semanTIK, Vol.4, No.2, Jul-Des 2018, pp. 29-36
ISSN: 2502-8928 (Online)
DOI : 10.5281/zenodo.1444898

ANALISIS PERBANDINGAN PERFORMA QoS, PPTP, L2TP, SSTP DAN IPSEC PADA JARINGAN VPN MENGGUNAKAN MIKROTIK

Wa Ode Zamalia*[1], L.M. Fid Aksara[2], Muh. Yamin[3]
[*1,2,3]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Halu Oleo, Kendari
e-mail : [*1]**zamalialia02@gmail.com**, [2]fid.aksara@uho.ac.id, [3]muh_yamin@uho.ac.id

Abstrak

Tunnel Point to Point Tunneling Protocol (PPTP), *Layer 2 Tunneling Protocol* (L2TP), *Secure Socket Tunneling Protocol* (SSTP), dan *Internet Protocol Security* (IPsec) merupakan jenis VPN yang telah banyak didukung oleh protokol jaringan untuk dapat diterapkan pada banyak perangkat jaringan komputer. Keempat metode tersebut diterapkan secara bergantian pada mikrotik. Setiap metode yang diterapkan, selanjutnya akan dianalisis dengan menggunakan aplikasi *Wireshark* dengan parameter *Quality of Service* (QoS) yang terdiri dari *Packet Loss, Delay,* dan *Throughput*. Pengujian dilakukan terhadap 4 *client* yang terhubung ke *access point* dengan dua skenario jaringan, skenario pertama semua *client* mengakses web berbasis *download* dan skenario kedua semua *client* pada jaringan mengakses web *streaming* video. Hasil pengujian keamanan antara *tunnel* PPTP, L2TP, SSTP, dan IPSec menunjukan bahwa tingkat keamanan yang dibagun oleh *tunnel* IPsec lebih baik dari *tunnel* PPTP, L2TP, dan SSTP. Sedangkan untuk hasil pengujian terhadap performa, keamanan serta temuan-temuan pengujian diperoleh bahwa *tunnel* VPN IPsec lebih baik dibandingkan *tunnel* VPN, PPTP, L2TP, dan SSTP.

Kata Kunci—*Layer 2 Tunneling Protocol, Point to Point Tunneling Protocol, Quality of Service* (QoS)*, Secure Socket Tunneling Protocol*, *Virtual Private Network*

Abstract

Tunnel Point to Point Tunneling Protocol (PPTP), *Layer 2 Tunneling Protocol (L2TP)*, *Secure Socket Tunneling Protocol (SSTP)*, *and Internet Protocol Security (IPsec) are VPN types that have been widely supported by network protocols to be applicable to many computer network devices. These four methods are applied alternately on mikrotik. In each applied method, will be analyzed using Wireshark application, with Quality of Service (QoS) parameters consisting of Packet Loss, Delay, and Throughput. Tests performed on four clients which connected to the access point. Testing is done with two kinds of networks, the first one in which all client access web for download purpose and the second one in which all client access web for streaming video. The security testing result between PPTP tunnels, L2TP, SSTP, and IPSec shows that security level built by IPsec tunnels better than the L2TP, SSTP, and PPTP tunnels. Moreover, based on the results of testing on performance, security and test findings obtained that IPsec VPN tunnel better than tunnel VPN PPTP L2TP and SSTP.*

Keywords— *Layer 2 Tunneling Protocol, Point to Point Tunneling Protocol, Quality of Service (QoS), Secure Socket Tunneling Protocol, Virtual Private Network*

1. PENDAHULUAN

Secara umum jaringan terbagi dalam dua area, yaitu jaringan *public* dan jaringan *local*. Jaringan *public* merupakan jaringan yang menghubungkan *interface* jaringan secara global, sedangkan untuk jaringan *local* merupakan jaringan yang menghubungkan *client-client* dalam satu jaringan lokal,seperti instansi atau perkantoran. Jaringan *local* dan *public* merupakan jaringan yang saling terhubung, namun ada beberapa batasan-batasan yang mengatur koneksi antara dua jaringan tersebut.

VPN (*Virtual Private Network*) adalah sebuah teknologi komunikasi yang memungkinkan untuk terkoneksi ke jaringan publik dan menggunakanya untuk bergabung ke jaringan lokal, dengan cara tersebut maka akan diperoleh hak dan pengaturan yang sama seperti halnya berada di dalam kantor atau jaringan itu sendiri, walaupun sebenarnya menggunakanjaringan publik. Jaringan VPN merupakan jaringan yang dibangun di atas sebuah *tunnel*.

Tunnel VPN memiliki fungsi sebagai jalur yang bertanggung jawab atas keamanan dari data yang berjalan di dalamnya. Pengujian dilakukan dengan cara membandingkan performa dan keamanan masing-masing *tunnel*. Pengujian performa dilakukan menggunakan beberapa parameter QoS (*Quality of Service*) untuk memperoleh kualitas dari keempat *tunnel* dan pengujian keamanan dilakukan dengan cara meretas sistem keamanan *tunnel*. Proses enkripsi dan dekripsi pada VPN membuat *delay* di dalam jaringan bertambah karena proses ini juga membutuhkan waktu. Keamanan data pada VPN pada akhirnya akan berpengaruh pada performansi QoS (*Quality of service*) [1].

Pada penelitian ini akan dianalisis perbandingan penggunaan protokol PPTP (*Point to Point Tunneling Protocol*), L2TP (*Layer 2 Tunneling Protocol*), SSTP (*Secure Soket Tunneling Protocol*) dan protokol IPSec (*Internet Protocol Security*) dengan pemodelan jaringan VPN terhadap parameter QoS, sehingga dapat diketahui pengaruh penggunaan protokol VPN terhadap QoS. Perbandingan yang akan digunakan sebagai ukuran parameter *Quality of Service* (QoS) yaitu *Delay, Packet Loss* dan *Throughput*. Dengan latar belakang tersebut Penulis bermaksud untuk melakukan penelitian tentang "Perbandingan Performa QoS (*Quality of Service*) PPTP (*Point To Point Tunneling protocol*), L2TP (*Layer 2 Tunneling protocol*), SSTP (*Secure Socket Tunneling protocol*) dan IPSec (*Internet Protokol Security*) pada Jaringan VPN Menggunakan Mikrotik".

2. METODE PENELITIAN

2.1 Jaringan Komputer

Konsep jaringan komputer lahir pada tahun 1940-an di Amerika dari sebuah proyek pengembangan komputer MODEL I di Laboratorium Bell dan group riset Harvard University yang dipimpin profesor H. Aiken. Pada mulanya proyek tersebut hanyalah ingin memanfaatkan sebuah perangkat komputer yang harus dipakai bersama. Untuk mengerjakan beberapa proses tanpa banyak membuang waktu kosong dibuatlah proses beruntun (*Batch Processing*), sehingga beberapa program bisa dijalankan dalam sebuah komputer dengan kaidah antrian.

Di tahun 1950-an ketika jenis komputer mulai membesar sampai terciptanya super komputer, maka sebuah komputer mesti melayani beberapa terminal. Untuk itu ditemukan konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (*Time Sharing System*), maka untuk pertama kali bentuk jaringan (*network*) komputer diaplikasikan. Pada sistem *Time Sharing System* (TSS) beberapa terminal terhubung secara seri kesebuah host komputer. Dalam proses *Time Sharing System* (TSS) mulai nampak perpaduan teknologi komputer dan teknologi telekomunikasi yang pada awalnya berkembang sendiri-sendiri [2].

2.2 Point to Point Tunneling Protocol (PPTP)

PPTP merupakan *protocol* jaringan yang memungkinkan pengamanan *transfer* data dari *remote client* ke *server* pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP. Teknologi jaringan PPTP merupakan pengembangan dari *remote access Point-to-Point Protocol* yang dikeluarkan oleh *Internet Engineering Task Force* (IETF). PPTP merupakan *protocol* jaringan yang merubah paket PPP menjadi IP datagram agar dapat ditransmisikan melalui internet. PPTP juga

dapat digunakan pada jaringan *private* LAN-to-LAN.

Salah satu protokol yang digunakan untuk membangun VPN adalah *Point to Point Tunneling protocol* (PPTP). VPN akan menawarkan tingkat *encryption* yang lebih baik selain menawarkan fitur *authentication*.

Cara kerja *Point to Point Tunneling protocol* (PPTP) yaitu dimulai dari sebuah *remote* atau PPTP *client mobile* yang membutuhkan akses ke sebuah LAN *private*. Pengaksesan menggunakan ISP *local*. *Client* menggunakan *Dial-Up Networking* dan protokol *remote access* PPP untuk terhubung ke sebuah ISP. Begitu terhubung, *client* bisa mengirim dan menerima paket data melalui internet. Setelah *client* membuat koneksi PPP ke ISP, panggilan *Dial-Up Networking* yang kedua dibuat melalui koneksi PPP yang sudah ada. Data dikirimkan menggunakan koneksi yang kedua dalam bentuk IP datagram yang berisi paket PPP yang telah terenkapsulasi. Panggilan yang kedua tersebut selanjutnya menciptakan koneksi VPN ke *server* PPTP pada LAN *private* perusahaan [3].

2.3 Layer 2 Tunneling Protokol (L2TP)

L2TP merupakan *tunneling protocol* yang memadukan dua buah *tunneling* protokol yaitu *Layer* 2 *Forwarding* milik Cisco dan PPTP yang dimiliki Microsoft. L2TP umumnya digunakan untuk membuat *Virtual Private Dial Network* (VPDN) yang dapat membawa semua jenis protokol komunikasi di dalamnya dan biasanya menggunakan *port* 1702 dengan protokol UDP.

Terdapat dua model *tunnel* yang dikenal, yaitu *compulsory* dan *voluntary*. Perbedaan utama keduanya terletak pada *endpoint tunnel*-nya. Pada *compulsory tunnel*, ujung *tunnel* berada pada ISP, sedangkan pada *voluntary* ujung *tunnel* berada pada *client remote* [4].

2.4 Secure Socket Tunneling Protokol (SSTP)

Secure Socket Tunneling Protokol adalah tembusan protokol yang tersedia pada *platform* Microsoft. Protokol ini berbasis pada kombinasi kedua teknologi, SSL dan TCP. Teknologi SSL menjaminkan tingkat keamanan transportasi dan integritas lalu lintas. SSL pada *server* dikonfigurasikan sedemikian rupa sehingga hanya metode enkripsi terkuatlah yang diaktifkan. Sejak sesi SSTP, dalam kenyataannya, sebuah sesi HTTPS, SSTP mungkin bisa digunakan melalui *firewall* atau ISP *throttling*. Di sisi lain, sejak SSTP beroperasi melalui TCP, dalam beberapa kasus akan dikendalikan IKEv2 atau protokol berbasis UDP lainnya. Secara keseluruhan, SSTP adalah pilihan terbaik dan dapat membantu menyelesaikan masalah konektivitas ataupun masalah kecepatan yang dimiliki.

Diperkenalkan oleh Microsoft Corporation dalam Windows Vista Service Package 1 (SP1), kanalisasi soket aman yang sekarang tersedia untuk SEIL, Linux dan RouterOS, namun masih diutamakan untuk *platform* Windows. Oleh karena protokol ini memakai SSL v3, sehingga memberikan keunggulan yang sama dengan OpenVPN, seperti kemampuan untuk mencegah masalah *firewall* NAT.

SSTP adalah protokol VPN yang stabil dan mudah digunakan, terutama disebabkan integrasinya ke dalam Windows. SSTP (*Secure Socket Tunneling protocol*) adalah bentuk VPN *tunnel* yang menyediakan mekanisme untuk mengirimkan *traffic* PPP atau L2TP melalui sebuah saluran SSL 3.0. SSL menyediakan *transport-level security* dengan *key-negotiation*, enkripsi dan *traffic integrity checking*. Penggunaan SSL melalui *port* TCP 443 mengizinkan SSTP untuk melewati secara virtual semua *firewall* dan *proxy server* kecuali untuk otentikasi web *proxy*.

SSTP *server* harus diotentikasi selama fase SSL. SSTP *client* dapat secara opsional diotentikasi selama fase SSL, dan harus diotentikasi selama fase PPP. Penggunaan PPP mendukung metode otentikasi secara umum seperti EAP-TLS dan MS-CHAP. SSTP dapat diterapkan di linux, BSD, dan Windows. Mikrotik *router* OS juga mengizinkan SSTP *client* dan *server*.

Salah satu fitur VPN yang ada di MikroTik adalah SSTP (*Secure Socket Tunneling protocol*). SSTP merupakan sebuah *PPP Tunnel* dengan *TLS 1.0 Channel*. Fitur ini berjalan pada protokol TCP dan *Port* 443. Supaya dapat memanfaatkan SSTP secara optimal dengan keamanan yang baik, maka diharuskan menambahkan sertifikat SSL untuk koneksi antara *server* dan *client*. Sertifikat

SSL itu bias didapatkan dengan membeli melalui vendor-vendor yang ada atau bisa dibuat sendiri menggunakan OpenSSL.

2.5 Internet Protokol Security (IPSec)

IPSec merupakan *tunneling protocol* yang bekerja pada layer 3. IPSec menyediakan layanan sekuritas pada IP layer dengan mengizinkan system untuk memilih *protocol* keamanan yang diperlukan, algoritma apa yang akan digunakan pada layanan, dan menempatkan kunci kriptografi yang diperlukan untuk menyediakan layanan yang diminta. IPSec bekerja dengan tiga cara yaitu: *Network-to-network, Host-to-network dan Host-to-host.*

IPSec adalah pengembangan dari protokol IP yang bertujuan untuk menyediakan keamanan pada suatu IP dan *layer* yang berada di atasnya. Pada dasarnya paket IP tidak memiliki keamanan, sehingga tidak ada jaminan bahwa paket yang diterima sama dengan paket ketika ditransmisikan oleh si pengirim paket. Paket IP yang tidak memiliki keamanan atau *security*, sangat mudah untuk diketahui isinya dan alamat IP itu sendiri. IPsec adalah metode yang bertujuan untuk menjaga keamanan IP datagram ketika paket diransmisikan pada *traffic*. Sehingga IPsec menjadi suatu mekanisme yang diimplementasikan pada VPN. IPSec berada pada *layer* tiga OSI yaitu *network layer* sehingga dapat mengamankan data dari *layer* yang berada di atasnya.

2.6 Quality of Service (QoS)

Dari segi *networking*, QoS mengacu kepada kemampuan memberikan pelayanan berbeda kepada lalu lintas jaringan dengan kelas-kelas yang berbeda. Tujuan akhir dari QoS adalah memberikan *network service* yang lebih baik dan terencana dengan *dedicated bandwidth*, *jitter* dan *latency* yang terkontrol dan meningkatkan *loss* karakteristik. Berikut adalah penjelasan mengenai parameter-parameter yang digunakan dalam penilaian QoS yang baik:

1. Delay

Delay adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ketujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama [5]. Menurut versi TIPHON, besarnya *delay* dapat diklasifikasikan seperti yang ditunjukkan pada Tabel 1.

Tabel 1 *Latency*

Kategori Latensi	Besar *Delay*	Indeks
Sangat Bagus	< 150 ms	4
Bagus	150 s/d 300 ms	3
Sedang	300 s/d 450 ms	2
Jelek	>450 ms	1

Untuk mengukur *delay* digunakan Persamaan (1).

$$Delay = \frac{Total\ delay}{Total\ paket\ yang\ diterima} \quad (1)$$

2. Packet Loss

Packet Loss merupakan parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang, dapat terjadi karena *collision* dan *congestion* pada jaringan dan hal ini berpengaruh pada semua aplikasi karena retransmisi akan mengurangi efesiensi jaringan secara keseluruhan meskipun jumlah *bandwidth* cukup tersedia untuk aplikasi-aplikasi tersebut. Jika terjadi kongesti yang cukup lama, *buffer* akan penuh, dan data baru tidak akan diterima [6]. Nilai *packet loss* sesuai dengan versi TIPHON ditunjukkan pada Tabel 2.

Tabel 2 *Packet Loss*

Kategori Degredasi	*Packel Loss*	Indeks
Sangat Bagus	0 %	4
Bagus	3 %	3
Sedang	15 %	2
Jelek	25 %	1

Untuk mengukur *packet loss* digunakan Persamaan (2).

$$PL = \frac{PTT - PT}{PTT}\ x\ 100\ \% \quad (2)$$

Ket :

$PL = Packet\ Loss$

$PTT = Paket\ Total\ Tercapture$

$PT = Packet\ Terkirim$

3. Throughput

Throughput yaitu kecepatan (*rate*) transfer data yang efektif yang diukur dalam bps. *Throughtput* merupakan jumlah total kedatangan paket yang sukses yang diamati

pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut [6]. Untuk mengukur *throughput* digunakan Persamaan (3).

$$T = \frac{JDK}{LP} \quad (3)$$

Ket :
$T = Throughput$
$JDK = Jumlah\ Data\ yang\ Dikirim$
$LP = Lama\ Pengamatan$

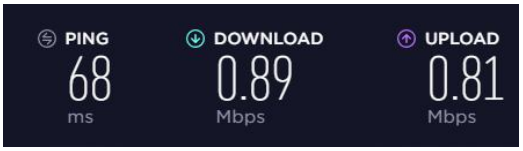
3. HASIL DAN PEMBAHASAN

3.1 Pengujian

Pada penelitian ini dimulai dari menyambungkan kabel LAN di *port* 1 *Router Board Mikrotik 941-2nD-TC,* kemudian melakukan konfigurasi *hostpot* untuk melakukan pengujian.

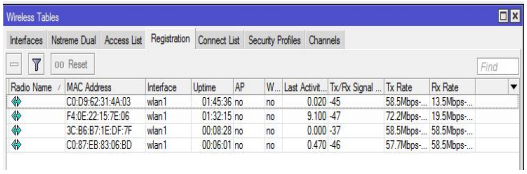
Pengujian ini dilakukan menggunakan *management bandwidth* dengan dua skema yaitu, skema *Download* dan *Streaming* dengan jumlah 4 *client*.

Sebelum melakukan uji QoS dengan aplikasi *Wireshark*, pengujian ini menggunakan bantuan dari situs *Speedtest* untuk mengukur besar nilai unduh dan unggah sesaat sebelum melakukan uji QoS. Data QoS diambil pada setiap PC *client* yang terhubung pada *server* (4 PC) yang sudah di-*instal*-kan aplikasi wireshark. Adapun hasil dari *Speed Test* dapat dilihat pada Gambar 1.



Gambar 1 Hasil *Speedtest* setelah Perangkat Terhubung

Jumlah perangkat yang terhubung pada *access point* ditunjukkan oleh Gambar 2.



Gambar 2 Jumlah Perangkat Terhubung pada *Access Point*

1. Perhitungan Delay

Perhitungan *delay* berdasarkan Persamaan (1) dari pengujian data QoS yang dilakukan pada PC 1 *Download* yaitu :

$$Delay = \frac{37{,}766}{539} = 0{,}0700\ \text{ms}$$

Summary Data QoS pada PC 1 *Download* ditunjukkan oleh Gambar 3.

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	570	539	94,561%	0	0,000%
Between first and last packet	40,316 sec	37,766 sec			
Avg. packets/sec	14,138	14,272			
Avg. packet size	1119 bytes	1178 bytes			
Bytes	637880	635163	99,574%	0	0.000%
Avg. bytes/sec	15822,136	16818,275			
Avg. MBit/sec	0,127	0,135			

Gambar 3 *Summary* Data QoS pada PC 1 *Download*

2. Perhitungan Packet Loss

Berdasarkan Gambar 3, perhitungan *packet loss* berdasarkan Persamaan (2) dari pengujian data QoS yang dilakukan yang diambil dari *download* PC 1 yaitu :

$$Packet\ loss = \frac{(570 - 539)}{570} x\ 100\%$$
$$= 5{,}4385\ \%$$

3. Perhitungan *Throughput*

Berdasarkan Gambar 3, perhitungan *throughput* berdasarkan Persamaan (3) dari pengujian data QoS yang dilakukan yang diambil dari *download* PC1 yaitu :

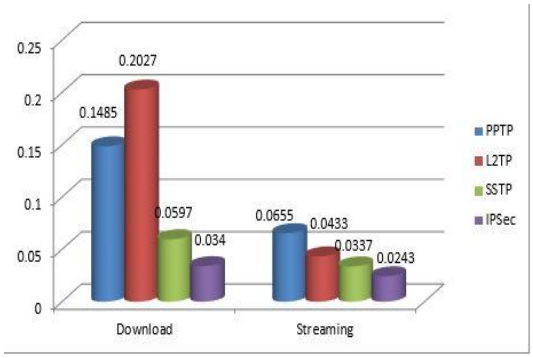
$$Throughput = \frac{635163}{37{,}766} = 16{,}819\ \text{bps}$$

3.2 Hasil Pengujian Metode Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protokol (L2TP), Secure Socket Tunneling Protocol (SSTP) dan Internet Protokol Security (IPSec)

Berdasarkan hasil uji QoS dengan metode PPTP, L2TP, SSTP dan IPSec maka dapat dibuatkan tabel yang membandingkan nilai *delay* antara metode PPTP, L2TP, SSTP dan IPSec dari tiap-tiap kondisi *download* dan *streaming* video yang ditunjukkan oleh Tabel 3 dan Gambar 4.

Tabel 3 Rata-Rata Nilai *Delay* Metode PPTP, L2TP, SSTP dan IPSec

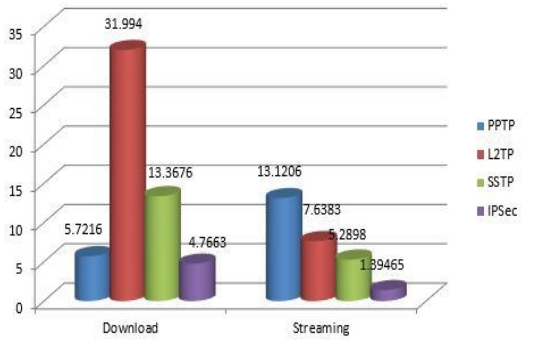
Delay	*Download*	*Streaming*
PPTP	0,1485 ms	0,0655 ms
L2TP	0,2027 ms	0,0433 ms
SSTP	0,0597 ms	0,0337 ms
IPSec	0,0340 ms	0,0385 ms



Gambar 4 Grafik Rata-Rata Nilai *Delay* Metode PPTP, L2TP, SSTP dan IPSec

Berdasarkan Tabel 3 dan Gambar 4 menunjukkan perbandingan QoS dari parameter *delay* pada delapan kondisi pengujian, dimana *delay* pada 4 metode dengan kondisi *download* menunjukkan perbedaan yang cukup signifikan yakni pada metode IPSec lebih baik dibandingkan dari metode SSTP,PPTP dan L2TP.

Grafik dan Tabel Rata-Rata Nilai *Paket Loss* Metode PPTP, L2TP, SSTP dan IPSec secara bertutut-turut ditunjukkan oleh Gambar 5 dan Tabel 4.



Gambar 5 Grafik Rata-Rata Nilai *Paket Loss* Metode PPTP, L2TP, SSTP dan IPSec

Tabel 4 Rata-Rata Nilai *Paket Loss* Metode PPTP, L2TP, SSTP dan IPSec

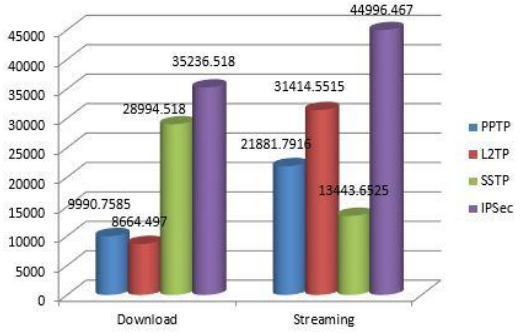
Paket Loss	*Download*	*Streaming*
PPTP	5,7216%	13,1206%
L2TP	31,994%	7,6383%
SSTP	13,3676%	5,2898%
IPSec	4,7663%	22,2428%

Berdasarkan Tabel 4 dan Gambar 5 menunjukkan perbandingan QoS dari parameter *paket loss* pada delapan kondisi pengujian, dimana *paket loss* pada 4 metode dengan kondisi *download* menunjukkan perbedaan yang cukup signifikan yakni pada metode IPSec lebih baik dibandingkan dari metode PPTP, SSTP dan L2TP.

Tabel dan Grafik Rata-Rata Nilai *Throughput* Metode PPTP, L2TP, SSTP dan IPSec secara bertutut-turut ditunjukkan oleh Tabel 5 dan Gambar 6.

Tabel 5 Rata-Rata Nilai *Throughput* Metode PPTP, L2TP, SSTP dan IPSec

Throughput	*Download* (bps)	*Streamin* (bps)
PPTP	9990,7585	21881,7916
L2TP	8664,497	31414,5515
SSTP	28994,518	13443,6525
IPSec	35236,9219	47397,5555



Gambar 6 Grafik Rata-Rata Nilai *Trogpuht* Metode PPTP, L2TP, SSTP dan IPSec

Dari Tabel 5 dan Gambar 6 menunjukkan perbandingan QoS dari parameter *throughput* pada delapan kondisi pengujian, dimana *throughput* pada 4 metode dengan kondisi *download* menunjukkan perbedaan yang cukup signifikan yakni pada metode IPSec lebih baik dibandingkan dari metode SSTP, PPTP dan L2TP.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan selama perancangan sampai analisis perbandingan QoS pada dua skema, skema pertama semua *client* melakukan *download* dan skema kedua semua *client* pada jaringan mengakses *streaming* video dengan menggunakan metode *Point to Point Tunneling protocol* (PPTP), *Layer 2 Tunneling Protokol* (L2TP), *Secure Socket Tunneling protocol* (SSTP) dan *Internet Protokol Security* (IPSec), maka dapat disimpulkan bahwa untuk pengujian *Download, Delay* terbaik dihasilkan pada metode IPSec, *Packet loss* terbaik dihasilkan pada metode IPSec dan *Throughput* terbaik dihasilkan metode IPSec. Sedangkan untuk pengujian *Streaming* video, *Delay* terbaik dihasilkan pada metode IPsec, *Packet loss* terbaik dihasilkan pada metode IPSec dan *Throughput* terbaik dihasilkan metode IPSec.

5. SARAN

Dari hasil penelitian ini, Penulis berharap dapat dijadikan suatu patokan untuk lebih mengembangkan performansi jaringan VPN. Masih banyak yang perlu dianalisa dalam jaringan VPN khusunya metode PPTP, L2TP, SSTP dan IPSec, baik dari sisi keamanan keempat metode tersebut, banyaknya client yang melakukan proses transmisi data, dan lain sebagainya yang mempengaruhi performansi jaringan VPN.

DAFTAR PUSTAKA

[1] I. Afrianto and E. B. Setiawan, "Kajian Virtual Private Network (VPN) Sebagai Sistem Pengamanan Data Pada Jaringan Komputer," *Maj. Ilm. UNIKOM*, Vol. 12, No. 1, 2011.

[2] D. M. Burgess, *Learn RouterOS*. USA: E-Book. Link Technologies, Inc. Oermann Rd. Dittmer, 2009.

[3] A. Budiadji, "Simulasi Untuk Membandingkan Kinerja PPTP dan L2TP untuk Berbagai Kelas Trafik, Depok," Universitas Indonesia, Depok, 2009.

[4] Ramdhani, A. Y, "Peracangan Dan Implementasi VPN Menggunakan Protokol PPTP Dan L2TP Berbasis Mikrotik," Politeknik Telkom Bandung, 2010.

[5] Tommy, "Perbandingan Metode PPTP, L2TP, SSL dan SSTP Pada Mikrotik sebagai Upaya Optimalisasi Layanan Jaringan Pada Fakultas Teknik Universitas Tanjungpura," Universitas Tanjungpura, 2015.

[6] I. Iskandar, "Analisa Quality of Service (QoS) Jaringan Internet Kampus (Studi Kasus: UIN Suska Riau)," UIN Suska Riau, 2015.