OtherTricks

Other Trick For Blocking Spam

This section is for other tricks to block spam that may or may not directly relate to SpamAssassin.

Fake MX Records

Fake MX records can work like greylisting and often much faster. It doesn't require the installation of new software. What you do is add a fake highest and lowest MX record. Normal email will probably retry but spammers often don't. This is especially true of virus infected windows zombie spam. Here's an example MX configuration.

```
fake0.example.com   10
realmx.example.com  20
fake1.example.com   30
```

The fake records should ultimately resolve to real IP addresses with port 25 closed. **On the lowest numbered MX, not resolving to a real IP address with port 25 CLOSED will cause serious interoperability problems with QMail**, which will never move up to the next MX record. If you it point at an unused or unreachable IP to which connection will simply time out, you may cause substantially longer delays than if the connection fails "hard." Pointing the MX to a name that has no A record or an A record that resolves to a generally unreachable IP (e.g., link-local, RFC1918 private, TEST-NET, etc.) can also cause problems with your mail's deliverability, as some sites test for such bogus MX records.

Fake Lowest MX

The reason for the fake lowest MX record is that where most email is delivered. Real servers will get the error and retry the middle MX and deliver the email with only a few seconds delay. Zombie spam will just move on to the next victim. No good email is lost but a huge amount of spam never makes it into the system at all. This not only reduces spam but also reduces system load as SA doesn't have to process any of this.

Fake Highest MX

Email is supposed to be sent to the lowest numbered MX record first with the higher MX records being backup servers. Spammers often with try the highest MX record first thinking that the backup servers have less spam filtering than the main email server. They try the highest MX record and then never come back. So I set my highest MX record to point to an IP address that always returns a temporary "Come Back Later" error.

A real email server will retry and get through. But the spammer will just go away. This trick saves having to process several million messages a day on my servers at JunkEmailFilter.com.

Optionally you can add a lot of fake MX records on the top side. Additional fake MX records on the lowest numbers end will cause some additional delay, but on the high end there's no penalty. The reason for additional higher MX records is if spammers start trying random MX records then this give them more dead MX records to try.

```
fake0.example.com   10
realmx.example.com  20
fake1.example.com   30
fake2.example.com   40
fake3.example.com   50
fake4.example.com   60
fake5.example.com   70
```

I (Marc Perkel/Junk Email Filter) have now been using this technique for almost 2 years now without any problems. I am now harvesting the data and developing black lists based on hosts that connect ONLY to the highest numbered MX records and do not close the connection with the QUIT command after receiving a 4xx error. The blacklist has grown to over a million entries. The block list is public using our hostkarma list. Go to http://wiki.junkemailfilter.com/index.php/Spam_DNS_Lists fo SA rules to use this list.

Help Junk Email Filter Build a Blacklist

If you want to get rid of some spam using fake high MX records and you want to help us (us being junkemailfilter.com) build a blacklist then you can use our host (tarbaby.junkemailfilter.com) for your fake MX record. We will return a 451 error after the DATA command. This blacklist will help us and everyone using our blacklist to track virus infected spambots. And you are welcome to use our blacklists to further reduce spam. Your MX records can be as simple as this:

```
mail.yourdomain.com  10
tarbaby.junkemailfilter.com 20
```

Detail can be found at Project Tarbaby. ***NOTE WELL:*** Pointing MX records to systems which you do not control carries a risk of legitimate mail being lost and/or leaked to a 3rd party.

Greylisting

Instead of a 2nd fake MX you can use greylisting, which returns a temporary "Come Back Later" error for users currently not known. It has the advantage of helping you on the primary MX directly, and rejects about 60% of the connections here. This is because spammers only try to send once, and if there is an error, they drop it. Real mail servers retry later.

A disadvantage could be that e-mail is delayed a bit, as some users seem to demand that e-mail arrives immediately, and cannot wait some minutes. Either you can tell your users to wait, and save lots of SPAM, or don't use greylisting *g*.

Very good greylist server for postfix are:
postgrey: http://isg.ee.ethz.ch/tools/postgrey/ (uses DB style files, easy to configure, good support) sqlgrey: http://sqlgrey.sourceforge.net/ (uses SQL databases)

exim: Marc Merlin wrote exim-sa, running SA during smtp time. With adaptive greylisting:

- mails with a low spam score are accepted without delay
- mails with an average spam score are greylisted, and only those are delayed
- mails with high spam scores are rejected regardless (no greylisting)

http://marc.merlins.org/linux/exim/sa.html

milter-greylist (http://hcpnet.free.fr/milter-greylist/) is an excellent greylisting solution for Sendmail. I've been using it for almost two years now, and the difference in the amount of mail SpamAssassin has to worry about is amazing.

Long delay (high latency)

I've seen that after changing my mail system from an old 486 with a very slow Internet connection (about 80 ms) to a fast server with just 5 to 10 ms, I got much much more spammail. Obviously spammers don't have much time to deliver one single mail. So it might help for a server which receives just some mails a day (maybe less than 200 a day) to increment the delay. I've seen no way to do this with iptables or ipfilter but maybe someone has an idea for this. – Rolf Winterscheidt

FYI: CommuniGate Pro and many others already have this implemented now. It is usualy called SMTP Prompt Delay. This delays an SMTP Prompt for a given time and in case a spammer connects to your server before it sent out the HELO prompt, all data received is dropped on the floor. We found this reduces a whole lot of spam as it effectively slows down their delivery. Any delay below 30 seems to work fine. Delays >=30 Seconds cause lots of problems with different ISPs which would then not be able to deliver mail to you. (Stefan Seiz)

qmail: Jon Lewis wrote smtp-delay; banner-delay code for the qmail MTA, with whitelisting capabilities among other extremely useful features... http://www.lewis.org/smtp-delay/ (Jeremy Eder)

exim: Marc Merlin wrote exim-sa, running SA during smtp time. With adjustable teergrubing. IMHO Exim + exim-sa offer the most sophisticated Spam controll any MTA has to offer... http://marc.merlins.org/linux/exim/sa.html

sendmail Sendmail already has a built in feature to enable delays, it is called greet_pause and you could add this line to your sendmail.mc config file to enable a 5 second delay:

```
FEATURE(`greet_pause', `5000')
```

postfix Add "sleep <number>" at begining smtpd_client_restrictions in main.cf:

```
...
# Sleep 5 seconds for each opening session
smtpd_client_restriction = sleep 5, <other restrictions>
...
```

Policy Daemons

Some MTAs such as postfix 2.1 and later can delegate a spam/ham decision to a policy server at any stage, i.e. before DATA or after. Before DATA, i.e. at RCPT TO stage has advances in such, that multirecipient mail remains intact and that it is possible to let the user decide whether or not to use the policy daemon. One example with greylisting, throttling, etc pp would be policyd: http://policyd.sourceforge.net/ another example, which acts like a mini-SpamAssassin but before the content has been received (i.e. at RCPT TO stage) would be policyd-weight: http://www.policyd-weight.org/. Both can drastically reduce your bandwidth and CPU-Cycles and other MTA resources.

Whois Records

There already exists a plugin to create rules based on country of origin, but this can be a rather blunt tool. http://linuxbox.co.uk/ip-address-whois-database.php contains a (freely available) CSV file mapping netblocks to owner/country. This makes it easy to, for example, match all dialup users from a particular country, all IP blocks belonging to a particular country etc. You can then either score these with Spamassassin, or add them to your firewall.

See Also

Experimental and Theoretical ideas for getting rid of spam.