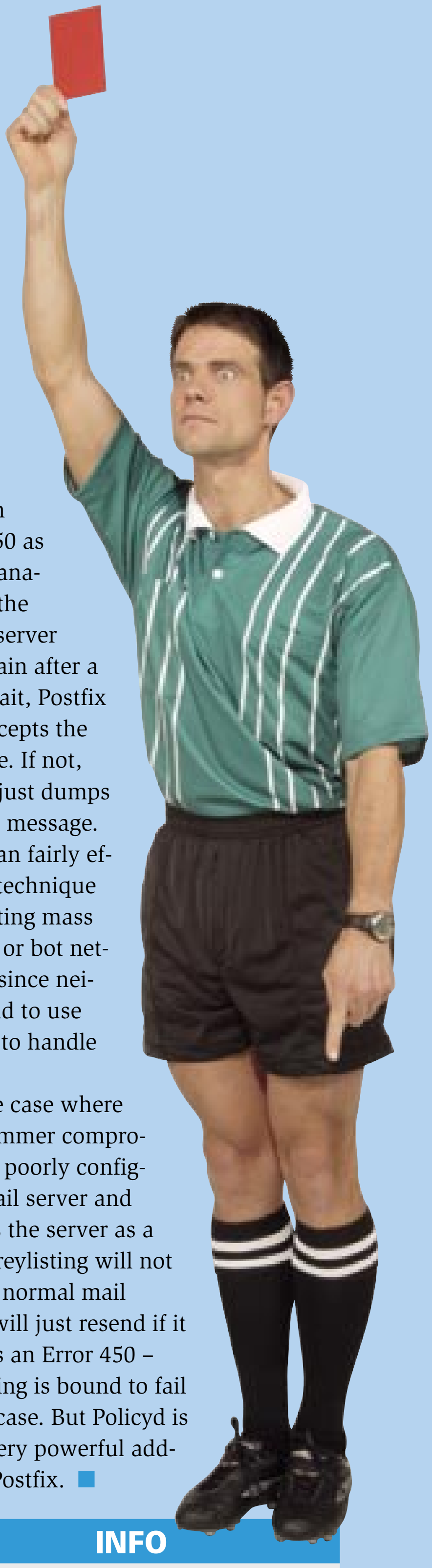

The Sysadmin's Daily Grind: Policyd

TURNED DOWN!

The Postfix Policyd plugin fights spam using techniques such as greylisting, source detection, volume measurements, blacklisting, and HELO rotation detection. **BY CHARLY KÜHNAST**

I've added many bits and bobs to my tried and trusted Postfix in the course of the years – Spamassassin and virus filters, for example. The latest member in the exclusive club of Postfix add-ons is Policyd. The Policyd tool does not use the *content_filter* mechanism to integrate with Postfix, in contrast to many other external tools. Instead, Policyd prefers the *check_policy_service*, which is available in Postfix 2.2 or newer.

This gives me the ability to slot Policyd into my existing ruleset at a location that makes sense. I don't need to send spam that has been rejected for other reasons to the policy daemon. The current release of the Policyd C program is version 1.73. You can download Policyd from [1], and installing the daemon is easy. After unpacking, just enter

```
gmake build
gmake install
```

in the *policyd* directory. MySQL is also required. Policyd gives you a SQL script that automatically creates the required tables. To finish off, you need to create a cron job:

```
0 * * * * /usr/local/policyd↲
/cleanup -c /usr/local/policyd↲
/policyd.conf
```

The job periodically removes obsolete entries from the database. The configuration file lets you enable or disable the various checks that Policyd performs on an individual basis. I find some of these checks quite useful.

HELO Randomization Prevention

Spammers almost always spoof the server identification in the *HELO* command, whereas legitimate MTA hosts send their FQDN. To keep off HELO blacklists, spammers tend to send mail with different HELO information. To combat this sneaky tactic, Policyd can reject messages that come from the same IP address but with different HELOs.

Of course, Policyd supports the HELO blacklists I just mentioned. There is one special rule that you might appreciate: if a mailer sends me the FQDN of *my own* server, I immediately slam the door in their face.

Sender Throttling

Policyd can prevent the same sender flooding a mail server with a large volume of messages. The From address or its domain part, the SASL username, or the IP address or network block are all useful detection criteria. And the number of messages or total size, whichever threshold comes first, are useful delimiting criteria.

Recipient Throttling

Policyd can prevent a user from receiving more than a specified number of messages within a certain period of time. Limits of this kind are useful in situations where you are dealing with generic addresses such as *info@doma.in* or *support@doma.in*.

Greylisting

If you enable greylisting, Postfix will first temporarily reject incoming mail and issue an Error 450 as an explanation. If the source server tries again after a short wait, Postfix then accepts the message. If not, Postfix just dumps the first message. This is an fairly effective technique for fighting mass mailers or bot networks, since neither tend to use queues to handle errors.

In the case where the spammer compromises a poorly configured mail server and exploits the server as a relay, greylisting will not help. A normal mail server will just resend if it receives an Error 450 – greylisting is bound to fail in that case. But Policyd is still a very powerful add-on for Postfix. ■

INFO

[1] Policyd: *http://policyd.sourceforge.net*

THE AUTHOR

Charly Kühnast is a Unix System Manager at the data-center in Moers, near Germany's famous River Rhine. His tasks include ensuring firewall security and availability and taking care of the DMZ (demilitarized zone).

SYSADMIN