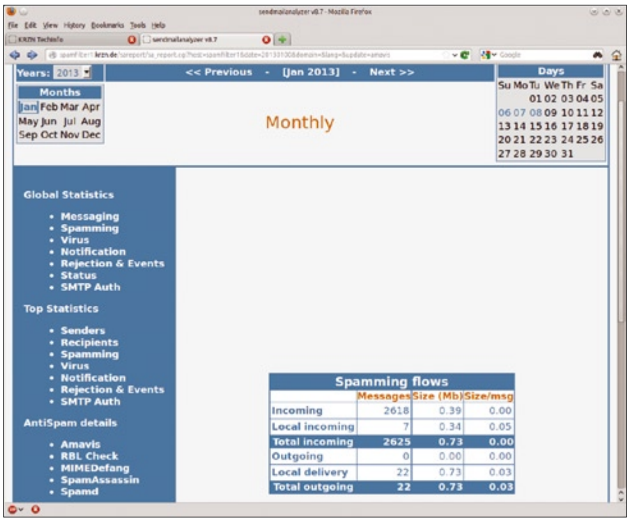
The sys admin's daily grind: SendmailAnalyzer

Troop Visit

During the ongoing battle against spam, admins should inspect their troop's battle lines from time to time. If you don't relish the thought of counting the dinnerware, you can use the services of a logfile inspector like SendmailAnalyzer, which works surprisingly well with Postfix and the like. *By Charly Kühnast*

I ran Sendmail 8.7 on the first mail server I operated for a large group of users, and it was hate at first sight. I kept up this War of the Roses until 8.9.0 and later moved to Postfix. In the years that followed, I lost track of the Sendmail Server Analyzer [1]. It was not until I read a small post online that I understood that SendmailAnalyzer also can evaluate Postfix logs and messages from Amavisd-new, ClamAV, SpamAssassin, Postgrey, and other MTA appendages. High time to try out the tool.

SendmailAnalyzer comes as a sleek `tar.gz` package and relies on the existence of Perl and the GD libraries. After the install, you need to set up a cronjob to take care of data caching. The analyzer itself can run in the foreground or as a system service; the developers have kindly included start/stop scripts to match. The configuration is handled in the `sendmailanalyzer.conf` file, although command-line parameters are also possible. The most important setting is right at the top of the configuration file:



Spamming flows

	Messages	Size (Mb)	Size/msg
Incoming	2618	0.39	0.00
Local incoming	7	0.34	0.05
Total incoming	2625	0.73	0.00
Outgoing	0	0.00	0.00
Local delivery	22	0.73	0.03
Total outgoing	22	0.73	0.03

Figure 1: Three days are all it takes to return intermediate results in Charly's battle against spam with SendmailAnalyzer.

```
LOG_FILE       /var/log/mail.log
```

A little lower down is the switch for debug mode. I enabled it during the trial period:

```
DEBUG          1
```

but you really only want to do it then, because verbose is definitely understated.

Facilitating the Work

If you use Postfix exclusively, as I do, you will want to truncate the `MTA_NAME` parameter to reflect the task in hand:

```
MTA_NAME      postfix
```

SendmailAnalyzer uses this parameter as a search term for crawling through logfiles, and I don't want to make the task more difficult than necessary – on good spam harvesting days, my spam filter logs seven- to eight-digit figures. For the same reason, I truncated the `SPAM_TOOLS` line to reflect the anti-spam tools that I actually use:

```
SPAM_TOOLS    dnsbl,amavis,spamd
```

The analyzer presents its results in HTML and needs a web server to do so. SendmailAnalyzer comes with a sample configuration for Apache and typically needs very little modification.

On my lab anti-spam filter, which has a quite low spam count of about 50 spam mails per minute, the results were as shown in Figure 1. SendmailAnalyzer shows the results in tabular and bar graph format. You can quickly see how effective individual anti-spam measures are, and you can look forward to several top 25 lists (most frequent spam target, most common source, and so on). Besides the results, the most important thing for me is that SendmailAnalyzer does its job without significantly burdening the system – the anti-spam filters have enough to do as it is. ■■■

INFO

[1] SendmailAnalyzer: *http://sareport.darold.net*

CHARLY KÜHNAST

Charly Kühnast is a Unix operating system administrator at the Data Center in Moers, Germany. His tasks include firewall and DMZ security and availability. He divides his leisure time into hot, wet, and eastern sectors, where he enjoys cooking, freshwater aquariums, and learning Japanese, respectively.