policyd-weight and some unorthodox approaches to eliminating spam

Ralf Hildebrandt

T-System Business Services

LinuxForum 2007
Copenhagen, 03. March 2007

policyd-weight by Robert Felber

- Perl policy daemon for the Postfix MTA (2.1 and later)
- intended to eliminate forged envelope senders and HELOs (e.g. in bogus mails)
- runs before any queueing is done
- score based on RBLs, RHSBLs, HELO, MAIL FROM and client IP address
- it allows you to REJECT messages which have a score higher than allowed
- it caches the most frequent client/sender combinations to reduce the number of DNS queries

Why, Chandler, why?

Postfix' built-in checks can be too tough for poorly configured clients:

- one hit, and the mail gets rejected.

Fairness

policyd-weight is designed to be fair:

- DynDNS MX users get through if their MTA is setup properly, even if their ISP net is listed in a DUL . . .
- . . . because its decisions whether to reject or accept a mail is based on **multiple** factors.

Running it

- Check the defaults:

```
/path/to/policyd-weight defaults
```

- Review config:

```
$EDITOR /path/to/policyd-weight.conf
```

- Start it:

```
/path/to/policyd-weight start
```

Make Postfix use it

```
smtpd_recipient_restrictions =
   permit_mynetworks,
   reject_unauth_destination,
   ... whitelists ...
   check_policy_service inet:127.0.0.1:12525
```

Checking the logs

```
Mar  2 22:32:01 outpost postfix/smtpd[29339]: NOQUEUE:
reject: RCPT from unknown[41.251.65.17]: 550 5.7.1
<floppy@floppy.org>: Recipient address rejected: Mail
appeared to be SPAM or forged. Ask your Mail/DNS-Administrator
to correct HELO and DNS MX settings or to get removed from
DNSBLs; MTA helo: 41.251.65.17, MTA hostname:
unknown[41.251.65.17] (helo/hostname mismatch);
from=<floppy@floppy.org> to=<floppy@floppy.org> proto=ESMTP
helo=<41.251.65.17>
```

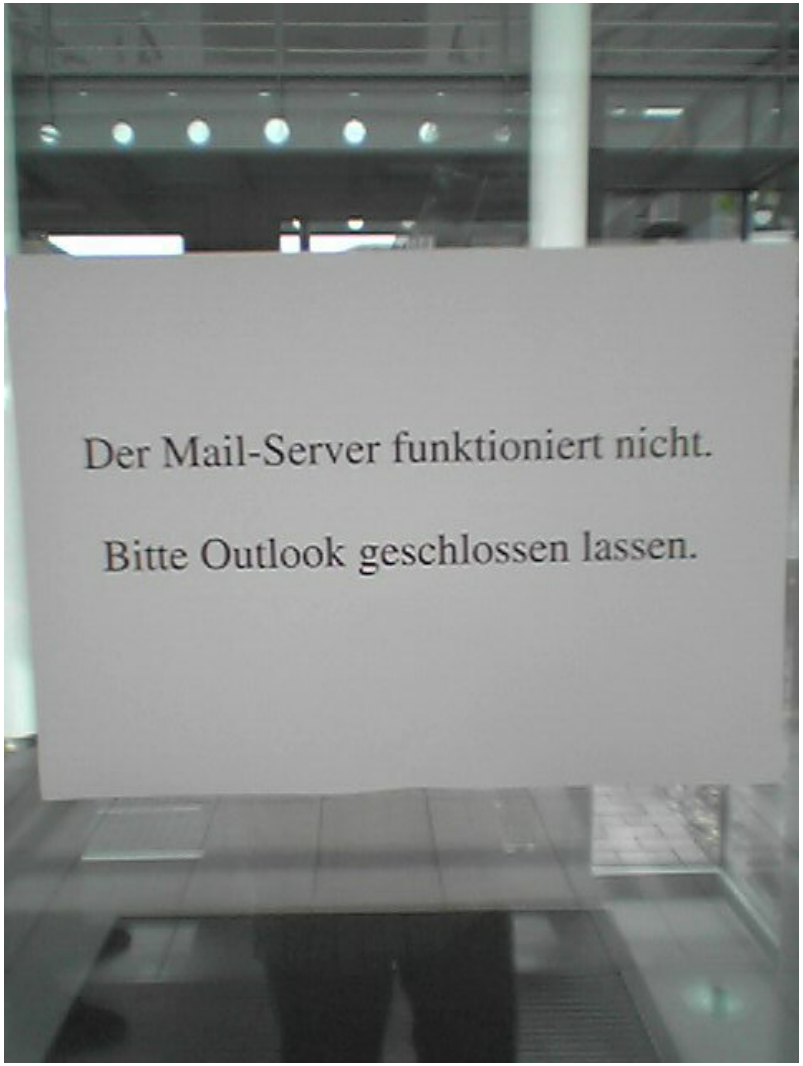
Trust no-one

```
$ host 41.251.65.17
Host 17.65.251.41.in-addr.arpa not found: 3(NXDOMAIN)
```

That IP is listed in:

- BLARS
- NJABL
- PSBL
- dnsbl-2.uceprotect.net

Unorthodox methods



“The mail server is not working. Keep Outlook closed.”

Try to see the bright side:

- No spam!
- No false positives either!!

- activate opportunistic STARTTLS encryption (`smtpd_use_tls = yes`)
- watch the amount of legitimate mail decrease

But why is that?

Some servers want to use `STARTTLS`...

. . .

but can't, since. . .

. . .

the admin forgot to install a x.509 certificate!

STUPID!

It works the other way round as well!

You can't send mail there since your server wants to use `STARTTLS` but can't, since...

. . .

the other admin forgot to install a x.509 certificate

STUPID!

Which braindead software allows the use of `STARTTLS` without a x.509 certificate?

It was a patched qmail installation.

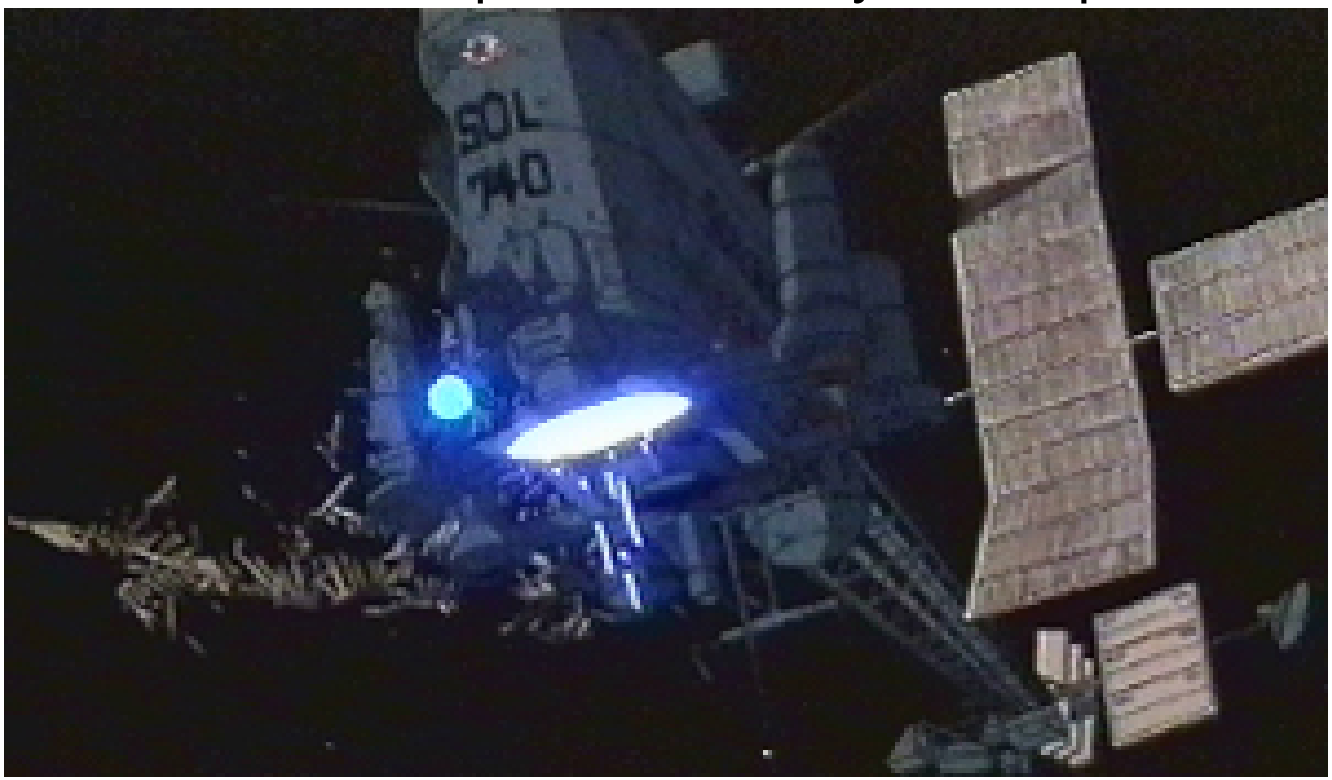
I've got the perfect system. I never need to do maintenance on it, or software upgrades, patches, or anything. It's great. It never wakes me up, spammed, or gets hacked into.
It's completely perfect.
That was the first step in my plan to build the perfect Postfix system.

The second step is to plug it in.

The appliance

Satellite Orbital Laser

Use GeoIP to find the origin of the spam, then nuke the site from orbit. The Japanese military will help – if asked nicely!



Everybody has these problems