The Sysadmin's Daily Grind: Postfilter

THE GOOD NEWS

If protocols were human beings, NNTP would be a kind and slightly confused person that always believes the best of other people – even if they drop trash in the mailbox. Postfilter gives NNTP a watchdog.

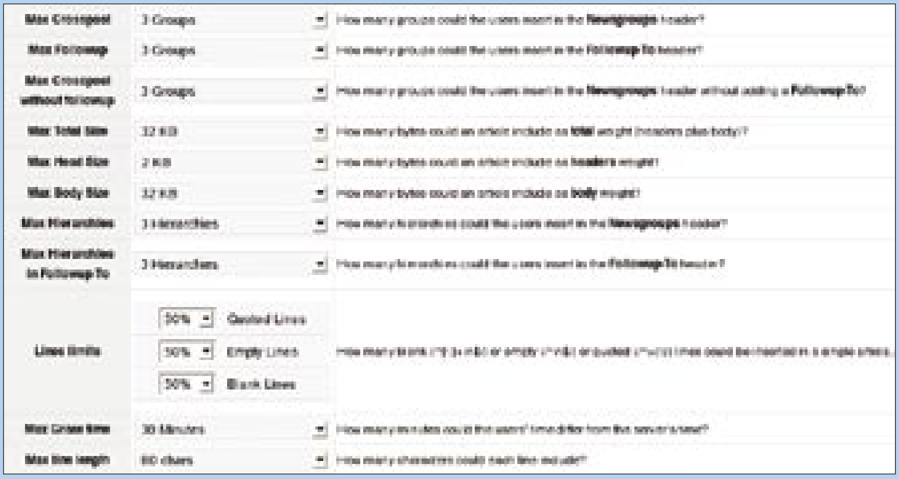
BY CHARLY KÜHNAST

Network News Transfer Protocol (NNTP) has been written off many times, but Usenet will probably still be around when the last Web 2.0 forum bites the dust. This wouldn't be such a bad thing if the protocol had some kind of protection mechanisms. As things stand, people on Usenet tend to misbehave. As an admin, I once infuriated the Usenet community (*abuse@kuehnast.com: Mailbox full*), and then the disbelief of the offender: "Wadya mean crossposting is bad?" Postfilter adds spam and abuse protection to your server. I won't go into the installation steps here, as the homepage [1] has a fantastic guide.

Postfilter directs posts from my users through a configurable ruleset, giving me the ability to filter bad words Spamassassin-style. Matches are scored, and the server blocks the post at a certain threshold. This said, restricting crossposting is more useful in production scenarios. The *max_crosspost* variable in *postfilter.conf* defines the number of newsgroups an article can be posted in – assuming the user sets follow-ups. The default of *10* is far too high in my opinion. Without follow-up, the value in *max_fup_no_crsspt* applies. The default of *3* here is better, but I have set this to *1* just to be on the safe side.

You can restrict the size of a post; *max_total_size* is set to 32 kbytes by default – this is generous, unless one of your users is a best-selling author. For more granular control, you can set the header and body sizes separately.

Long quotes, posts that mainly comprise the effusions of previous contributors, are a constant irritation in newsgroups. Postfilters response to this lazy behavior is *max_quoted_ratio*. The variable accepts values between *0.0* and *1.0*. Setting a value of *0.7* means a maximum of 70 percent of the post can be quotes.



Max Crosspost	3 Groups	How many groups could the users insert in the Newsgroups header?
Max Followup	3 Groups	How many groups could the users insert in the Followup-To header?
Max Crosspost without followup	3 Groups	How many groups could the users insert in the Newsgroups header without adding a Followup-To?
Max Total Size	32 KB	How many bytes could an article include as total weight (headers plus body)?
Max Head Size	2 KB	How many bytes could an article include as headers weight?
Max Body Size	32 KB	How many bytes could an article include as body weight?
Max Hierarchies	3 Hierarchies	How many hierarchies could the users insert in the Newsgroups header?
Max Hierarchies in Followup-To	3 Hierarchies	How many hierarchies could the users insert in the Followup-To header?
Lines limits	50% Quoted Lines 50% Empty Lines 50% Blank Lines	How many blank [illegible] or empty [illegible] or quoted [illegible] lines could be inserted in a single article
Max Grace time	30 Minutes	How many minutes could the users' time differ from the server's one?
Max line length	80 chars	How many characters could each line include?

Figure 1: If you are allergic to vi, the Web gives you limited options for pointing and clicking to create a Postfilter configuration.

Is That the Time?

While these restrictions are mainly designed to prevent my users from making fools of themselves, there are other parameters that give you protection against spammers, and rogue or just badly configured clients. First, look at the time and date: spammers tend to use a future date in the header to get to the top of the unread message list. Postfilter has a *max_grace_time* variable that denies posts with times that disagree with the server time. The default is 1800 seconds, that is, half an hour.

Of course, you can exercise more granular control over posting frequencies. In fact, you can specify how many messages, and the size in bytes, candidates allowed to post over a specific period of time sorted by user, domain, or IP address, and how many errors they are allowed to produce in the process before Postfilter shuts them down. *allow_control_cancel* isn't bad either; it allows or denies cancel messages.

Conclusions

Provided you don't overdo the limits, admins can avoid trouble and keep the exothermic Usenet mob at bay. After all, believing in people doesn't have to be a bad thing. ■

INFO

[1] Postfilter: *http://news.aioe.org/spip.php?rubrique24*

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).