possible
```

## freebsd-isp: Re: Antispam solutions

```
# ${scq}/tmp is a temp for this function ${scq} is temp for this program
score=`spamc -x -c <"$tmp"` # score it with spamd
sce=$?
echo $score # for the logs
case $sce in
0) # ham
    sleep 0 # if system starts swapping, reduce incoming concurrency, and add 20 seconds
    host=`cat control/me`
    formail -f -A "X-spamc: ${score} by ${host}; `date -R`" \
        | bin/qmail-queue # mark it and pass to the regular queue
    qqe=$?
    rm "$tmp"
    exit $qqe # return whatever qmail-queue exits as
;;
1) # spam
    sleep 0 # if system starts swapping, reduce incoming concurrency, and add 20 seconds
    maildir "${scq}" >/dev/null <"$tmp" # save it to verify no falseys
    rm "$tmp"
    exit 31
;;
*) # spamc error,
    echo "$0 error, spamc exit $sce"
    exit 71
esac
exit 81 # Internal bug

my /service/spamd/run

#!/bin/sh
exec spamd -i -A 127.0.0.0/8,10.0.0.0/8,192.168.0.0/16 -m ${MAX} --username=qmaild --syslog=stderr
2>&1

// George

--
George Georgalis, systems architect, administrator Linux BSD IXOYE
http://galis.org/george/ cell:646-331-2027 mailto:george@galis.org

-----
freebsd-isp@freebsd.org mailing list
http://lists.freebsd.org/mailman/listinfo/freebsd-isp
To unsubscribe, send any mail to "freebsd-isp-unsubscribe@freebsd.org"
```