ANALISA PERFORMANSI KEAMANAN JARINGAN VPN PPTP DAN L2TP/IPSEC UNTUK FTP SERVER DI POLITEKNIK NEGERI MALANG

Muliatama Putra Mahardiyanto[1], Nugroho Suharto[2],Hendro Darmono.[3]
[123]Program Studi Jaringan Telekomunikasi Digital, Jurusan Teknik Elektro, Politeknik Negeri Malang

Abstrak

Komunikasi pertukaran data mengalami perkembangan yang mengarah pada komunikasi terpusat, dan untuk mewujudkan komunikasi tersebut diperlukan jenis komunikasi data yang datanya ditampung pada server dan dapat diakses oleh client, seperti di Politeknik Negeri Malang. Sebagai instansi yang bergerak dalam dunia pendidikan, perkembangan komunikasi data secara terpusatdengan memanfaatkan jaringan intranet yang telah terbentuk. Penggunaan jaringan intranet memungkinkan akan komunikasi data yang rentan penyadapan. Untuk mengatasinya menggunakan jaringan VPN. VPN PPTP dan VPN L2TP/IPsec mempunyai performansi yang berbeda terutama dalam tingkat keamanan yang diberikan. Dalam penelitian ini dilakukan analisa peformansi jaringan VPN PPTP dan VPN L2TP/IPsec yang diimplementasikan pada FTP Server pada server Raspberry Pi dan router Mikrotik untuk konfigurasi VPN-nya.

Pada penelitian ini merancang VPN PPTP dan VPN L2TP/IPsec dengan cara mengkonfigurasi router Mikrotik RB9412nD-TC dan konfigurasi FTP Server menggunakan aplikasi proftpd di server Raspberry Pi. Untuk analisa keamanan menggunakan metode hacking untuk mendapatkan data login VPN Server dan metode sniffing untuk mendapatkan data login FTP Server, FTP data. Untuk analisa performansi menggunakan parameter delay, throughput, dan packet loss.

Berdasarkan hasil pengujian dan pembahasan, diperoleh bahwa jaringan VPN PTP mengamankan proses autentikasi data password ke VPN Server dengan mengenkripsi menjadi format MS-CHAP dan saat transfer data mengamankan data dengan enkripsi dan enkapsulasi dengan protokol PPP Compp dan GRE. Sedangkan jaringan VPN L2TP/IPsec mengamankan proses autentikasi data dengan mengamankan layer IP saat pengiriman data autentikasi dan saat transfer data mengamankan data dengan enkripsi dan enkapsulasi dengan protokol ESP. Untuk parameter delay pada jaringan intranet, delay download sebesar 0.66 ms dan delay upload sebesar 5.9 ms. Pada VPN PPTP, rata-rata delay download sebesar 36.38 ms dan delay upload sebesar 67.03 ms. Pada VPN L2TP/IPsec, delay download sebesar 43.71 ms dan delay upload sebesar 80.87 ms. Tergolong dalam kategori Excellent (<150 ms) dan kategori Excellent (150 ms sampai 300 ms) menurut standart ITU-T. Untuk parameter throughput pada jaringan intranet, throughput download sebesar 23.8 Mbit/s dan throughput upload sebesar 23.89 Mbit/s. Pada VPN PPTP, throughput download sebesar 21.09 Mbit/s dan throughput upload sebesar 20.9 Mbit/s. Pada VPN L2TP/IPsec, throughput download sebesar 8.77 Mbit/s dan throughput upload sebesar 9.6 Mbit/s. Untuk parameter packet loss baik jaringan intranet, VPN PPTP, dan VPN L2TP/IPsec bernilai 0 %, tergolong dalam kategori Sangat Bagus menurut standart ITU-T. Untukkepadatanjaringanpada jam 09.00-09.35 jumlah user mencapai 460 dengan bandwidth tiap user 159.3 Kbps. Pada jam 13.10-13.45 mengalamikenaikanjumlah user 11.95% danpenurunan bandwidth tiap user 10.67%. Pada jam 14.45-15.20 mengalamipenurunanjumlah user 1.95% dankenaikan bandwidth tiap user 2%.

Kata kunci :*VPN PPTP, VPN L2TP/IPsec, FTP Server, Hacking, Sniffing, QoS.*

I. Pendahuluan

Komunikasi pertukaran data mengalami perkembangan yang mengarah pada komunikasi terpusat, dan untuk mewujudkan komunikasi tersebut diperlukan jenis komunikasi data yang datanya ditampung pada server dan dapat diakses oleh client, seperti di Politeknik Negeri Malang. Sebagai instansi yang bergerak dalam dunia pendidikan, perkembangan komunikasi data secara terpusatdengan memanfaatkan jaringan intranet yang telah terbentuk. Penggunaan jaringan intranet memungkinkan akan komunikasi data yang rentan penyadapan. Untuk mengatasinya menggunakan jaringan VPN.VPN PPTP dan VPN L2TP/IPsec mempunyai performansi yang berbeda terutama dalam tingkat keamanan yang diberikan. Keduatipejaringan VPN tersebutdapatdiimplementasikansebagaiujiperformansikeamananjaringan. Untukmembangunkomunikasi data terpusatpadaPoliteknikNegeri Malang, salahsatunyamenggunakan FTP *Server* Raspberry Pi dan router Mikrotiksebagai media membentukjaringan VPN.Denganmengimplementasikan FTP *Server*pada Raspberry Pi sebagai media komunikasi data terpusatdanpenggunaanjaringan VPN PPTP, L2TP/IPsec di PoliteknikNegeri Malangdapatdianalisakeamanandanperformansijaringan yang diberikanoleh VPN tersebut.

Berdasarkanhaltersebut, maka dapat dirumusankansebagaiberikut:

1. Bagaimana perbandingan keamanan jaringan VPN PPTP dan VPN L2TP/IPsec dalam pembacaan data *login* VPN *Server* menggunakan metode *Hacking*?
2. Bagaimana perbandingan keamanan jaringan intranet, VPN PPTP dan VPN L2TP/IPsec dalam pembacaan data *login* FTP *Server* dan FTP data menggunakan metode *Sniffing*?

3. Bagaimanaperbandingan performansi jaringan intranet, VPN PPTP dan VPN L2TP/IPsec berdasarkan *delay*, *throughput*, dan *packetloss* saat *downloadupload*?

II. Kajian Pustaka

2.1 *File Transfer Protocol* (FTP)

FTP merupakan salah satu protokol Internet yang paling awal dikembangkan, dan masih digunakan hingga saat ini untuk melakukan pengunduhan (download) dan pengunggah (upload) berkas-berkas komputer antara klien FTP dan server FTP.

2.2 Raspberry Pi

Raspberry Pi merupakan *single-board computer* yang dikembangkan di Inggris oleh Raspberry Pi Foundation. Raspberry Pi memiliki dua model, yaitu model A dan model B+. Model A menggunakan memori 256 MB sedangkan model B+ 512 MB. Selain itu model B+ juga sudah dilengkapi dengan port Ethernet.

2.3 Mikrotik

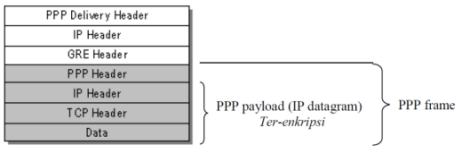
Mikrotik adalah sebuah perusahaan yang bergerak di bidang produksi perangkat keras (hardware) dan perangkat lunak (Software) yang berhubungan dengan sistem jaringan komputer yang berkantor pusat di Latvia, bersebelahan dengan Rusia. Jenis Mikrotik ada 2, yakni :

- Mikrotik RouterOS
- MikrotikRouterboard

2.4 *Virtual Private Network*

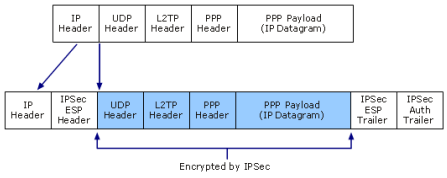
Virtual Private Network (VPN) adalahsebuahjaringankomputer yang berlapis-lapis (jaringan yang ada di atasjaringankomputer yang lain). VPN umumnyatidakterlihat, atau di enkapsulasi, lalulintasjaringan yang mendasarinya.

- VPN PPTP



Gambar 1. Paket Data L2TP

- VPN L2TP/IPsec



Gambar 2.Paket Data L2TP/IPsec

2.5 Keamanan Jaringan

Dengan semakin penting dan berharganya informasi dan ditunjang oleh kemajuan pengembangan software, menarik minat para pembobol (hacker) dan penyusup (intruder) untuk terus bereksperimen mempergunakan setiap kelemahan yang ada dari konfigurasi sistem informasi yang telah ditetapkan yang mana terdapat bermacam-macam peluang ancaman data yaitu diantaranya :

- *Session Hijacking*
  Pembajakan suatu komunikasi antar kedua belah pihak atau yang biasa disebut session hijacking.
- *Sniffing*
  Sniffing merupakan bentuk kecurangan lain pada media jaringan bersama seperti ethernet based IP network.

2.6 *Quality of Service* (Qos)

Quality of Service (QoS) merupakan mekanisme jaringan yang memungkinkan aplikasi-aplikasi atau layanan dapat beroperasi sesuai dengan yang diharapkan. cukup besar bagi banyak aplikasi Parameter – parameter dariQoS, antaralain :

- **Delay**

Delay (latency) adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan.

$$Delay = T_{terima} - T_{kirim}$$

Tabel1. KategoriBesarnya*Delay*
(Sumber: : Standar ITU-T G.1010)

Kategori	Besar*Delay*
Excellent	< 150 ms
Good	150 s/d 300 ms
Poor	300 s/d 450 ms
Unacceptable	> 450 ms

- **Throughput**

Throughput dari sistem merupakan perbandingan antara jumlah byte data yang diterima dan waktu pengiriman.
Rumus yang digunakan untuk mengihitung nilai *throughput* :

$$Throughput = \frac{Jumlah\ data\ yang\ dikirim\ (bit)}{Waktu\ pengiriman\ (second)}$$

- **Packet Loss**

Merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang.
Rumus yang digunakan untuk mengihitung nilai *packet loss* :

$$Packet\ Loss = \frac{Paket\ terkirim - Paket\ diterima}{Paket\ Kirim}\ x\ 100\%$$

Tabel 2.Kategori*Degradasi*Pada*Packet Loss*
(Sumber: :Standar ITU-T G.1010)

Kategori*Degradasi*	*Packet Loss*
SangatBagus	0%
Bagus	3%
Sedang	15%
TidakBagus	25%

2.6.1 Wireshark

Wireshark adalah paket *analyzer* gratis dan *opensource*. Hal ini digunakan untuk mengatasi masalah jaringan, analisis, pengembangan perangkat lunak dan protokol komunikasi, dan pendidikan

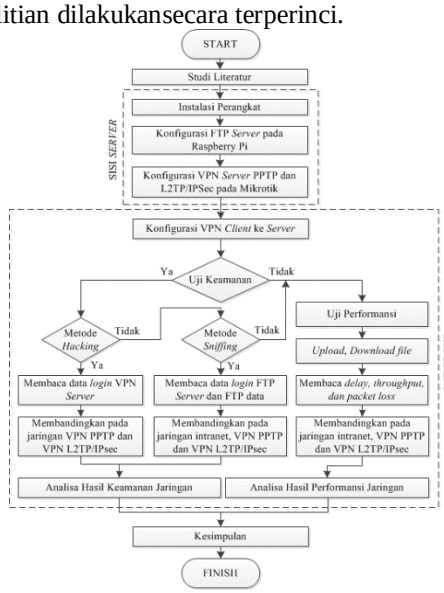
2.6.2 Ettercap

Ettercap memungkinkan membentuk serangan melawan protokol ARP dengan memposisikan diri sebagai "penengahdan akan memungkinkan untuk melihat password pada protokol-protokol seperti FTP,HTTP, POP, SSH1, dll

III. Metodologi Penelitian

3.1 Tahapan Penelitian

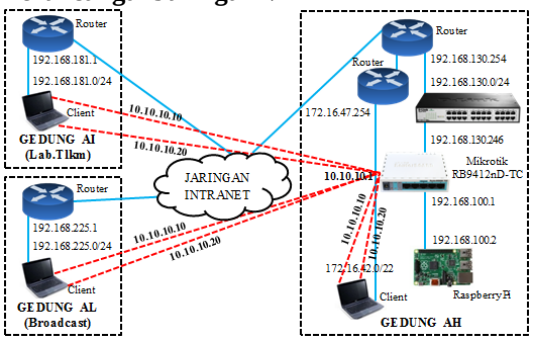
Tahapan penelitian disusundenganmaksudagar penelitian dilakukansecara terperinci.



Gambar 3. Tahapan Penelitian

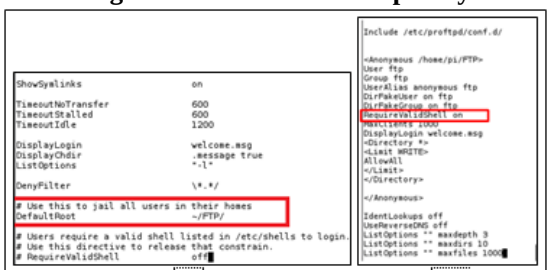
IV. Perencanaan Sistem

4.1 PerancanganJaringan VPN



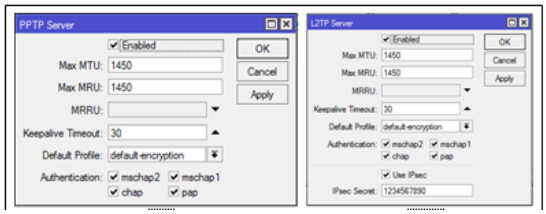
Gambar 4. Skema VPN Pada Intranet Polinema

4.2 Konfigurasi FTP *Server*Di Raspberry Pi



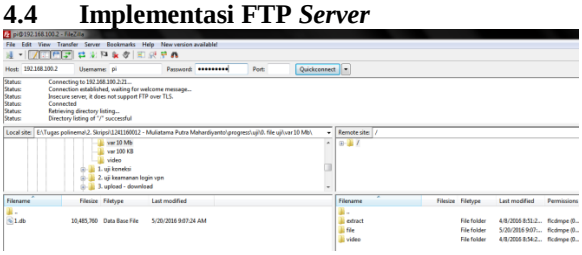
Gambar 5. Konfigurasi IP *Static* Pada Raspberry Pi

4.3 Konfigurasi VPN *Server* PPTP dan L2TP/IPsec



Gambar6.Konfigurasi PPTP *Server*dan L2TP *Server*

4.4 Implementasi FTP *Server*

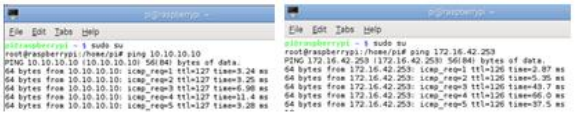


Gambar7.TampilanFTP *Server*

V. Pengujian dan Analisa

5.1 Pengujian Koneksi

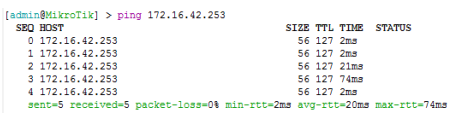
Pengujian koneksi dilakukan untuk memastikan koneksi yang terhubung dengan jaringan VPN yang telah dibuat dapat berjalan lancar serta *server-client* dapat saling terkoneksi dengan melakukan test ping dari *server* ke *client* dan dari router ke *client*. Hasil test ping antara *server* dan *client* diperlihatkan pada Gambar 8 dan hasil test ping antara *server* dan *client* diperlihatkan pada Gambar 9.



Gambar 8. Test Ping antara*server* dan *client*

Tabel 1. Uji Koneksi *Server* dan*Client* VPN

Client VPN		*Client* gedung	
VPN PPTP	Berhasil	Gedung AH	Berhasil
VPN L2TP/IPsec	Berhasil	Gedung AI	Berhasil
		Gedung AL	Berhasil



Gambar 9. Test Ping AntaraRouterdan*Client*

Tabel 2. Uji Koneksi Antara RouterDengan *client*

Client gedung	
Gedung AH	Berhasil
Gedung AI	Berhasil
Gedung AL	Berhasil

Tabel1danTabel 2menunjukkanbahwasaat*client*terhubungdenganjaringan VPN, *client* dapatterkoneksidengan*server* dan router.

5.2 Pengujian Keamanan Jaringan

Pengujian keamanan jaringan tersebut dilakukan untuk mengetahui keamanan yang diberikan antara

VPN PP TP maupun VPN L2TP/IPsec dan sebagai pembanding saat terhubung dengan jaringan intranet.

5.2.1 Pengujian Keamanan Jaringan Teknik*Hacking*

Pengujian keamanan jaringan menggunakan teknik*hacking* yakni melakukan penyadapanpada *client* untuk mendapatkan *username* dan *password*VPN *Server*.Penyadapan dilakukan pada setiap gedung, dengan data *account* yang sama, dan dengan variasi data *account*.Hasil penyadapan di jaringan VPNdiperlihatkan pada Gambar 10.

VPN	Hasil	
PPTP	*Username*	vpn1
	Password	0000000000000000000000000000000000000000000000000:583C85OA653BA842AE4D165716A4C27BB0EA99658B718B0C:875BAFCB2D22EEA
L2TP /IPsec	*Username*	tidak terbaca
	Password	tidak terbaca

Gambar 10. HasilPenyadapan di Jaringan VPN

Tabel 3. Penyadapan Pada Setiap Gedung

Gedung	Jaringan	Data Account	
		Username	*Password*
Gedung AH	VPN PPTP	Terbaca	Terenkripsi MS-CHAP
	VPN L2TP/IPsec	Tidak Terbaca	
Gedung AI	VPN PPTP	Terbaca	Terenkripsi MS-CHAP
	VPN L2TP/IPsec	Tidak Terbaca	
Gedung AL	VPN PPTP	Terbaca	Terenkripsi MS-CHAP
	VPN L2TP/IPsec	Tidak Terbaca	

Tabel 4. Penyadapan Dengan *Username* dan *Password*Yang Sama

Sample	Jaringan	Data Account	
		Username	*Password*
1	VPN PPTP	Terbaca	Terenkripsi MS-CHAP
	VPN L2TP/IPsec	Tidak Terbaca	
2	VPN PPTP	Terbaca	Terenkripsi MS-CHAP
	VPN L2TP/IPsec	Tidak Terbaca	
3	VPN PPTP	Terbaca	Terenkripsi MS-CHAP
	VPN L2TP/IPsec	Tidak Terbaca	
4	VPN PPTP	Terbaca	Terenkripsi MS-CHAP
	VPN L2TP/IPsec	Tidak Terbaca	
5	VPN PPTP	Terbaca	Terenkripsi MS-CHAP
	VPN L2TP/IPsec	Tidak Terbaca	

Tabel 5. Penyadapan Dengan *Username*dan *Password* Yang Berbeda

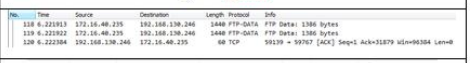
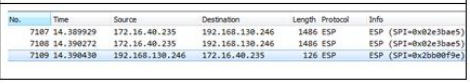
User Name	*Pass word*	Jaringan	Data Account	
			Username	*Password*
q	q	VPN PPTP	Terbaca	Terenkripsi MS-CHAP
		VPN L2TP/IPsec	Tidak Terbaca	
AS	AS	VPN PPTP	Terbaca	Terenkripsi MS-CHAP
		VPN L2TP/IPsec	Tidak Terbaca	
12345	12345	VPN PPTP	Terbaca	Terenkripsi MS-CHAP
		VPN L2TP/IPsec	Tidak Terbaca	
!@#$%^ &*()	!@#$%^ &*()	VPN PPTP	Terbaca	Terenkripsi MS-CHAP
		VPN L2TP/IPsec	Tidak Terbaca	
qwertyA SDFG12345^&*()	qwertyA SDFG12345^&*()	VPN PPTP	Terbaca	Terenkripsi MS-CHAP
		VPN L2TP/IPsec	Tidak Terbaca	

Data dariTabel3, Tabel4danTabel5menunjukkanbahwajaringan VPN PPTP, mengamankan data*password* denganenkripsiformatMS-CHAP.SedangkanVPNL2TP/IPSec,mengamankandata padatingkat*layer* IP.

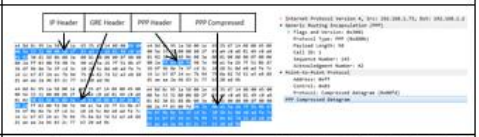
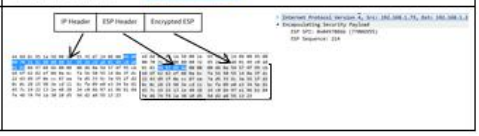
5.2.2 Pengujian Keamanan Jaringan Teknik*Sniffing*

Pengujian keamanan jaringan menggunakan teknik*sniffing* yakni melakukan pembacaan terhadap paket data yang dikirimkan.Pengujian dilakukan saat pembacaan *login* FTP *Server* dan saat pembacaan *transfer file*.

Tabel 6.*Capture* Paket Data Saat *Client Login* FTP *Server*

Jaringan	*Capture* paket data
Intranet	
VPN PPTP	
VPN L2TP/IPsec	

Tabel 7. Capture Paket Data Saat *Transfer File*Dari *Client* Ke *Server*

Jaringan	*Capture* paket data pada *transport layer*
Intranet	
VPN PPTP	
VPN L2TP/ IPsec	

Tabel 6 dan Tabel 7 memperlihatkan bahwa jaringan VPN PPTP, enkripsi data menggunakan PPP Compp dan enkapsulasi menggunakan GRE. Sedangkan jaringan VPN L2TP/IPsec,enkripsi data dan enkapsulasi menggunakan ESP.

5.3 Pengujian Performansi Jaringan

5.3.1 *Delay*

Tabel 8. Rata–Rata *Delay* Jaringan di Gedung AH

No	Jam	*delay download* (ms)			*delay upload* (ms)		
		Intra net	VPN PPTP	VPN L2TP/ Ipsec	Intra net	VPN PPTP	VPN L2TP/ IPsec
1	09.00-09.35	1.58	11.33	18.19	5.06	21.35	33.15
2	13.10-13.45	2.14	15.55	23.83	6.27	24.35	42.77
3	14.45-15.20	1.58	8.90	20.96	4.34	18.30	28.85
Rata-rata		**1.77**	**11.93**	**20.99**	**5.22**	**21.33**	**34.93**

Tabel 9. Rata–Rata *Delay* Jaringan di Gedung AI

No	Waktu	*delay download* (ms)			*delay upload* (ms)		
		Intra net	VPN PPTP	VPN L2TP/ IPsec	Intra net	VPN PPTP	VPN L2TP/ IPsec
1	09.00-09.35	1.41	9.95	16.18	4.73	14.80	28.19
2	13.10-13.45	1.63	11.91	18.27	5.14	17.79	31.41
3	14.45-15.20	1.38	7.39	15.40	4.18	12.99	26.19
Rata-rata		**1.47**	**9.75**	**16.62**	**4.68**	**15.19**	**28.60**

Tabel 10. Rata–Rata *Delay* Jaringan di Gedung AL

No	Waktu	*delay download* (ms)			*delay upload* (ms)		
		Intra net	VPN PPTP	VPN L2TP/ IPsec	Intra net	VPN PPTP	VPN L2TP/ IPsec
1	09.00-09.35	1.48	10.31	17.16	4.88	18.31	30.84
2	13.10-13.45	1.71	12.40	20.26	5.61	21.09	37.12
3	14.45-15.20	1.49	8.10	18.29	4.26	15.49	26.95
Rata-rata		**1.56**	**10.27**	**18.57**	**4.84**	**18.37**	**31.77**

Tabel8, Tabel9, danTabel10memperlihatkanbahwasaatpengujian di gedung AH, gedung AI, dangedung ALmemperlihatkanperbedaan data *delay* di setiapjaringan. Dimana*delay* semakinbesarsaatmenggunakanjaringan VPN. Untukwaktupengujianmenentukannilai*delay* karenakepadatanjaringan intranet. Membuktikan *packet loss* tergolong dalam kategori *Excellent*.

5.3.2 Throughput

Tabel 11. Rata-Rata *Throughput* Jaringan di Gedung AH

No	Waktu	*throughput download* (Mbit/s)			*throughput upload* (Mbit/s)		
		Intra net	VPN PPTP	VPN L2TP/ IPsec	Intra net	VPN PPTP	VPN L2TP/ IPsec
1	09.00-09.35	32.79	24.17	9.46	24.36	17.05	6.38
2	13.10-13.45	24.11	19.50	8.25	20.56	14.92	5.03
3	14.45-15.20	36.81	27.42	11.41	26.29	18.61	6.87
Rata-rata		**31.24**	**23.69**	**9.71**	**23.74**	**16.86**	**6.10**

Tabel 12. Rata-Rata *Throughput* Jaringan di Gedung AI

No	Waktu	*throughput download* (Mbit/s)			*throughput upload* (Mbit/s)		
		Intra net	VPN PPTP	VPN L2TP/ IPsec	Intra net	VPN PPTP	VPN L2TP/ IPsec
1	09.00-09.35	35.83	26.25	10.50	25.37	19.25	7.54
2	13.10-13.45	28.67	24.59	9.73	23.36	16.83	6.58
3	14.45-15.20	39.58	30.53	12.87	29.32	21.17	8.77
Rata-rata		**34.69**	**27.12**	**11.03**	**26.02**	**19.08**	**7.63**

Tabel 13. Rata-Rata *Throughput* Jaringan di Gedung AL

No	Waktu	*throughput download* (Mbit/s)			*throughput upload* (Mbit/s)		
		Intra net	VPN PPTP	VPN L2TP/ IPsec	Intra net	VPN PPTP	VPN L2TP/ Ipsec
1	09.00-09.35	34.33	25.21	9.92	24.97	18.17	7.04
2	13.10-13.45	25.90	22.78	9.16	21.83	15.77	5.81
3	14.45-15.20	37.98	29.10	12.08	28.72	19.83	8.07
Rata-rata		**32.74**	**25.70**	**10.38**	**25.17**	**17.92**	**6.98**

Tabel11, Tabel12, danTabel 13memperlihatkanbahwasaatpengujian di gedung AH, gedung AI, dangedung ALmemperlihatkanperbedaan data *throughput*di setiapjaringan. Dimana*throughput*semakinkecilsaatmenggunakanjaringan VPN. Untukwaktupengujianmenentukannilai*throughput*karenafaktorkepadatanjaringan intranet.

5.3.3 Packet Loss

Tabel 14. Hasil *Packet Loss* Jaringan di Gedung AH

No	Waktu	*packet loss download* (%)			*packet loss upload* (%)		
		Intra net	VPN PPTP	VPN L2TP/ IPsec	Intra Net	VPN PPTP	VPN L2TP/ Ipsec
1	09.00-09.35	0.0	0.0	0.0	0.0	0.0	0.0
2	13.10-13.45	0.0	0.0	0.0	0.0	0.0	0.0
3	14.45-15.20	0.0	0.0	0.0	0.0	0.0	0.0

Tabel 15.Hasil *Packet Loss* Jaringan di Gedung AI

No	Waktu	*packet loss download* (%)			*packet loss upload* (%)		
		Intra net	VPN PPTP	VPN L2TP/ IPsec	Intra Net	VPN PPTP	VPN L2TP/ Ipsec
1	09.00-09.35	0.0	0.0	0.0	0.0	0.0	0.0
2	13.10-13.45	0.0	0.0	0.0	0.0	0.0	0.0
3	14.45-15.20	0.0	0.0	0.0	0.0	0.0	0.0

Tabel 16. Hasil *Packet Loss* Jaringan di Gedung AL

No	Waktu	*packet loss download* (%)			*packet loss upload* (%)		
		Intra net	VPN PPTP	VPN L2TP/ IPsec	Intra Net	VPN PPTP	VPN L2TP/ Ipsec
1	09.00-09.35	0.0	0.0	0.0	0.0	0.0	0.0
2	13.10-13.45	0.0	0.0	0.0	0.0	0.0	0.0
3	14.45-15.20	0.0	0.0	0.0	0.0	0.0	0.0

Tabel 14, Tabel 15 dan Tabel 16memperlihatkan bahwa *packet loss* pada gedung AH, Gedung AI dan Gedung AL berdasarkan waktu pengujian memiliki nilai 0 %. Membuktikan *packet loss* tergolong dalam kategori Sangat Bagus.
Berdasarkanwaktupengujianmengalamiperbedaanperformansi, halinidikarenakankepadatandaripenggunajaringan intranet.

No	Waktu	Jumlah *user*	Total *Bandwidth*	*Bandwidth* tiap *user*
1	09.00-09.35	460	73.3 Mbps	159.3 Kbps
2	13.10-13.45	515		142.3 Kbps
3	14.45-15.20	451		162.5 Kbps

Tabel 17. Hasil Pengguna Jaringan Intranet

5.4 Perbandingan Keamanan dan Performansi tiap jaringan

Tabel 18. Perbandingan tingkat keamanan pada masing–masing jaringan

Tujuan	Parameter	Tools	Hasil yang diharapkan	Jaringan					
				Intra Net		VPN PPTP		VPN L2TP/ IPsec	
				Y	T	Y	T	Y	T
capture username VPN login	data login VPN *client*	Etter cap	*username* tidak terbaca / terenkripsi				V	V	
capture password VPN login	data login VPN *client*	Etter cap	*password* tidak terbaca / terenkripsi			V		V	
capture username dan *password* FTP *server*	data login FTP *server*	Wire shark	*username* dan *password* tidak terbaca / terenkripsi		V	V		V	
capture FTP data	FTP data	Wire shark	data tidak terbaca / terenkripsi		V	V		V	
capture compress datagram	*compress datagram*	Wire Shark	*compress datagram* tidak terbaca				V	V	

Keterangan : (tidak diujikan)

Tabel 18 menunjukkan bahwa hasil *capture username* dan *password* pada VPN PPTP dan VPN L2TP/IPsec memiliki perbedaan. Dimana saat proses *login* atau autenikasi, VPN PPTP mengamankan data berbasis *password* menggunakan MS-CHAP.

Sedangkan di VPN L2TP/IPsec pengamanan data hingga tingkat *layer* IP. Berdasarkan hasil *capture* data *login* FTP dan *capture* FTP data untuk kedua VPN sama-sama tidak dapat terbaca atau mengalami enkripsi, sedangkan pada jaringan intranet *capture* data *login* FTP dan *capture* FTP data dapat terbaca. Hal ini dikarenakan data yang dikirimkan pada jaringan VPN dilewatkan melalui *tunneling*, sehingga data terenkripsi dan terenkapsulasi. Untuk hasil *capturecompress datagram* pada VPN PPTP dapat terlihat atau terbaca, sedangkan di VPN L2TP/IPsec tidak terlihat atau terbaca. Hal ini dikarenakan di VPN PPTP proses enkripsi dan enkapsulasi dibedakan yakni protokol PPP untuk proses enkripsi dan GRE untuk proses enkapsulasi, sedangkan di VPN L2TP/IPsec proses enkripsi dan enkapsulasi dilakukan oleh protokol ESP yang membuat data *compress datagram* tidak terlihat. Jaringan intranet digunakan sebagai pembanding keamanan jaringan karena semua data dapat terbaca.

Tabel 19.Perbandingan tingkat performansi pada masing – masing jaringan

No	Tempat	Intra net	VPN PPTP	VPN L2TP/ IPsec	Intra net	VPN PPTP	VPN L2TP/ IPsec
		***delay download* (ms)**			***delay upload* (ms)**		
1	Gedung AH	1.77	11.93	20.99	5.22	21.33	34.93
2	Gedung AI	1.47	9.75	16.62	4.68	15.19	28.60
3	Gedung AL	1.56	10.27	18.57	4.84	18.37	31.77
		***throughput download* (Mbit/s)**			***throughput upload* (Mbit/s)**		
1	Gedung AH	31.24	23.69	9.71	23.74	16.86	6.10
2	Gedung AI	34.69	27.12	11.03	26.02	19.08	7.63
3	Gedung AL	32.74	25.70	10.38	25.17	17.92	6.98
		***packet loss download* (%)**			***packet loss upload* (%)**		
1	Gedung AH	0.0	0.0	0.0	0.0	0.0	0.0
2	Gedung AI	0.0	0.0	0.0	0.0	0.0	0.0
3	Gedung AL	0.0	0.0	0.0	0.0	0.0	0.0

Tabel 19 menunjukkan bahwa performansi pada jaringan intranet, VPN PPTP dan VPN L2TP/IPsec berbeda. Parameter *delay* secara kesuluruhan berada pada kategori *Excellent* (<150 ms). Bila dibandingkan *delay* antar jaringan, jaringan intranet memiliki rata-rata *delay* terendah, dimana untuk *delay* pada VPN PPTP mengalami kenaikan berkisar 4.5 kali lipat dari *delay* intranet. Untuk *delay* VPN L2TP/IPsec mengalami kenaikan berkisar 2.8 kali lipat dari *delay* intranet.Parameter *throughput* secara keseluruhan pada jaringan intranet memiliki nilai rata-rata *throughput* tertinggi. Untuk *throughput* pada VPN PPTP mengalami penurunan berkisar 1.5 kali lipat dari *delay* intranet. Untuk *delay* VPN L2TP/IPsec mengalami penurunan berkisar 2.4 kali lipat dari *delay* intranet.Parameter *packet loss* bernilai 0 % pada semua jaringan baik saat *download* maupun *upload*. Hal ini dikarenakan jaringan diimplementasikan untuk *transfer file* yang menggunakan protokol TCP dimana saat ada data gagal terkirim secara otomatis akan mengirim ulang.

VI. Kesimpulan dan Saran

6.1 Kesimpulan

Berdasarkanpengujian yang telahdilakukanmakapenulisdapatmenarikkesimpulan, diantaranyasebagaiberikut

1. Jaringan VPN PPTP mengamankan proses autentikasi data password dengan mengenkripsi format MS-CHAP dan jaringan VPN L2TP/IPsec mengamankan proses autentikasi pada layer IP.
2. Pada Jaringan VPN PPTP mengamankan proses transfer data dengan protokol PPP Compp dan GRE dan jaringan VPN L2TP/IPsec mengamankan proses transfer data dengan protokol ESP.
3. Parameter delay pada jaringan intranet, delay download sebesar 0.66 ms dan delay upload sebesar 5.9 ms. Pada VPN PPTP, rata-rata delay download sebesar 36.38 ms dan delay upload sebesar 67.03 ms. Pada VPN L2TP/IPsec, delay download sebesar 43.71 ms dan delay upload sebesar 80.87 ms. Tergolong dalam kategori Excellent (<150 ms) menurut standart ITU-T. Untuk parameter throughput pada jaringan intranet, throughput download sebesar 23.8 Mbit/s dan throughput upload sebesar 23.89 Mbit/s. Pada VPN PPTP, throughput download sebesar 21.09 Mbit/s dan throughput upload sebesar 20.9 Mbit/s. Pada VPN L2TP/IPsec, throughput download sebesar 8.77 Mbit/s dan throughput upload sebesar 9.6 Mbit/s. Untuk parameter packet loss baik jaringan intranet, VPN PPTP, dan VPN L2TP/IPsec bernilai 0 %, tergolong dalam kategori Sangat Bagus menurut standart ITU-T.Untukkepadatanjaringanpada jam 09.00-09.35 jumlah user mencapai 460 dengan bandwidth tiap user 159.3 Kbps. Pada jam 13.10-13.45 mengalamikenaikanjumlah user 11.95% danpenurunan bandwidth tiap user 10.67%. Pada jam 14.45-15.20 mengalamipenurunanjumlah user 1.95% dankenaikan bandwidth tiap user 2%.

6.2 Saran

Berdasarkanpengujian yang telahdilakukanpenulis, selainmelakukankesimpulanjugaadabeberapa saran untukpengembangansisteminiantaralain :

1. Penerapan jaringan VPN bisa dibandingkan dengan VPN yang lain seperti VPN SSTP, Open VPN.
2. Bisa juga dibandingkan performansinya bila diterapkan dengan *multiuser*.
3. Untuk jaringan *tunnel* bisa diterapkan dengan cara LAN to LAN (router *server* dengan router *client*).

Daftar Pustaka

Aldo Alifanto Maulana (2015), "RANCANG BANGUN FILE SHARING SERVER MENGGUNAKAN RASPBERRY PI PADA JARINGAN VPN", Politeknik Negeri Malang, Malang.

Hamsir Azwar (2014), "IMPLEMENTASI FTP SERVER DAN MONITORING CLIENT MENGGUNAKAN MIKROTIK PADA UBUNTU 10.4", Institut Teknologi Telkom, Bandung.

Ryan, Nathan Gusti. 2012. Membangun VPN Server & Client Dengan Mikrotik.

Sofana, Iwan. 2008. Membangun Jaringan Komputer, Bandung, Informatika.

Yulianto Fazmah Arif (2009), "Analisis dan Implementasi Penggunaan IPsec (IPSecurity) dalam Proses Pengamanan Layer Dua Tunneling Protokol (L2TP)", Institut Teknologi Telkom, Bandung.

https://technet.microsoft.com/en-us/library/cc771298. Diakses pada tanggal 6 Desember 2015, pukul 22.00.

www.mikrotik.co.id/artikel_lihat.php?id=61. Diakses pada tanggal 6 Desember 2015, pukul 19.00.