IMPLEMENTASI *MAIL SERVER* MENGGUNAKAN POSTFIX

Kusmaya

Teknik Informatika, Fakultas Teknik
Universitas Langlangbuana

ABSTRAK

E-mail (Electronic Mail) adalah fasilitas yang digunakan sebagai sarana untuk mengirim dan menerima surat elektronik (e-mail) kepada dan dari pemakai komputer lain yang terhubung di internet, selain itu mengirim surat dapat menyertai file sebagai lampiran (attachment). Melalui email kita dapat mengirim surat elektronik baik berupa teks maupun gabungan dengan gambar, yang dikirimkan dari satu alamat email ke alamat lain di jaringan internet. Adakalanya e-mail digunakan oleh perusahaan tertentu sebagai alat pelaporan, maka dibutuhkan sebuah *mail server* yang dapat mengelola *e-mail*. *Postfix* sebagai *mail server* diharapkan dapat mengatasi kebutuhan *mail server* di perusahaan apapun. *Postfix* disediakan secara gratis, selain itu *postfix* diakui tiga kali lebih cepat dibanding kompetitor utamanya seperti Qmail. *Postfix* juga memiliki kompatibilitas yang baik. *User* yang sebelumnya menggunakan *Sendmail* sebagai *mail server* bisa bermigrasi ke *postfix*. *Postfix* mendukung SSL untuk mengenkripsi komunikasi *e-mail*. Selain itu Postfix dapat diintegrasikan dengan anti virus dan anti *spam* seperti *ClamAV* dan *SpamAssassin*.

Kata kunci: *ClamAV, mail server, Postfix, SpamAssassin,* SSL.

1. PENDAHULUAN

Pesan elektronik atau yang biasa disebut *e-mail* adalah sebuah teknologi pengiriman surat secara elektronik melalui media jaringan atau internet. Banyak penyedia layanan *e-mail* yang biasa digunakan secara gratis seperti Yahoo! Mail atau Gmail. Perusahaan-perusahaan milik pemerintah atau swasta menggunakan layanan *e-mail* untuk berinteraksi dengan masyarakat untuk meningkatkan produktifitas perusahaan mereka.

Sebuah perusahaan yang sedang mengembangkan teknologi komunikasi dan informasi tidak langsung sepenuhnya menerapkan teknologi tersebut dengan pertimbangan bernacam-macam. Adakalanya kebutuhan akan perangkat lunak (*software*) dan perangkat keras (*hardware*) menggunakan pihak ketiga, seperti pengadaan sebuah *server* yang dapat mengelola *e-mail* masih bergantung pada layanan *hosting*. Padahal dengan adanya *mail* server, karyawan-karyawan yang bekerja di suatu perusahaan dapat saling mengirim *e-mail* secara lokal.

2. METODE KAJIAN

2.1 Metode Bidang Kajian

a. Analisis

Analisis dilakukan untuk menganalisis semua kebutuhan jaringan. Analisis dilakukan dengan cara melakukan wawancara atau survey lapangan, sehingga didapatkan peta atau gambaran untuk merancang (*design*) pola atau model yang akan digunakan.

b. Perancangan

Tahap perancangan dilakukan dengan cara pembuatan topologi dalam pembangunan *mail* server sesuai dengan kondisi dan sumber daya yang terdapat di perusahaan.

c. Implementasi

Tahap implementasi adalah tahap instalasi dan konfigurasi *mail server* dengan *postfix* sebagai aplikasinya dan aplikasi-aplikasi pendukung yaitu BIND, Dovecot, ClamAV, SpamAssassin, SquirrelMail, dan Mozilla Thunderbird.

d. Pengujian

Tahap pengujian dilakukan dengan cara menguji *mail* server. Pengujian dilakukan untuk membuktikan bahwa instalasi dan konfigurasi yang dilakukan dapat berjalan sesuai dengan topologi yang telah dibuat.

2.2. Tinjauan Pustaka

2.2.1 *E-mail*

Pesan elektronik, atau akrab disebut *e-mail* merupakan istilah populer untuk pesan/surat elektronik; biasanya berbentuk pesan teks sederhana yang ditulis seseorang (*user*) melalui sebuah sistem komputer dan ditransmisikan ke komputer lain yang dituju dengan melintasi jaringan komputer. Saat ini *e-mail* banyak digunakan karena ekonomis, lebih simpel, sangat cepat, mudah dikelola, dan mampu mentransmisi beragam format dokumen. (Rahmat, 2006)

2.1.2. *Mail* Server

Aplikasi yang digunakan untuk menangani penghantaran pesan mail adalah *mail server*. *Mail server* ini senantiasa menerima pesan dari *e-mail client* yang digunakan

user, atau mungkin dari *server e-mail* lainnya. Sesuai dengan namanya, *server e-mail* adalah pusat kendali sistem *e-mail*. Sebuah *mail server* biasanya terdiri dari area penyimpanan, set konfigurasi *user*, daftar *user*, dan seri modul komunikasi (Rahmat 2006).

1. Area penyimpanan (*storage area*) – adalah tempat pesan *mail* disimpan untuk *user*, dan sebagai transit pesan sebelum menuju tujan lainnya.
2. Set konfigurasi user – adalah aturan untuk *user* yang menetapkan bagaimana *mail server* harus beraksi saat menerima pesan tertentu, atau mungkin mengambil keputusan untuk pengirim tertentu. Sebagai contoh, *address* tertentu mungkin dibatasi untuk hanya dapat mengirim pesan dalam lingkungan perusahaan saja.
3. Daftar user – adalah *database* akun *user* yang dikenali *mail server* dan akan berkomunikasi dengan mereka secara lokal.
4. Modul komunikasi – adalah komponen yang aktualnya menangani *transfer* pesan ke dan dari *server e-mail* lain dan atau klien *e-mail* (*e-mail client*). Modul yang terinstal dalam *mail server* ini dapat berbeda-beda, bergantung kebutuhan.

2.1.3. DNS Server

DNS atau *Domain Name System* adalah *distribute database system* yang digunakan untuk pencarian nama komputer di jaringan yang menggunakan TCP/IP (Transmission Control Protocol/Internet Protocol). DNS biasa digunakan pada aplikasi yang terhubung ke internet seperti *web browser* atau *e-mail*, dimana DNS membantu memetakan *hostname* sebuah komputer ke IP *Address* (Tri, 2009).

2.1.4. SSL/TLS

SSL (*Secure Socket Layer*) adalah protokol yang sering digunakan untuk mengatur keamanan dalam pengiriman pesan pada internet. SSL baru-baru ini digantikan oleh *Transport Layer Security* (TLS), yang didasarkan pada SSL. SSL menggunakan sistem enkripsi *public-and-private key* dari RSA, yang juga mencakup penggunaan *digital certificate*. Dengan menggunakan SSL/TLS, *mail server* dapat mengenkripsi lalu lintas *e-mail* sehingga keamanan lebih baik (Imam, 2013).

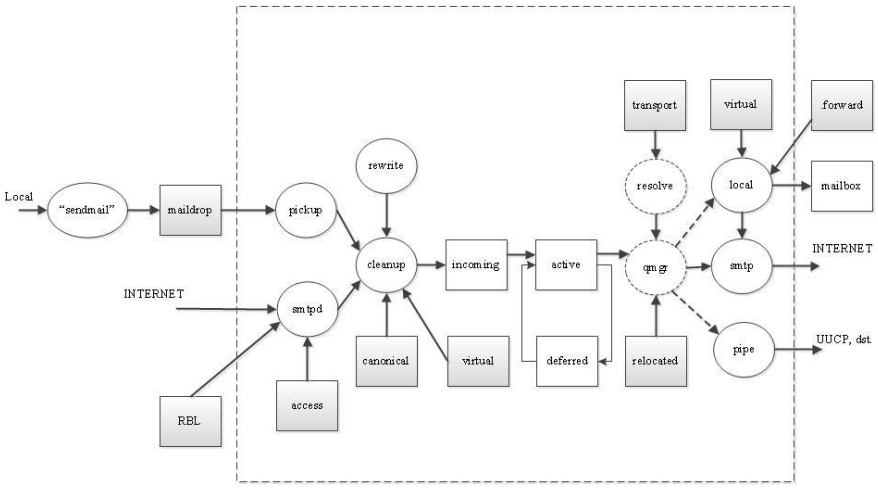
2.1.5. *Postfix*

a. Sejarah

Postfix ditulis oleh Wietse Venema (http://www.porcupine.org/wietse/) dan termasuk salah satu proyek *freeware*. Mulai digarap Wietse saat berkunjung ke IBM T. J. Watson Research. Wietse diberi kesempatan oleh IBM untuk menulis *software* ini. *Original*-nya *software* tersebut diberi nama Vmailer, namun diganti menjadi Postfix atas saran IBM. (Rahmat, 2006).

b. Cara Kerja *Postfix*

Dalam proses pengiriman *e-mail* Postfix menggunakan empat antrian utama yaitu *maildrop, incoming, active*, dan *deferred*. Cara kerja Postfix dapat dilihat pada Gambar 1.



Gambar 1 Konstruksi sistem Postfix

Pesan *mail* diposting secara lokal disimpan ke antrian *maildrop* dan diambil oleh *daemon pickup*. Dari *daemon pickup* diteruskan ke *daemon cleanup*. Fungsi *daemon pickup* adalah menambahkan *header From*: dan memperbaiki *header-header* pesan yang salah, menyusun penulisan ulang (*rewriting*) *address* ke bentuk standar yaitu user@fully.qualified.domain. Setelah dilakukan pengecekan pada *daemon cleanup*, *mail* diteruskan ke antrian *incoming*. Antrian *incoming* digunakan untuk *mail* yang belum diperhatikan oleh *queue manager*. Dari antrian *incoming* diteruskan ke antrian *active*. Antrian *active* merupakan antrian terbatas (dalam *size*-nya) untuk *mail-mail* yang telah dibuka *queue manager* untuk dihantarkan. *Mail* yang belum bisa dihantarkan akan diserahkan ke antrian *deferred* secara langsung sehingga tidak membebani antrian

active. Dari *daemon queue manager* maka *mail* dapat dikirim ke *mailbox* pada jaringan lokal (Rahmat, 2006).

2.1.6. SquirrelMail

SquirrelMail adalah salah satu paket *webmail* standar yang ditulis dalam bahasa pemrograman PHP4. Pemrograman PHP-nya sudah mendukung protokol POP, IMAP, dan SMTP, dan seluruh halamannya di-*render* ke dalam HTML (tanpa *Java Script*) untuk memaksimalkan penampilan saat di *browser*. Untuk itu tentu saja harus mengaktifkan web server. Di dalam paket SquirrelMail sudah terdapat seluruh fungsi *e-mail*, termasuk *address book* dan manipulasi *folder* atau direktori (Tri, 2009).

2.1.7. Dovecot

Dovecot adalah open source server POP3 dan IMAP untuk Linux atau Unix. Program ini melengkapi Postfix dengan kinerja tinggi, kemudahan administrasi, dan keamanan yang solid. Dovecot merupakan sebuah aplikasi yang dijalankan untuk mengikuti protokol IMAP dan POP3 (Tri, 2009).

2.1.8. ClamAV

ClamAV adalah anti virus *open source* (GPL) yang dirancang untuk mendeteksi *trojan*, virus, *malware*, dan ancaman berbahaya lainnya. Secara *de facto* ClamAV adalah standar untuk pemindaian *mail gateway* (ClamAV, 2013).

2.1.9. SpamAssassin

SpamAssassin adalah *mail* filter untuk mengidentifikasi *spam*. SpamAssassin adalah filter *e-mail* cerdas yang menggunakan beragam tes untuk mengidentifikasi *e-mail* yang tidak diinginkan, yang lebih dikenal sebagai *spam*. Tes diterapkan pada *e-mail header* dan konten untuk menggolongkan *e-mail* menggunakan metode statistik canggih. Sebagai tambahan, SpamAssassin memiliki arsitektur modular yang memungkinkan teknologi lain cepat digunakan untuk melawan spam dan dirancang untuk integrasi yang mudah ke hampir semua sistem *e-mail* (Ulcha, 2009).

3. Implementasi Mail Server Menggunakan Postfix

3.1. Analisis Jaringan

3.1.1. Analisis Masalah

Analisis masalah ini dilakukan dengan mengamati kondisi jaringan di perusahaan dan juga dengan cara melakukan wawancara, sehingga diketahui kebutukan perangkat apa saja yang digunakan untuk mengelola pesan *e-mail*. Selain itu aplikasi-aplikasi pendukung *mail* server juga dipasang seperti anti virus, anti *spam*, dan aplikasi *webmail*.

3.1.2. Analisis Kebutuhan

a. Perangkat Keras

Perangkat keras yang digunakan dalam pembangunan *mail* server adalah sebagai berikut :

1. *Personal Computer* (PC) server.
2. *Personal Computer* (PC) dan laptop *client.*
3. Kabel UTP.

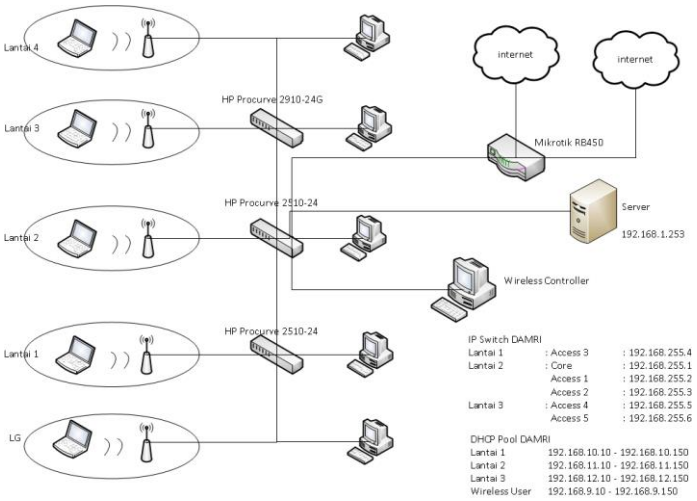
b. Perangkat Lunak

Perangkat lunak yang digunakan dalam pembangunan *mail* server ini adalah sebagai berikut :

1. Sistem Operasi PC server: Fedora 17.
2. Sistem Operasi PC dan laptop *client*: Windows XP Professional SP3 dan Windows 7.
3. Aplikasi postfix-2.9.5-1.fc17.i686.
4. Aplikasi dovecot-2.1.13-1.fc17.i686.
5. Aplikasi bind-9.9.2-3.P1.fc17.i686.
6. Aplikasi clamav-0.97.6-1700.fc17.i686.
7. Aplikasi clamsmtp-1.10-9.fc17.i686.
8. Aplikasi spamassassin-3.3.2-14.fc17.i686.
9. Aplikasi openssl-1.0.0k-1.fc17.i686.
10. Aplikasi squirrelmail-1.4.22-7.fc17.noarch.
11. Aplikasi Mozilla Thunderbird 17.0.6.

3.2. Perancangan

Tahap perancangan ini bertujuan untuk memberikan gambaran berupa rancangan topologi yang digunakan serta alokasi IP Address pada perangkat jaringan yang digunakan. Contoh topologi jaringan *mail server* dapat dilihat pada Gambar 2.



Gambar 2 Topologi Jaringan

3.3. Implementasi

3.3.1. DNS Server

DNS *server* berfungsi untuk menerjemahkan nama domain ke alamat IP dan sebaliknya. Aplikasi yang digunakan sebagai DNS server adalah BIND. Instalasi BIND dilakukan menggunakan yum. Berikut ini adalah perintah yang digunakan untuk melakukan instalasi BIND.

```
yum install bind
```

a. Konfigurasi named.conf

Aplikasi BIND memiliki berkas utama yaitu named.conf. Berkas named.conf berada di /etc. Perintah yang digunakan untuk mengonfigurasi named.conf adalah sebagai berikut :

```
vi /etc/named.conf
```

b. Konfigurasi berkas *zone*

Konfigurasi berkas *zone* berisi data mengenai domain dan subdomain yang digunakan pada server. Berkas ini berlokasi di /var/named. Berikut ini adalah perintah yang dijalankan untuk membuat berkas zone. Berkas ini diberi nama db.xxxxx.

```
vi /var/named/db.xxxxx
```

c. Konfigurasi *Reverse Zone*

Memetakan alamat IP ke sebuah *hostname* merupakan fungsi dari berkas *reverse zone*. Lokasi berkas tersebut berada di /var/named. Berkas *reverse zone* ini dibuat dengan nama 1.rev.

```
vi /var/named/1.rev
```

3.3.2. Postfix

Postfix adalah *mail* server gratis berbasis *open source* yang dibuat oleh Wietse Venema. Untuk menjalankan Postfix, maka paket Postfix harus di-*install* perintah berikut ini.

```
yum install postfix
```

a. Konfigurasi main.cf

Berkas konfigurasi utama dari Postfix adalah main.cf. Lokasi berkas tersebut terletak di /etc/postfix. Untuk melihat berkas main.cf, dapat menggunakan teks editor dengan vi menjalankan perintah di bawah ini.

```
vi /etc/postfix/main.cf
```

b. Konfigurasi header_checks

Berkas header_checks digunakan untuk mengecek *header* dari *e-mail*. Secara *default* lokasi header_cheks berada di /etc/postfix. Berikut ini adalah parameter yang ditambahkan pada header_checks.

```
#reject if email address is empty
/^From:.*<#.*@.*>/ REJECT
/^Return-Path:.*<#.*@.*>/ REJECT

#drop spam
/^X-Spam-Flag: YES/ DISCARD SpamAssassin
Confirmed Spam Content
/^(Subject: \[SPAM\])(.+)$/ DISCARD Spam
Content
/^X-Spam-Level: \*{15,}.*/ DISCARD
```

Parameter-parameter ini disimpan mulai dari baris pertama pada header_checks. Parameter pertama digunakan untuk menolak *e-mail* jika *e-mail address*-nya kosong. Parameter kedua digunakan untuk membuang *e-mail* jika *e-mail* terdeteksi sebagai *spam*. Parameter kedua aktif jika *mail* server sudah dipasang aplikasi anti *spam* seperti SpamAssassin.

3.3.3. Dovecot

Dovecot digunakan untuk melengkapi Postfix sebagai *mail* server. Dovecot adalah aplikasi POP3 dan IMAP server yang bertugas untuk meneruskan *e-mail* dari server ke *client*. Aplikasi Dovecot di-*install* melalui terminal dengan perintah berikut ini.

```
yum install dovecot
```

a. Konfigurasi dovecot.conf

Berkas konfigurasi utama dari Dovecot adalah dovecot.conf. Berkas ini berada di /etc/dovecot. Berkas dovecot.conf dapat dikonfigurasi dengan menggunakan perintah berikut ini.

```
vi /etc/dovecot/dovecot.conf
```

Protokol yang digunakan pada Dovecot harus ditentukan. Di bawah ini adalah parameter yang digunakan untuk menentukan protokol tersebut.

```
protocols = imap imaps pop3 pop3s lmtp
```

Parameter protocols terdapat pada baris 20 dan diisi dengan IMAP, IMAPS, POP3, POP3S, dan LMTP. Protokol tersebut digunakan untuk membuka atau mengirimkan *e-mail* dari server ke *client*. Protokol IMAP dan IMAPS digunakan untuk membaca *e-mail* tanpa men-*download* ke direktori lokal. Perbedaan dari IMAP dan IMAPS adalah IMAPS sudah menerapkan metode enkripsi sehingga lebih aman. POP3 dan POP3S adalah protokol yang digunakan untuk men-*download e-mail* dari server ke

direktori lokal. Perbedaan POP3 dan POP3S adalah POP3S sudah menerapkan metode enkripsi. LMTP merupakan protokol yang digunakan untuk memproses permintaan pengiriman pesan dari *daemon queue manager* milik Postfix.

Selain parameter protocols, parameter listen juga harus diubah. Parameter listen digunakan untuk menentukan versi alamat IP yang digunakan pada jaringan. Berikut ini adalah pengaturan untuk parameter listen.

```
listen = *
```

Parameter listen berisi tanda bintang (*). Tanda bintang ini digunakan jika versi yang digunakan hanya IPv4.

b. Konfigurasi 10-auth.conf

Berkas 10-auth.conf digunakan untuk proses autentikasi *user* yang *login*. Terdapat dua parameter yang diubah pada berkas 10-auth.conf. Berikut ini adalah parameter-parameter tersebut.

```
disable_plaintext_auth = no
```

Parameter ini terdapat pada baris 9. Dengan member nilai no, parameter ini memungkinkan *password* dapat melalui jaringan yang tidak menggunakan enkripsi.

```
auth_mechanism = plain login
```

Parameter ini terdapat pada baris 99. Dengan member nilai plain login, parameter ini memungkinkan proses autentikasi ditransmisikan tanpa enkripsi.

c. Konfigurasi 10-mail.conf

Berkas 10-mail.conf digunakan untuk menentukan lokasi *mailbox* yang digunakan. Hanya ada satu parameter yang diubah yaitu mail_location. Berikut ini pengaturan dari parameter tersebut.

```
mail_location = maildir:~/Maildir
```

Parameter mail_location terdapat pada baris 30. Konfigurasi main.cf milik Postfix terdapat pengaturan *mailbox* yang digunakan adalah Maildir, maka mail_location dipilih maildir:~/Maildir.

d. Konfigurasi 10-master.conf

Berkas 10-master.conf dapat digunakan untuk menentukan server SMTP yang akan digabungkan dengan Dovecot. Server SMTP yang digunakan adalah Postfix. Berikut ini adalah parameter yang diubah pada berkas 10-master.conf.

```
unix_listener   /var/spool/postfix/private/auth
{
        mode = 0666
        user = postfix
        group = postfix
}
```

Berkas *auth* terdapat di direktori /var/spool/postfix/private. Berkas ini memiliki hak eksekusi *read* dan *write* untuk *user*, *group*, dan *other*. *User* dan *group* yang memiliki berkas *auth* adalah postfix.

e. Konfigurasi 10-ssl.conf

Berkas 10-ssl.conf digunakan untuk mengatur SSL pada Dovecot. Terdapat parameter ssl yang digunakan untuk mengaktifkan atau menonaktifkan SSL. Berikut ini adalah pengaturan dari parameter ssl.

```
ssl = yes
```

Dengan mengisikan nilai yes pada parameter ssl, maka Dovecot akan melakukan enkripsi terhadap *e-mail* yang masuk pada protokol IMAP dan POP3.

3.3.4. SSL

SSL digunakan untuk mengenkripsi *e-mail* sehingga lebih aman. Sertifikat SSL memiliki dua bagian utama yaitu sertifikat itu sendiri dan kunci publik. SSL diletakkan di /etc/nginx/ssl karena SSL juga digunakan oleh aplikasi Nginx. Direktori SSL dibuat dengan cara di bawah ini.

```
mkdir /etc/nginx/ssl
```

Direktori ssl yang terletak di /etc/nginx digunakan untuk menyimpan sertifikat-sertifikat yang dibuat.

a. Membuat kunci pribadi

Membuat kunci pribadi dapat dilakukan dengan perintah seperti di bawah ini.

```
openssl genrsa -des3 -out xxxxx.key 1024
```

Aplikasi genrsa digunakan untuk membuat kunci pribadi dengan menggunakan *cipher* DES3 dan panjang 1024 bit. Genrsa menggunakan algoritma RSA. Kunci pribadi ini disimpan ke dalam berkas xxxxx.key.

b. Membuat CSR (Certificate Signing Request)

Pembuatan sertifikat publik dilakukan dengan perintah berikut ini.

```
openssl req -new -key xxxxx.key -out xxxxx.csr
```

Perintah di atas akan memunculkan daftar konfigurasi yang perlu diatur.

c. Menghapus frase sandi

Frase sandi dapat dihapus dengan mengetikkan perintah berikut ini.

```
cp xxxxx.key xxxxx.key.org
openssl rsa -in xxxxx.key.org -out xxxxx.key
```

d. Menandatangani sertifikat permohonan

Sertifikat permohonan yang telah dibuat harus ditandatangani. Untuk menandatangi sertifikat permohonan, menggunakan perintah sebagai berikut.

```
openssl x509 -req -days 1825 -in xxxxx.csr -
signkey xxxxx.key -out xxxxx.crt
```

Perintah tersebut akan membuat sertifikat publik dengan nama xxxxx.crt yang tersimpan di /etc/nginx/ssl. Masa berlaku dari sertifikat permohonan yang dibuat adalah selama 5 tahun. Empat kunci yang ada didalam folder SSL yang dibuat, yaitu :

1 xxxxx.key : Berkas berisi kunci pribadi CA
2 xxxxx.crt : Berkas sertifikat public CA
3 xxxxx.csr : Berkas sertifikat permohonan xxxxx.co.id
4 xxxxx.key.org : Berkas hasil copy dari xxxxx.key

e. Konfigurasi SSL pada main.cf

SSL pada Postfix diaktifkan dengan menambahkan beberapa parameter pada berkas main.cf. Berikut ini adalah parameter-parameter yang ditambahkan pada main.cf.

```
smtpd_use_tls = yes
smtpd_tls_cert_file = /etc/nginx/ssl/xxxxx.crt
smtpd_tls_key_file = /etc/nginx/ssl/xxxxx.key
smtpd_tls_session_cache_database =
btree:/etc/postfix/smtpd_scache
```

Berikut ini adalah penjelasan dari parameter-parameter di atas.

1. smtpd_use_tls = yes

   Parameter di atas digunakan untuk mengaktifkan SSL pada Postfix.

2. smtpd_tls_cert_file = /etc/nginx/ssl/xxxxx.crt

   Parameter di atas digunakan untuk menentukan dimana berkas sertifikat SSL yang digunakan.

3. smtpd_tls_key_file = /etc/nginx/ssl/xxxxx.key

   Parameter di atas digunakan untuk menentukan dimana berkas kunci pribadi SSL yang digunakan.

4. smtpd_tls_session_cache_database = btree:/etc/postfix/smtpd_scache

   Parameter di atas digunakan untuk menentukan dimana *session cache database* disimpan.

f. Konfigurasi SSL pada master.cf

Berkas master.cf berada di /etc/postfix. Berkas ini mengatur proses yang berjalan pada Postfix. Berikut ini adalah parameter yang diubah pada berkas master.cf.

```
smtps     inet   n     -     n     -     -
smtpd
  -o syslog_name=postfix/smtps
  -o smtpd_tls_wrappermode=yes
```

Parameter di atas berada pada baris 22 sampai 24 dan diaktifkan dengan menghapus tanda # di depan parameter tersebut. Parameter di atas digunakan untuk mengaktifkan protokol SMTPS, yaitu protokol SMTP yang sudah *secure* karena melalui proses enkripsi.

g. Konfigurasi SSL pada 10-ssl.conf

Berkas 10-ssl.conf berada di /etc/dovecot/conf.d. Sebelumnya parameter ssl pada 10-ssl.conf sudah diaktifkan, tetapi sertifikat dan kunci publik belum ditentukan. Berikut ini parameter yang diubah pada 10-ssl.conf.

```
ssl_cert =
</etc/nginx/ssl/xxxxx.crt
ssl_key =
</etc/nginx/ssl/xxxxx.key
```

Parameter ssl_cert dan ssl_key berada pada baris 14 dan 15. Parameter ini digunakan untuk menentukan letak sertifikat dan kunci publik dari SSL.

3.3.5. ClamAV dan ClamSMTP

ClamAV merupakan anti virus bersifat *open source*. ClamAV didesain untuk mendeteksi virus, *trojan*, dan *malware*. Sedangkan ClamSMTP merupakan anti virus yang berjalan pada protokol SMTP. Berikut ini adalah proses instalasi dari ClamAV dan ClamSMTP.

```
yum install clamav clamav-update clamsmtp
```

a. Konfigurasi freshclam.conf

Berkas freshclam.conf berada di direktori /etc. Berkas freshclam.conf mengatur konfigurasi mengenai proses *update database* virus ClamAV. Berikut ini pengaturan yang dilakukan agar dapat melakukan *update database* virus.

```
#Example
```

Pada baris delapan terdapat kata Example, jika tidak diberi tanda # maka tidak dapat melakukan *update database* virus. Proses *update database* virus dapat dilakukan dengan mengetikkan perintah freshclam pada terminal.

b. Konfigurasi clamsmtpd.conf

Berkas clamsmtpd.conf berada di direktori /etc. Berkas ini berisi pengaturan mengenai perlindungan *e-mail* dari virus. Ada beberapa parameter yang diubah agar *e-mail* yang masuk ke server dapat diperiksa oleh ClamAV. Berikut ini adalah parameter-parameter yang diubah pada clamsmtpd.conf.

1 OutAddress: 127.0.0.1:10026

Parameter OutAddress berada pada baris enam. Parameter ini digunakan untuk meneruskan *e-mail* yang sudah diperiksa oleh ClamSMTP. Alamat IP yang digunakan adalah alamat *localhost* dan *port* yang digunakan adalah *port* 10026.

2 Listen: 127.0.0.1:10025

Parameter Listen berada pada baris 22. Parameter ini digunakan untuk memeriksa *e-mail* yang masuk ke *mail* server. Alamat IP yang digunakan adalah alamat *localhost* dan *port* yang digunakan adalah *port* 10025.

3 Header: X-Virus-Scanned: ClamAV using ClamSMTP

Parameter diatas berada pada baris 28. Parameter ini diaktifkan sebagai pemberitahuan bahwa *e-mail* diperiksa oleh ClamSMTP.

4 Action: drop

Parameter Action berada pada baris 34. Parameter ini digunakan jika ada virus yang terdeteksi. Dengan member nilai drop maka virus akan langsung dibuang.

c. Konfigurasi ClamSMTP pada main.cf

Terdapat satu parameter yang ditambahkan pada baris terakhir main.cf. Berikut ini adalah parameter tersebut.

```
content_filter = scan:127.0.0.1:10025
```

Parameter di atas digunakan untuk melakukan filter terahadap e-mail yang masuk ke server dengan melakukan scan terhadap alamat IP localhost milik server.

d. Konfigurasi ClamSMTP pada master.cf

Ada beberapa parameter yang ditambahkan pada baris terakhir master.cf. Berikut ini adalah parameter tersebut.

```
scan unix -       -       n       -       16
smtp
   -o smtp_data_done_timeout=1200
   -o smtp_send_xforward_command=yes
    -o disable_dns_lookups=yes
127.0.0.1:10026 inet n       -       n       -
16       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,r
eject
   -o mynetworks_style=host
   -o
smtpd_authorized_xforward_hosts=127
.0.0.0/8
```

Parameter di atas dimasukkan pada master.cf untuk dilakukan *scan* oleh ClamSMTP dan mengecek *e-mail* setelah dilakukan filter.

3.3.6. SpamAssassin

SpamAssassin adalah anti *spam* yang berbasis *open source*. SpamAssassin memeriksa *header* dan isi dari *e-mail* untuk menentukan apakah itu *spam* atau bukan. Berikut ini adalah *syntax* yang digunakan untuk meng-*install* SpamAssassin.

```
yum install spamassassin razor-agents pyzor
```

Berkas konfigurasi utama dari SpamAssassin adalah local.cf. Berkas ini terdapat pada direktori /usr/share/spamassassin. SpamAssassin dapat menandakan apakah e-mail yang masuk ke server berisi spam atau bukan dengan mengaktifkan parameter berikut ini.

```
rewrite_header Subject *****SPAM*****
```

Parameter di atas mengubah *subject* dari *e-mail* dengan menambahkan kata [SPAM] pada *e-mail* yang berisi *spam*.

3.3.7. SquirrelMail

Aplikasi SquirrelMail adalah sebuah aplikasi *webmail* yang berbasis *open source*. SquirrelMail dibangun dengan bahasa PHP dan mendukung protokol SMTP dan IMAP. Berikut ini adalah *syntax* yang digunakan untuk men-*download* dan meng-*install* SquirrelMail.

```
yum install squirrelmail
```

Ada beberapa *plugin* yang digunakan untuk meningkatkan kinerja SquirrelMail. *Plugin* tersebut adalah compatibility, empty_trash, secure_login, login_check, dan username. *Plugin-plugin* tersebut harus disimpan di /usr/share/squirrelmail/plugins. Berikut ini adalah perintah yang digunakan untuk men-*download plugin-plugin* tersebut.

```
wget
http://www.squirrelmail.org/plugins/compatibil
ity-2.0.16-1.0.tar.gz
wget
http://www.squirrelmail.org/plugins/empty_tras
h-1.4-1.2.2.tar.gz
wget
http://www.squirrelmail.org/plugins/secure_log
in-1.4-1.2.8.tar.gz
wget
http://www.squirrelmail.org/plugins/login_chec
k-1.0-1.4.10.tar.gz wget
http://www.squirrelmail.org/plugins/username-
2.3-1.0.0.tar.gz
```

Berkas konfigurasi utama dari SquirrelMail adalah conf.pl yang berada di /usr/share/squirrelmail/config. Perintah yang digunakan untuk menjalankan berkas conf.pl adalah /usr/share/squirrelmail/config/conf.pl.

Terdapat beberapa menu yang harus diatur agar SquirrelMail dapat berjalan dengan baik. Menu-menu yang diatur adalah *Organization Preferences*, Server *Settings*, *General Defaults*, dan *Plugins*. Masuk ke menu *Organization Preferences* dapat dilakukan dengan mengetik angka 1.

Pengaturan yang dilakukan pada *Organization Preferences* adalah *Organization Name*, *Organization Logo*, Org. *Logo Width/Height*, *Organization Title*, dan *Signout Page*. Pengaturan server yang digunakan untuk SquirrelMail terdapat pada menu Server *Settings*.

Pengaturan umum pada Server *Settings* adalah pada Domain dan Sendmail or SMTP. Pengaturan Domain berisi domain yang digunakan yaitu xxxxx.co.id. Sendmail or SMTP diisikan SMTP. Server *Settings* memiliki pengaturan lebih untuk IMAP dan SMTP server.

Domain mail.xxxxx.co.id digunakan sebagai *hostname* dari IMAP server. Dovecot dipilih pada Server *Software* karena IMAP server yang digunakan adalah Dovecot. *Delimiter* dipilih *detect* agar *delimiter* yang digunakan menyesuaikan dengan *software* IMAP server yang digunakan.

Domain mail.xxxxx.co.id digunakan sebagai *hostname* dari SMTP server. Autentikasi untuk SMTP server dipilih *login*. Pengaturan selanjutnya adalah *General Options*.

Pengaturan pada *General Options* terdapat pada *Hide* SM *attributions* yang diubah nilainya menjadi *true*.

Ada beberapa *plugin* yang ditambahkan pada SquirrelMail. Secara *default* plugin delete_move_next, squirrelspell, dan newmail sudah digunakan. Berikut ini adalah penjelasan dari beberapa *plugin* yang ditambahkan untuk SquirrelMail.

1 compatibility

Plugin compatibility digunakan agar setiap *plugin* yang dimasukkan pada dapat cocok dengan SquirrelMail yang digunakan.

2 empty_trash

Plugin empty_trash digunakan agar *trash* pada setiap user yang menggunakan SquirrelMail dapat dihapus otomatis secara periodik.

3 secure_login

Plugin secure_login digunakan untuk mengaktifkan fitur HTTPS ketika ada user yang login ke SquirrelMail.

4 login_check

Plugin login_check digunakan agar hanya bisa satu *user* yang dapat *login* SquirrelMail pada satu browser.

5 Username

Plugin username digunakan untuk memunculkan *username* pada halaman *login* SquirrelMail.

Konfigurasi conf.pl dapat disimpan dengan mengetik huruf S dan Q untuk keluar dari conf.pl. Halaman *login* SquirrelMail dapat diakses dengan mengetikkan www.xxxxx.co.id/webmail pada *browser*.

Terdapat konfigurasi tambahan pada *plugin* login_check, secure_login, dan username. Konfigurasi *plugin* login_check dapat dilakukan dengan masuk ke direktori /usr/share/squirrelmail/plugins/login_check. Berkas config.sample.php disalin menggunakan *syntax* cp config.sample.php config.php. Berkas config.php dapat dikonfigurasi dengan menjalankan *syntax* vi config.php. Berikut ini adalah parameter yang diubah pada config.php.

```
$change_back_to_http_after_login = 0;
```

Dengan memberi nilai 0 pada parameter $change_back_to_http_after_login, maka protokol HTTPS tetap digunakan ketika *login* sudah dilakukan. Konfigurasi *plugin* secure_login dapat dilakukan dengan masuk ke direktori /usr/share/squirrelmail/plugins/ secure_login. Berkas utama secure_login adalah config_default.php. Berkas

config_default.php dapat dijalankan dengan *syntax* vi config_default.php. Berikut ini adalah konfigurasi yang dilakukan pada config_default.php.

```
$login_check_method = 3;
```

Dengan memberi nilai 3 pada parameter $login_check_method, maka secure_login akan men-*redirect user* yang sebelumnya sudah *login* pada SquirrelMail. Konfigurasi *plugin* username dilakukan setelah *user* melakukan *login*.

Submenu *Display Preferences*. Mengubah menu *Show Username*, *Show Username Position*, dan *Show Username in Message of The Day* dapat memunculkan nama *user* yang sedang menggunakan SquirrelMail.

3.3.8. Mozilla Thunderbird

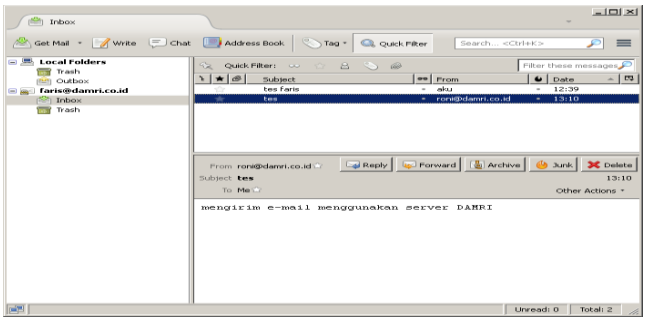
Mozilla Thunderbird adalah salah satu *mail client* gratis yang digunakan sebagai alternatif dari *mail client* yang berbayar seperti Microsoft Outlook. Mozilla Thunderbird dapat di-*download* di http://www.mozilla.org/thunderbird.

SSL sudah dipasang pada Postfix dan Dovecot maka pengaturan protokol POP3 dan SMTP yang digunakan Mozilla Thunderbird menggunakan port 995 untuk POP3S dan 465 untuk SMTPS.

3.4. Pengujian

3.4.1. Pengiriman *E-mail*

Pengiriman *e-mail* dilakukan dengan aplikasi Mozilla Thunderbird dan *webmail* SquirrelMail. Hasil pengujian pengiriman *e-mail* ditunjukan pada Gambar 3.



Gambar 3 *User* menerima e-mail menggunakan Mozilla Thunderbird

3.4.2. Pengujian ClamAV

Pengujian anti virus menggunakan ClamAV dilakukan untuk menguji server *e-mail* apakah dapat memblok *e-mail* yang berisi virus atau tidak. *Script* virus yang digunakan dari EICAR.

Pesan *e-mail* yang berisi virus tidak akan diterima karena sudah diblok oleh ClamAV. Berikut ini adalah *log* yang menunjukkan jika virus sudah diblok.

```
Apr 14 17:51:01 localhost clamsmtpd: 100001:
accepted connection from: 127.0.0.1
Apr 14 17:51:01 localhost postfix/smtpd[2710]:
connect from localhost[127.0.0.1]
Apr 14 17:51:01 localhost postfix/smtpd[2710]:
D775921F7B: client=localhost[127.0.0.1]
Apr 14 17:51:01 localhost postfix/smtp[2708]:
B742B21F88: to=<nur@xxxxx.co.id>,
relay=127.0.0.1[127.0.0.1]:10025, delay=0.53,
delays=0.47/0.01/0.05/0, dsn=2.0.0, status=sent
(250 Virus Detected; Discarded Email)
Apr 14 17:51:01 localhost postfix/qmgr[1945]:
B742B21F88: removed
Apr 14 17:51:01 localhost clamsmtpd: 100001:
from=faris@xxxxx.co.id, to=nur@xxxxx.co.id,
status=VIRUS:Eicar-Test-Signature
Apr 14 17:51:01 localhost postfix/smtpd[2710]:
disconnect from localhost[127.0.0.1]
```

3.4.3. Pengujian SpamAssassin

Pengujian anti *spam* menggunakan SpamAssassin dilakukan untuk menguji server *e-mail* apakah dapat memblok *e-mail* yang berisi *spam* atau tidak. *Script spam* yang digunakan dari GTUBE. Pesan *e-mail* yang berisi *spam* tidak diterima karena sudah diblok oleh SpamAssassin.

4. KESIMPULAN

4.1. Kesimpulan

Dengan adanya server di suatu perusahaan, semua *e-mail* dikelola oleh admin tanpa harus melakukan *remote* ke layanan *hosting*. Postfix merupakan salah satu aplikasi *mail* gratis yang dibuat oleh Wietse Venema. Postfix dapat diintegrasikan dengan Dovecot agar *client* dapat membaca dan mengambil *e-mail* dari *server*. Selain itu penggunaan ClamAV sebagai anti virus dan SpamAssassin sebagai anti *spam* dapat meningkatkan keamanan *e-mail* dan *mail* server dari gangguan virus dan *spam*.

Penggunaan SquirrelMail sebagai *webmail* juga bisa digunakan jika *client* tidak memiliki sebuah aplikasi *mail client* seperti Mozilla Thunderbird.

4.2. Saran

Pembangunan *mail* server dapat dikembangkan lagi. LDAP dapat digunakan sebagai *database* untuk menyimpan informasi *user*. Selain itu aplikasi AmaVis dapat digunakan sebagai perantara antara Postfix dengan anti virus dan anti *spam*.

5. DAFTAR PUSTAKA

Cartealy, Imam. 2013. *LINUX NETWORKING Ubuntu, Kubuntu, Debian, ddl*. Jakarta: Jasakom.

Savitri, Tri Ratna. 2009. Membangun E-mail Server Menggunakan Postfix, Dovecot, dan SquirrelMail di Direktorat Jendral Planologi Departemen Kehutanan [Tugas Akhir]. Bogor (ID): Direktorat Jendral Planologi Departemen Kehutanan

Sofana, Iwan. 2007. *Mudah Membangun Server dengan Fedora Core.* Bandung: Informatika Bandung.

http://wiki.apache.org/spamassassin/SpamAssassin (15 Mei 2013)