Linux Mail Messaging System

The Proposal

Outline

- A brief view of email service
- Email System Architecture
- Design of a suitable email system
  - Webmail
- Postfix and configuration
- Spam and virus filtering

Overview

- Electronic mail service will be used on local and on the internet.
- The service availability will depend on power and internet service.

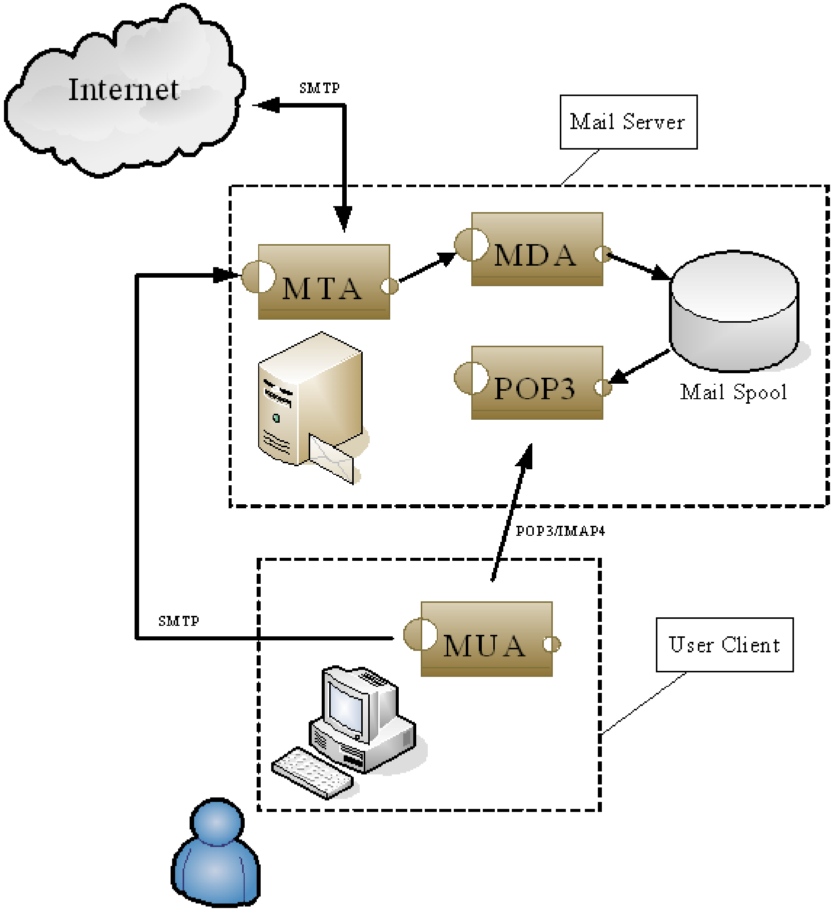
Brief View of NIDA eMail Service

- Current requirement
  - Number of users : 500
  - Quota per user : 500 MB
- Server Design
  - Server Hardware already provisioned
  - Public and Private IP already provided
  - MX, DNS Records are in place
  - Server Hardware already behind Firewall

Brief View of NIDA eMail Service

- Proposed Mission
  - Installation of Mail Transfer Agent
    - Sending and Forwarding email
  - Installation of Mail Delivery Agent
    - Delivering emails to recipients
  - POP3 and IMAP
    - Downloading user mailboxes
  - Installation of Mail User Agent(Webmail)
    - For Reading and Composing emails
  - Installation of Antispam and Antivirus
    - For Filtering smap mails and virus infected emails

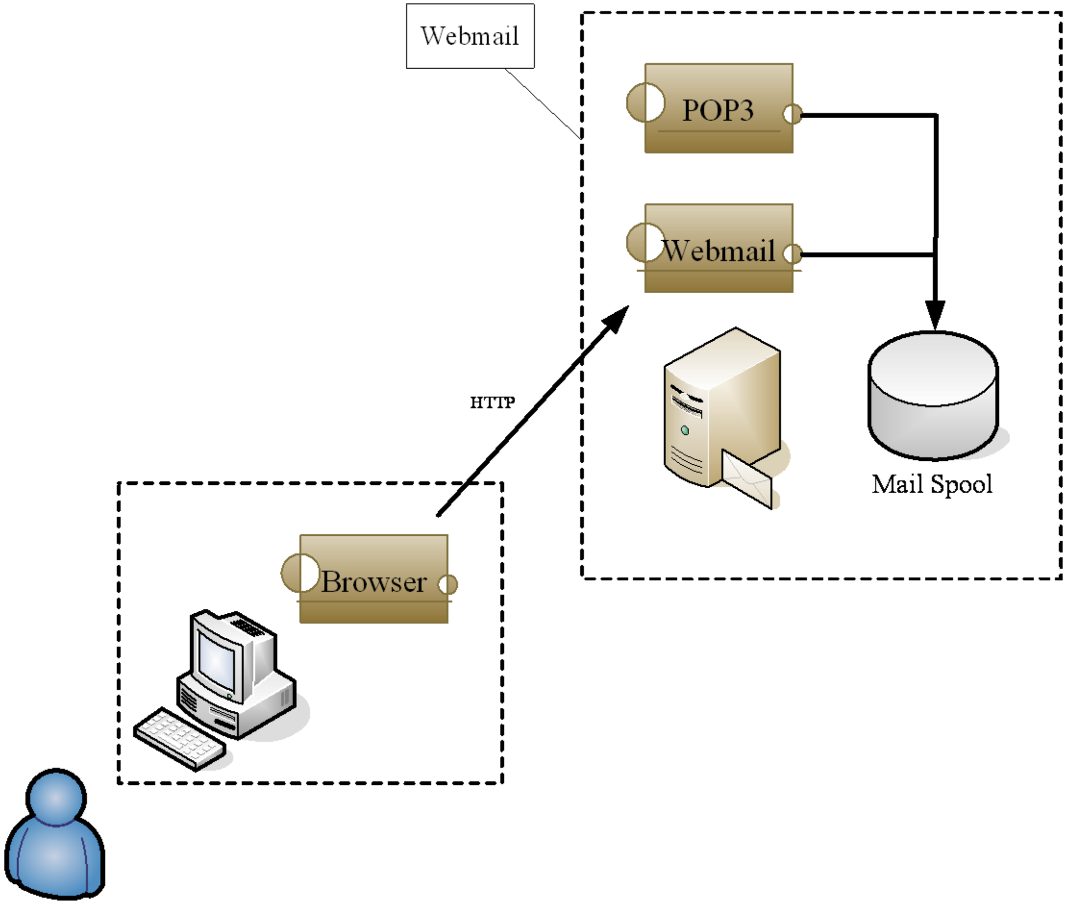
Mail System Architecture



Linux Components Installation

- MTA
  - Postfix
- POP3/IMAP
  - Dovecot
- Antivirus and antispam
  - ClamAV, SpamAssasin and Amavisd-new
- MUA
  - squirrelmail

Webmail Architecture



Postfix Installation

- Debian Linux
  - apt-get install postfix-tls libsasl7 libsasl-modules-plain courier-imap
- Redhat/Fedora Linux
  - rpm -ivh postfix-2.2.x.i386.rpm
  - rpm -ivh cyrus-sasl-2.1.21.i386.rpm

Post Installation

- Postfix Configuration
  - master.cf
    - Similar to inetd.conf
    - Control the behavior of small programs
      - In contrast against sendmail, with one binary and one config file
  - main.cf
    - The main configuration of the mail system
  - In general cases, no modification is required for a simple setup.
- postfix program Controls
  - postfix start
  - postfix stop
  - postfix reload

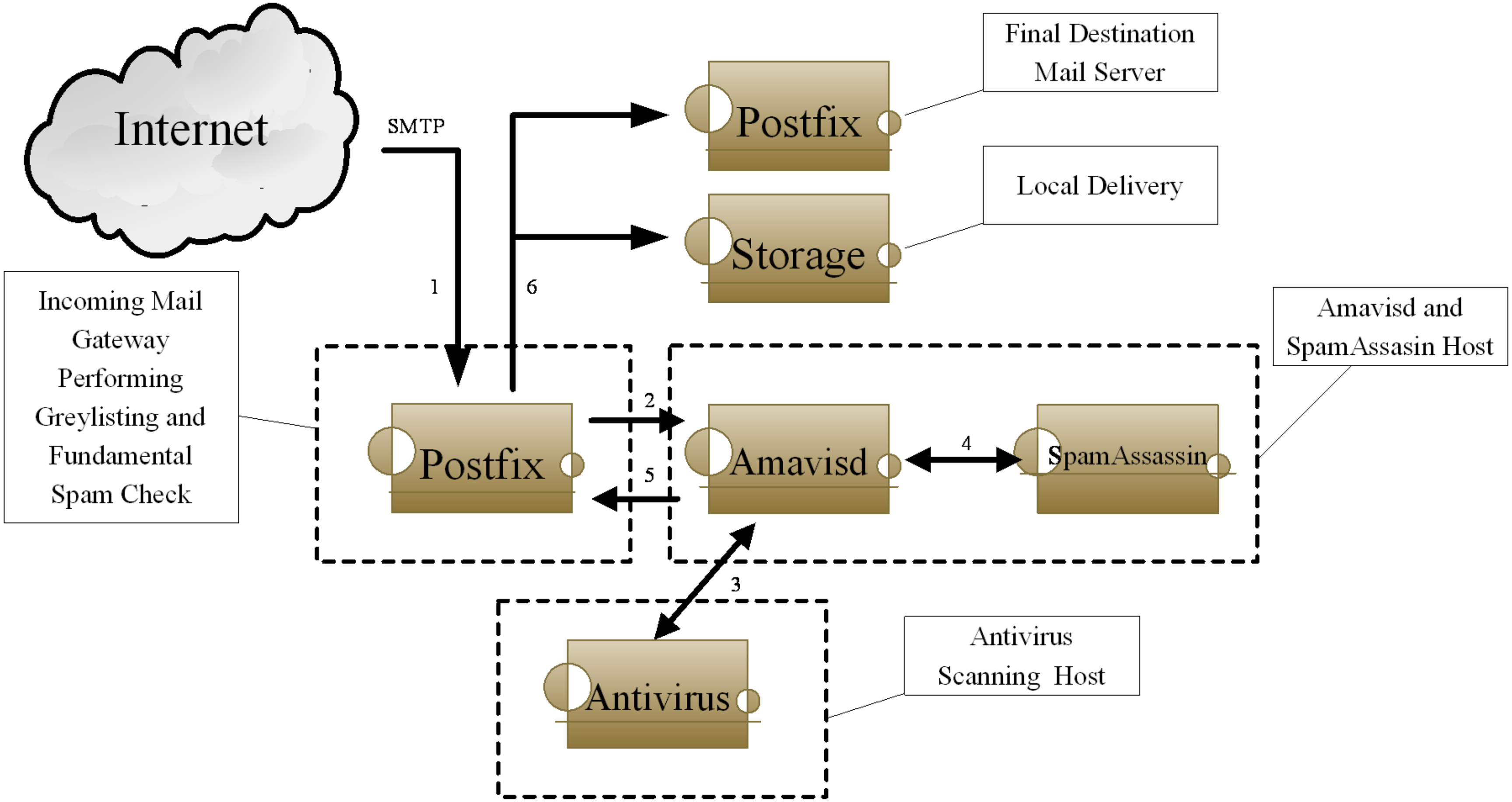
SSL Configuration

- main.cf
  - smtpd_enforce_tls = yes
  - smtpd_use_tls = yes
  - smtpd_tls_cert_file = /usr/local/etc/ssl/smtp.cert
  - smtpd_tls_key_file = /usr/local/etc/ssl/smtp.key
  - smtpd_tls_CAfile = /usr/local/etc/ssl/nida.crt
  - smtpd_tls_loglevel = 1
  - smtpd_tls_received_header = yes
  - smtp_enforce_tls = yes
  - smtp_tls_cert_file = $smtpd_tls_cert_file
  - smtp_tls_key_file = $smtpd_tls_key_file
  - smtp_tls_CAfile = $smtpd_tls_CAfile
  - smtp_tls_loglevel = 1
  - smtp_use_tls = yes
  - smtp_tls_note_starttls_offer = yes
  - tls_random_exchange_name = /var/run/prng_exch
  - tls_random_source = dev:/dev/urandom
  - tls_daemon_random_source = dev:/dev/urandom
- master.cf
  - tlsmgr fifo - - n 300 1 tlsmgr

SMTP Authentication Configuration

- main.cf
  - smtpd_sasl_auth_enable = yes
  - smtpd_sasl_security_options = noanonymous
  - smtpd_tls_auth_only = yes
  - smtpd_recipient_restrictions = reject_unknown_recipient_domain, reject_non_fqdn_recipient, permit_sasl_authenticated, reject_unauth_destination
- master.cf
  - smtps inet n - n - - smtpd -o smtpd_tls_wrappermode=yes
- The smtpd will listen on port 465 instead of 25.

Architecture for Filtering



Final Destination Mail Server

Local Delivery

Incoming Mail Gateway Performing Greylisting and Fundamental Spam Check

Amavisd and SpamAssasin Host

Antivirus Scanning Host

Amavisd-new

- A high performance interface between MTA and content checkers.
  - Calling external antivirus programs to do virus scanning.
  - Calling external spamassassin program to do spam level determination.
  - CPU intensive workloads.
  - Can be flexibly configured to pass, discard, or quarantine mails based on user defined policy.
    - Pass spam mails with score > 10 with subject prepended the *** SPAM *** keyword.
    - Quarantine spam mails with score > 20.
    - Discard spam mails with score > 30.
    - Quarantine virus mails.

Spamassassin

- Spam level scoring software.
- Rich set of tests to identify various spam signatures.
  - Keywords, bad headers, encodings
- Use bayesian analysis to help scoring.
  - Training the bayesian database using know spam and ham mails.
  - Default to enable the auto-learn feature.
- Calling external programs to check if the mail was a known spam.
  - Use hash of mail content as the query key.
  - Razor, DCC, Pyzor.

Spamassassin

- RBL(realtime black list) look up based on sender ip address.
  - RBL may contains too many ill-administrated sites.
  - Use the result as an addition of spam score.
  - Do not block remote sites depend solely on RBL.
- SURBL(Spam URI realtime black list) look up based on the URIs within the content of mail.
  - Spammers may keep changing their sending IP addresses.
  - The URIs in the content may be the final destination the advertisement want people to visit

Postfix: Content Filter Configuration

- master.cf

  -
    ```
    smtp-amavis unix - - y/n - 2 smtp
      -o smtp_data_done_timeout=1200
      -o smtp_send_xforward_command=yes
      -o disable_dns_lookups=yes
    ```

  -
    ```
    127.0.0.1:10025 inet n - y/n - - smtpd
      -o content_filter=
      -o local_recipient_maps=
      -o relay_recipient_maps=
      -o smtpd_restriction_classes=
      -o smtpd_client_restrictions=
      -o smtpd_helo_restrictions=
      -o smtpd_sender_restrictions=
      -o smtpd_recipient_restrictions=permit_mynetworks,reject
      -o mynetworks=127.0.0.0/8
      -o strict_rfc821_envelopes=yes
      -o smtpd_error_sleep_time=0
      -o smtpd_soft_error_limit=1001
      -o smtpd_hard_error_limit=1000
    ```
- main.cf

  -
    ```
    content_filter = smtp-amavis:127.0.0.1:10024
    ```

Amavisd-new Configuration

- amavisd.conf
  - $max_servers = 30; # number of pre-forked children
  - @av_scanners = (….
  - $final_virus_destiny   = D_DISCARD; # (defaults to D_BOUNCE)
  - $final_banned_destiny = D_BOUNCE; # (defaults to D_BOUNCE)
  - $final_spam_destiny   = D_DISCARD; # (defaults to D_REJECT)
  - $final_bad_header_destiny = D_PASS; # (defaults to D_PASS), D_BOUNCE suggested
  - $QUARANTINEDIR = '/var/virusmails/infected';
  - $sa_tag_level_deflt = 1; # add spam info headers if at, or above that level
  - $sa_tag2_level_deflt = 9; # add 'spam detected' headers at that level
  - $sa_kill_level_deflt = 20; # triggers spam evasive actions
  - $sa_dsn_cutoff_level = 20; # spam level beyond which a DSN is not sent
  - $sa_quarantine_cutoff_level = 30;
- Raise the tag2 value to avoid removing users' mail.

SpamAssassin Configuration

- Built-in tests
  - http://spamassassin.apache.org/tests.html
- local.cf
  - ok_languages en ja zh
  - ok_locales en ja zh
  - score SUBJ_ILLEGAL_CHARS 0
  - score FROM_ILLEGAL_CHARS 0
  - score HEAD_ILLEGAL_CHARS 0
  - score CHARSET_FARAWAY 1.0
  - score CHARSET_FARAWAY_HEADER 1.0
  - score MIME_CHARSET_FARAWAY 1.0

  - header   NIDA_SMTP Received score   NIDA_SMTP -15.0
  - describe NIDA_SMTP
  - header   HINET_MSR Received score   HINET_MSR -10.0