OpenSMTPD for the Real World Mail Server Tutorial

Aaron Poffenberger

2016-06-09 Thu

Outline

Introduction – Background

- Software developer
  - 30+ years
  - 17+ years professionally
  - Security software developer
  - Design and implement secure APIs
  - Consulting
- IT Background
  - Boeing
  - ISP (dial-up land)
  - Consulting
  - DevOps
- Software Development Experience
  - PentaSafe Technologies
  - NetIQ
  - TheAnimenetwork.com
  - BRS Labs
  - Giant Gray
- InfoSec
  - Software vulnerability assessment
  - Auditing
  - CISSP 2005+
  - US Army

Introduction – Other

- OpenBSD user
- Amateur radio enthusiast
- Electronics hobbyist

Introduction – You

- Enough about me, let's talk about you...

Introduction – You

- Enough about me, let's talk about you...
- Who runs:

Introduction – You

- Enough about me, let's talk about you...
- Who runs:
  - OpenBSD

Introduction – You

- Enough about me, let's talk about you...
- Who runs:
  - OpenBSD
  - FreeBSD

Introduction – You

- Enough about me, let's talk about you...
- Who runs:
  - OpenBSD
  - FreeBSD
  - NetBSD

Introduction – You

- Enough about me, let's talk about you...
- Who runs:
  - OpenBSD
  - FreeBSD
  - NetBSD
  - DragonFly BSD

Introduction – You

- Enough about me, let's talk about you...
- Who runs:
  - OpenBSD
  - FreeBSD
  - NetBSD
  - DragonFly BSD
  - HardenedBSD

Introduction – You

- Enough about me, let's talk about you...
- Who runs:
  - OpenBSD
  - FreeBSD
  - NetBSD
  - DragonFly BSD
  - HardenedBSD
  - MidnightBSD

Introduction – You

- Enough about me, let's talk about you...
- Who runs:
  - OpenBSD
  - FreeBSD
  - NetBSD
  - DragonFly BSD
  - HardenedBSD
  - MidnightBSD
- Anyone want to admit to:

Introduction – You

- Enough about me, let's talk about you...
- Who runs:
  - OpenBSD
  - FreeBSD
  - NetBSD
  - DragonFly BSD
  - HardenedBSD
  - MidnightBSD
- Anyone want to admit to:
  - Debian GNU/kFreeBSD

Introduction – You

- Enough about me, let's talk about you...
- Who runs:
  - OpenBSD
  - FreeBSD
  - NetBSD
  - DragonFly BSD
  - HardenedBSD
  - MidnightBSD
- Anyone want to admit to:
  - Debian GNU/kFreeBSD
  - UbuntuBSD

Introduction – You

- Enough about me, let's talk about you...
- Who runs:
  - OpenBSD
  - FreeBSD
  - NetBSD
  - DragonFly BSD
  - HardenedBSD
  - MidnightBSD
- Anyone want to admit to:
  - Debian GNU/kFreeBSD
  - UbuntuBSD
  - Windows with Bash shell

Tutorial Goals

- Configure smtpd as a Mail Transfer Agent (MTA) for single and multi-domain use
- Install a certificate and configure smtpd to provide or require TLS
- Accept or reject mail based on criteria like recipient, source, sender and domain
- Tag mail
- Configure Spam Assassin
- Configure ClamAV
- Configure smtpd to work with Spam Assassin, ClamAV and Local-Mail-Transfer-Protocol (LMTP) services (in series or individually)

Tutorial Goals

- Deliver mail to Dovecot
- Troubleshoot smtpd issues using smtpd's syntax checker, logs and by sending mail manually via telnet

Tutorial Prerequisites

- One of the supported OSs
  - Unless you want to port it to your OS ;-)
  - *N.B.* - If you brought a Linux box to the tutorial you will be heckled ;-)
- Amavisd (amavisd-new)
- ClamAV
- Dovecot
- mail/mailx
- OpenSMTPD
- OpenSSL/LibreSSL
- SpamAssasin
- Spamd
- Optional but Recommended:
  - OpenBGPD

OpenSMPTD Overview

- man smtpd(8):
  - History: The smtpd program first appeared in OpenBSD 4.6.
- Started by Gilles Chehade in late 2008
- ISC license
- Primarily developed by:
  - Gilles Chehade, Eric Faurot, Charles Longeau and Sunil Nimmagadda
  - And cast of others
- Portable version begun by Charles Longeau
- Found on:
  - NetBSD, FreeBSD, DragonFlyBSD, Mac OS X, Linux

OpenSMTPD Overview - Notes

- OpenSMDTP scrupulously follows RFCs
  1. It's a good idea
  2. Spammers don't . . . extra layer of protection
- If you're trying a manual process (*e.g.*, sending mail manually via telnet) and it fails, you're probably doing it incorrectly. *E.g.:*
  - Correct: rcpt to:<user@domain>
  - Incorrect: rcpt to:user@domain
  - Incorrect: rcpt to: <user@domain>
  - Incorrect: rcpt to: user@domain

Important Keywords

- include
- Macros
- table
- pki
- listen
- tag
- accept|reject
- deliver
- userbase

Important Keywords - Macros

- Expanded in context
- Names must start with a letter, digit, or underscore, and may contain any of those characters
- May not be reserved words
- *N.B.* - Are not(!) expanded within quotation marks

Important Keywords - table

- Use to provide additional configuration information:
  - Lists or key-value mappings
- Types: db or file
- May also be inlined with comma-separated values (list or key=value)

Important Keywords - pki

- Several uses for this keyword:
  - Specify a given hostname with a specific certile
  - Specify a key file for a specific certfile
  - Specify which certificate to present in a listen directive
  - Specify which certificate to present in a relay directive

Important Keywords - listen

- Specify a socket or an interface for incoming connections
- Multiple listeners may be specified
- May specify:
  - hostname to present in the greeting banner
    - default is server name or name in ${ETC}/mail/mailname
  - port
  - tls/ssl requirements
  - address family (inet4 | inet6)
  - directives to tag traffic

Important Keywords - accept|reject

- Accept or reject messages based on SMTP session info
- Criteria for evaluation:
  - tagged [!] tag-name: tag applied as part of client session from any: match all
  - from [!] local: match only local connections (default, not necessary)
  - from [!] source <table>: match connections from clients whose address is declared in the specified table
  - sender [!] <senders>: match senders email address found in table senders. Address may specify entire domain with @: @example.org

Important Keywords - accept|reject

- Criteria for evaluation:
  - for any [alias <aliases>]: Match regardless of the domain sent to. If an alias table is specified, lookup alternative destination for all addresses.
  - for any virtual <vmap>: match regardless of domain sent to, lookup virtual-domain mapping in table vmap.
  - for [!] domain domain [alias <aliases>]: Match based on specified domain. If an alias table is specified, lookup alternative destination for all addresses.
  - for [!] domain <domain> [alias <aliases>]: Match based on domains specified table domain. If an alias table is specified, lookup alternative destination for all addresses.

Important Keywords - accept|reject

- Criteria for evaluation:
  - virtual <users> may be used with each of the above rather than alias <aliases>.
  - recipient [!] <recipients>: Match only if the recipient's email address is found table recipients.
  - [userbase <table>]: Look-up users in table table instead of looking users up using getpwnam(3).

Important Keywords - deliver

- Specify where the mail is to be delivered.
- deliver to lmtp [host:port | socket] [rcpt-to] [as user]: Deliver mail via lmtp protocol.
  - lmtp - queue-less version of SMTP protocol. Useful for sending to MDAs or filter applications like amavisd.
- deliver to maildir [path]: Deliver to maildir directory. Default is ~/Maildir.
- delivery to mbox: Deliver mail to system mailbox in /var/mail.
- deliver to mda program [as user]: Pipe mail to specified program. Optionally run mda as specified user.

OpenSMTPD Configuration

- man smtpd.conf(5)
- Simple, English-like syntax very similar to PF and other OpenBSD-projects
- Typical ${ETC}/mail/smtpd.conf
- May reference other configuration files
  - include "/etc/mail/smtpd.conf.local"
- See example in etc/mail/smtpd.conf in tarball

PF Overview

- man pf(4)
  - History: The pf packet filtering mechanism first appeared in OpenBSD 3.0.
- Packet Filter (PF) is OpenBSD's system for filtering TCP/IP traffic and doing Network Address Translation. PF is also capable of normalizing and conditioning TCP/IP traffic, as well as providing bandwidth control and packet prioritization.
- Originally written by Daniel Hartmeier and is now maintained and developed by the entire OpenBSD team.
- Ported to:
  - FreeBSD (somewhat incompatible now), NetBSD, Mac OS X
  - Oracle (seriously . . . and doing really good work on SMP!)

PF Configuration

- Need to add a few rules
- See rules subset in etc/pf.conf in tarball

BGP-Spamd - Overview

- Distribution of whitelist and blacklist IPs using bgp protocol.
- BGP: purpose is to exchange information concerning "network reachability" with other BGP systems.
- Project run by Peter Hessler (phessler@ OpenBSD)
- Receives blacklist and whitelist data from several sources, including Peter Hansteen
- Works with pf and spamd
  - pf by modifying a specific white-list table
  - spamd by creating file create by a cron job

BGP-Spamd - Configuration

- ${ETC}/bgpd.conf
- Select a private AS id (autonomous system): default == 65001
- Un-comment a neighbor close to you
- Add pass rule to ${ETC}/pf.conf
- See rules subset in etc/pf.conf in tarball

BGP-Spamd - Configuration

- Add source to ${ETC}/mail/spamd.conf
- See example in etc/mail/smtpd.conf in tarball

BGP-Spamd Cron Job

- Add line to root crontab:

```
0 * * * * \
sleep $((RANDOM \% 1800)) && \
/usr/local/sbin/bgp-spamd.black.sh
```

Amavisd Overview

- amavisd-new is a high-performance interface between mailer (MTA) and content checkers: virus scanners, and/or SpamAssassin
- Runs as a service
- Manages sending email through multiple services like ClamAV and SpamAssassin
- Supports LMTP or (E)SMTP
- LMTP is a queue-less counterpart to SMTP
  - Which raises the question: How do I ensure my mail isn't lost while it's in the LMTP receiver?
  - Several solutions possible. Amavisd does not return success to the caller until it has delivered the mail to the next hop.
  - `https://www.ijs.si/software/amavisd/#sec-loss`

Amavisd - Configuration

- Amavisd configuration file is a dog's breakfast
- Fortunately, just a few changes are necessary
  - Lots of optional dials and knobs
- See example in etc/amavisd.conf in tarball

ClamAV - Overview

- ClamAV is an open source antivirus engine for detecting trojans, viruses, malware & other malicious threats.
- Runs as a service or can be called ad-hoc
- Includes freshclam service to download up-to-date definitions

ClamAV - Configuration

- Just a few changes are necessary
  - Lots of optional dials and knobs
- See example in etc/clamd.conf in tarball
- See example in etc/freshclam.conf in tarball
- *N.B.* - Must comment out word "Example" near top of file!
  - Already done in example in tarball

Dovecot - Overview

- Dovecot is an open source IMAP and POP3 email server for Linux/UNIX-like systems, written with security primarily in mind.
- High performance
- Standards compliant
- Plugin architecture

Dovecot - Configuration

- Very easy to configure
- Edit file ${ETC}/dovecot/local.conf to override default settings
- Virtual user password algorithm option identical to OpenSMTPD
- See example in etc/dovecot/local.conf in tarball
- See example in etc/dovecot/passwd in tarball

SpamAssassin - Overview

- Open Source anti-spam platform giving system administrators a filter to classify email and block spam (unsolicited bulk email)
- It uses a robust scoring framework and plug-ins to integrate a wide range of advanced heuristic and statistical analysis tests on email headers and body text including text analysis, Bayesian filtering, DNS blocklists, and collaborative filtering databases

SpamAssassin - Configuration

- Not many necessary changes
  - Lots of optional dials and knobs
- Most notably, the option: *trusted_networks*
  - Not critical, but will exclude mail from listed addresses from checking

Conclusion

- You have questions, I may have answers

Contact Details

- Aaron Poffenberger
- akp@hypernote.com
- `http://akpoff.com`
- @akpoff
- This presentation, look for blog post on `http://akpoff.com`
- KG5DQJ

Resources

- *N.B.* - Most of these are links
- Amavisd
- BGP-Spamd - Peter Hessler
- ClamAV
- Dovecot
- OpenBSD PF FAQ
- SpamAssassin

Blogs and Other Information

- Other Blogs and Posts about BSD Mail Serving
  - Frozen Geek
  - Hugo Osvaldo Barrera - Good discussion about using Sqlite for Virtual Users
- That Grump BSD Guy - Peter Hansteen
  - Spamd
  - BSDly - Blog about OpenBSD, PF and greytrapping