Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.202071869
Vol. 7, No. 3, Juni 2020, hlm. 493-500 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 30/E/KPT/2018 e-ISSN: 2528-6579

SISTEM KEAMANAN MULTI MAIL SERVER DENGAN TEKNIK ENKRIPSI OPENPGP PADA ZIMBRA EXCHANGE OPEN SOURCE SOFTWARE

Amrul Faruq*[1], Khaeruddin[2] , Merinda Lestandy[3]

[1, 2, 3]Jurusan Teknik Elektro, Fakultas Teknik, Universitas Muhammadiyah Malang
Email: [1]faruq@umm.ac.id, [2]lamone@umm.ac.id, [3]merindalestandy@umm.ac.id
*Penulis Korespondensi

(Naskah masuk: 12 Maret 2019, diterima untuk diterbitkan: 22 April 2020)

Abstrak

Surat elektronik atau *email* merupakan media komunikasi yang sangat populer. Untuk mengirim dan menerima email, diperlukan sebuah penyedia *(server)* yang di dalamnya terdapat layanan *email*. *Zimbra Collaboration Suite (ZCS)* merupakan salah satu aplikasi *mail server powerfull* yang dapat dipergunakan sebagai aplikasi *mail server* dalam jumlah user puluhan hingga ribuan. Pada penelitian ini, sistem enkripsi pada Zimbra *multiple-mail server* menggunakan metode OpenPGP diimplementasikan untuk mengamankan isi *email* yang dikirim maupun yang diterima, yaitu dengan memanfaatkan *public key* dan *private key*. Hasil pengujian menunjukkan metode *OpenPGP* mampu bekerja dengan baik untuk keamanan sistem pengiriman dan atau penerimaan *email* pada *multi mail server*.

Kata kunci: *multi mail server, Zimbra, keamanan jaringan, OpenPGP*

MULTI MAIL SERVER SECURITY SYSTEM USING OPENPGP ENCRYPTION TECHNIQUE IN ZIMBRA EXCHANGE OPEN SOURCE SOFTWARE

Abstract

Electronic mail or e-mail is a very popular communication medium. To send and receive e-mails, a provider (server) is needed in which there is an e-mail service. Zimbra Collaboration Suite (ZCS) is one powerful mail server application that can be used as a mail server application in the number of users from tens to thousands. In this study, the encryption system on the Zimbra multiple-mail server uses the OpenPGP method to be implemented to secure the contents of e-mails sent and received, namely by using the public key and private key. The test results show that the OpenPGP method works well for the security of the email sending/receiving system on a multi-mail server.

Keywords: *multi mail server, Zimbra, email security, OpenPGP*

1. PENDAHULUAN

Surat elektronik atau elektronik *mail (E-mail)* merupakan media komunikasi yang sangat populer. Untuk mengirim dan menerima *email*, diperlukan sebuah penyedia *(server)* yang di dalamnya terdapat layanan *email*. Istilah *email server* atau dalam bahasa jaringan komputer disebut juga *Mail Transfer Agent* (MTA) merupakan salah satu komponen penting dalam *server internet*. Ada beragam MTA yang bisa dipilih oleh seorang administrator jaringan komputer dalam membangun atau mengembangkan *server email*. Pertimbangan yang lebih teliti biasanya dilakukan dalam membangun *server email* dibandingkan membangun sebuah server *website* sebab setiap situs harus mendaftarkan *mail exchanger* yang digunakannya pada *Domain Name Server (DNS)* global.

Mail Server yaitu sebuah *server* yang digunakan untuk menyimpan dan mengirim sebuah *email*. *Mail Server* dapat diartikan juga sebagai perangkat lunak program yang mendistribusikan *file* atau informasi sebagai respon atas permintaan yang dikirim via *email* yang saling berkomunikasi satu dengan yang lainnya melalui jaringan LAN/WAN yang memberikan komunikasi antara *client* dengan *server*. Untuk mengirim sebuah *email* dari alamat *email* yang satu kealamat *email* yang lain digunakan sebauh *protocol* (aturan) yaitu *Simple Mail Transfer Protocol* (SMTP). SMTP merupakan protokol yang digunakan untuk mengirim *email* (komunikasi antar *mail server*), dan tidak digunakan untuk berkomunikasi dengan *client*.

Dalam penggunaannya, jika transaksi pengiriman dan penerimaan *email* mencapai ratusan ribu *email* dalam 1 hari, mekanisme *single server* akan terbebani trafik. Akses *email* akan terasa lambat karena disaat yang bersamaan, *resources server* harus dipergunakan untuk menangani *service* lain seperti MTA, anti *spam* dan anti *virus*. Untuk mengantisipasinya, kita bisa menggunakan Zimbra *mail server* dengan skema *multi server* (Sugianto, M., 2015). Penggunaan multi mail server dan multi *platform* semakin banyak perhatian dalam pekerjaan bidang istem informasi, salah satunya adalah untuk administrasi jaringan komputer (Suhatman, 2016).

Sementara itu, *Zimbra Collaboration Suite* (ZCS) merupakan salah satu aplikasi *mail server powerful* yang dapat dipergunakan sebagai aplikasi *mail server* dalam jumlah *user* puluhan hingga ribuan. Untuk menangani transaksi beberapa ribu hingga belasan ribu *email* dalam 1 hari, *SysAdmin* cukup menggunakan 1 buah *mail server* berbasis Zimbra. Semua *service* Zimbra dijalankan di dalam 1 mesin sehingga hemat biaya investasi dan mudah ditangani.

Dalam skala lebih sederhana, hal di atas bisa diterapkan untuk skema kantor cabang dan kantor pusat. Misalnya untuk Jakarta sebagai pusat, layanan yang diinstall adalah *Lightweight Directory Access Protocol* (LDAP) *Server* untuk semua authentikasi, MTA *server* untuk Jakarta dan *mailbox* untuk Jakarta sedangkan untuk kota lain cukup *mailbox server* (dan jika perlu, MTA *server*) (Sugianto, M., 2015).

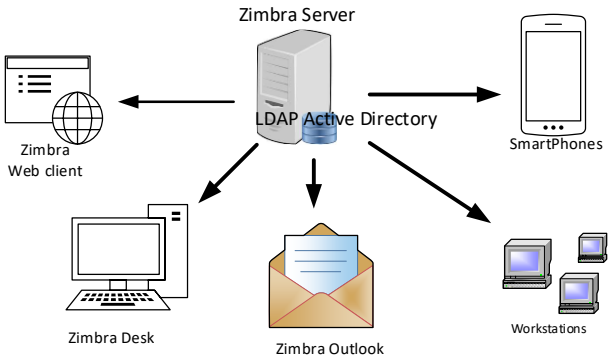
Model *multi server* ini akan mudah dikembangkan, berapapun banyaknya *site* yang harus dijangkau. Jika satu waktu ada tambahan kantor cabang baru di Papua, misalnya, kita cukup melakukan instalasi *mailbox server* dan MTA server di Papua. *Site* di Jakarta hanya untuk keperluan authentikasi saja. Meski banyak *site*, aksesnya tetap bisa menggunakan 1 nama domain dan juga 1 akses (Sugianto, M., 2015).

OpenPGP adalah salah satu metode enkripsi yang menggunakan model sertifikasi di mana setiap entitas dapat mengesahkan entitas lain. Metode eknripsi ini merupakan gabungan antara *Pretty Good Privacy (PGP)* dan *GNU Privacy Guard (GnuPG)*, selain digunakan untuk metode enkripsi pada *email* juga bisa di implementasikan pada *web server* (Ulrich, 2011). Implementasi PGP sebagai sistem pengaman sudah dikerjakan pada penelitian sebelumnya, dan diterapkan untuk Zimbra mail server (Hostiadi, 2017). Namun hanya sebatas menguji pada *platform* single *email* server. Artikel tersebut juga belum menyajikan pengiriman *email* dari daftar alamat *email* yang diijinkan atau ditolak dalam daftar *blacklist*.

Oleh karena itu, pengembangan dan penambah baikan penelitian keamanan *email* ditingkatkan melalui *multi-email server*. Pada penelitian ini, sistem enkripsi pada Zimbra *multiple server* menggunakan algoritma *OpenPGP* diimplementasikan untuk mengamankan isi *email* yang dikirim maupun yang diterima, yaitu dengan memanfaatkan *public key* dan *private key*. Di mana antara server *email* penerima dan pengirim sudah mempunyai *public key* masing-masing, dan saling mendaftarkan di *server*.

2. TINJAUAN PUSTAKA

Zimbra Collaboration Suite (ZCS) merupakan salah satu aplikasi *mail server* powerful yang dapat dipergunakan sebagai aplikasi *mail server* dalam jumlah *user* puluhan hingga ribuan. Untuk menangani transaksi beberapa ribu hingga belasan ribu *email* dalam 1 hari, *SysAdmin* cukup menggunakan 1 buah *mail server* berbasis Zimbra. Semua *service* Zimbra dijalankan di dalam 1 mesin sehingga hemat biaya investasi dan mudah ditangani. Ilustrasi ZCS bisa dilihat pada Gambar 1.



Gambar 1. Ilustrasi Zimbra Collaboration Suites

Penelitian tentang Zimbra dan implementasinya sudah banyak dkerjakan baik di lingkungan perguruan tinggi maupun instansi atau perusahaan. Ada beberapa aplikasi *exchange* mail *server* yang banyak digunakan, salah satu yang populer adalah *Google mail*. Jinsheng Xu (Xu, 2008) dan koleganya telah melakukan *survey* terhadap sepuluh *collaboration tools* dan fitur-fitur yang disediakan, termasuk ZCS di dalamnya. Hasilnya memberikan pilihan kepada *user* untuk menentukan *collaboration tools* sesuai dengan kebutuhannya. Komponen yang diujikan antara lain adalah kestabilan dan performansi sistem, ketersedian berbagi informasi, kelompok kalender dan fitur tentang manajemen proyek. Kelebihan lain dari Zimbra adalah sebuah aplikasi terbuka dan berjalan pada *platform* sistem operasi Linux. Implementasi Zimbra sebagai *mail server* telah dikerjakan pada penelitian sebelumnya (Kusuma, 2012), dengan diinstal pada sistem operasi Centos 5.0. Belum optimalnya performansi *mail server* ini merupakan tantangan tersendiri untuk pekerjaan selanjutnya.

Beberapa penelitian tentang Zimbra dan implementasinya sudah dikerjakan sebelumnya oleh

I Gede Chandra Kusuma pada tahun 2012. Pada penelitian yang artikelnya diterbitkan oleh Jurnal Elektronik Ilmu Komputer Universitas Udayana tersebut, I Gede Chandra Kusuma berhasil membangun dan menerapkan sistem manajemen *user* secara terpusat menggunakan aplikasi ZCS LDAP atau yang lebih dikenal dengan Zimbra LDAP (Kusuma, 2012). Hal ini menunjukkan bahwa Zimbra juga *compatible* terhadap aplikasi penanganan *account* seperti LDAP.

Data yang berhasil ditunjukkan pada penelitian yang lain (Jain, 2013) bahwa Zimbra sudah berhasil menduduki peringkat kedua penggunaan *exchange email server* setelah Gmail milik Google, yakni 40% institusi di Amerika Serikat menggunakan Zimbra sebagai solusi hosting emailnya.

Studi analisis terkait keamanan jaringan komputer dalam *multi server* berbasis Moodle dan Zimbra telah dikerjakan oleh Rafal Grzybowski dan Blazej Feret (Grzybowski, 2015). Mereka menguji tingkat keamanan dari *multi server* E-Learning pada penelitiannya ini. Dengan menggunakan metode *Central Authentication System (CAS)* dan beberapa area kemanan jaringan diantaranya adalah performansi aplikasi, pusat data *(database)* dan pengelolaan jaringan. Terlihat bahwa pada area *session management* memberikan efek yang tinggi terhadap keamanan jaringan komputer. Kesalahan dasar mencapai 78% pada percobaan ini.

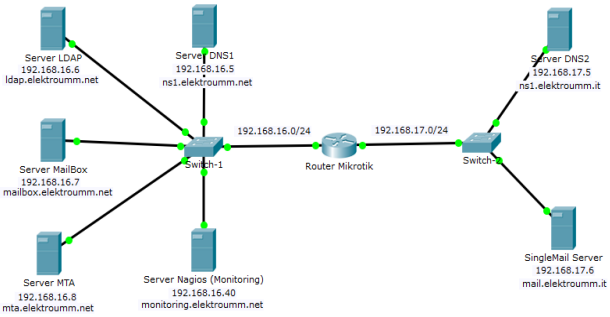
Sementara itu, lebih jauh lagi, pengembangan algoritma enkripsi disajikan oleh Liu dan koleganya, (Liu, 2018). Algoritma AES dan DH dibandingkan dalam pekerjaan mereka. Penerapan keamanan jaringan yang lain pada Zimbra *mail server* telah dibuktikan oleh Made Sudarma dan Dandy P. Hostiadi (Sudarma, 2016). Dalam hal ini, mereka menggunakan metode *pretty good privacy (PGP)* untuk mengamati keamanan komunikasi surat elektronik melalui enkripsi pesan dan lampiran yang dipakai dalam surat elektronik tersebut. Hasil akhir dalam pekerjaan ini adalah metode PGP berhasil digunakan sebagai metode untuk analisis keamanan jaringan pada Zimbra *mail server*.

3. DESAIN MULTI MAIL SERVER

Pada sebuah sistem layanan *email* dikenal ada dua jenis yaitu : *SingleMail Server dan Multiplemail Server*, semua jenis *service* yang berkaitan dengan *email* berjalan dalam satu *server* ini disebut *SingleMail Server* sedangkan pada *MultipleMail Server* ada beberapa *service email* yang berjalan di *server* terpisah tetapi tetap menjadi satu sistem *email*. *MultipleMail Server* merupakan sebuah solusi untuk meningkatkan performansi dan kinerja sebuah sistem layanan *email* dari sebuah instansi/institusi/lembaga yang setiap waktunya membutuhkan akses/transaksi melalui *email*. Layanan *email* yang menggunakan *Multiplemail Server* memisahkan *service-service* inti yang ada pada *server email*, adapun *service* tersebut adalah *MTA (Mail Transfer Agent), LDAP (Account) dan MailBox.* Tujuan dari pemisahan *service* ini adalah untuk meringankan kinerja dari *server*, sehingga bisa meningkatkan performansi layanan sistem *email.*

3.1. Desain Topologi Multi Mail Server

Dalam penelitian ini menggunakan jaringan skala laboratorium di mana domain yang ada tidak terkoneksi dengan internet, sehingga domain-domain yang digunakan *email* tidak terbaca jika diakses dari internet, berikut topologi yang digunakan dalam Gambar 2.



Gambar 2. Topologi Rancangan Jaringan *MultipleMail Server*

Dari Gambar 2 terdapat sebuah *router mikrotik* yang digunakan untuk membagi jaringan menjadi dua yaitu *network* 192.168.16.0/24 dan 192.168.17.0/24, di mana *network* 192.168.16.0/24 digunakan untuk jaringan *Multiplemail Server* dan *network* 192.168.17.0/24 digunakan untuk jaringan *Singlemail Server.*

Secara garis besar *service* dalam layanan *email* dibagi menjadi tiga yaitu: *Account,* layanan dalam *Zimbra* yang berfungsi sebagai pembuatan dan penyimpanan *account* adalah *service ZimbraLDAP*, *MailBox,* layanan dalam Zimbra yang berfungsi sebagai *storage* atau penyimpanan *email* adalah *service ZimbraMailbox, MTA (Mail Transfer Agents),* layanan dalam Zimbra yang berfungsi sebagai pengatur keluar masuknya *email* adalah *service ZimbraMTA.*

3.2. Desain DNS Server

Rancangan sistem *DNS server* yang bekerja dengan baik adalah syarat utama dalam membuat sebuah sistem layanan *email*, oleh karena itu perlu dilakukan konfigurasi yang sesuai dengan kebutuhan dan standar *Zimbra Multiplemail Server*, di mana masing-masing *service* harus dibuatkan *MX (Mail eXchange)* di *server* DNS, agar *email* bisa diarahkan ke sisi penerima/pengirim *email*. Aplikasi yang dipakai pada pekerjaan ini untuk DNS *server* adalah open source *Bind9*. Setelah instalasi *Bind9* berhasil, dilanjutkan dengan konfigurasi untuk DNS *server* dan dilakukan pengujian DNS *service*.

3.3. Account LDAP Multimail Server

Service *ZimbraLDAP* berfungsi untuk memanajemen *user*, pada *service* ini yang mengatur *login/logout user*, *create/delete user*, *service* ini di bangun pertama kali karena *service* MailBox dan MTA *(Mail Transfer Agents)* membutuhkan LDAP untuk memverifikasi servernya, jika tidak terverifikasi atau error pada saat verifikasi maka MultiMail *Server* tidak akan bisa berjalan.

3.4. Desain Mailbox *(storage)*

Service MailBox ini merupakan yang paling penting, karena tanpa adanya *service* ini Zimbra Mail Server tidak bisa diakses via *website*, tanpa adanya service ini tidak bisa melakukan *management user* maupun melihat *user* yang *login* atau bermasalah dengan emailnya.

3.5. Desain Multi Transfer Agent (MTA)

MTA *(Mail Transfer Agents)* adalah *service* yang mengatur lalu lintas *email* yang masuk ke dalam *server*, jika ada kesalahan konfigurasi yang dilakukan besar kemungkinan sistem layanan *email* yang dibuat tidak akan bisa melakukan pengiriman/penerimaan *email*.

3.6. Desain Sistem Monitoring

Untuk mendukung sistem layanan *email* yang sudah dirancang dalam penelitian dibuat sebuah *server* yang difungsikan sebagai *server monitoring* di mana di dalamnya ditanam aplikasi *monitoring Nagios*. *Nagios* biasanya digunakan untuk memonitoring layanan-layanan yang berjalan pada *server*, bisa juga untuk melihat grafik *server* tetapi kita harus menginstall pluginsnya.

3.6. Desain Sistem Enkripsi *OpenPGP*

Sistem enkripsi pada Zimbra multiple *email server* berfungsi untuk mengamankan isi *email* yang dikirim maupun yang diterima, yaitu dengan memanfaatkan *public key*. Di mana antara *server email* penerima dan pengirim sudah mempunyai public key masing-masing, dan saling mendaftarkan di *server*. Teknik enksripsi *email* teks yang lain bisa dijumpai pada artikel ini (Arfriandi, 2018). OpenPGP akan diimplementasikan sebagai pengaman *mail server* dalam pekerjaan ini. Lebih detail instalasi dan konfigurasi teknik OpenPGP bisa dijumpai pada artikel ini (Zaien, M., 2016) dan pada artikel ini (Hostiadi, 2017).

3.6. Sistem Filter Spam dengan *SpamAssasin*

Beberapa contoh aplikasi filter spam email banyak diulas pada artikel ilmiah baru-baru ini. Dan salah satu contoh bagus adalah SpamAssain (Dada, G.E., 2019). Untuk itu, *filter spam* yang digunakan pada penelitian ini merupakan fitur default dari Zimbra sendiri, yang difilter pada penelitian ini hanya berdasarkan *email* yang diblacklist, dimana pada konfigurasi *SpamAssasin* sudah ditentukan *email* mana yang telah di*blacklist*, dan *email* mana yang masuk ke daftar *whitelist*. *Email* yang di *blacklist* secara otomatis tidak bisa masuk ke dalam *inbox* ataupun junk, tapi bisa dilihat pada *log* Zimbra dan muncul catatan bahwa *email* pengirim terindikasi sebagai *spam*.

4. HASIL PENGUJIAN DAN ANALISA

4.1. Pengujian DNS Server

Pengujian DNS *Server* lebih menitikberatkan untuk memastikan *server* berjalan dengan baik, dan domainnya bisa *nslookup* atau bisa *dig*, ada beberapa langkah dalam melakukan pengujian DNS *server*; (i) Melakukan pengujian DNS *server* untuk domain elektroumm.net, disini memastikan domain yang digunakan untuk *MultipleMail server* bisa digunakan atau tidak. (ii) Melakukan pengujian DNS *server* untuk domain elektroumm.net. Serta melakukan pengujian untuk mengetahui domain yang ada di domain elektroumm.net dan *elektroumm.it.*

4.2. Pengujian MultiMail Server

Pertama yang perlu dilihat adalah hasil *LDAP Server* untuk mengetahui *service LDAP* berjalan dengan baik pada system. Pengujian untuk mengetahui *service* berjalan dengan baik, masuk ke sistem dengan melakukan *login* ke dalam shell Ubuntu, setelah *user login* melakukan pengecekan *service LDAP* berjalan, seperti pada Gambar 3.

```
root@ldap:~# su - zimbra
zimbra@ldap:~$ zmcontrol status
Host ldap.elektroumm.net
        ldap                    Running
        stats                   Running
        zmconfigd               Running
zimbra@ldap:~$
```

Gambar 3. Service *LDAP* berjalan

Selanjutnya adalah pengujian *MailBox Server* untuk mengetahui *service MailBox* berjalan dengan baik pada system. Pengujian untuk mengetahui *service* berjalan dengan baik, masuk ke sistem dengan melakukan *login* ke dalam *shell Ubuntu*, setelah *user login* melakukan pengecekan *service* MailBox berjalan, seperti pada Gambar 4.

```
zimbra@mailbox:~$ zmcontrol status
Host mailbox.elektroumm.net
        logger                  Running
        mailbox                 Running
        spell                   Running
        stats                   Running
        zmconfigd               Running
zimbra@mailbox:~$
```

Gambar 4. service *MailBox* berjalan

Dilanjutkan dengan pengujian MTA *Server* untuk mengetahui *service* MTA berjalan dengan

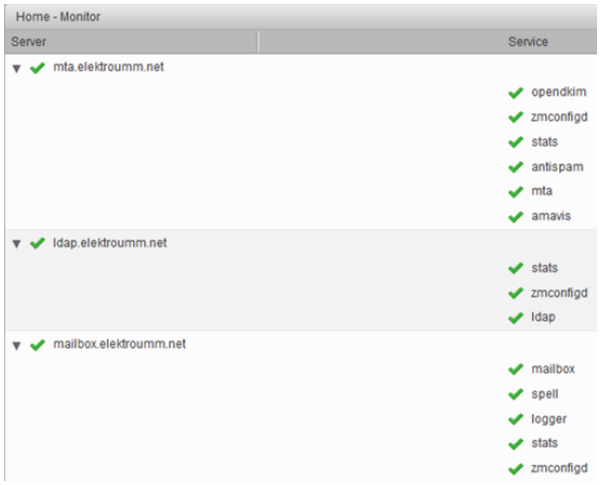
baik pada sistem. Pengujian untuk mengetahui *service* berjalan dengan baik, masuk ke sistem dengan melakukan *login* ke dalam *shell Ubuntu*, setelah *user login* melakukan pengecekan *service* MTA berjalan, seperti pada Gambar 5.

```
zimbra@mta:~$ zmcontrol status
Host mta.elektroumm.net
        amavis                  Running
        antispam                Running
        mta                     Running
        opendkim                Running
        stats                   Running
        zmconfigd               Running
zimbra@mta:~$
```

Gambar 5. Service MTA berjalan

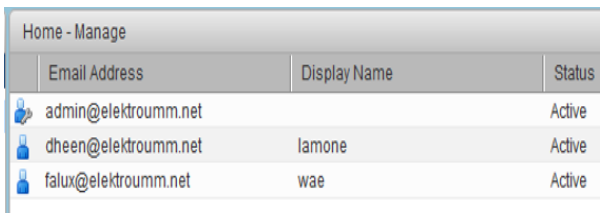
Pengujian MultipleMail *Server* secara keseluruhan adalah untuk mengetahui sistem layanan *email* berjalan dengan baik dan bisa digunakan untuk melakukan pengiriman dan penerimaan *email*. Juga untuk mengetahui *service-service* yang dipisah secara fisik tapi bisa menyatu secara *logic*, ini terlihat pada pengujian.

Pengujian untuk mengetahui *service* berjalan dengan baik, masuk ke sistem dengan melakukan *login* ke dalam halaman *web* administrator *https://mailbox.elektroumm.net:7071 login* dengan menggunakan *user* default dari Zimbra yaitu *user* = admin dan passwordnya = elektroumm1 , setelah *user login* melakukan pengecekan *service* secara keseluruhan berjalan, seperti pada Gambar 6.



Gambar 6. Service Secara Keseluruhan Berjalan

Buat beberapa *account* untuk melakukan proses pengiriman *email*, seperti pada Gambar 7.

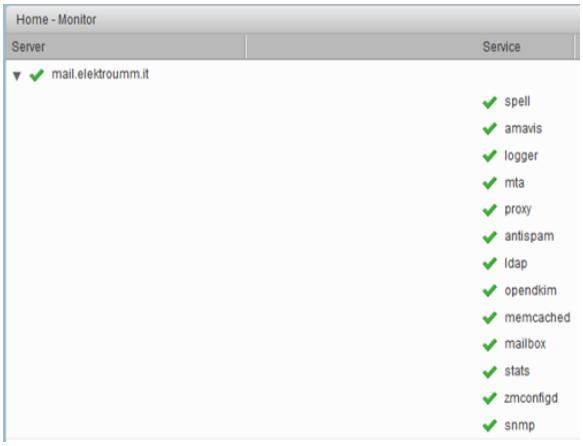


Gambar 7. Contoh user yang sudah dibuat pada Email

Pengujian *SingleMail Server* untuk mengetahui sistem layanan email berjalan dengan baik dan bisa digunakan untuk melakukan pengiriman dan penerimaan *email*.

Pengujian untuk mengetahui *service* berjalan dengan baik, masuk ke sistem dengan melakukan *login* ke dalam *shell* Ubuntu, setelah *user login* melakukan pengecekan *service* MTA berjalan.

Pengujian untuk mengetahui *service* berjalan dengan baik, masuk ke sistem dengan melakukan *login* ke halaman *web* administrator https://mail.elektroumm.it:7071 *login* dengan menggunakan *user* default dari Zimbra yaitu *user* = admin dan passwordnya = elektroumm1, setelah *user login* melakukan pengecekan *service* secara keseluruhan berjalan seperti pada Gambar 8.



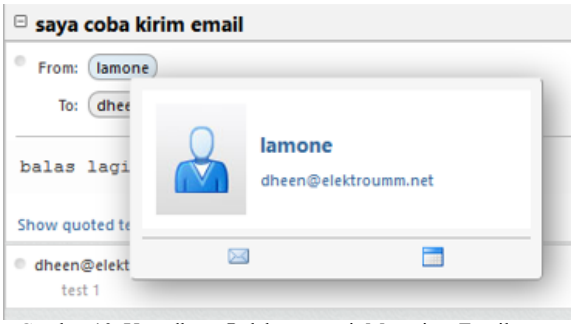
Gambar 8. Service *SingleMail server* berjalan

Selanjutnya adalah pengujian keseluruhan siuste. Pengujian ini untuk mengetahui sistem layanan *email* bisa melakukan proses pengriiman dan penerimaaan *email*.

Untuk *user* yang dibuatkan pada *server* elektroumm.net melakukan *login* ke alamat https://mailbox.elektroumm.net *login* dengan *account* yang sudah dibuat dan untuk *user* yang dibuatkan pada *server* elektroumm.it melakukan *login* ke alamat https://mail.elektroumm.it .

Melakukan proses pengiriman dan reply *email* seperti pada Gambar 9. Pada masing-masing *account* terlihat *email* pengirim dan *email* penerima, seperti pada Gambar 10.

Gambar 9. User dheen@elektroumm.net menerima email yang dikirim dari User faruk@elektroumm.it



Gambar 10. User dheen@elektroumm.it Menerima Email yang Dikirim dari User dheen@elektroumm.net

4.3. Pengujian Server Nagios

Pengujian ini untuk mengetahui sistem layanan *email* bisa dimonitoring dari *server Nagios*, yang dimonitoring disini adalah *service*nya apakah berjalan atau tidak semua bisa dilihat pada *server monitoring Nagios*, yang bisa diakses di 192.168.16.40 atau monitoring.elektroumm.net. Untuk memastikan *server-server email* Zimbra LDAP, MailBox, MTA sudah terkoneksi dengan *server monitoring* bisa dilihat pada *syslog* yang ada pada tiap-tiap server,

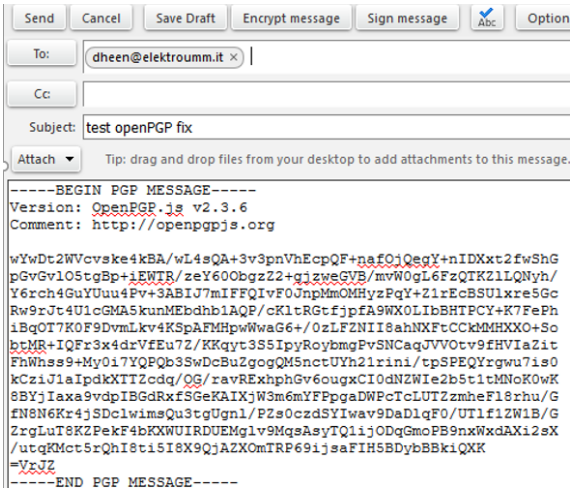
Ketika *server monitoring.elektroumm.net* sudah terkoneksi dengan tiap-tiap *client*nya, secara otomatis pada *server monitoring* muncul beberapa client yang sudah terkoneksi akan ditampilkan dalam portal monitoring sistem dalam hal ini adalah *Nagios*. Selanjutnya adalah melakukan proses pengujian *OpenPGP* yaitu melakukan pengiriman *email* melalui salah satu *account email*.

Email yang sudah terenkripsi terlihat pesan yang sebelumnya test satu dua tiga menjadi *file* yang sudah terenkripsi, menandakan *email* sudah terenkripsi. Sementara Gambar 11 memperlihatkan *email* hasil enkripsi yang sudah siap dikirim.

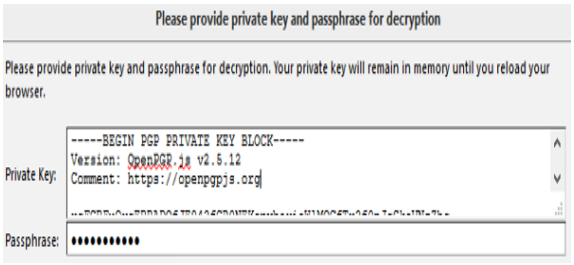
Buka *browser* lain arahkan ke https://mail.elektroumm.it *login* menggunakan *email* dheen@elektroumm.it buka inbox klik *email* yang baru diterima, maka akan muncul permintaan *passphrase* dan *private key* klik OK dan hasilnya ditunjukkan seperti pada Gambar 12.

Setelah *email* terbuka, yang semula isinya hanya terlihat kode enkripsi dan muncul isi *email* test satu dua tiga juga ditandai dengan tulisan OpenPGP : *Got a good Signature* ini menandakan bahwa isi *email* berhasil terenkripsi dan juga berhasil didekripsi sehingga terlihat hasilnya pada Gambar 13.

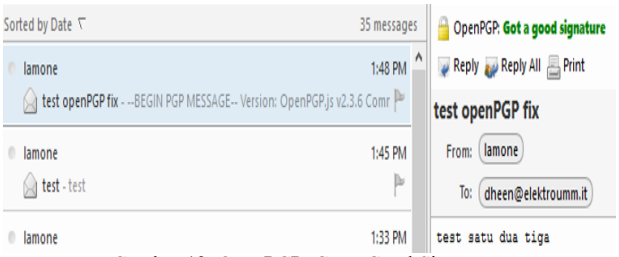
Untuk memastikan *signature* dan *encrypt* berfungsi dengan baik, integrasikan kedua metode ini untuk mengirimkan *email* yang pertama *email* dienkripsi dulu kemudain diberikan tanda bahwa *email* itu benar-benar dikirimkan oleh dheen@elektroumm.it.



Gambar 11. Email terenkripsi sudah siap dikirimkan



Gambar 12. Permintaan *Passphrase* dan *Private Key*

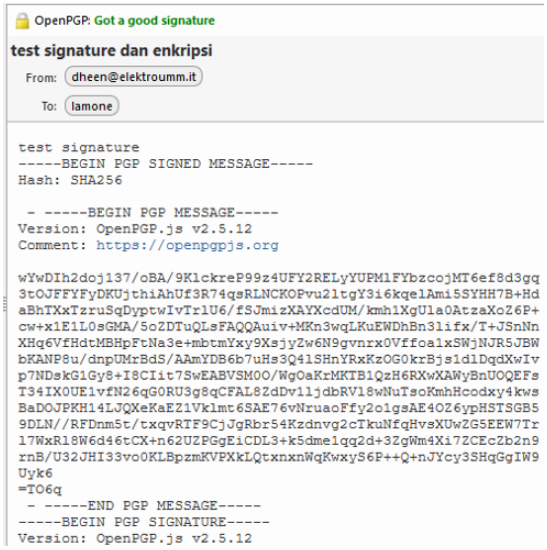


Gambar 13. OpenPGP Got a Good Signature

Email yang dikirimkan oleh *account* dheen@elektroumm.it telah diterima oleh *account* dheen@elektroumm.net dengan signature sebagai tanda bahwa *email* tersebut benar-benar berasal dari dheen@elektroumm.it dan telah dienkripsi isinya, OpenPGP *Got a good signature* sebagai tanda bahwa OpenPGP bekerja dengan baik dalam proses enkripsi maupun memberikan tanda. Seperti dilihatkan pada Gambar 14.

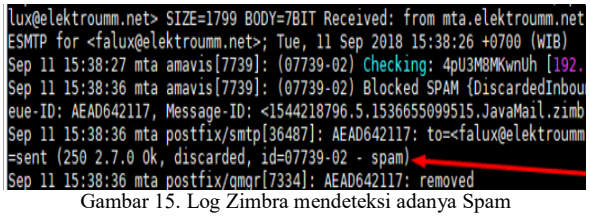
Selanjutnya adalah melakukan pengujian *SpamAssassin.* Pada penelitian ini meliputi dua hal yaitu *email* yang masuk dalam daftar *blacklist* dan *email* yang masuk dalam daftar *whitelist, email* yang masuk dalam daftar *blacklist* adalah *falux@elektroumm.it* dan untuk *email* yang masuk dalam daftar *whitelist* adalah *dheen@elektroumm.it*. *account* yang masuk dalam daftar *blacklist* emailnya tidak akan sampe ke sisi penerima karena diblock oleh sistem dan ditandai sebagi *spam* di *Zimbra.log*. Sedangkan *account* yang masuk dalam daftar

whitelist email akan sampai ke sisi penerima dengan ditandai *delivered* pada *Zimbra.log*.



Gambar 14. Email *signature* dan *encrypt* pada email yang dikirim

Arahkan *browser* menuju alamat https://mail.elektroumm.it *login* menggunakan *account* falux@elektroumm.it kirimkan *email* ke alamat falux@elektroumm.net. Setelah *email* dikirimkan masuk ke *server mta.elektroumm.net* melalui terminal untuk melihat *Zimbra.log* menggunakan *command tail –f /var/log/Zimbra.log*. Gambar 15 menunjukkan rekaman *spam* Zimbra.



Gambar 15. Log Zimbra mendeteksi adanya Spam

Email yang dikirimkan oleh falux@elektroumm.it ke alamat *email* tujuan falux@elektroumm.net dideteksi sebagai spam sehingga statusnya menjadi discarded atau ditolak.

Untuk mengirimkan *email* dengan menggunakan *account* yang masuk daftar *whitelist*, arahkan *browser* menuju alamat https://mail.elektroumm.it *login* menggunakan *account* dheen@elektroumm.it kirimkan *email* ke alamat dheen@elektroumm.net. Dengan mengirimkan *email* menggunakan *account* yang masuk daftar *whitelist* Setelah *email* dikirimkan masuk ke *server* mta.elektroumm.net via terminal untuk melihat *Zimbra.log* menngunakan command *tail –f /var/log/Zimbra.log*. Jika Log Zimbra Tidak Mendeteksi Adanya Spam *email* yang dikirimkan oleh *dheen@elektroumm.it* tujuan *dheen@elektroumm.net* tidak dideteksi sebagai *spam* sehingga statusnya menjadi *delivery OK* atau diterima seperti terlihat pada panah merah pada Gambar 16.

Gambar 16. Mengirimkan Email Dengan Menggunakan Account yang Masuk Daftar *Whitelist*

5. KESIMPULAN

Sistem keamanan multi mail *server* pada Zimbra *exchange software* berhasil diterapkan pada peneltitian ini dengan metode OpenPGP sebagai teknik pengamannya. Dari hasil pengujian diketahui bahwa *email* yang dikirim dengan menggunakan metode enkripsi OpenPGP tidak terbaca isi *email* jika tidak sesuai kode dekripsinya. Untuk *email* yang di*blacklist* menggunakan *SpamAssasin* hanya bisa terlihat di *log server email* tidak akan terkirim ke inbox yang dituju. Jika *service-service* yang ada pada *server* multi mail pada kondisi off atau *error* bisa terlihat di sistem *monitoring Nagios*. Dalam hasil penelitian ini, terlihat perbedaan *mail header* di mana pengamanan OpenPGP memberikan identitas enkripsi sedangkan pada *email* tanpa OpenPGP tidak dijumpai adanya identitas enskripsi.

Pada pekerjaan penelitian berikutnya, implementasi *security-tools* selain OpenPGP bisa menjadi alternative sebagai sistem pembanding dan menguji efektifitas sistem keamanan multi-mail server. Yang pada akhirnya bisa menjadi suatu *platform* uji sistem keamanan pada jaringan multi-mail server dengan aplikasi yang berbeda.

UCAPAN TERIMA KASIH

Penulis dan tim peneliti mengucapkan terima kasih dan penghargaan kepada Jurusan Teknik Elektro, Fakultas Teknik dan Direktorat Penelitian dan Pengabdian Masyarakat (DPPM), Universitas Muhammadiyah Malang atas dukungan dan pembiayaan sehingga terselenggaranya pekerjaan penelitian ini.

DAFTAR PUSTAKA

ARFRIANDI, A., 2018. Pengamanan Teks Pada Dokumen Email Menggunakan Enkripsi Rotor. *Edu Komputike Jurnal*. 5(1). p. 23-32.

DADA, G.E., BASSI, S.J., CHIROMA, H., ABDULHAMID, M.S., 2019. Machine learning for email spam filtering: review, approaches and open research problems. *Heliyon*. 5. p. 1-23.

GRZYBOWSKI, R. AND FERET, B., 2015, September. "The Analysis of Security in a Multi-Server E-Learning Environment Based

on Moodle and Zimbra Software". *In The Fourth International Conference on E-Learning and E-Technologies in Education (ICEEE2015)* (p. 41).

HOSTIADI, P.D., dan SUDARMA, B.I., 2017. Implementasi Pengamanan PGP pada Platform Zimbra Mail Server. Lontar Komputer. 8(1). p. 41-52.

IS SUPRIHATIN., AGUSHINTA, D.R., 2009, "Optimizing Mail Server Using Zimbra Collaboration Suite 5.0.2 in Operating System Centos 5.0" *Jurnal Ilmiah Informatika Komputer*. 14 (1), p.19.

JAIN, A. AND PANDEY, U.S., 2013. "Role of Cloud Computing in Higher Education". *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(7).

KUSUMA, CHANDRA,. GI., 2012, "Perancangan dan Implementasi LDAP pada LTSP dan Terintegrasi Dengan Zimbra LDAP", *Jurnal Elektronik Ilmu Komputer*, Universitas Udayana, 2 (1), p.24.

LIU, J., FAN, C.L., TIAN, X.Y., dan DING, Q. 2018. Email encryption system based on AES algorithm and DH algorithm. *Journal of Information Hiding and Multimedia Signal Processing*. 9(1). p. 11-20.

SUDARMA, M. AND HOSTIADI, D.P., 2016. "Implementation of Email Security using PGP at Zimbramail Server". *International Journal of Computer Science Issues* (IJCSI), 13(6), p.113.

SUHATMAN, R., 2016. Analisa Performansi Server Cloud Berbasis Proxmox Ve untuk Multi Mail dan Multi Platform pada Praktikum Administrasi Jaringan Komputer. *Jurnal Politeknik Caltex Riau*. 2 (1). p. 17-26.

SUGIANTO, M. V., 2015, "Zimbra multi server: Solusi untuk Mail Server Multi Site", Exellent Infotama Kreasindo, www.excellent.co.id, Jakarta.

ULRICH A, HOLZ R, HAUCK P, CARLE G, 2011, September. "Investigating the OpenPGP Web of Trust" . *European Symposium on Research in Computer Security (ESORICS)*. pp 489-507.

XU, J., ZHANG, J., HARVEY, T. AND YOUNG, J., 2008. A survey of asynchronous collaboration tools. *Information Technology Journal.* 7(8), pp.1182-1187.

ZAIEN, M., FAISAL, R.M., dan NUGROHO, A.R., 2016. UJI PERFORMANSI OpenPGP PADA KOMUNIKASI DATA WEB SERVICE BERBASIS RESTFull. *Kumpulan Jurnal Ilmu Komputer (KLIK).* 4(1). p. 61-70.