Postfix MTA

SANOG 16 – July 15th - 19th 2010
Paro, Bhutan

Phil Regnauld <regnauld@nsrc.org>

Short history

- Originally developed in the late 90s at IBM by Wietse Venema, author of security software (SATAN, TCPwrappers, …), as ”IBM Secure Mailer”
- Place under an Open Source license, and renamed ”Postfix”
- Intended as a replacement for then insecure mail systems, such as Sendmail

Design goals

- Safety
- Robustness
- Performance
- Modularity
- Compatibility

Safety

- Postfix makes it very hard to lose mails – many checks to ensure that mail has been written to disk or delivered
- Back off mechanisms in case of repeated failure

Security

- Collection of daemons working together
- Doesn't use environment for communication
- Very paranoid about input checking, all allocation is dynamic (avoiding buffer overflows)
- chroot support out of the box for almost all processes & daemons
- No data is *ever* exchanged directly between processes – all is done via IPC, and files on disk
- Conservative ressource usage

Performance

- Designed to be fast from the ground up
- Also behaves well with neighbors, doesn't flood them with mail, and instead uses a throughput adaptation
- Will not block delivery for a message if one recipient domain fails

Modular

- One program, one function
- All programs controlled from ”master.cf”
- Many small programs working together, with limited privileges
- Compatible with Sendmail's /etc/aliases and .forward conventions

Features

- Virtual domains – domains and users are completely independent of system (UNIX) users
- Aliases – sendmail compatible
- Rewriting – senders, recipients, globally
- RBL support (Realtime Blackhole Lists) support
- Content filtering using pipes, SMTP or milter
- Support for arbitrary mail manipulation with policy services (custom programs talking to postfix)

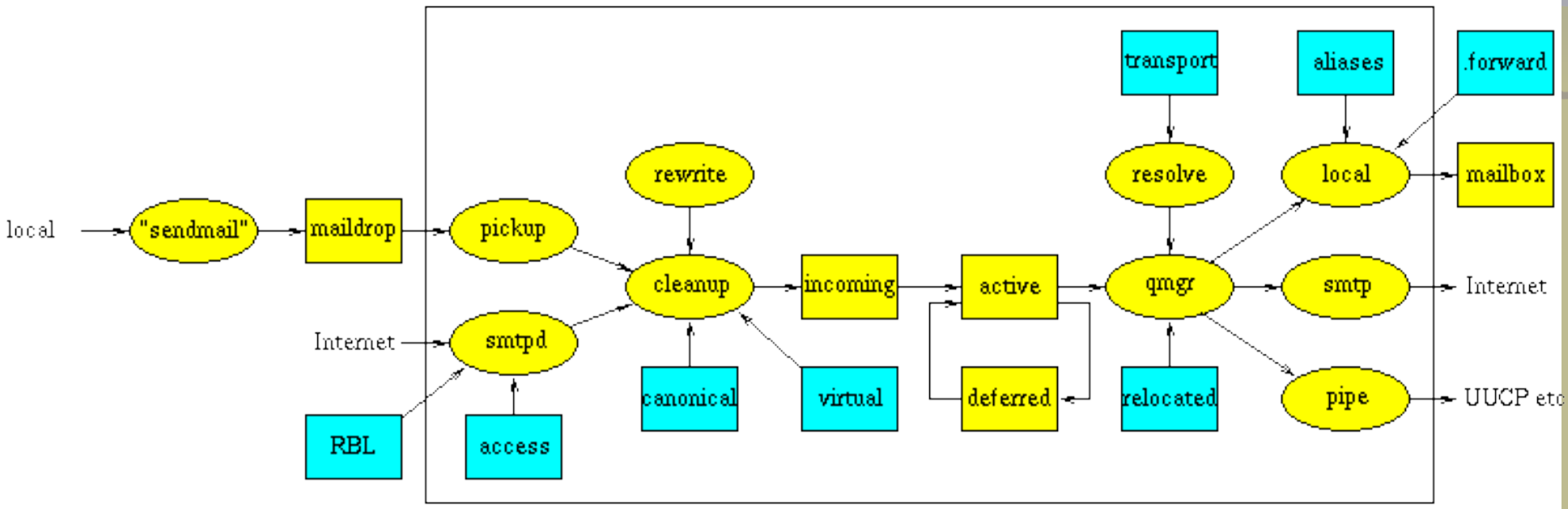
More features

- Restriction classes
  - Conditional filtering
- Sender or recipient address verification (test email addresses before accepting mail from them)
- TLS support

Core concept: maps

- In postfix, everything is looked up in a map (table)
- Maps can be in many formats or use many data sources:
  - hash/btree
  - regexp/PCRE
  - CIDR
  - NIS
  - LDAP, *SQL (user defined queries)

Architecture



Basic Postfix configuration

- Two primary configuration files
- main.cf
  - Main configuration file where all the subsystems are configured (smtp, smtpd, cleanup, routing, …)
- master.cf
  - File controlling how the ”master” process of postfix will launch all the necessary postfix daemons to perform mail routing, on-demand

Other configuration files

- Reside in ”maps” mentioned earlier
- Tables containing values and conditions, referred to from main.cf, controlling all aspects such as:
  - Virtual and local domains
  - Routing rules
  - Access control
  - Rewriting
  - ...

Configuration: postconf command

- postconf – used to view and edit configuration parameters
  - For changing the configuration, it is usually done vi editing ”main.cf” directly

Some basic main.cf

```
# what domains do I accept mail for (user@...)
mydestination =  $myhostname, localhost, \
      bhutan.ws3.conference.sanog.org

# who do I send mail as ?
myorigin=        $mydomain

# what clients do I consider local (and trust them)
Mynetworks =     127.0.0.0/8 192.168.1.0/24

# Send all outgoing mail to this server
relayhost =          mail.example.com
# Aliases
alias_maps = hash:/etc/aliases
```

Some basic main.cf (cont'd)

* **in the file /etc/aliases:**

```
root:                   sanog
steve:                  scg@stevegibbard.com
Phil:                   regnauld@nsrc.org
```

More advanced main.cf

```
cf = $config_directory
smtpd_helo_required =        yes
smtpd_client_restrictions  =  permit_mynetworks
smtpd_helo_restrictions =   reject_invalid_hostname

smtpd_sender_restrictions =     reject_non_fqdn_sender,
                          reject_unknown_sender_domain,
          check_sender_access   hash:$cf/sender-access,
           check_client_access  cidr:$cf/client-access,
          reject_rbl_client  cbl.abuseat.org

smtpd_recipient_restrictions =
                              reject_non_fqdn_recipient,
                        reject_unknown_recipient_domain,
                                    permit_mynetworks,
     check_recipient_access pcre:$cf/recipient-access,
```

Contents of ”sender-access”, ”recipient-access”, ”client-access”

* **sender-access file:**

```
spammer@aol.com                 554 We don't want your mail
@aol.com                        OK
```

* **recipient-access file:**

```
someuser@mydomain.com           554 User does not accept mail
@mydomain.com                   OK
```

* **client-access file:**

```
119.2.100.0/24                  REJECT no thank you
119.2.100.245                   OK from you it's ok
```

Actions in the ”access” maps

REJECT
    Go away
OK
    Accept address/IP/...
DUNNO
    Pretend you didn't find it and continue
HOLD
    place in the HOLD queue
DISCARD
    Trash. DISCARD 250 I took good care of your message!
FILTER transport:destination
    Send the mail via transport to destination -- ususally a content filter.
restriction...
    Apply a restriction (UCE) / restriction class

Virtual domains

- Allows having multiple mail domains on one machine
- They can be *completely* different than your own hostname/domainname
- Example:
  - **in main.cf:**
    ```
    virtual_maps = $cf/virtual-domains
    ```
  - **in virtual-domains file:**
    ```
    superdomain.bt          VIRTUAL
    phil@superdomain.bt     phil@nsrc.org, pr@eu.org
    @superdmain.bt          sanog@localhost
    ```

Rewriting

- Allows you to have multiple domains without having to configure them all
- Example:
  - **in main.cf:**
    ```
    recipient_canonical_maps = $cf/recipient-rewrite
    ```
  - **in recipient-rewrite file:**

    ```
    phil@superdomain.com      pr@superdomain.bt
    @superdomain.com          @superdomain.bt
    ```

Controlling postfix

- postfix start – start the postfix system
- postfix stop – stop the postfix system
- postfix check – verify the configuration
- newaliases – rebuild the local aliases
- mailq -- show the mails in the queue currently being processed

References

- Links
  - http://www.postfix.org/
  - http://www.ijs.si/software/amavisd/
- Books:
  - "Postfix", Richard Blum, ed. Sams (1st ed. May 15, 2001), 624 p., ISBN: 0672321149
  - "The book of Postfix", Ralf Hildebrandt, Patrick Koetter ed. No Starch Press (October 2003), 328 p., ISBN: 1593270011