Postfix

by Rod Roark
http://www.sunsetsystems.com/

Terminology

- MTA
- MDA
- MUA
- SMTP
- IMAP
- POP3
- UCE

Mail Transfer Agent

- Receives mail from or sends mail to other computers
- Talks with other MTAs and certain other agents
- Analogous to post offices
- SMTP is the language of MTAs
- MTAs are security-conscious
- Examples: Postfix, Sendmail, Exim
- SMTP: RFCs 821, 1123, 2821
- Terminology: Client, Server

Mail Delivery Agent

- Deposits received mail on the local computer
- Common storage formats are Mbox and Maildir
- Analogous to a mail carrier
- Usually invoked by an MTA
- Examples: Maildrop, Procmail

POP3 Server

- Post Office Protocol
- Provides for temporary storage and retrieval of mail
- Mail is usually deleted after retrieval
- Supported by most mail clients
- RFC 1939 and others define POP3

IMAP Server

- Internet Message Access Protocol
- Provides temporary and long-term storage and retrieval of mail
- More sophisticated than POP3
- Provides folders for organizing and archiving
- Supported by most mail clients
- Examples: Qmail, Courier IMAP
- RFC 3501 defines IMAP4rev1

Mail User Agent

- Mail Client
- your tool for composing, reading, searching, archiving, etc.
- Commonly understands SMTP, POP3, IMAP and local storage formats
- Examples: Mutt, KMail, Evolution, Pine, Mozilla Thunderbird, MS Outlook

SMTP Conversation

```
$ telnet localhost 25
helo somewhere.org
mail from: me@somewhere.org
rcpt to: rod@dapper.livepenguin.com
data
From: Me
To: Rod
Subject: Test
Hi, are you there?
Regards,
Me
.
quit
```

Message Content

- Headers
- Body
- Attachments

Postfix Features

- High performance, small footprint
- Sendmail-compatible but easier to administer and more secure
- Virtual domains
- Extensive junk mail controls
- Authentication and encryption
- Flexible database support
- Powerful support for plugins
- Address manipulation
- Maildir or mailbox delivery

Postfix Processes

- master
- smtpd
- smtp
- qmgr
- cleanup
- local
- Others: anvil, bounce, defer, trace, flush, proxymap, scache, showq, spawn, tlsmgr, verify

Postfix Utilities

- postfix
- postmap
- postsuper
- postqueue
- sendmail, newaliases
- others

Basic Configuration

- dpkg-reconfigure postfix (Debian)
- main.cf
- master.cf
- aliases

main.cf Basics

- myhostname
- relayhost
- inet_interfaces
- mynetworks_style, mynetworks
- alias_maps, alias_database

Virtual Domains

- Alias other domains to local recipients
- virtual_alias_domains
- virtual_alias_maps
- /etc/postfix/virtual

Lookup Tables

- Used extensively in Postfix configuration
- E.g. alias_maps, header_checks
- Referenced as type:table
- Tables store key/value pairs
- Types: btree, cdb, cidr, dbm, environ, hash, ldap, mysql, netinfo, nis, nisplus, pcre, pgsql, proxy, regexp, sdbm, static, tcp, unix (passwd, group)

Postgres Lookup Table

main.cf:

```
virtual_mailbox_maps = pgsql:/etc/postfix/vm.pgsql.cf
```

/etc/postfix/vm.pgsql.cf:

```
hosts = localhost
user = rod
password = secret
dbname = refercare
query = SELECT userid || '/' FROM users WHERE userid = '%u'
    AND 'refercare.org' = '%d' AND password IS NOT NULL
```

What is Spam?

- Unsolicited
- Sent in bulk

Not Protected Speech

UNITED STATES SUPREME COURT

"We therefore categorically reject the argument that a vendor has a right under the Constitution or otherwise to send unwanted material into the home of another. If this prohibition operates to impede the flow of even valid ideas, the answer is that no one has a right to press even 'good' ideas on an unwilling recipient. That we are often 'captives' outside the sanctuary of the home and subject to objectionable speech and other sound does not mean we must be captives everywhere. See Public Utilities Comm. of District of Columbia v. Pollak, 343 U.S. 451 (1952). The asserted right of a mailer, we repeat, stops at the outer boundary of every person's domain."

- ROWAN v. U. S. POST OFFICE DEPT. , 397 U.S. 728 (1970)

Right to Fight Spam

UNITED STATES CONGRESS
TITLE II--SPAMMING

SEC. 201. SENSE OF THE CONGRESS.

October 2, 1998

"It is the responsibility of the private sector to adopt, implement, and enforce measures to deter and prevent the improper use of unsolicited commercial electronic mail."

Restriction Stages

In the order applied, they are:

- smtpd_client_restrictions
- smtpd_helo_restrictions
- smtpd_sender_restrictions
- smtpd_recipient_restrictions
- smtpd_data_restrictions

Each stage may contain *restrictions* evaluating to OK, REJECT or DUNNO.

Client Restrictions

- check_client_access
- permit_mynetworks
- reject_rbl_client
- reject_unknown_client
- reject_unauth_pipelining
- others

HELO Restrictions

- check_helo_access
- reject_invalid_hostname
- reject_non_fqdn_hostname
- reject_unknown_hostname
- others

Sender Restrictions

- check_sender_access
- reject_non_fqdn_sender
- reject_rhsbl_sender
- others

Recipient Restrictions

- check_recipient_access
- reject_non_fqdn_recipient
- reject_unauth_destination
- others

Data Restrictions

- reject_unauth_pipelining
- others

Global Restrictions

- header_checks
- body_checks (show example)
- smtpd_helo_required
- strict_rfc821_envelopes
- smtpd_reject_unlisted_sender
- smtpd_reject_unlisted_recipient
- before-queue content checking
- others

Content Inspection

- Before Queueing
- After Queueing
- Problems with each

DNS-based Blacklists

...Client host [69.81.114.241] blocked using bl.spamcop.net;

$ nslookup -sil 241.114.81.69.bl.spamcop.net
...
Name: 241.114.81.69.bl.spamcop.net
Address: 127.0.0.2

$ nslookup -sil 136.54.218.66.bl.spamcop.net
...
** server can't find 136.54.218.66.bl.spamcop.net: NXDOMAIN

Spamhaus DNS

/etc/bind/named.conf:

```
zone "spamhaus.org" IN {
  type forward;
  forwarders { 216.168.28.44; 204.69.234.1; 204.74.101.1;
    204.152.184.186; };
};
```

Other Useful Software

- Courier IMAP - excellent standalone IMAP/POP3 server
- Postgrey - Greylisting agent
- Amavisd-new - hosts plug-in spamfighting tools
- ClamAV - free virus scanner with automated updates
- SpamAssassin - extremely versatile content inspection
- TLS(SSL) - encryption of SMTP traffic
- SquirrelMail - easy and popular IMAP Web mail client
- Other clients: KMail, Evolution, Mutt, Thunderbird