DIY Small Mail Servers

STLLUG – 16 Oct 2014

Helpful Hints for running a personal or small business mail server.

About Me

I work as an independent consultant performing system and small network administration, and writing specialized technical documentation.

I run a mail server for a client using Debian Linux, exim4, uw-imap, spamassassin, fail2ban, ipset, and iptables.

Job Description: Mailserver Admin

- Successful delivery of outgoing mail

- Intact receipt of desired* incoming mail

Roadmap for Mailserver DIY'ers

- 'spam' rules your world – how and why
- Assuring delivery of outgoing mail, or, *Don't look like a spammer*
- Keeping inboxes clean
- Email client issues
- Alternatives

Definitions

- Mail Transfer Agent (MTA) – uses SMTP to route mail to the destination MTA, or vice versa.

- Examples: Exim, Sendmail, Qmail, Postfix....

Definitions

- Mail Delivery Agent (MDA) – uses POP or IMAP (usually) to get received mail to the recipient.

- Examples – UW-imap, Dovcot, Courier

Definitions

- MUA – uses SMTP to send outgoing mail to the 'local' MTA; uses POP or IMAP to fetch mail from the MDA.

- Examples – Outlook, Thunderbird, Squirrelmail, Gmail

The road not taken, mostly

- Choosing or configuring an MTA – exim4/postfix/qmail/...
- Choosing or configuring an MDA - uw-imap/dovecot/courier/...
- Choosing or configuring an MUA - Outlook/Thunderbird/webmail clients/...

'spam' – a coarse definition

- Email you (and others!) do not want to receive
- Trying to sell you something – drugs/stock/etc.
- Con Artists – 419 email
- Phishing – trying to steal passwords, then money

'spam' – a coarse definition

- Email you (and others!) do not want to receive
- Botnet recruitment
- Extortion – Ransomware (Crypto Locker)
- Stealing your time...

Roadmap for Mailserver DIY'ers

- 'spam' rules your world – how and why
- Assuring delivery of outgoing mail, or, *Don't look like a spammer*
- Keeping inboxes clean
- Email client issues
- Alternatives

'spam' Rules Your World – Volume

- On the server I administer, at least 90% of the sending IP addresses are hostile. (Can't count mail...)
- Bandwith
- Diskspace
- CPU
- Air conditioning
- Rack space...

'spam' Rules Your World – Direct Damage to You

- User's time and annoyance
- Financial loss from Phishing
- Botnet recruitment
- Data destruction from Ransomware
- Restoring compromised systems...

'spam' Rules Your World – Collateral Damage

- 'spam' costs and annoys large providers and companies so much they are willing to do almost anything to stop it.
- If you get caught in their defenses the cost to them is small, unpredictable, and probably unknown to them. The cost of 'spam' is large, predictable, and in their face every day.
- Who wins?

Roadmap for Mailserver DIY'ers

- 'spam' rules your world – how and why
- Assuring delivery of outgoing mail, or,
  Don't look like a spammer
- Keeping inboxes clean
- Email client issues
- Alternatives

Don't look like a spammer

- Do the right things
- Don't do the wrong things

- Right and Wrong are measured by spamhaus, Barracuda, Google, and by the admins of the mailservers used by your customers, suppliers, and friends.

Do the right things

- Reverse IP lookup that matches your MX record. Or at least the domain matches.
- Use SPF records
- SPF (Sender Policy Framework) is defined in IETF RFC 7208.
- SPF is a tool to combat forged email headers
- Are you who you say you are?

Prevent the wrong things

- Require encrypted access to send and receive mail – prevent easy password stealing from road warriors.
- (This is not end-to-end encryption!)
- Requires an SSL certificate – you may want a real one, for reasons named later.
- Successful password thieves WILL use your mail server to send spam.

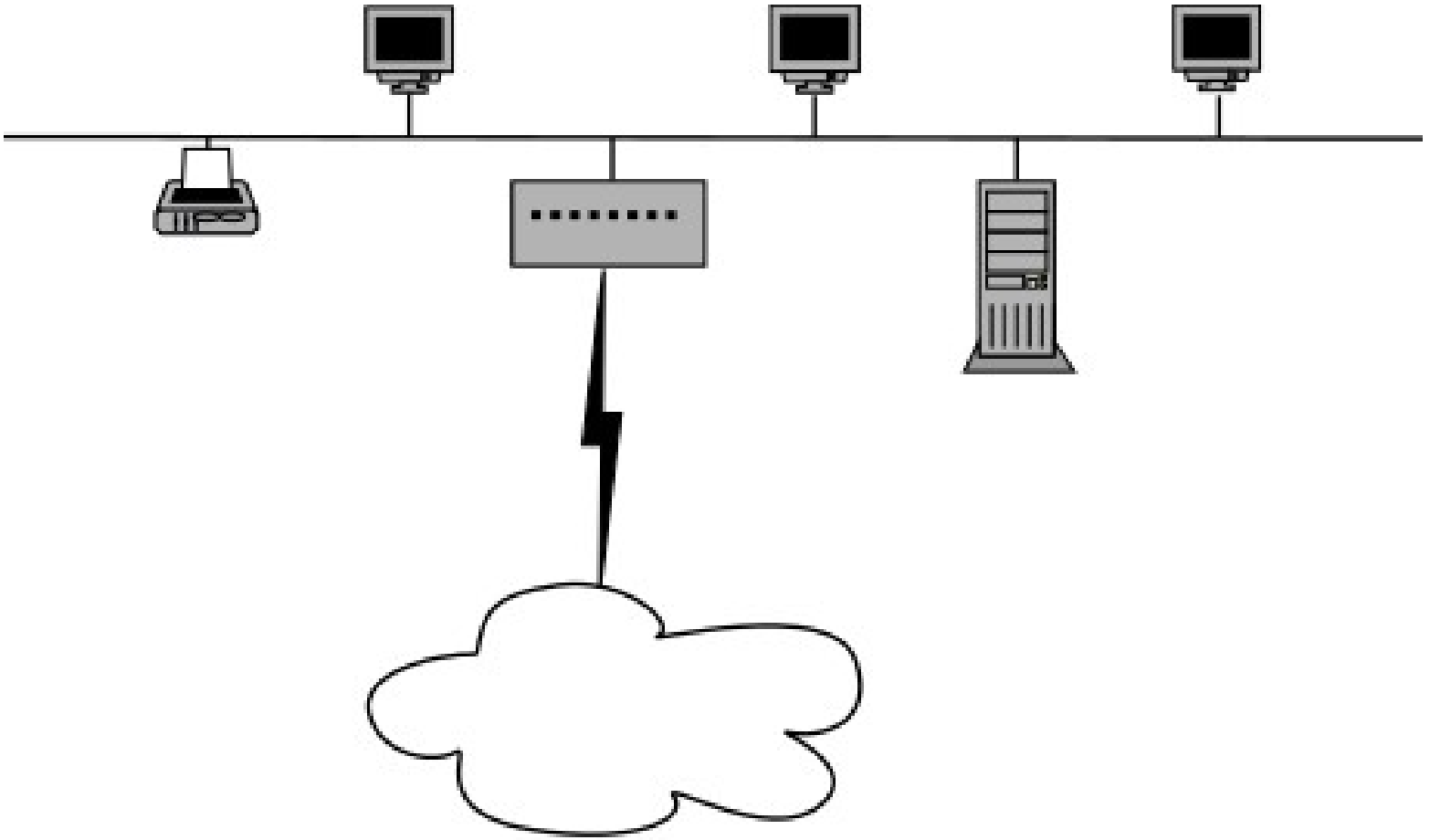
Prevent the wrong things

- Protect your mail server from brute-force attacks.
- Evil-doers will get a list of your users and try to brute-force their passwords.
- Fail2ban can stop them.
- Successful password crackers will probably use your mail server to send spam. (and other evil!)

Prevent the wrong things

- Use spamassassin on your outgoing mail, too.
- Think 'belt and suspenders'
- Possible protection from disgruntled employee, compromised PC, stolen passwords...

A small network



Prevent the wrong things

- A compromised PC behind the same NAT router as your server is a bushel basket of trouble.
- It can send spam directly.
- It can steal email addresses of your users.
- It can steal passwords of your users.
- http://www.spamhaus.org/lookup/

Prevent the wrong things

- A compromised PC behind the same NAT router as your server is a bushel basket of trouble.
- It can send spam through your email server.
- It can talk to a captured botnet C&C node.
- http://www.spamhaus.org/lookup/

Prevent the wrong things

- Enforce PC hygiene –

- Use Data Execution Prevention – All programs.
- Use AdBlock and FlashBlock.
- Use non-privileged accounts.

Prevent the wrong things

- Enforce PC hygiene –

- Teach: Don't open mail from strangers.
- Use some sort of anti-virus (MSE?).
- Keep updated.

Prevent the wrong things

- Use packet filters on your router – only your mailserver can send on port 25.

- More packet filters – only allow DNS lookups to your designated DNS servers.

Prevent the wrong things

- Running a listserve through your mailserver?

- Require confirmed signup
- Make unsubscribe very easy.
- Process rejects as unsubscribe requests
- Get someone else to do it

Roadmap for Mailserver DIY'ers

- 'spam' rules your world – how and why
- Assuring delivery of outgoing mail, or, *Don't look like a spammer*
- Keeping inboxes clean
- Email client issues
- Alternatives

Keeping Inboxes Clean

- Use spamassassin
- Use fail2ban to block hostile IP addresses
- They are most powerful working together!

- Use ipset/iptables if you can/should block geographic areas or areas where rule of law is weak – http://data.worldjusticeproject.org/

Email user life cycle

- Current
- Forward
- Reject
- Blackhole and spamtrap

- Skip the first 3 steps for at least two usernames

spamassassin

- Uses a multi-test rating system
- Accept, Flag, and Reject categories
- Positive ratings are bad, negative good
- spamassassin can be beaten...

fail2ban

- fail2ban monitors log file for signs of hostile activity, blocks (using iptables) hostile IP addresses for a configurable period of time

- Protect MUAs and MDAs from brute-force password hacking

- Protect against spam (the first one gets thru)

spamassassin - suggestions

- Use blacklist_to for the spamtrap users
- Make sure automatic purge of saved spam is working
- Adjust the flag/reject settings if you need to

fail2ban – suggested applications

- MTAs and MDAs – block for 1-2 hours after 3 login failures
- Rejected spam – block IP addr. for 6-10 hours
- Rejected spam – block /24 net for 1-2 hours

fail2ban – suggested applications

- Two flagged spam – block IP address for 1-2 hours
- No reverse lookup – block IP address for 6-10 hours
- Unrouteable – block IP addr. for 6-10 hours

Roadmap for Mailserver DIY'ers

- 'spam' rules your world – how and why
- Assuring delivery of outgoing mail, or, *Don't look like a spammer*
- Keeping inboxes clean
- Email client issues
- Alternatives

Email Client Issues

- Set up secure access, add certificate
- Gmail needs a real certificate
- Set up filtering and filing of flagged email

Roadmap for Mailserver DIY'ers

- 'spam' rules your world – how and why
- Assuring delivery of outgoing mail, or, *Don't look like a spammer*
- Keeping inboxes clean
- Email client issues
- Alternatives

Alternatives to DIY

- Google Apps for Work ($50/user/year)
- Paid services at Outlook.com
- Yahoo small business services

DIY Small Mail Servers

STLLUG – 16 Oct 2014