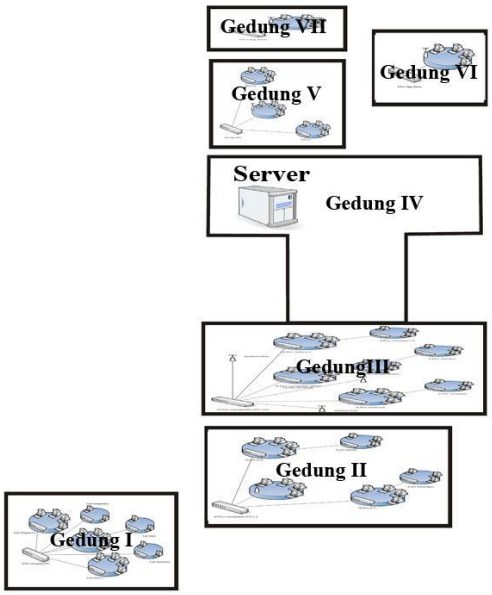
BAB 3
PEMBAHASAN

3.1 Kegiatan Kerja Praktek

Kegiatan kerja praktek dilakukan selama dua bulan di Kantor Balai Besar Bahan dan Barang Teknik (B4T) mulai dari tanggal 9 Juli sampai dengan tanggal 9 Agustus 2012, hari kerja praktek bebas karena dari pihak tempat kerja praktek tidak mewajibkan untuk datang setiap hari. Pelaksanaan kerja praktek dimulai dari jam 08.00-16.00 WIB. Dalam melaksanakan kerja praktek ini dibantu oleh pembimbing bernama Galih Ginanjar,S.Si.,MT.

3.2 Analisis Fisik Bangunan

Kantor Balai Besar Bahan dan Barang Teknik (B4T) terdiri dari 7 gedung yang terdiri dari beberapa lantai yang didalamnya terdapat beberapa ruangan. Dari hasil analisis yang telah dilakukan di Balai Besar Bahan dan Barang Teknik (B4T) memiliki denah bangunan sebagai berikut :

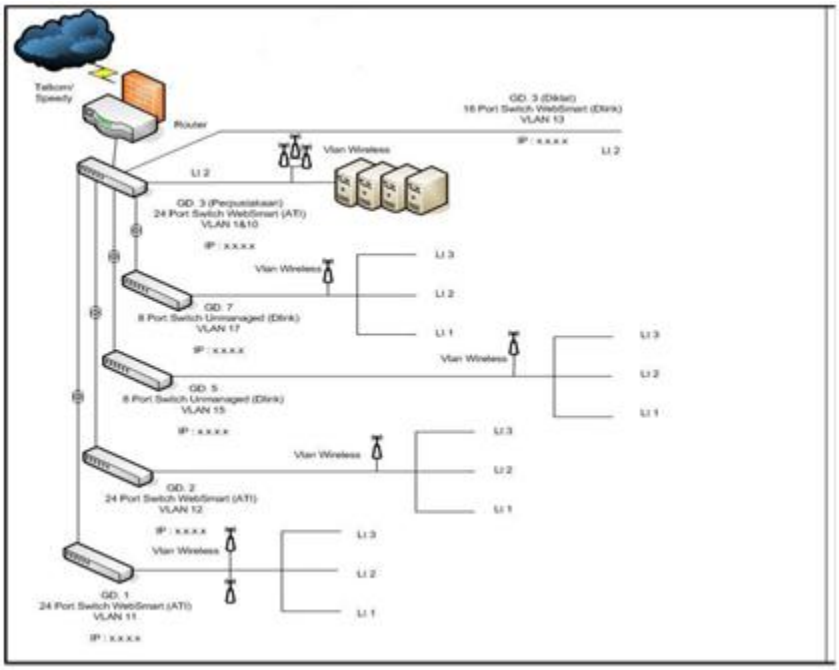


Gambar 3.1 Denah Bangunan B4T

3.3 Analisis Jaringan

Topologi yang diterapkan pada intranet di kantor ini adalah topologi bintang dengan menggunakan media transmisi kabel. Penerapan topologi ini dikarenakan fleksibilitas yang tinggi, kemudahan dalam pendeteksian kesalahan atau kerusakan pada jaringan dan bila ada salah satu komputer atau perangkat yang mengalami kerusakan maka tidak akan mempengaruhi yang jaringan yang lainnya. Adapun media transmisi kabel yang digunakan adalah *twisted pair* jenis UTP tipe CAT5 dengan konektor RJ-45. Dalam pemasangan kabel UTP ke konektor RJ-45 digunakan tipe penyambungan *straight* untuk kabel yang terhubung antara komputer dengan switch. Jenis protokol yang digunakan dalam jaringan ini ialah protokol TCP/IP yang merupakan jenis protokol yang umum dipakai jaringan komputer.

Balai Besar dan Barang Teknik (B4T) memiliki sebuah jaringan dimana berfungsi untuk komunikasi atau pengiriman data. Secara umum skema intranet pada kantor Balai Besar Bahan dan Barang Teknik digambarkan seperti gambar 3.2 dibawah ini.



Gambar 3.2 Skema Jaringan Intranet

Keterangan gambar :

a. Modem Speedy

Internet Service Provider yang digunakan pada instansi B4T adalah Telkom Speedy.

b. MikroTik RouterOS™

B4T menggunakan MikroTik RouterOS™ sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router network

c. *Proxy*

B4T menggunakan *Proxy Server* berbasis Windows Server.

d. *Switch*

Hub ini berfungsi untuk menerima sinyal dari satu komputer dan mentransmisikannya ke komputer yang lain.

e. *Client*

Client ini merupakan komputer yang terhubung ke HUB yang memiliki akses lokal maupun internet.

3.4 Analisis Perangkat Keras

Spesifikasi Perangkat Keras *server* dan klien di kantor Balai Besar Bahan dan Barang teknik diantaranya :

Tabel 3.1 Spesifikasi Perangkat Keras Server

Processor	Intel Core 2 Duo
Memory	1GB
HDD	SEAGATE 4TB
Power	Power Suply 450 W
CD/DVD Rom	ASUS DVD RW
System Operasi	Ubuntu Server 12.04

Tabel 3.2 Spesifikasi Perangkat Keras Klien

Processor	Pentium 4
Memory	1GB
HDD	160 GB
Power	Power Suply 450 W
CD/DVD Rom	ASUS DVD RW
System Operasi	Windows XP

3.5 Analisis Sistem

Analisis sistem dapat didefinisikan sebagai penguraian dari suatu sistem yang utuh ke dalam bagian-bagian komponennya dengan maksud untuk mengidentifikasikan dan mengevaluasi permasalahan-permasalahan, kesempatan-kesempatan, hambatan-hambatan yang terjadi dan kebutuhan-kebutuhan yang diharapkan sehingga dapat diusulkan perbaikan - perbaikannya.

3.5.1 Analisis masalah

Aplikasi intranet berisi informasi yang berkaitan dengan B4T namun tidak semua hal bisa diatasi oleh aplikasi intranet. Salah satunya pengiriman *e-mail*. *Email Server* yang digunakan saat ini di B4T menggunakan *e-mail server* luar. *E-mail* ini digunakan untuk memfasilitasi apabila ada keluhan dari *client* mengenai standarisasi, sertifikasi, dan inspeksi bahan dan barang teknik. Keterbatasan pada intranet menimbulkan beberapa permasalahan yang mendorong untuk membangun e-mail server yang diharapkan dapat mengatasi permasalahan yang terjadi. Beberapa permasalahan yang mendorong untuk membangun e-mail server antara lain :

1. Terbatasnya kapasitas media penyimpanan jika menggunakan *server* luar sehingga pegawai tidak perlu khawatir akan habisnya kuota penyimpanan.
2. Tidak efisiennya pengiriman dan penerimaan *e-mail* sehingga respon balasan *e-mail* dari pegawai B4T lambat .
3. Tidak adanya kontrol atau monitoring dalam pengelolaan *e-mail* sehingga admin tidak mengetahui berapa lintas data dan berapa banyak pengguna e-mail yang mengakses e-mail.

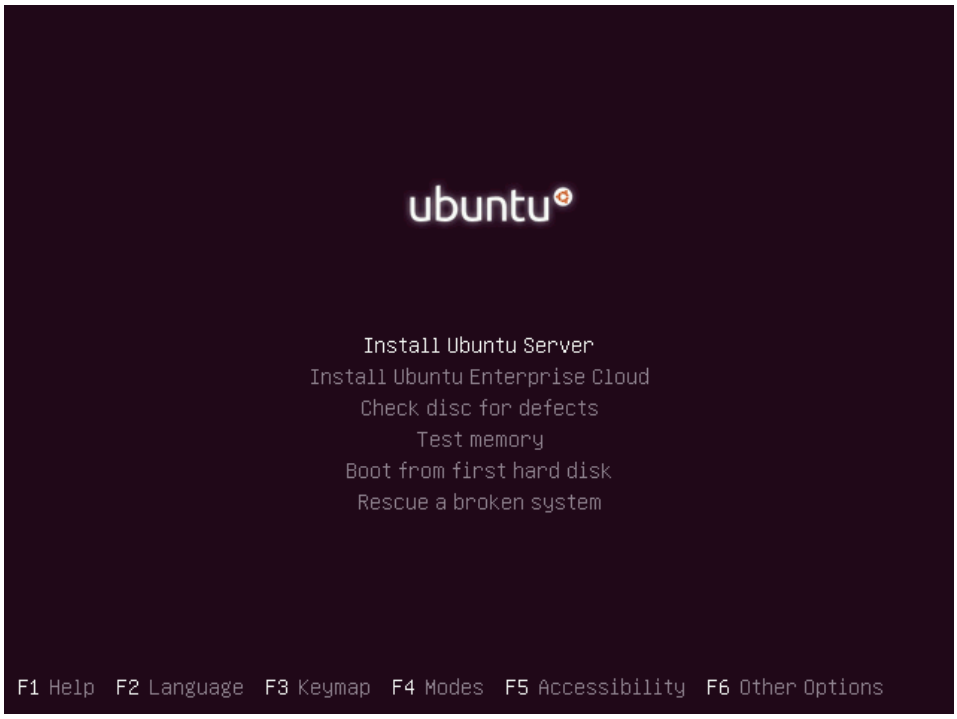
3.5.2 Analisis Sistem Yang Sedang Berjalan

Berdasarkan hasil wawancara dan observasi di Balai Besar Bahan dan Barang Teknik (B4T) pada sistem e-mail yang sedang berjalan saat ini *e-mail server* yang digunakan masih menggunakan server luar bukan server yang berada di dalam jaringan intranet B4T. Tentunya dalam sebuah kantor, institusi yang mempunyai banyak pengguna akan sangat tidak praktis jika menggunakan *e-mail server* luar karena memiliki banyak keterbatasan. Diantaranya keterbatasan media penyimpanan yang mengakibatkan pengguna e-mail menjadi terbatas dan keterbatasan untuk mengontrol dalam pengelolaan *e-mail* sehingga admin tidak dapat mengolah e-mail dengan baik yang nantinya sebagai bahan analisa berapa besar lintas data dan berapa banyak pengguna *email* yang mengakses *email*. Maka diperlukannya e-mail server dengan melakukan konfigurasi *e-mail server* sebagai pusat *e-mail* berbasis *web*.

3.6 Implementasi

3.6.1 Instalasi Ubuntu Server

Pertama tama siapakan CD Ubuntu server 12.04, jika tidak memilikinya maka perlu men-*download* versi *server* Ubuntu 12.04 dari situs ubuntu ini setelah itu membuat CD dan mulai boot dengan CD. Jika anda sudah mempunyai CD untuk installasi pastikan *boot* komputer anda sudah berada pada *option boot* CD ROM lalu masukan CD ubuntu server 12.04.



Gambar 3.3 Tampilan Awal Instalasi

3.6.2 Konfigurasi Mail Server

3.6.2.1 Konfigurasi Dasar

Konsep dasar Ubuntu adalah melacak setiap paket yang mungkin diperlukan. Login sebagai root karena sebagian besar kebutuhan untuk mengkonfigurasi server haruslah menggunakan akses sebagai root:

```
sudo su
```

Setting IP elastis untuk memberikan IP address secara permanen. AWS instance akan memberikan IP yang aneh dikarenakan IP tersebut adalah IP bawaan (default). Maka pada domain harus dilakukan perubahan:

```
hostname staf.b4t.go.id
```

Atur isi di /etc/hostname menjadi hostname yang telah ditentukan:

```
staf.b4t.go.id
```

Tambahkan hostname yang telah ditentukan pada langkah diats di baris pertama pada file /etc/hosts:

```
127.0.0.1 staf.b4t.go.id localhost

# Usually some IPv6 configuration below the first line, but leave that alone.
...
```

Sekarang langkah dimana harus men-regenerate self-signed SSL certiticate yang harus cocok dengan nama domain. Ini berguna untuk mengamankan mail server jika siap untuk dijalankan. Konsekuensinya akan memberikan peringatan pada layar ketika menggunakan host webmail di server dan memberikan peringatan dari Microsoft Outlook ketika menghubungkannya via POP, IMAP ataupun SMTP. Ketikan perintah dibawah ini:

```
apt-get install ssl-cert
make-ssl-cert generate-default-snakeoil --force-overwrite
```

3.6.2.2 LAMP Web Server

LAMP (Linux, Apache, MySQL, PHP) web server berguna untuk mengelola pengguna dikarenakan menggunakan interface berbasis web untuk administrasi pengguna nya. Jadi misalnya harus menyediakan di server Ubuntu berupa service webserver adalah langkah yang paling bagus untuk memulai. Ada jalan pintas untuk instalasi paket LAMP ndengan cara meng update data repostori. Ketikan perintah di bawah ini, tanda '^' pada akhir perintah sangatlah penting:

```
apt-get update
apt-get upgrade
apt-get install lamp-server^
```

Selama proses instalasi, akan diminta untuk memasukan password untuk MySQL pada hak akses root. Untuk mendukung server perlu juga menambahkan berbagai aplikasi seperti paket PHP dasar, APC bytecode caching, memcache support, cURL, an XML parser, and GD image processing. Ketikan perintah di bawah ini:

```
apt-get install php-apc php5-memcache php5-curl php5-gd php-xml-parser
```

3.6.2.3 Konfigurasi PHP

Konfigurasi default untuk PHP dan paket tambahan yang disebutkan di atas sudah cukup untuk penggunaan awam. Kecuali jika server yang ingin di buat memiliki kerumitan dan high-powered dalam pemrosesan, mungkin harus mengubah pengaturan yang ada di expose_php seting di dalam /etc/php5/apache2/php.ini buatlah menjadi "Off":

```
. . .
; Decides whether PHP may expose the fact that it is installed on the server
; (e.g. by adding its signature to the Web server header).  It is no security
; threat in any way, but it makes it possible to determine whether you use PHP
; on your server or not.
; http://php.net/expose-php
expose_php = Off
```

3.6.2.4 Konfigurasi Apache

Hasil akhir yang di harapkan untuk Apache adalah akan bisa menyediakan sebuah *single site* dengan berpasangan berjalannya sebuah web aplocation. Web mail dan postfix admin akan disembunyikan di *subdirectory*. Semua lalu lintas akan menuju ke HTTPS yang akan disediakan oleh web server.

Langkah pertama konfigurasi adalah dengan mengubah baris pada /etc/apache2/conf.d/security untuk meminimalisir informasi dimana Apache memberikan respon di headers. Lakukan seperti di bawah ini:

```
....
#
# ServerTokens
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of:  Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#
ServerTokens Prod
#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of:  On | Off | EMail
#
ServerSignature Off
```

Pastikan bahwa mod_rewrite, mod_ssl dan default SSL virtual host telah berjalan atau aktif. Pada baris perintah di bawah ini dibutuhkan untuk bisa menggunakan HTTPS:

```
a2enmod rewrite ssl
a2ensite default-ssl
```

Konfigurasi default site di dalam /etc/apache2/sites-available/default dapat diedit seperti di bawah ini:

```
<VirtualHost *:80>
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www
  <Directory "/">
    Options FollowSymLinks
    AllowOverride All
  </Directory>

  ErrorLog ${APACHE_LOG_DIR}/error.log
  # Possible values include: debug, info, notice, warn, error, crit,
  # alert, emerg.
  LogLevel warn

  CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Tapi tentu saja tergantung kepada kebutuhan yang mungkin berbeda. Untuk menjaga agar tetap sederhana dan seragam, maka pada bagian atas konfigurasi SSL di / etc/apache2/sites-available/default-ssl dapat diatur sebagai berikut:

```
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerAdmin webmaster@localhost

    DocumentRoot /var/www
    <Directory "/">
      Options FollowSymLinks
      AllowOverride All
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log

    # Possible values include: debug, info, notice, warn, error, crit,
    # alert, emerg.
    LogLevel warn

    CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined

    #   SSL Engine Switch:
    #   Enable/Disable SSL for this virtual host.
    SSLEngine on
    #

    # ... more default SSL configuration ...

    # You will probably need to change this next Directory directive as well
    # in order to match the earlier one.
    <Directory "/">
      SSLOptions +StdEnvVars
    </Directory>

    # ... yet more default SSL configuration ...
```

Jika menggunakan tidak menggunakan self-signed SSL certificate dan menggunakan CA certificate dengan cara membundel dari penerbit maka harus merubah baris pada /etc/apache2/sites-enabled/default-ssl seperti di bawah ini:

```
#   A self-signed (snakeoil) certificate can be created by installing
#   the ssl-cert package. See
#   /usr/share/doc/apache2.2-common/README.Debian.gz for more info.
#   If both key and certificate are stored in the same file, only the
#   SSLCertificateFile directive is needed.
SSLCertificateFile    /path/to/my/cert.crt
SSLCertificateKeyFile /path/to/my/key.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form the
#   certificate chain for the server certificate. Alternatively
#   the referenced file can be the same as SSLCertificateFile
#   when the CA certificates are directly appended to the server
#   certificate for convinience.
SSLCertificateChainFile /path/to/my/ca-bundle.crt
```

Agar *user* bisa menggunakan HTTPS, tempatkan beberapa perintah yang serupa seperti yang di bawah ini:

```
RewriteEngine On
RewriteCond %{SERVER_PORT} 80
RewriteRule ^(.*) https://staf.b4t.go.id/$1 [L]
```

3.6.2.5 Install dan Konfigurasi Memcached

Perlunya meng install Memcached adalah untuk mendukung webmail apalication yang dimaksudkan untuk menjalankan nya di server ini. Perintah untuk meng install memcached adalah sebagai berikut:

```
apt-get install memcached
```

Konfigurasi default pada file /etc/memcached.conf cukup untuk server yang berukuran kecil. Sehingga mengunci akses ke localhost dan penyedia umum yang konfigurasinya masih masuk akal menggunakan beberapa nilai parameter. Sedangkan untuk mesin server yang lebih besar dalam penggunaan nya, perlunya menyediakan alokasi memory yang lebih besar dari default nya yaitu 64M:

```
# Start with a cap of 64 megs of memory. It's reasonable, and the daemon default
# Note that the daemon will grow to this size, but does not start out holding this much
# memory
-m 64
```

3.6.2.6 Install Mail Server Packages

Adapun LAMP server mempunyai beberapa jalan pintas untuk menginstal paket paket dasar untuk sebuah mail server saja. Seperti perintah di bawah ini:

```
apt-get install mail-server^
```

Ketika menginstall postfix perlunya untuk memilih tipe umum dari konfigurasi mail. Pilih "Internet site" lalu tentukan nama sistem mail nya, dimana harus sesuai dengan hostname pada mail server. Ini memberikan mail server untuk mengelola pengguna sebagai pengguna unix secara langsung dimana ini tidak meggunakan SQL database untuk menyimpan data. Sehingga diperlukan nya MySQL sebagai pendukung bagi postfix dan dovecot serta beberapa paket spam-mashing. Di bawah ini adalah perintah perintah untuk mengistall paket paket mailserver:

```
pt-get install postfix-mysql dovecot-mysql postgrey
apt-get install amavis clamav clamav-daemon spamassassin
apt-get install php5-imap
```

Paket php5-imap benar-benar mendukung POP3 serta protokol IMAP, dan akan dibutuhkan oleh Postfix Admin dan banyak pilihan yang mungkin mendukung untuk aplikasi PHP webmail. Restart Apache untuk memsatikan bahwa berjalan dan siap untuk digunakan:

```
service apache2 restart
```

Selanjutnya dibutuhkan lagi beberapa paket opsional yang akan memperluas kemampuan dalam penanganan spam dan deteksi virus. Memungkinkan untuk pemeriksaan yang lebih besar pada file lampiran:

```
apt-get install libnet-dns-perl pyzor razor
apt-get install arj bzip2 cabextract cpio file gzip nomarch pax unzip zip
```

3.6.2.7 Membuat Mail Database dan User dalam MySQL

Log in ke MySQL sebagai user root, kemudian masukan password yang telah diseting sebelumnya:

```
mysql -uroot -p
```

Sekarang set database dan user untuk mail software. Database ini akan menyimpan informasi dari akun dan domain mail, menggunakan skema yang di set oleh paket postfix admin. Lakukan perintah di bawah ini:

```
create database mail;
grant all on mail.* to 'mail'@'localhost' identified by 'mailpassword';
mysql -uroot -p
```

3.6.2.8 Install Postfix Admin dam Skema MySQL

Postfix Admin diinstal sebagai berikut. Untuk memulai download lalu unpack dan kemudian pindahkan ke dalam sub direktory ke webroot. Ini mungkin akan memerlukan juga mengubah ownership ke user www-data. Lakukan perintah perintah di bawah ini:

```
wget http://downloads.sourceforge.net/project/postfixadmin/postfixadmin/postfixadmin-
2.3.5/postfixadmin-2.3.5.tar.gz
gunzip postfixadmin-2.3.5.tar.gz
tar -xf postfixadmin-2.3.5.tar
mv postfixadmin-2.3.5 /var/www/postfixadmin
chown -R www-data:www-data /var/www/postfixadmin
```

Selanjutnya langkah menarik yaitu menarik dari dua pase dalam setup proses. Pertama ubah baris berikut di / var / www / postfixadmin / config.inc.php:

```
/**********************************************************************
 *  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
 * You have to set $CONF['configured'] = true; before the
 * application will run!
 * Doing this implies you have changed this file as required.
 * i.e. configuring database etc; specifying setup.php password etc.
 */
$CONF['configured'] = true;
```

```
// Postfix Admin Path

// Set the location of your Postfix Admin installation here.

// YOU MUST ENTER THE COMPLETE URL e.g. http://domain.tld/postfixadmin

$CONF['postfix_admin_url'] = 'https://staf.b4t.go.id/postfixadmin';
```

```
/ Database Config
// mysql = MySQL 3.23 and 4.0, 4.1 or 5
// mysqli = MySQL 4.1+
// pgsql = PostgreSQL
$CONF['database_type'] = 'mysql';
$CONF['database_host'] = 'localhost';
$CONF['database_user'] = 'mail';
$CONF['database_password'] = 'mailpassword';
$CONF['database_name'] = 'mail';
```

```
// Site Admin
// Define the Site Admins email address below.
// This will be used to send emails from to create mailboxes.
$CONF['admin_email'] = 'me@staf.b4t.go.id';


// Mail Server
// Hostname (FQDN) of your mail server.
// This is used to send email to Postfix in order to create mailboxes.
//
// Set this to localhost for now, but change it later.
$CONF['smtp_server'] = 'localhost';
$CONF['smtp_port'] = '25';
```

```
// Encrypt
// In what way do you want the passwords to be crypted?
// md5crypt = internal postfix admin md5
// md5 = md5 sum of the password
// system = whatever you have set as your PHP system default
// cleartext = clear text passwords (ouch!)
// mysql_encrypt = useful for PAM integration
// authlib = support for courier-authlib style passwords
// dovecot:CRYPT-METHOD = use dovecotpw -s 'CRYPT-METHOD'. Example: dovecot:CRAM-MD5
$CONF['encrypt'] = 'md5crypt';
```

```
// Mailboxes
// If you want to store the mailboxes per domain set this to 'YES'.
// Examples:
//   YES: /usr/local/virtual/domain.tld/username@domain.tld
//   NO:  /usr/local/virtual/username@domain.tld
$CONF['domain_path'] = 'NO';
// If you don't want to have the domain in your mailbox set this to 'NO'.
// Examples:
//   YES: /usr/local/virtual/domain.tld/username@domain.tld
//   NO:  /usr/local/virtual/domain.tld/username
// Note: If $CONF['domain_path'] is set to NO, this setting will be forced to YES.
$CONF['domain_in_mailbox'] = 'YES';
```

Selanjutnya buka browser web dan mengunjungi mail server di:

```
https://staf.b4t.go.id/postfixadmin/setup.php
```



Gambar 3.4 Tampilan Setup Postfix Admin

Ikuti petunjuk pada halaman tersebut untuk memilih password setup, dan menghasilkan hash dari password itu. Tambahkan hash yang ke file konfigurasi dan simpan:

```
// In order to setup Postfixadmin, you MUST specify a hashed password here.
// To create the hash, visit setup.php in a browser and type a password into the field,
// on submission it will be echoed out to you as a hashed value.
$CONF['setup_password'] = '...a long hash string...';
```

Kemudian kembali ke halaman setup. Sekarang dapat menggunakan password yang dipilih untuk membuat account administrator awal. Postfix Admin juga akan secara otomatis membuat skema database-nya saat ini.

Hal ini mungkin cukup bijaksan untuk membatasi akses ke / var / www / postfixadmin / setup.php setelah menggunakannya. Buat file / var / www / postfixadmin / .htaccess dan menempatkan instruksi berikut ke dalamnya:

```
<Files "setup.php">
deny from all
</Files>
```

3.6.2.9 Membuat Domain dan Accounts dalam Postfix Admin

Sekarang masuk ke menu utama postfix admin dengan cara:

```
https://staf.b4t.go.id/postfixadmin/
```



Gambar 3.5 Tampilan Login Postfix Admin

Login sebagai akun administrator yang baru kemudian pilih “New Domain” di bawah pilihan “Domain List” untuk membuat domain pada server. Sekarang bisa menambah mail untuk user (“Add Mailbox”) dan membuat alias ("Add alias"). Hal ini akan membuat skema database secara otomatis, tapi ini tidak semua database mail server akan dibuat. Untuk point ini hanya bisa melihat konfigurasi database.

Postfix Admin juga mempunyai fungsi lain selama proses panjang ini. Fungsi tersebut memungkinkan untuk mengirim e-mail untuk local user dengan menggunakan interface postfix admin sendiri. Yang mana membantu untuk melakukan test ketika mengkonfigurasi dan menentukan error yang terjadi di sebelah mana.



Gambar 3.6 Tampilan membuat Domain



Gambar 3.7 Tampilan Membuat Mailbox

3.6.2.10 Membuat User untuk Menangani Virtual Mail Direktori

Virtual mail user tidak tersedia dalam sistem user Unix . dan tidak memakai method autentifikasi atau pengiriman e-mail dan tidak berada di direktori utama. Cara untuk mengolah Virtual mail user adalah sebagai berikut :

1. Mail user sudah dikenal oleh postfix admin dibandingkan dengan sisitem yang ada di Unix.
2. Pesan e-mail akan tersimpan di subdomain per domain dan akun akan terletak pada /var/vmail.
3. Setelah membuat domain pesan akan berada di direktori /var/vmail/example.com/me.
4. Semua mail direktori ini akan dipunyai oleh satu user saja yang bernama vail dan dovecot akan menggunakan vmail dalam membuat dan menyusun perubahan file pesan e-mail.

Berikut ini adalah perintah perintah dari langkah langkah diatas:

```
useradd -r -u 150 -g mail -d /var/vmail -s /sbin/nologin -c "Virtual maildir handler" vmail
mkdir /var/vmail
chmod 770 /var/vmail
chown vmail:mail /var/vmail
```

Hal yang mungkin perlu diperhatikan adalah user dan direktori virtual mail menggunakan folder dalam group “mail” dan akan mengikuti user lain nya yang ada di dalam group yang isinya sudah dimodifikasi.

3.6.2.11 Konfigurasi Dovecot

Tool yang digunakan ialah dovecot sebagai transport email yang telah mendukung keamanan dimana dovecot dapat digunakan pada port *imap/imaps* dan pop3/pop3s, serta dukungan TLS,SSL dan quota. Dovecot akan mengelola IMAP dan koneksi POP3, direktori email lokal, menerima surat masuk yang diserahkan dari Postfix dan juga mengelola autentikasi untuk koneksi SMTP.

```
# Look up user passwords from a SQL database as
# defined in /etc/dovecot/dovecot-sql.conf.ext
passdb {
  driver = sql
  args = /etc/dovecot/dovecot-sql.conf.ext
}
# Look up user information from a SQL database as
# defined in /etc/dovecot/dovecot-sql.conf.ext
userdb {
  driver = sql
  args = /etc/dovecot/dovecot-sql.conf.ext
}
```

Sekarang edit baris / etc / dovecot / dovecot-sql.conf.ext sedemikian rupa. Menggunakan database MySQL digunakan untuk Postfix Admin.

```
# Database driver: mysql, pgsql, sqlite
driver = mysql
```

```
# Examples:
#   connect = host=192.168.1.1 dbname=users
#   connect = host=sql.example.com dbname=virtual user=virtual password=blarg
#   connect = /etc/dovecot/authdb.sqlite
#
connect = host=localhost dbname=b4tmail user=mail password=mailpassword
```

```
# Default password scheme.

#

# List of supported schemes is in

# http://wiki2.dovecot.org/Authentication/PasswordSchemes

#

default_pass_scheme = MD5-CRYPT
```

```
# Define the query to obtain a user password.
password_query = \
  SELECT username as user, password, '/var/vmail/%d/%n' as userdb_home, \
  'maildir:/var/vmail/%d/%n' as userdb_mail, 150 as userdb_uid, 8 as userdb_gid \
  FROM mailbox WHERE username = '%u' AND active = '1'
```

```
# Define the query to obtain user information.
user_query = \
  SELECT '/var/vmail/%d/%n' as home, 'maildir:/var/vmail/%d/%n' as mail, \
  150 AS uid, 8 AS gid, concat('dirsize:storage=', quota) AS quota \
  FROM mailbox WHERE username = '%u' AND active = '1'
```

Kemudian mengubah definisi pengendalian dalam / etc/dovecot/conf.d/10-auth.conf sehingga Dovecot akan membaca file konfigurasi SQL.

```
# Disable LOGIN command and all other plaintext authentications unless
# SSL/TLS is used (LOGINDISABLED capability). Note that if the remote IP
# matches the local IP (ie. you're connecting from the same computer), the
# connection is considered secure and plaintext authentication is allowed.
        disable_plaintext_auth = yes
```

```
# Space separated list of wanted authentication mechanisms:
#   plain login digest-md5 cram-md5 ntlm rpa apop anonymous gssapi otp skey
#   gss-spnego
# NOTE: See also disable_plaintext_auth setting.
auth_mechanisms = plain login
```

```
##
## Password and user databases
##


#
# Password database is used to verify user's password (and nothing more).
# You can have multiple passdbs and userdbs. This is useful if you want to
# allow both system users (/etc/passwd) and virtual users to login without
# duplicating the system users into virtual database.
#
# <doc/wiki/PasswordDatabase.txt>
#
# User database specifies where mails are located and what user/group IDs
# own them. For single-UID configuration use "static" userdb.
#
# <doc/wiki/UserDatabase.txt>

#!include auth-deny.conf.ext
#!include auth-master.conf.ext

#!include auth-system.conf.ext
# Use the SQL database configuration rather than any of these others.
!include auth-sql.conf.ext
#!include auth-ldap.conf.ext
#!include auth-passwdfile.conf.ext
#!include auth-checkpassword.conf.ext
#!include auth-vpopmail.conf.ext
#!include auth-static.conf.ext
```

Selanjutnya beritahu Dovecote dimana harus meletakan pesan di direktori virtual user. Untuk merubahnya kebutuhan tersebut terletak pada direktori /etc/dovecot/conf.d/10-mail.conf rubahlah seperti baris di bawah ini:

```
# Location for users' mailboxes. The default is empty, which means that Dovecot
# tries to find the mailboxes automatically. This won't work if the user
# doesn't yet have any mail, so you should explicitly tell Dovecot the full
# location.
#
# If you're using mbox, giving a path to the INBOX file (eg. /var/mail/%u)
# isn't enough. You'll also need to tell Dovecot where the other mailboxes are
# kept. This is called the "root mail directory", and it must be the first
# path given in the mail_location setting.
#
# There are a few special variables you can use, eg.:
#
#   %u - username
#   %n - user part in user@domain, same as %u if there's no domain
#   %d - domain part in user@domain, empty if there's no domain
#   %h - home directory
#
# See doc/wiki/Variables.txt for full list. Some examples:
#
#   mail_location = maildir:~/Maildir
#   mail_location = mbox:~/mail:INBOX=/var/mail/%u
#   mail_location = mbox:/var/mail/%d/%1n/%n:INDEX=/var/indexes/%d/%1n/%n
#
# <doc/wiki/MailLocation.txt>
#
mail_location = maildir:/var/vmail/%d/%n
```

```
# System user and group used to access mails. If you use multiple, userdb
# can override these by returning uid or gid fields. You can use either numbers
# or names. <doc/wiki/UserIds.txt>
mail_uid = vmail
mail_gid = mail
```

```
# Valid UID range for users, defaults to 500 and above. This is mostly
# to make sure that users can't log in as daemons or other system users.
# Note that denying root logins is hardcoded to dovecot binary and can't
# be done even if first_valid_uid is set to 0.
#
# Use the vmail user uid here.
first_valid_uid = 150
last_valid_uid = 150
```

Ubah baris yang terdapat di **/etc/dovecot/conf.d/10-ssl.conf.** pada bagian ini paket CA certfikat menyediakan salah satu dari certificate issuer.

```
# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
ssl = yes

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf
ssl_cert = </path/to/my/cert.pem
ssl_key = </path/to/my/key.pem

# If key file is password protected, give the password here. Alternatively
# give it when starting dovecot with -p parameter. Since this file is often
# world-readable, you may want to place this setting instead to a different
# root owned 0600 file by using ssl_key_password = <path.
#ssl_key_password =

# PEM encoded trusted certificate authority. Set this only if you intend to use
# ssl_verify_client_cert=yes. The file should contain the CA certificate(s)
# followed by the matching CRL(s). (e.g. ssl_ca = </etc/ssl/certs/ca.pem)
#ssl_ca = </path/to/ca.pem
```

Ubahlah baris pada file yang terdapat di /etc/dovecot/conf.d/10-master.conf untuk menambah pilihan pada Postfix:

```
service auth {
  # auth_socket_path points to this userdb socket by default. It's typically
  # used by dovecot-lda, doveadm, possibly imap process, etc. Its default
  # permissions make it readable only by root, but you may need to relax these
  # permissions. Users that have access to this socket are able to get a list
  # of all usernames and get results of everyone's userdb lookups.
  unix_listener auth-userdb {
   mode = 0600
    user = vmail
    group = mail
  }

  unix_listener /var/spool/postfix/private/auth {
    mode = 0660
    # Assuming the default Postfix user and group
    user = postfix
    group = postfix
  }
```

Ubah konfigurasi dovecot agar bisa diakses oleh dovecot dan vmail users:

```
chown -R vmail:dovecot /etc/dovecot
chmod -R o-rwx /etc/dovecot
```

3.6.2.12 Konfigurasi Amavis, ClamAV dan Spamassassin

Sebelum memasuki ke tahap konfigurasi Postfix terlebih dahulu konfigurasi kebutuhan yang akan menangani tentang spam dan virus. Langkah pertama adalah tambahkan user untuk Amavis dan ClamAV untuk mengaktifkan kolaborasi antara keduanya, perintahnya asalah sebagai berikut:

```
adduser clamav amavis

adduser amavis clamav
```

Untuk mengaktifkan Amavis rubahlah baris pada /etc/amavis/conf.d/15-content_filter_mode:

```
use strict;

# You can modify this file to re-enable SPAM checking through spamassassin
# and to re-enable antivirus checking.

#
# Default antivirus checking mode
# Please note, that anti-virus checking is DISABLED by
# default.
# If You wish to enable it, please uncomment the following lines:

@bypass_virus_checks_maps = (
 \%bypass_virus_checks, \@bypass_virus_checks_acl, \$bypass_virus_checks_re);

#
# Default SPAM checking mode
# Please note, that anti-spam checking is DISABLED by
# default.
# If You wish to enable it, please uncomment the following lines:

@bypass_spam_checks_maps = (
  \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);

1;  # ensure a defined return
```

Aktifkan juga SpamAssassin dan rubahlah baris pada /etc/default/spamassassin:

```
# Change to one to enable spamd

ENABLED=1
```

```
# Cronjob
# Set to anything but 0 to enable the cron job to automatically update
# spamassassin's rules on a nightly basis
CRON=1
```

Restart konfigurasi ini untuk melanjutkan konfigurasi berikutnya

```
service amavis restart
service spamassassin restart
```

3.6.2.13 Konfigurasi Postfix

Postfix menangani surat masuk melalui protokol SMTP dan file konfigurasi telah dibentuk untuk mengintegrasikan dengan paket-paket lain . di level yang lebih tinggi Postfix menangani pesan yang masuk lalu diteruskan ke pengecekan virus dan spam sebelum diteruskan ke dovecot untuk dikirimkan. Postfix juga menangani proses authentifikasi pengguna virtual yang menghubungkan dengan SMTP untuk mengirim email.

Pertama buat file yang menjelaskan tentang dimana Postfix dapat menemukan informasi tentang user dan domain nya. Catatan untuk “host” yang harus sama dengan "bind-address" di / etc / mysql / my.cnf. Jika satu sisi di seting "localhost" dan sisi lain di seting "127.0.0.1" maka memungkinkan bahwa Postfix tidak dapat terhubung ke MySQL. Berikut adalah file yang diperlukan oleh Postfix:

/etc/postfix/mysql_virtual_alias_domainaliases_maps.cf

```
user = mail
password = mailpassword
hosts = 127.0.0.1
dbname = mail
query = SELECT goto FROM alias,alias_domain
  WHERE alias_domain.alias_domain = '%d'
  AND alias.address=concat('%u', '@', alias_domain.target_domain)
  AND alias.active =  1
```

/etc/postfix/mysql_virtual_alias_maps.cf

```
user = mail
password = mailpassword
hosts = 127.0.0.1
dbname = mail
table = alias
select_field = goto
where_field = address
additional_conditions = and active = '1'
```

/etc/postfix/mysql_virtual_domains_maps.cf

```
user = mail
password = mailpassword
hosts = 127.0.0.1
dbname = mail
table = domain
select_field = domain
where_field = domain
additional_conditions = and backupmx = '0' and active = '1'
```

/etc/postfix/mysql_virtual_mailbox_domainaliases_maps.cf

```
user = mail
password = mailpassword
hosts = 127.0.0.1
dbname = mail
query = SELECT maildir FROM mailbox, alias_domain
  WHERE alias_domain.alias_domain = '%d'
  AND mailbox.username=concat('%u', '@', alias_domain.target_domain )
  AND mailbox.active = 1
```

/etc/postfix/mysql_virtual_mailbox_maps.cf

```
user = mail
password = mailpassword
hosts = 127.0.0.1
dbname = mail
table = mailbox
select_field = CONCAT(domain, '/', local_part)
where_field = username
additional_conditions = and active = '1'
```

Buatlah file /etc/postfix/header_checks, yang mana akan langsung menghapus konten certain header ketika membalas pesan. Ini akan memprivsdi untuk pengiriman users sontohnya saja IP Address dan mail software identifiers, file ini akan mengacu pada main Postfix konfigurasi:

```
/^Received:/              IGNORE
/^User-Agent:/            IGNORE
/^X-Mailer:/              IGNORE
/^X-Originating-IP:/      IGNORE
/^x-cr-[a-z]*:/           IGNORE
/^Thread-Index:/          IGNORE
```

Selanjutnya konfigurasi file pada /etc/postfix/main.cf, yang mana mengandung pilihan yang komplek bagaimana pesan bisa terkirim dan bagaimana sifat dari SMTP. Pada bagian ini akan menjelaskan setiap pilihan yang terbaik atau detail dalam parameter konigurasi.

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete version

# The first text sent to a connecting process.
smtpd_banner = $myhostname ESMTP $mail_name
biff = no
# appending .domain is the MUA's job.
append_dot_mydomain = no
readme_directory = no

# SASL parameters
# ---------------------------------

# Use Dovecot to authenticate.
smtpd_sasl_type = dovecot
# Referring to /var/spool/postfix/private/auth
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
broken_sasl_auth_clients = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain =
smtpd_sasl_authenticated_header = yes

# TLS parameters
# ---------------------------------

# Replace this with your SSL certificate path if you are using one.
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
# The snakeoil self-signed certificate has no need for a CA file. But
# if you are using your own SSL certificate, then you probably have
# a CA certificate bundle from your provider. The path to that goes
# here.
#smtpd_tls_CAfile=/path/to/ca/file
smtpd_use_tls=yes
smtp_tls_security_level = may
smtpd_tls_security_level = may
#smtpd_tls_auth_only = no
smtp_tls_note_starttls_offer = yes
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom
#smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
#smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

# SMTPD parameters
# ---------------------------------
# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h
# will it be a permanent error or temporary
unknown_local_recipient_reject_code = 450
```

```
# how long to keep message on queue before return as failed.
# some have 3 days, I have 16 days as I am backup server for some people
# whom go on holiday with their server switched off.
maximal_queue_lifetime = 7d
# max and min time in seconds between retries if connection failed
minimal_backoff_time = 1000s
maximal_backoff_time = 8000s
# how long to wait when servers connect before receiving rest of data
smtp_helo_timeout = 60s
# how many address can be used in one message.
# effective stopper to mass spammers, accidental copy in whole address list
# but may restrict intentional mail shots.
smtpd_recipient_limit = 16
# how many error before back off.
smtpd_soft_error_limit = 3
# how many max errors before blocking it.
smtpd_hard_error_limit = 12

# This next set are important for determining who can send mail and relay mail
# to other servers. It is very important to get this right - accidentally producing
# an open relay that allows unauthenticated sending of mail is a Very Bad Thing.
#
# You are encouraged to read up on what exactly each of these options accomplish.

# Requirements for the HELO statement
smtpd_helo_restrictions = permit_mynetworks, warn_if_reject reject_non_fqdn_hostname,
reject_invalid_hostname, permit
# Requirements for the sender details
smtpd_sender_restrictions = permit_sasl_authenticated, permit_mynetworks, warn_if_reject
reject_non_fqdn_sender, reject_unknown_sender_domain, reject_unauth_pipelining, permit
# Requirements for the connecting server
smtpd_client_restrictions = reject_rbl_client sbl.spamhaus.org, reject_rbl_client
blackholes.easynet.nl, reject_rbl_client dnsbl.njabl.org
# Requirement for the recipient address. Note that the entry for
# "check_policy_service inet:127.0.0.1:10023" enables Postgrey.
smtpd_recipient_restrictions = reject_unauth_pipelining, permit_mynetworks,
permit_sasl_authenticated, reject_non_fqdn_recipient, reject_unknown_recipient_domain,
reject_unauth_destination, check_policy_service inet:127.0.0.1:10023, permit
smtpd_data_restrictions = reject_unauth_pipelining

# require proper helo at connections
smtpd_helo_required = yes
# waste spammers time before rejecting them
smtpd_delay_reject = yes
disable_vrfy_command = yes
```

```
 # General host and delivery info
# ----------------------------------
myhostname = staf.b4t.go.id
myorigin = /etc/hostname
mydestination = staf.b4t.go.id, localhost
#relayhost =
# If you have a separate web server that sends outgoing mail through this
# mailserver, you may want to add its IP address to the space-delimited list in
# mynetworks, e.g. as 111.222.333.444/32.
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
mynetworks_style = host

# This specifies where the virtual mailbox folders will be located.
virtual_mailbox_base = /var/vmail
# This is for the mailbox location for each user. The domainaliases
# map allows us to make use of Postfix Admin's domain alias feature.
virtual_mailbox_maps = mysql:/etc/postfix/mysql_virtual_mailbox_maps.cf,
mysql:/etc/postfix/mysql_virtual_mailbox_domainaliases_maps.cf
# and their user id
virtual_uid_maps = static:150
# and group id
virtual_gid_maps = static:8
# This is for aliases. The domainaliases map allows us to make
# use of Postfix Admin's domain alias feature.
virtual_alias_maps = mysql:/etc/postfix/mysql_virtual_alias_maps.cf,
mysql:/etc/postfix/mysql_virtual_alias_domainaliases_maps.cf
# This is for domain lookups.
virtual_mailbox_domains = mysql:/etc/postfix/mysql_virtual_domains_maps.cf

# Integration with other packages
# ---------------------------------------
# Tell postfix to hand off mail to the definition for dovecot in master.cf
virtual_transport = dovecot
dovecot_destination_recipient_limit = 1
# Use amavis for virus and spam scanning
content_filter = amavis:[127.0.0.1]:10024

# Header manipulation
# ---------------------------------------
# Getting rid of unwanted headers. See: https://posluns.com/guides/header-removal/
header_checks = regexp:/etc/postfix/header_checks
# getting rid of x-original-to
enable_original_recipient = no
```

Tambahkan baris baris berikut pada **/etc/postfix/main.cf:**

```
# Replace this with your SSL certificate path if you are using one.
smtpd_tls_cert_file=/path/to/my/cert.pem
smtpd_tls_key_file=/path/to/my/key.key
# The snakeoil self-signed certificate has no need for a CA file. But
# if you are using your own SSL certificate, then you probably have
                    # a CA certificate bundle from your provider. The path to that goes
# here.
#smtpd_tls_CAfile=/path/to/ca/file
```

Tambahakan beberapa material ke /etc/postfix/master.cf. di bawah ini adalah isi keseluruhan dari file tersebut agar lebih jelas, termasuk juga default material dari paket yang telah terinstall:

```
# Postfix master process configuration file.  For details on the format
# of the file, see the master(5) manual page (command: "man 5 master").
#
# Do not forget to execute "postfix reload" after editing this file.
#
#
==========================================================================
====
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
#
==========================================================================
====
smtp      inet  n       -       -       -       -       smtpd
#smtp      inet  n       -       -       -       1       postscreen
#smtpd     pass  -       -       -       -       -       smtpd
#dnsblog   unix  -       -       -       -       0       dnsblog
#tlsproxy  unix  -       -       -       -       0       tlsproxy
#submission inet n       -       -       -       -       smtpd
#  -o syslog_name=postfix/submission
                                    #  -o smtpd_tls_security_level=encrypt
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
smtps     inet  n       -       -       -       -       smtpd
  -o syslog_name=postfix/smtps
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_tls_auth_only=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject_unauth_destination,reject
  -o smtpd_sasl_security_options=noanonymous,noplaintext
  -o smtpd_sasl_tls_security_options=noanonymous
#  -o milter_macro_daemon_name=ORIGINATING
```

```
#628       inet  n       -       -       -       -       qmqpd
pickup     fifo  n       -       -       60      1       pickup
  -o content_filter=
  -o receive_override_options=no_header_body_checks
cleanup    unix  n       -       -       -       0       cleanup
qmgr       fifo  n       -       n       300     1       qmgr
#qmgr      fifo  n       -       n       300     1       oqmgr
tlsmgr     unix  -       -       -       1000?   1       tlsmgr
rewrite    unix  -       -       -       -       -       trivial-rewrite
bounce     unix  -       -       -       -       0       bounce
defer      unix  -       -       -       -       0       bounce
trace      unix  -       -       -       -       0       bounce
verify     unix  -       -       -       -       1       verify
flush      unix  n       -       -       1000?   0       flush
proxymap   unix  -       -       n       -       -       proxymap
proxywrite unix  -       -       n       -       1       proxymap
smtp       unix  -       -       -       -       -       smtp
relay      unix  -       -       -       -       -       smtp
#       -o smtp_helo_timeout=5 -o smtp_connect_timeout=5
showq      unix  n       -       -       -       -       showq
error      unix  -       -       -       -       -       error
retry      unix  -       -       -       -       -       error
discard    unix  -       -       -       -       -       discard
local      unix  -       n       n       -       -       local
virtual    unix  -       n       n       -       -       virtual
lmtp       unix  -       -       -       -       -       lmtp
anvil      unix  -       -       -       -       1       anvil
scache     unix  -       -       -       -       1       scache
#
# ====================================================================
# Interfaces to non-Postfix software. Be sure to examine the manual
# pages of the non-Postfix software to find out what options it wants.
#
# Many of the following services use the Postfix pipe(8) delivery
# agent.  See the pipe(8) man page for information about ${recipient}
# and other message envelope options.
# ====================================================================
#
# maildrop. See the Postfix MAILDROP_README file for details.
# Also specify in main.cf: maildrop_destination_recipient_limit=1
#
maildrop  unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail argv=/usr/bin/maildrop -d ${recipient}
#
 # ====================================================================
#
# Recent Cyrus versions can use the existing "lmtp" master.cf entry.
#
# Specify in cyrus.conf:
#   lmtp    cmd="lmtpd -a" listen="localhost:lmtp" proto=tcp4
# ====================================================================
```

```
# Specify in main.cf one or more of the following:
#  mailbox_transport = lmtp:inet:localhost
#  virtual_transport = lmtp:inet:localhost
#
# ====================================================================
#
# Cyrus 2.1.5 (Amos Gouaux)
# Also specify in main.cf: cyrus_destination_recipient_limit=1
#
#cyrus     unix -       n       n       -       -       pipe
#  user=cyrus argv=/cyrus/bin/deliver -e -r ${sender} -m ${extension} ${user}
#
# ====================================================================
# Old example of delivery via Cyrus.
#
#old-cyrus unix -       n       n       -       -       pipe
#  flags=R user=cyrus argv=/cyrus/bin/deliver -e -m ${extension} ${user}
#
# ====================================================================
#
# See the Postfix UUCP_README file for configuration details.
#
uucp      unix -       n       n       -       -       pipe
  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
#
# Other external delivery methods.
#
ifmail    unix -       n       n       -       -       pipe
  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
bsmtp     unix -       n       n       -       -       pipe
  flags=Fq. user=bsmtp argv=/usr/lib/bsmtp/bsmtp -t$nexthop -f$sender $recipient
scalemail-backend unix -       n       n       -       2       pipe
  flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store ${nexthop} ${user} ${extension}
mailman   unix -       n       n       -       -       pipe
  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
  ${nexthop} ${user}
```

```
# The next two entries integrate with Amavis for anti-virus/spam checks.
#
amavis      unix  -       -       -       -       2       smtp
        -o smtp_data_done_timeout=1200
        -o smtp_send_xforward_command=yes
        -o disable_dns_lookups=yes
        -o max_use=20
127.0.0.1:10025 inet  n       -       -       -       -       smtpd
        -o content_filter=
        -o local_recipient_maps=
        -o relay_recipient_maps=
        -o smtpd_restriction_classes=
        -o smtpd_delay_reject=no
        -o smtpd_client_restrictions=permit_mynetworks,reject
        -o smtpd_helo_restrictions=
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o smtpd_data_restrictions=reject_unauth_pipelining
        -o smtpd_end_of_data_restrictions=
        -o mynetworks=127.0.0.0/8
        -o smtpd_error_sleep_time=0
        -o smtpd_soft_error_limit=1001
        -o smtpd_hard_error_limit=1000
        -o smtpd_client_connection_count_limit=0
        -o smtpd_client_connection_rate_limit=0
        -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks

#
# Integration with Dovecot - hand mail over to it for local delivery, and
# run the process under the vmail user and mail group.
#
dovecot     unix  -       n       n       -       -       pipe
        flags=DRhu user=vmail:mail argv=/usr/lib/dovecot/dovecot-lda -d $(recipient)
```

3.6.2.14 Restart dan Test Server

Restart semua proses untuk menyimpan perubahan konfigurasi:

```
service postfix restart
service spamassassin restart
service clamav-daemon restart
service amavis restart
service dovecot restart
```

Perhatikan juga /var/log/mail.err dan /var/log/mail.log untuk pesan errorr dan coba login ke dalam POP dan IMAP, kemudian kirim pesan ke akun yang terdapat pada server. Langkah ini bertujuan untuk mengecek apakah mail server yang telah di konfigurasi telah berjalan.

3.6.2.15 Install dan Seting Monit Untuk Monitoring

Monit sangat berguna untuk memonitoring tool services yang melindungi server dari gagalnya proses. Instal paket Monit dengan perintah di bawah ini.

```
apt-get install monit
```

Dengan mengikuti langkah langkah di bawah ini, bahwa dengan menggunakan monit akan megawasi seluruh proses yang penting pada server tetapi tanpa memberikan pemberitahuan melainkan merestart pada bagian yang terdapat kegagalan. Buat file seperti pada contoh konfigurasi Monit di bawah ini:

Pada file /etc/monit/conf.d/amavis:

```
check process amavisd with pidfile /var/run/amavis/amavisd.pid
  group mail
  start program = "/etc/init.d/amavis start"
  stop  program = "/etc/init.d/amavis stop"
  if failed port 10024 protocol smtp then restart
  if 5 restarts within 5 cycles then timeout
```

Pada file /etc/monit/conf.d/apache2:

```
check process apache2 with pidfile /var/run/apache2.pid
  group www
  start program = "/etc/init.d/apache2 start"
  stop program = "/etc/init.d/apache2 stop"
  if failed host localhost port 80 protocol http
    with timeout 10 seconds
    then restart
  if 5 restarts within 5 cvcles then timeout
```

Pada file /etc/monit/conf.d/dovecot:

```
check process dovecot with pidfile /var/run/dovecot/master.pid
  group mail
  start program = "/etc/init.d/dovecot start"
  stop program = "/etc/init.d/dovecot stop"
  group mail
  if failed port 993 type tcpssl sslauto protocol imap for 5 cycles then restart
  if 3 restarts within 5 cycles then timeout
```

Pada file /etc/monit/conf.d/mysql:

```
check process mysqld with pidfile /var/run/mysqld/mysqld.pid
  group database
  start program = "/etc/init.d/mysql start"
  stop program = "/etc/init.d/mysql stop"
  if failed host localhost port 3306 protocol mysql then restart
  if 5 restarts within 5 cycles then timeout
```

Pada file /etc/monit/conf.d/memcached:

```
check process memcached with pidfile /var/run/memcached.pid
  group www
  start program = "/etc/init.d/memcached start"
  stop program = "/etc/init.d/memcached stop"
  if failed host localhost port 11211 then restart
  if 5 restarts within 5 cycles then timeout
```

Pada file /etc/monit/conf.d/postfix:

```
check process postfix with pidfile /var/spool/postfix/pid/master.pid
  group mail
  start program = "/etc/init.d/postfix start"
  stop  program = "/etc/init.d/postfix stop"
  if failed port 25 protocol smtp then restart
  if 5 restarts within 5 cycles then timeout
```

Pada file /etc/monit/conf.d/spamassassin:

```
check process spamassassin with pidfile /var/run/spamd.pid
  group mail
  start program = "/etc/init.d/spamassassin start"
  stop  program = "/etc/init.d/spamassassin stop"
  if 5 restarts within 5 cycles then timeout
```

Pada file /etc/monit/conf.d/sshd:

```
check process sshd with pidfile /var/run/sshd.pid
  start program "/etc/init.d/ssh start"
  stop program "/etc/init.d/ssh stop"
  if failed host 127.0.0.1 port 22 protocol ssh then restart
   if 5 restarts within 5 cycles then timeout
```

Kemudian restart Monit untuk menyimpan file dan mengaktifkan semua services:

```
service monit restar
```

3.6.2.16 Installasi dan Konfigurasi Roundcube sebagai MUA

Selanjutnya adalah mengunduh *file roundcube* di *website* resminya di www.roundcube.net, ambil versi *update*-an terakhir. Disini menggunakan versi *update* terbaru yaitu *roundcubemail-* 0.7.1.*tar.gz.* Berikut cara instalasi dan konfigurasi *roundcubemail* :

```
$ mysql -uroot –p
create database roundcubedb;
create user usercube;
Set password for ‘usercube’ = password(‘usercube’);
```

1. Buat database dan user untuk roundcube di MySQL.

```
grant all privileges on roundcubedb.* to ‘usercube’ identified by ‘usercube’;
```

2. Dalam hal ini Roundcube Webmail akan dipasang di direktori / var / www / webmail. Download dan ekstrak Arsip Roundcube Webmail ke direktori / var / www / webmail

```
cd /tmp && wget -0 roundcubemail-0.7.1.tar.gz http://goo.gl/zGnGZ
sudo tar –xzvf roundcubemail-0.7.1.tar.gz –C /var/www
sudo mv /var/www/roundcubemail-0.7.1/ /var/www/webmail
```

ubah direktori kepemilikan /var/www/webmail/temp dan /var/www/webmail/log ke user dan group www-data

```
sudo chown –R www-data.www-data /var/www/webmail/temp
sudo chown –R www-data.www.-data /var/www/webmail/logs
```

3. *Import database* Roundcube ke mysql *server*, *login* ke mysql *server* dengan perintah :

```
mysql –u root –p roundcubedb < /var/www/webmail/SQL/mysql.initial.sql
```

4. Gunakan browser dengan mengetikan alamat staf.b4t.go.id/webmail/installer untuk melakukan instalasi roundcube.

5. Melakukan pemeriksaan terhadap konfigurasi server. Jika muncul pesan NOT AVAIABLE artinya fitur ini tidak tersedia di server dan instalasi bisa di lanjutkan tetapi jika muncul pesan NOT OK artinya setting server tidak siap untuk melakukan instalasi Roundcube dan harus dibuat menjadi OK supaya bisa melanjutkan instalasi Roundcube. Klik Next jika konfigurasi server sudah siap semua.
6. Setelah itu melakukan konfigurasi. Berikut bagian-bagian yang perlu di konfigurasi :
   b General configuration

     product_name : B4T Webmail

   c Database Setup

     Database type : mysql
     Database server : localhost
     Database name : roundcubedb
     Database user : userdb
     Database password : isikan password dari userdb

   d IMAP dan SMTP setting

     Default_host : staf.b4t.go.id
     Default_port : 143
     Smtp_server : staf.b4t.go.id
     Smtp_port : 25

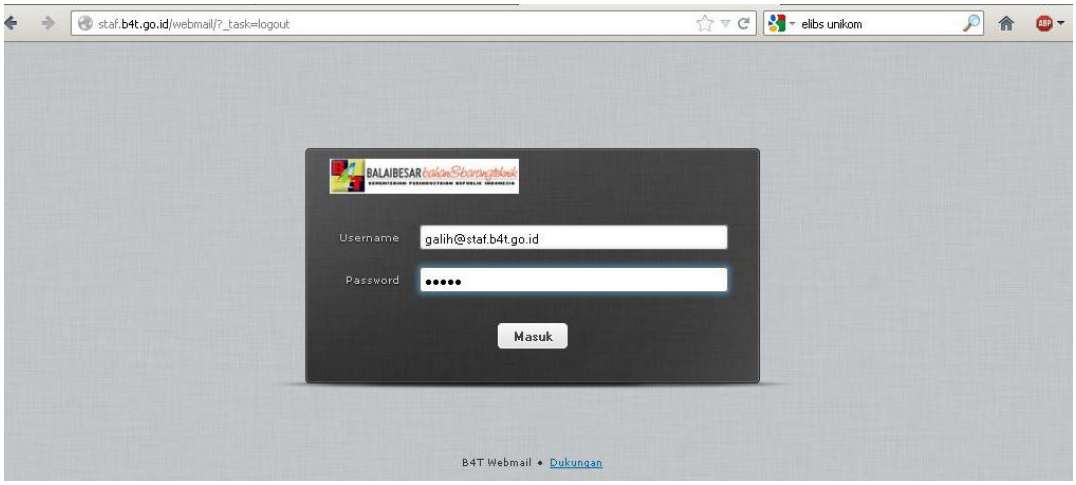
7. Unduh file main.inc.php dan db.inc.php lalu copy ke direktori /var/www/webmail/config

```
Sudo cp main.inc.php db.inc.php /var/www/webmail/config
```

8. Instalasi Roundcube Webmail selesai, hapus folder installer di direktori /var/www/webmail/installer

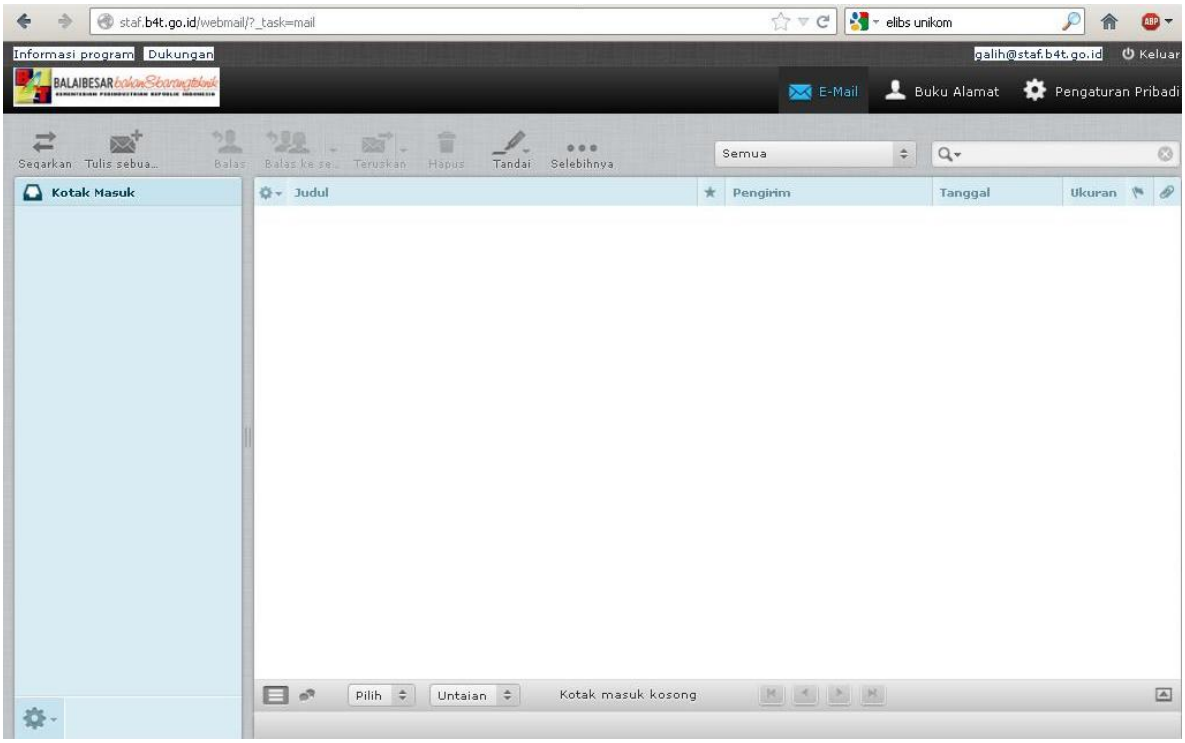
```
sudo rm –rf    /var/www/webmail/installer
```

Setelah melakukan konfigurasi, untuk melakukan pengujian pada web browser masukan alamat http://staf.b4t.go.id/webmail jika selanjutnya pada web browser muncul pengisian user dan password, artinya konfigurasi berhasil



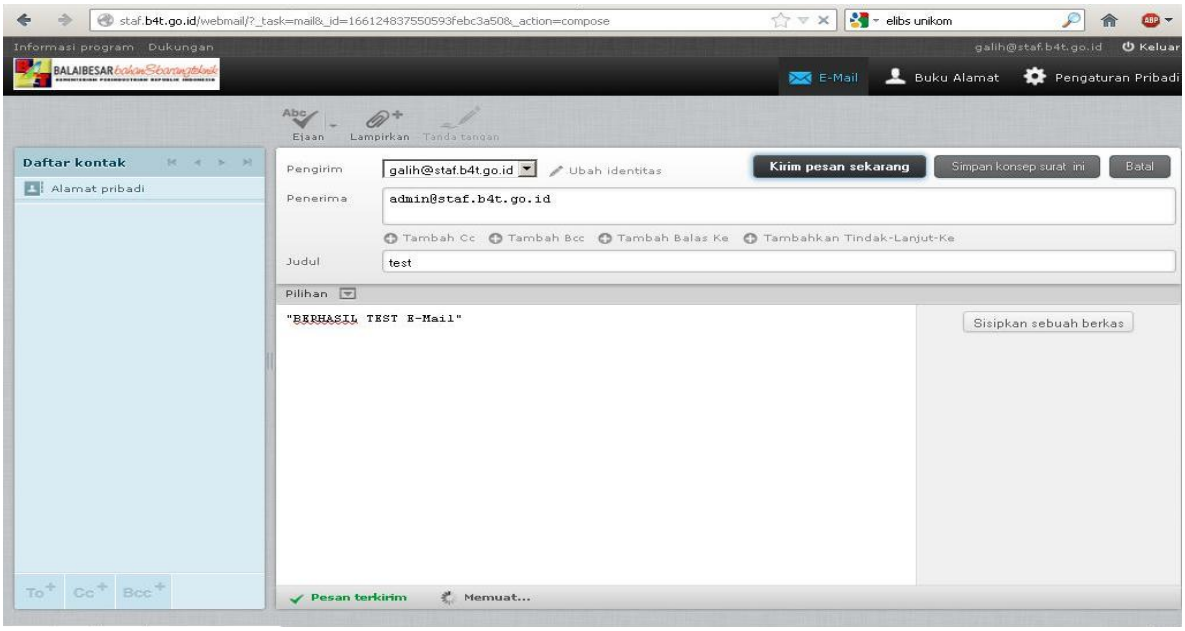
Gambar 3.8 Tampilan Login Webmail

Jika username dan password yang dimasukan sesuai maka sistem akan menampilkan tampilan utama dari webmail. Berikut ini merupakan tampilan utama dari webmail.



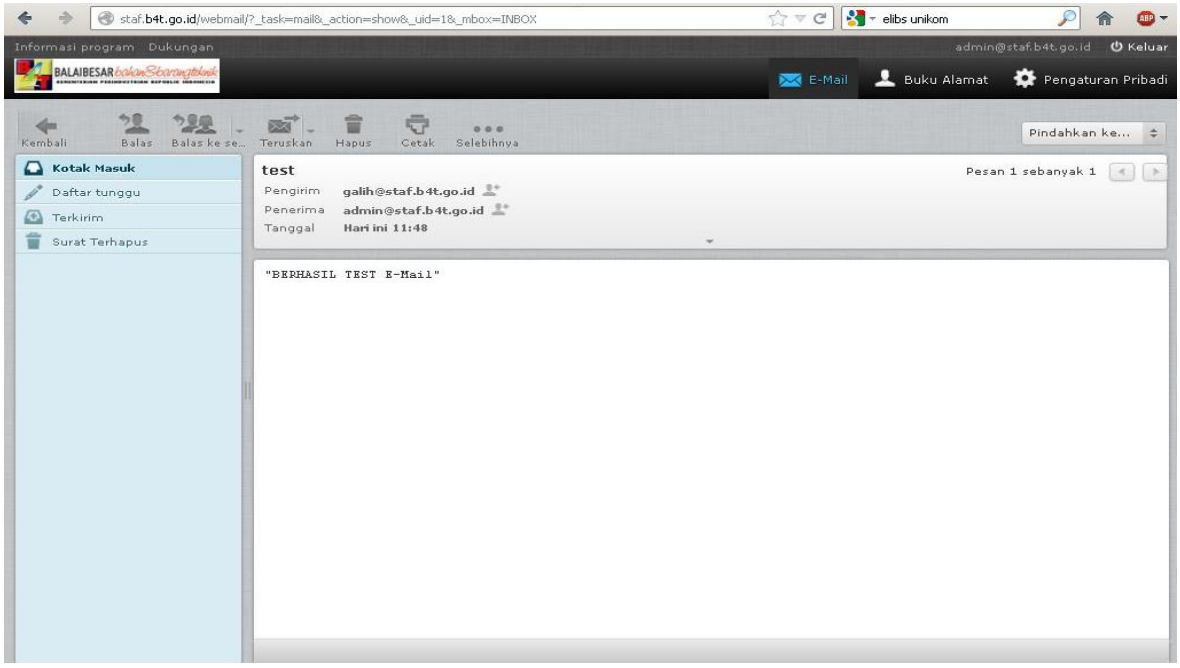
Gambar 3.9 Tampilan Utama Webmail

Berikut ini tampilan webmail pada saat akan melakukan pengiriman pesan.atau *e-mail* kepada admin.



Gambar 3.10 Tampilan proses pengiriman e-mail

Berikut ini merupakan tampilan untuk kotak masuk atau *inbox* sebagai tempat menampung pesan/*e-mail* yang baru masuk



Gambar 3.11 Tampilan kotak masuk / inbox

3.7 Hasil Pengolahan Data

Pengumpulan data yang dilakukan ialah melalui kuesioner yang disebarkan kepada pegawai Balai Besar Bahan dan Barang Teknik (B4T). Jumlah responden ditentukan sebanyak 20 orang. Hasil dari kuesioner di analisis menggunakan skala likert.

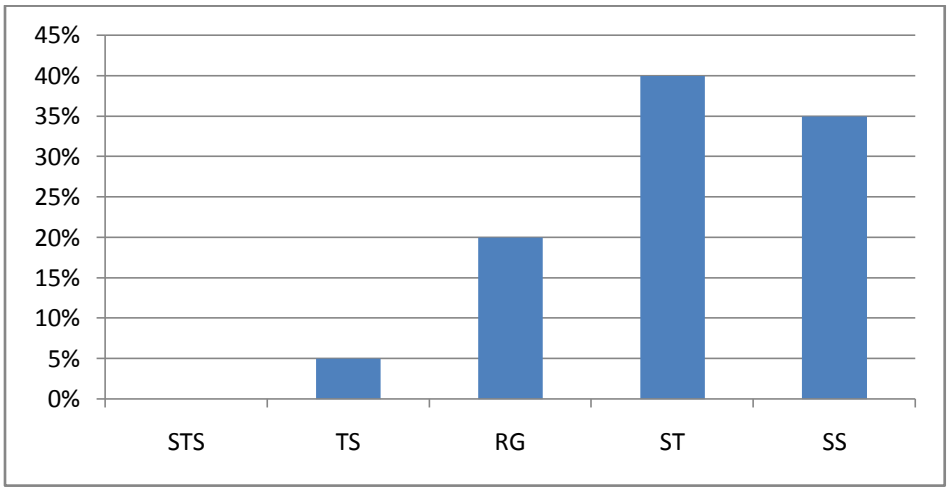
3.8 Hasil Kuesioner

Berikut ini adalah tabel hasil kuesioner mengenai apakah dengan pengaksesan e-mail berbasis web sudah efisien.

Tabel 3.3 Hasil Kuesioner, pengaksesan e-mail berbasis web sudah efisien

Pilihan Jawaban	Jumlah Responden	Metode Presentase
Sangat Setuju (SS)	7	35 %
Setuju (ST)	8	40 %
Ragu-ragu (RG)	4	20 %
Tidak Setuju (TS)	1	5 %
Sangat Tidak Setuju(STS)	0	0 %
	20	100%

Berikut ini adalah grafik dari hasil kuesioner mengenai apakah dengan pengaksesan e-mail berbasis web sudah efisien.



Gambar 3.12 Grafik hasil kuisioner