Spamfilter Relay Mailserver

Mark McSweeney

CentraLUG, February 1, 2010

Overview

- Scope
- Little bit about me
- Why I built the spamfilter
- Deployment environment
- Spamfilter details
- Tuning and maintainance
- Other resources

Scope

- Explanation of how and why I did this
- Show all software packages used
- Point towards resources to learn more

A little about me

- Compliance Test engineer @ Compliance Worldwide
- 9 ½ years USAF installing CO and microwave relay stations
- Started tinkering w/ Linux ~ 2001
- Not a professional Linux engineer
- No formal CS background/education

Why I built spamfilter

- I personally was getting > 500 spam mails /day
- Probably > 2000 to entire company
- Tried anti-spam plugins – not very effective
- Commercial solutions very expensive
- Couldn't find anything viable for our Exchange Server

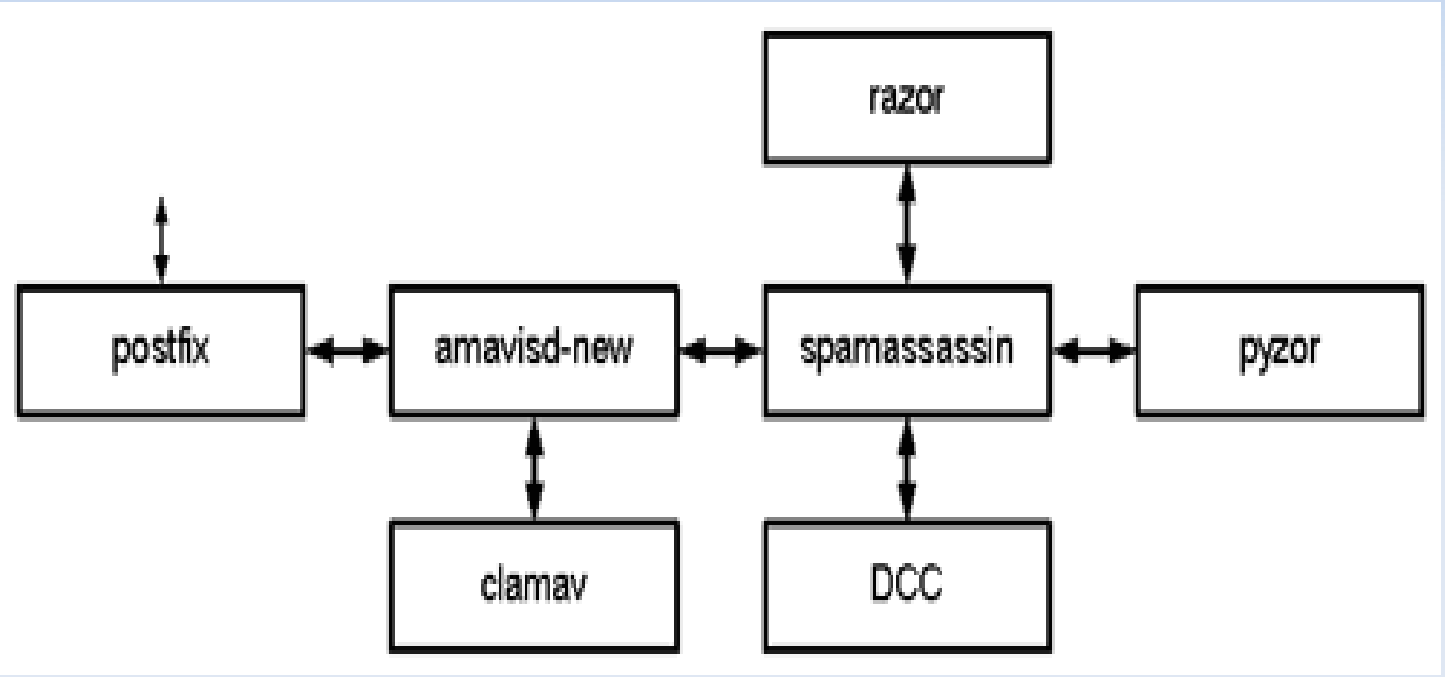
Deployment environment

- Initially 100% MS in back office
- Windows NT Server
- MS Exchange
- Clients – MS Outlook
- Suggested minimum Pentium II 450 MHz w/ 512 Mbit RAM
- My setup Pentium II 350 w/ 256 Mbit RAM

Overview of spamfilter

- Found it initially through site written by Scott Henderson
- Built on RH 9.0
- Scott stopped maintaining document ~ 2008
- freespamfilter.org started to continue project
- Contains initial RH build as well as Debian, FreeBSD, OpenBSD, Gentoo, Fedora builds
- I use the Debian build

Overview of spamfilter



Software Packages

- Postfix
- Amavisd-new
- SpamAssassin
- Razor
- DCC
- Pyzor
- ClamAV

Postfix

- Mailer written by Wietse Venema that started life at IBM research as an alternative to the widely-used but difficult to configure Sendmail program.
- Key files are master.cf and main.cf
- A lot of values stored in lookup tables that are turned into hash tables using command: *postmap foo*
- Many settings stop mail from being accepted ”at the front door”

Amavisd-new

- amavisd-new is a high-performance interface between mailer and content checkers: virus scanners, and/or SpamAssassin.
- Settings used in online document are what might be used at small business (perfect for me).
- Many more settings that scale highly for larger deployments

SpamAssassin

- Apache project
- Assigns a score to each email depending on how ”spammy” it calculates it to be.
- Called by amavisd-new
- Querys DCC, Pyzor, Razor servers to score mail
- Also queries real time blacklists (RBLs)

Pyzor

- Collaborative, networked system to detect and block spam using digests of messages.
- Pyzor queries similar to DNS requests - uses UDP port 24441

Razor

- Distributed, collaborative, spam detection and filtering network.
- Through user contribution, Razor establishes a distributed and constantly updating catalogue of spam in propagation that is consulted by email clients to filter out known spam.
- Detection is done with statistical and randomized signatures
- User input is validated through reputation assignments based on consensus on report and revoke assertions which in turn is used for computing confidence values associated with individual signatures.

DCC

- Distributed Checksum Clearinghouse
- The basic logic in DCC is that most spam mails are sent to many recipients. The same message body appearing many times is therefore bulk email.
- DCC identifies bulk email by taking a checksum and sending that checksum to a Clearinghouse (server).
- Server responds with the number of times it has received that checksum. An individual email will create a score of 1 each time it is processed.
- Bulk mail can be identified because the response number is high.
- Content is not examined.
- Uses UDP protocol and uses little bandwidth.

ClamAV

- Cross-platform antivirus software tool-kit capable of detecting many types of malicious software, including viruses.
- Used as a server-side email virus scanner.
- Owned by Sourcefire, maker of Snort

Maintainance and Tuning

- ClamAV lets you know when new versions are available in /var/log/clamav/freshclam.log
- Since Postfix is run in a chroot jail it will complain about files differing. When this happens, we need to run a script that is supplied with the Postfix source code (called LINUX2) that will once again copy all the files that Postfix needs to where it needs them.

Maintainance and Tuning (more)

- Postfix has sections dealing with whitelisting and blacklisting.
- Amavisd also has sections dealing with whitelisting and blacklisting.
- Several scripts for updating, log checking, intrusion detection, etc.

Resources

- www.freespamfilter.org
- www.postfix.org
- http://razor.sourceforge.net/
- http://www.ijs.si/software/amavisd/
- http://spamassassin.apache.org
- http://sourceforge.net/apps/trac/pyzor/
- http://www.clamav.net/