Analisis Perbandingan Kinerja Jaringan Secure Socket Tunneling Protocol (Sstp) Dan Layer Two Tunneling Protocol (L2tp) + Internet Protocol Security (Ipsec) Menggunakan Metode Quality Of Service (Qos)

Lukman[1], Aiman Mukhlishah[2]
Informatika Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
Jl. Ring Road Utara Condong Catur, Depok, Sleman, Yogyakarta 55283
[1]masman@amikom.ac.id, [2]aiman.mukhlishah@students.amikom.ac.id

INTISARI

Kinerja jaringan yang buruk tentu akan berdampak buruk pada kerugian bagi sebuah perusahaan atau instansi, ketika kinerja jaringan yang digunakan oleh perushaan berubah menjadi lambat, pasti sangat berpengaruh terhadap kinerja perusahaan itu sendiri, terlebih jika sebuah perusahaan selalu bergantung pada internet untuk kelancaran bisnisnya. Semakin banyaknya perusahaan perusahaan yang membutuhkan kinerja jaringan yang cepat dan aman maka untuk mengatasi hal tersebut, ada beberapa metode yang bisa digunakan seperti banyaknya pilihan metode VPN (Virtual Private Network).

Teknologi VPN adalah suatu komunikasi dalam jaringan sendiri yang terpisah dari jaringan umum. Private network sendiri dianggap lebih efisien karena kecepatan transfer data yang lebih besar dari pada kecepatan transfer data pada jaringan Internet, selain itu masalah keamanan dianggap lebih bagus karena hanya bergerak dalam lingkup terbatas saja. Secara umum, VPN adalah sebuah proses dimana jaringan umum (public network atau internet) diamankan kemudian difungsikan menjadi sebuah jaringan privat (private network). Sebuah VPN tidak didefinisikan oleh rangkaian khusus atau router, tetapi didefinisikan oleh mekanisme keamanan dan prosedur-prosedur yang hanya mengijinkan penggunanya yang ditunjuk akses ke VPN dan informasi yang mengalir melaluiya.

Masalah yang dihadapi saat ini yaitu ketika performa jaringan yang lambat akan berpengaruh pada kinerja perusahaan, untuk berhubungan antar kantor menggunakan internet dan email untuk mengirim data dan berkomunikasi maka dibutuhkan jaringan privat untuk memudahkan mengakses file terhadap suatu tempat yang berbeda lokasi. Namun dalam Pemilihan VPN yang akan digunakan memungkinkan kurang tepatnya pemilihan metode yang digunakan dalam mengelola jaringan intranet untuk perusahaannya.

Dari uraian diatas maka penulis melakukan analisis perbandingan sebuah teknik tunneling dengan menggunakan SSTP dan L2TP+IPSec. SSTP dan L2TP+IPSec merupakan protokol jaringan yang dapat melindungi jaringan dari ancaman luar seperti konflik IP, MAC dan DHCP server jahat, serta membuat performa jaringan lebih baik, dengan metode penggunaan jalur tersendiri yang di lalui atau dilewati. Dari kedua metode tersebut penulis melakukan perbandingan performa jaringan ketika di terapkan metode SSTP dan L2TP+IPSec sehingga mengetahui performa jaringan mana yang lebih bagus dan cocok digunakan sesuai dengan kebutuhan pengguna.

Hasil dari penelitian ini diharapkan dapat membantu siapapun untuk menentukan metode tunneling VPN yang akan digunakan kelak dalam suatu jaringan. Sedangkan dari hasil penelitian bisa diambil kesimpulan bahwa L2TP+IPSec lebih baik dibanding SSTP, dinilai dari parameter QOS yang sudah diuji dan dibandingkan.

Kata kunci: *Tunneling, VPN, SSTP, L2TP, IPSec, Quality Of Service*

ABSTRACT

Poor network performance will certainly have a bad impact on losses for a company or agency, when the network performance used by the company turns out to be slow, it must be very influential on the performance of the company itself, especially if a company always relies on the internet for the smooth running of its business. More and more companies need fast and secure network performance. To overcome this, there are several methods that can be used such as the choice of VPN (Virtual Private Network) methods.

VPN technology is communication within one's own network that is separate from public networks. Private network itself is considered more efficient because the data transfer speed is greater than the data transfer speed on the Internet network, besides that security issues are considered better because it only moves in a limited scope. In general, VPN is a process in which a public network (public network or internet) is secured and then functioned as a private network. A VPN is not defined by a specific circuit or router, but is defined by security mechanisms and procedures that only allow their designated users access to the VPN and the information that flows through it.

The problem currently faced is when slow network performance will affect company performance, to connect between offices using the internet and email to send data and communicate, then a private network is needed to facilitate accessing files to a different location. However, the selection of VPNs that will be used allows less precise selection of methods used in managing intranet networks for the company.

From the description above, the authors conducted a comparative analysis of a tunneling technique using SSTP and L2TP + IPSec. SSTP and L2TP + IPSec are network protocols that can protect networks from external threats such as IP, MAC and DHCP server conflicts, and make network performance better, by using separate paths that are traversed or traversed. From these two methods, the writer makes a comparison of network performance when applied SSTP and L2TP + IPSec methods so that it knows which network performance is better and is suitable for user needs.

The results of this study are expected to help anyone determine the VPN tunneling method that will be used later in a network. While the results of the study can be concluded that L2TP + IPSec is better than SSTP, judged by the QOS parameters that have been tested and compared.
Keywords: *Tunneling, VPN, SSTP, L2TP, IPSec, Quality Of Service*

I. PENDAHULUAN

A. Latar Belakang Masalah

Kinerja jaringan yang buruk tentu akan berdampak buruk bagi sebuah perusahaan atau instansi, ketika kinerja jaringan yang digunakan oleh perusahaan berubah menjadi lambat, pasti sangat berpengaruh terhadap kinerja perusahaan itu sendiri, terlebih jika sebuah perusahaan selalu bergantung pada internet untuk kelancaran bisnisnya. Semakin banyaknya perusahaan-perusahaan yang membutuhkan kinerja jaringan yang cepat dan aman maka untuk mengatasi hal tersebut, salahsatu caranya adalah mengimplementasikan teknologi jaringan VPN (*Virtual Private Network*).

Teknologi VPN adalah suatu komunikasi dalam jaringan sendiri yang terpisah dari jaringan umum. *Private network* sendiri dianggap lebih efisien karena kecepatan transfer data yang lebih besar dari pada kecepatan transfer data pada jaringan Internet, selain itu masalah keamanan dianggap lebih bagus karena hanya bergerak dalam lingkup terbatas saja. Secara umum, VPN adalah sebuah proses dimana jaringan umum (*public network* atau internet) diamankan kemudian difungsikan menjadi sebuah jaringan privat. Sebuah VPN tidak didefinisikan oleh rangkaian khusus atau router, tetapi didefinisikan oleh mekanisme keamanan dan prosedur-prosedur yang hanya mengijinkan penggunanya yang ditunjuk akses ke VPN dan informasi yang mengalir melaluiya.

Metode tunnelling pada VPN yang digunakan pada suatu jaringan akan menentukan seberapa bagus dan lancarnya kualitas suatu jaringan itu sendiri, maka dari itu penulis melakukan analisis perbandingan sebuah teknik tunneling dengan menggunakan SSTP dan L2TP+IPSec. SSTP dan L2TP+IPSec merupakan protokol jaringan yang dapat melindungi jaringan dari ancaman luar seperti konflik IP, MAC dan DHCP server jahat, serta membuat performa jaringan lebih baik, dengan metode penggunaan jalur tersendiri yang di lalui atau dilewati. Dari kedua metode tersebut penulis melakukan perbandingan performa jaringan ketika di terapkan metode SSTP dan L2TP+IPSec sehingga mengetahui performa jaringan mana yang lebih bagus dan cocok digunakan sesuai dengan kebutuhan pengguna.

B. Maksud dan Tujuan Penelitian

Maksud dan tujuan dari analisis perbandingan kinerja jaringan SSTP dan L2TP+IPSec yang ingin dicapai dalam penelitian ini antara lain:

1. Mengetahui prinsip kerja SSTP dan L2TP + IPSec.
2. Menganalisis kemampuan kinerja jaringan SSTP dan L2TP + IPSec.

3. Mengetahui perbandingan nilai serta performa jaringan dengan parameter Quality of Service.

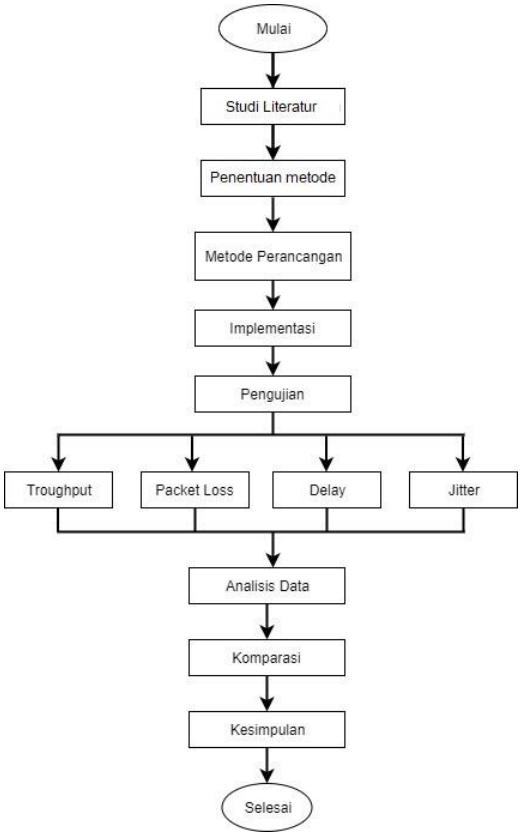
II. METODOLOGI PENELITIAN

Penelitian menggunakan Metode VPN SSTP dan L2TP + IPSec ini akan dilakukan dengan kondisi terkendali dimana bisa mencapai tujuan untuk menemukan data perbandingan dan pengaruh pada jaringan yang ada.Penelitian ini bertujuan untuk menjelaskan perbandingan antara dua metode yang berbeda pada sebuah jaringan VPN dilihat dari kinerja QoS setelah di terapkan.

Penelitian ini dilakukan dengan mengumpulkan, menganalisa dan menampilkan data dalam bertuk angka untuk mendapatkan hasil perbandingan. Penulis melakukan penyusunan rencana, pengumpulan dan menganalisis data yang kemudian dijelaskan dengan bentuk dokumen hasil penelitian. Data yang dikumpulkan berbentuk data kuantitatif didapat dari hasil perhitingan dan perbandingan pada jaringan VPN yang menggunakan metode SSTP dan L2TP+IPSec.

Alur penelitian ini yaitu memungkinkan tahapan dalam perancangan pada panelitian ini. Dalam tahapan ini peneliti mencoba memahami topologi serta kinerja jaringan yang akan diterapkan, sehingga bisa menganalisa perbandingan kinerja SSTP dan L2TP+IPSecurity berdasarkan parameter yang digunakan yaitu Troughput, delay, packet loss dan jitter. Setelah diuji, selanjutnya yaitu membandingkan hasil pengujian dari dua metode tunneling untuk performa jaringan tersebut dengan menganalisis serta menyimpulkan hasil pengujian yang telah didapat. Adapun alur penelitian ditunjukan pada gambar 1.

Pada penelitian ini hardware yang digunakan pada penerapan kedua metode tunneling SSTP dan L2TP+IPSec yang nantinya akan dibandingkan kedua performa dari kedua konsep tersebut menggunakan beberapa perangkat di tunjuk pada table I.



Gambar 1. Tahapan penelitian

TABEL I.
KEBUTUHAN HARDWARE

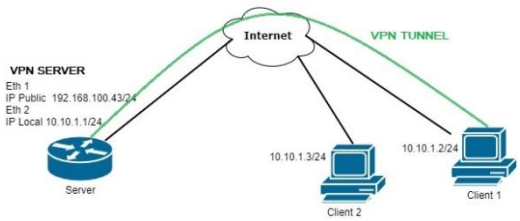
Hardware	**Spesifikasi**
Laptop Acer	Processor : Intel(R) Celeron(R) CPU N2840 @2.16GHz
	RAM : 2 GB
	HDD : 500 GB
	OS : WIN 10 Pro
Mikrotik RB931-2^{nD}	Processor : QCA9533 650MHz
	RAM : 32MB
	Storage : 16MB
	Wireless Frekuensi : 2.4GHz (802.11b/g/n)
	Ethernet : 3 Ports
	OS : RouterOS
	Router OS License : Level4
Router AP D-Link DIR-612	Wireless Frekuensi: 2.4 ~ 2.4835GHz
	Ethernet : 4 ports
	Kecepatan WIFI : 300 Mbps
	Router OS License

Adapun software yang digunakan pada penerapan metode tunneling SSTP dan L2TP+IPSecurity, dari kedua metode tunneling menggunakan beberapa software ditunjukkan pada table II.

TABEL II.
KEBUTUHAN SOFTWARE

No	Software	Keterangan
1	Windows 10 Ultimate	System operasi VPN dan VPN Client
2	Winbox	Aplikasi yang menampilakan pengaturan RouterOS secara GUI (Graphical User Interface) untuk melakukan konfigurasi pada mikrotik.
3	Wireshark	Aplikasi untuk merekam lalu lintas data dalam jaringan VPN serta melihat parameter QoS untuk dianalisis
4	Draw.io	Tool online untuk mendesign topologi jaringan.
5	Speedtest	Tools untuk melakukan pengujian kecepatan internet yang terkoneksi pada client

Dalam penelitian ini rancangan jaringan VPN yang terdiri dari topology dengan pengalamatan IP di setiap perangkatya. Tahap perancangan ini penulis menggunakan tools Draw.io untuk membuat topologi jaringan VPN. Rancangan topology pada pengujian metode ini tidaklah berbeda antara metode SSTP dan L2TP+IPSec dan dibangun berdasarkan konsep dan gambaran dari perangkat sebenarnya. Menggunakan mikrotik RB931 yang berfungsi sebagai VPN Server dan 1 unit laptop berfungsi sebagai VPN Client.



Gambar 2. Topologi jaringan VPN

Pada peracangan topology ini konfigurasi VPN Server dilakukan pada Mikrotik. Router mikrotik terhubung menggunakan kabel LAN pada port ethernet 1, client menggunakan port Ethernet 2 untuk terhubung pada mikrotik. Pada perancanga jaringan SSTP, VPN Client adalah Remote Client yang bekerja sebagai pengguna dari layanan SSTP yang menggunakan router sebagai perangkat untuk dapat menggunkan SSTP tunnel. Setelah koneksi SSTP tunnel terbentuk Remote Client akan mendapatkan alamat IP secara otmatis yang berasal dari SSTP Server. Pada perancangan L2TP memiliki kinerja yang hampir sama dengan SSTP tetapi L2TP tidak dilengkapi dengan enkripsi sehingga dibutuhkan layanan tambahan yaitu IPSec (Internet Protocol Security).

Pada perancangan IP address baik untuk SSTP tunnel maupun L2TP+IPSec tunnel menggunakan alokasi IP address yang sama ditunjuk pada tabel III.

TABEL III.
DESAIN ALAMAT IP

No	Nama	Port	Alamat IP
1	Access Point	Eth1	192.168.100.1/24
2	SSTP Server	Eth1	192.168.100.43/24
		Eth2	10.10.1.1/24
3	L2TP Server	Eth1	192.168.1.43/24
		Eth2	10.10.1.1/24
4	VPN Client	NIC	10.10.1.2/24

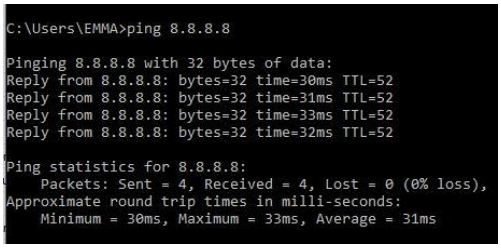
III. HASIL DAN PEMBAHASAN

A. Implementasi

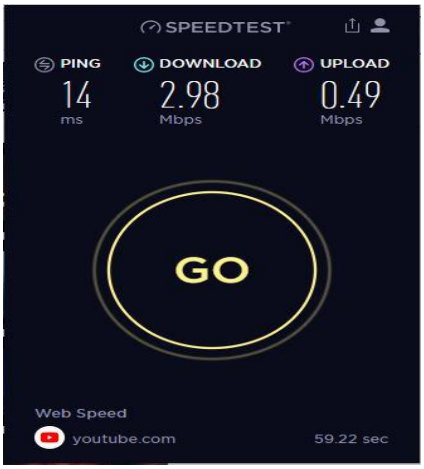
Pada tahap ini, penulis membangun system jaringan VPN dengan memasang seluruh perangkat sesuai dengan rancanga jaringan VPN yang telah dibuat sebelumnya. Melakukan konfigurasi dasar setiap perangkat dalam system jaringan VPN dengan alamat IP sehingga dapat saling berkomunikasi. Tahap konfigurasi metode SSTP dan L2TP+IPSec untuk membangun jaringan VPN dilakukan menggunakan aplikasi bantu Winbox pada Mikrotik RB931Ui-2^{nD}.

Langkah pertama kali pada proses implementasi adalah konfigurasi SSTP pada jaringan VPN sampai selesai kemudian mengecek konfigurasi VPN tersebut dengan perintah “ping” ke koneksi internet, selain itu juga bisa menggunakan tool “speedtest” untuk mengetahui kecepatan pada koneksi VPN tersebut.

Langkah berikutnya adalah konfigurasi L2TP yang dikombinasikan dengan IPSec sampai selesai kemudian cek konfigurasi dengan menguji koneksi ke internet dan cek kecepatan koneksi VPN tersebut.



Gambar 3. Uji koneksi internet



Gambar 4. Uji kecepatan koneksi internet

B. Pengujian

Setelah dilakukan penerapan jaringan VPN dan konfigurasi system berhasil, penulis melakukan pengambilan data hasil pengujian jaringan. Pengujian jaringan dilakukan pada metode SSTP dan L2TP + IPSec dengan 2 parameter yaitu steraming Youtube selama 5 menit serta melakukan streaming + download menggunakan video youtube berkualitas 480 px selama 5 menit. Data dikumpulkan menggunakan Aplikasi Wireshark.

Pengujian SSTP dan L2TP+IPSec dilakukan dalam keadaan setiap alat hidup degan fungsi yang sama sesuai dengan kebutuhan masing-masing. Pengujian ini menggunakan beberapa parameter yang dilihat pada tabel IV.

TABEL IV.
PARAMETER PENGUJIAN

SSTP	Pengujian 1	Pengujian 2
Parameter QoS	1. Troughput 2. Packet loss 3. Delay 4. Jitter	1. Troughput 2. Packet loss 3. Delay 4. Jitter
Parameter pengujian	Streaming youtube 480 px	Streaming youtube 480 px + Download Video 480 px pada situs anoboy.org
Lama Pengujian	5 menit	5 menit
Bandwith kapasitas	3 M	3 M

Pengujian dilakukan untuk mengumpulkan data-data melalui wireshark yang akan digunakan untuk menganalisis nilai Troughput, Packet loss, Delay dan jitter. Pada pengujian nilai troughput yang akan di analisa yaitu jumlah total semua paket data yang berhasil diterima melalui media transmisi jaringan. Pada pengujian packet loss yang dianalisa yaitu jumlah total paket yang hilang selama melakukan transmisi data pada jaringan. Pada pengujian delay yang dianalisa yaitu waktu tunda yang dibutuhkan suatu paket data yang dikirim oleh sumber sampai tujuan. Dan pada pengujian jitter yang dianalisa yaitu perbedaan selang waktu antara paket pada jaringan.

Sebagai contoh pengambilan data untuk pengujian 1 SSTP. Pengambilan data troughput dilakukan pengamatan dengan parameter yang dihitung dari nilai yang diperoleh, maka didapatkan rata-rata sebagai berikut:

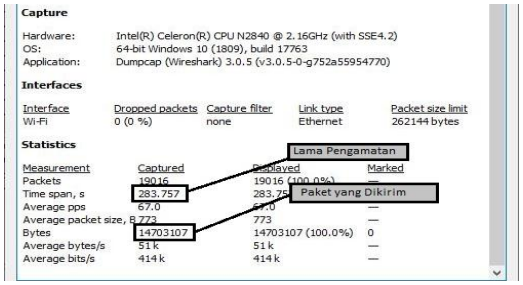
Troughput = Paket data yang diterima / Lama Pengamatan
= 14703107 / 283.757
= 51815.8389 bytes/s
= 404 Kbps

Dari percobaan diatas Troughput yang dihasilkan 404 Kbps dilihat pada tabel TIPHON nilai Troughput ikut dalam kategori sangat bagus karena 100% dari total bandwith yang ileh ISP.

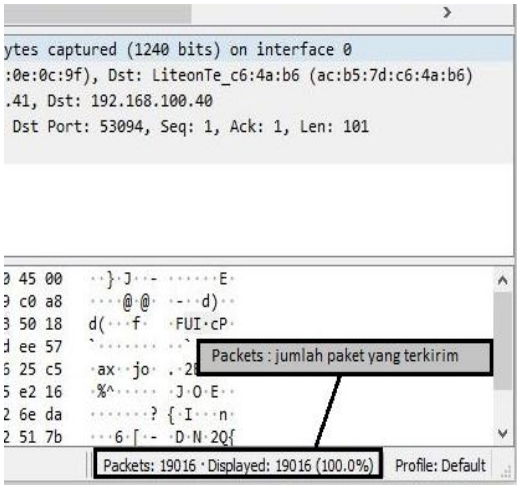
Untuk mencari packet loss dapat di lihat pada wireshark bagian bawah kanan seperti yng terlihat peda gambar diatas. Parameter yang di hitung dilihat dari nilai yang diperoleh.

Packet loss = ((total paket yang dikirim – total paket yang diterima) / total paket yang dikirim) x 100%
= ((19016-19016) / 19016) x 100%
= 0%

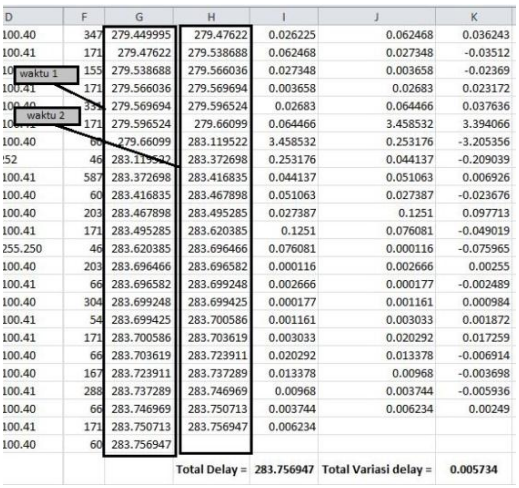
Dari hasil perhitungan diatas berdasarkan tabel TIPHON packet loss 0% masuk dalam kategori sangat bagus kearena tidak ada paket data yang hilang pada transmisi data dalam jaringan.



Gambar 5. Data troughput SSTP pengujian 1



Gambar 6. Data packet loss SSTP pengujian 1



Gambar 7. Data delay SSTP pengujian 1

Pada hasil capture file properties wireshark Time span adalah Waktu total delay yang di dapat saat melakukan pengujian ini.

Untuk dapat melakukan perhitungan Delay file Wireshark di export menjadi file CSV kemudian data time diolah untuk mencari delay dengan persamaan, waktu 2 - waktu 1. Total variasi delay diperoleh dari penjumlahan : (delay2-delay1) + (delay3-delay2) + ….+ (delayN –delay(N-1))

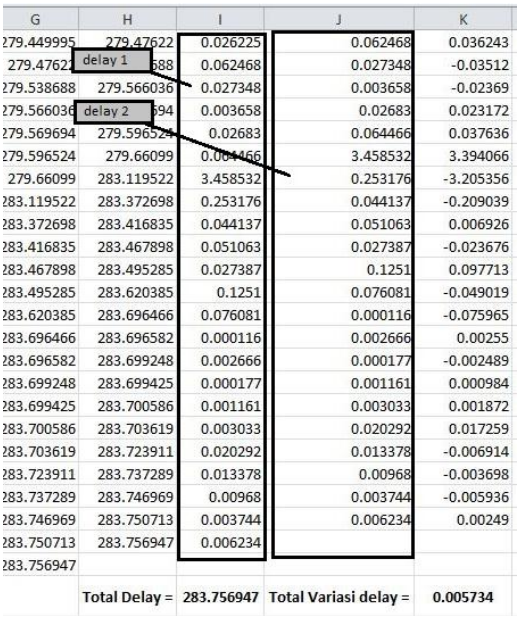
Delay rata-rata = total delay / total paket yang dikirim
= 283.756947 / 19016
= 0,0149219787 s
= 14.9219787 ms

Dari percobaan yang dilakukan, rata rata delay yaitu 14.9219787 ms, berdasarkan TIPHON ini termaksud dalam kategori sangat bagus, semakin kecil delay yang dihasilkan maka akan semakin bagus performa jaringan tersebut.

Kemudian kita hitung juga nilai jitter-nya sebagai berikut.

Jitter = Total Variasi delay / Total paket yang diterima -1
= 0.005734 / 19016 – 1
= 3.01551407e-7 s
= 0.000301551 ms

Dari percobaan yang dilakukan nilai jitter yang diperoleh 0.000301551 ms, berdasarkan TIPHON ini termaksud dalam kategori Bagus, semakin kecil jitter yang diperoleh maka akan semakin bagus performa jaringan tersebut.

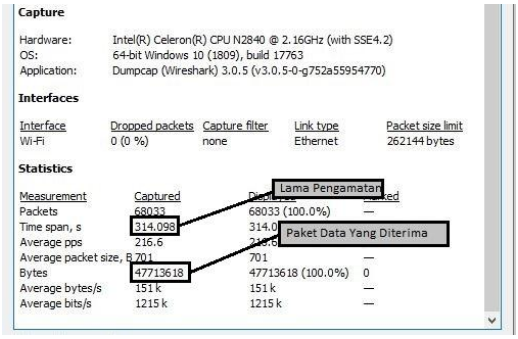


Gambar 8. Data jitter SSTP pengujian 1

Pengambilan data untuk pengujian 2 SSTP. Pengambilan data troughput dilakukan pengamatan dengan parameter yang dihitung dari nilai yang diperoleh, maka didapatkan rata-rata sebagai berikut:

Troughput = Paket data yang diterima / Lama Pengamatan
= 47713618 / 314.098
= 151906.787 bytes/s
= 1186 Kbps

Dari percobaan diatas Troughput yang dihasilkan 1186 Kbps dilihat pada tabel TIPHON nilai Troughput ikut dalam kategori sangat bagus karena 100% dari total bandwith yang ileh ISP.

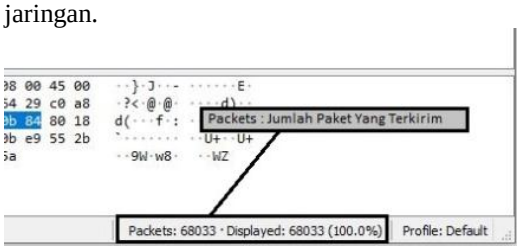


Gambar 9. Data troughput SSTP pengujian 2

Untuk mencari packet loss dapat di lihat pada wireshark bagian bawah kanan seperti yng terlihat peda gambar diatas. Parameter yang di hitung dilihat dari nilai yang diperoleh.

Packet loss = ((total paket yang dikirim – total paket yang diterima) / total paket yang dikirim) x 100%
= ((68033-68033) / 68033) x 100%
= 0%

Dari hasil perhitungan diatas berdasarkan tabel TIPHON packet loss 0% masuk dalam kategori sangat bagus karena tidak ada paket data yang hilang pada transmisi data dalam jaringan.



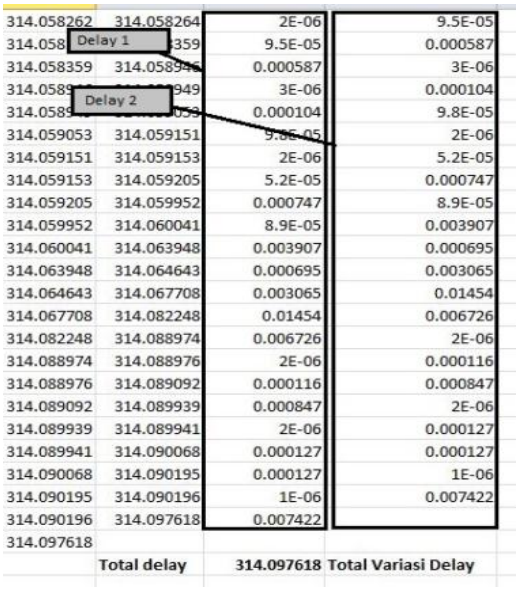
Gambar 10. Data packet loss SSTP pengujian 2

Pada hasil capture file properties wireshark Time span adalah Waktu total delay yang di dapat saat melakukan pengujian ini.

Untuk dapat melakukan perhitungan Delay file Wireshark di export menjadi file CSV kemudian data time diolah untuk mencari delay dengan persamaan, waktu 2 - waktu 1. Total variasi delay diperoleh dari penjumlahan : (delay2-delay1) + (delay3-delay2) + ….+ (delayN –delay(N-1))

Delay rata-rata = total delay / total paket yang dikirim
= 314.097618 / 68033
= 0.00461684209 s
= 4.61684209 ms

Dari percobaan yang dilakukan, rata rata delay yaitu 4.61684209 ms, berdasarkan TIPHON ini termaksud dalam kategori sangat bagus, semakin kecil delay yang dihasilkan maka akan semakin bagus performa jaringan tersebut.

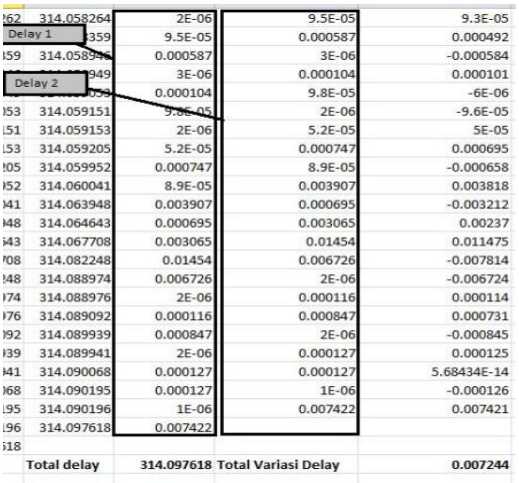


Gambar 11. Data delay SSTP pengujian 2

Kemudian kita hitung juga nilai jitter-nya sebagai berikut.

Jitter = Total Variasi delay / Total paket yang diterima -1
= 0.007244/ 68033 – 1
= 1.06479304e-7 s
= 0.000106479 ms

Dari percobaan yang dilakukan nilai jitter yang diperoleh 0.000106479 ms, berdasarkan TIPHON ini termaksud dalam kategori Bagus, semakin kecil jitter yang diperoleh maka akan semakin bagus performa jaringan tersebut.



Gambar 12. Data jitter SSTP pengujian 2

Dengan cara yang sama, lakukan pada pengujian 1 dan pengujian 2 untuk

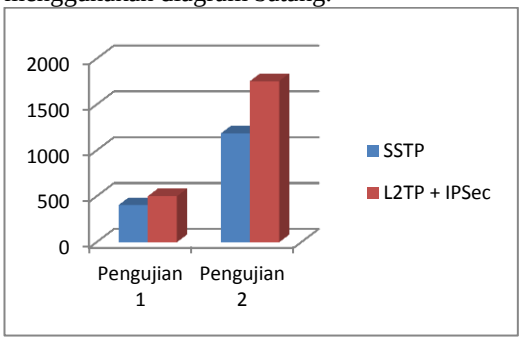
L2TP+IPSec, sehingga didapatkan hasil sebagai berikut.

Pengujian 1 L2TP+IPSec, troughput = 501 Kbps, packet loss = 0%, delay = 15.3199236 ms, jitter = 0.000161821 ms.

Pengujian 2 L2TP+IPSec, troughput = 1757 Kbps, packet loss = 0%, delay = 4.42344006 ms, jitter = 0.000444307 ms.

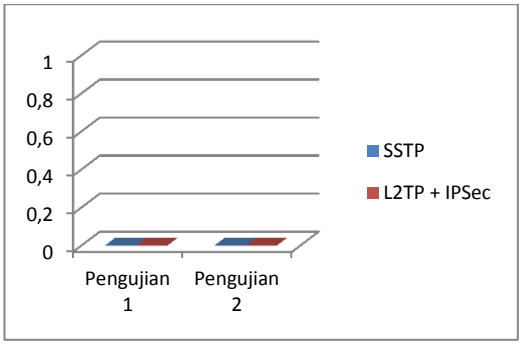
C. Perbandingan

Tahap ini penguji mulai membandingkan hasil pengujian yang telah dilakukan dengan menggunakan diagram batang.



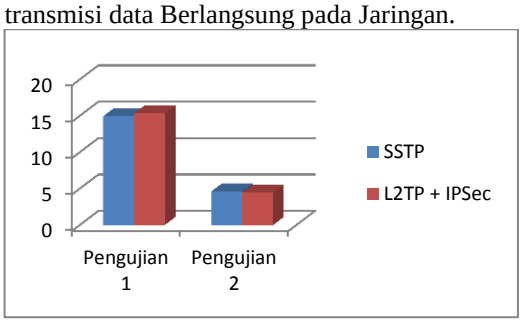
Gambar 13. Diagram perbandingan troughput

Pada diagram diatas pengujian 1 SSTP memiliki nilai 404 Kbps dan L2TP + IPSec 501 Kbps. Pada pengujan 2 nilai SSTP 1186 Kbps dan L2TP + IPSec memiliki nilai 1757 Kbps. Pada pengujian Pertama L2TP + IPSec lebih unggul dengan selisih 97 Kbps. Selanjutnya pada pengujian ke 2 L2TP+ IPSec masih unggul dengan niai pebandingan yang cukup besar yaitu 571 Kbps. Dengan melihat hasil tersebut dapat disimpulkan pada variable Troughput L2TP + IPSec lebih bagus dari pada SSTP.



Gambar 14. Diagram perbandingan packet loss

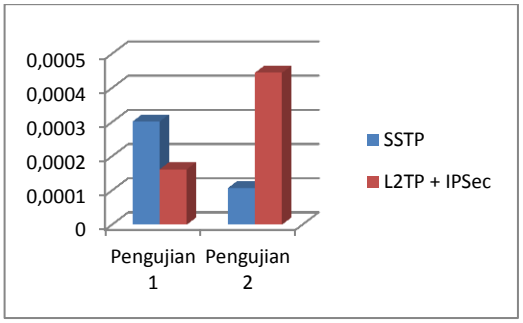
Pada diagram diatas packet loss yang dihasilkan oleh metode SSTP dan L2TP+IPSec memiliki nilai yang sama baik pada pengujian pertama dan pengujian kedua yaitu 0%. Pada pengujian Packet Loss tidak terdapat perbedaan antara kedua metede SSTP dan L2TP + IPSec serta tidak terdapatnya paket hilang ketika transmisi data Berlangsung pada Jaringan.



Gambar 15. Diagram perbandingan delay

Dari diagram diatas pada pengujian 1 menunjukan nilai SSTP 14.9219787 ms dan nilai L2TP+IPSec 15.3199236 ms. Sedangkan pada pengujian 2 L2TP+IPSec 4.42344006 ms dan SSTP dengan nilai 4.61684209 ms.

Pada pengujian delay semakin kecil nilai delay yang dihasilkan dalam satuan ms maka semakin bagus performa suatu jaringan. Pada pengujian 1 data diagram SSTP lebih unggul dengan nilai yang lebih kecil dibandingkan dengan L2TP + IPSec, selisih nilai keduanya 0.3979449 ms. Selanjutnya pada pengujian 2 L2TP + IPSec lebih unggul dengan nilai yang lebih kecil dibanding dengan SSTP, selisih nilai keduannya 0.19340203 ms. Pada pengujian delay SSTP lebih unggul ketika melakukan Streaming video saja, sedangkan L2TP + IPSec lebih efektif dan unggul untuk melakukan download + streaming yang berarti semakin berat beban kinerja jaringan yang di jalankan maka semakin cepat dan baik kualitas jaringan yang ada.



Gambar 16. Diagram perbandingan jitter

Dari diagram diatas pada pengujian 1 menunjukan nilai jitter SSTP 0.000301551 ms dan nilai jitter L2TP+IPSec 0.000161821 ms. Sedangkan pada pengujian 2 SSTP 0.000106479 ms dan L2TP+IPSec dengan nilai 0.000444307 ms.

Pada pengujian Jitter semakin kecil nilai jitter yang dihasilkan maka semakin bagus performa jaringan yang berjalan. Pada

pengujian 1 L2TP + IPSec lebih unggul dari SSTP dengan nilai yang lebih Kecil dibanding dengan SSTP, selisih nilai keduanya 0.00013973 ms. Selanjutnya pada pengujian 2 SSTP lebih unggul dari L2TP + IPSec dengan nilai yang lebih Kecil dibanding SSTP, selisih keduanya 0.000337828.

Pengujian jitter pada metode SSTP semakin banyaknya transmisi data yang berjalan maka nilai jitter semakin menurun berarti performa jaringan akan lebih baik ketika banyaknya lalu lintas jaringan yang terjadi. Sedangkan pada pengujian jitter metode L2TP + IPSec semakin banyaknya transmisi data yang berjalan maka nilai jitter akan semakin naik yang berarti performa akan menurun.

IV. KESIMPULAN

Dari hasil analisis perbandingan antara SSTP dengan L2TP+IPSec diatas, diperoleh beberapa kesimpulan sebagai berikut:

1. Jaringan dengan metode L2TP + IPSec menunjukan nilai troughput lebih besar dari metode SSTP. Pada pengujian 1 SSTP 404 Kbps dan L2TP + IPSec 501 Kbps. Pada pengujan 2 nilai SSTP 1186 Kbps dan L2TP + IPSec memiliki nilai 1757 Kbps. Nilai kedua metode ini dalam parameter QoS berdasarkan tabel TIPHON memiliki kedudukan yang sama yaitu masuk pada kategori Sangat Bagus dengan angka presentase 100% data terkirim. Semakin besar nilai troughput, maka semakin baik kualitas pengiriman data yang dihasilkan.
2. Pada jaringan dengan metode SSTP setiap parameter pengujian 1 maupun pengujian 2 menunjukan nilai packet loss sebesar 0%. Begitu pula dengan jaringan dengan metode L2TP+IPSec setiap parameter pengujian 1 dan pengujian 2 menunjukan nilai packet loss 0 %. Nilai kedua metode ini dalam parameter QoS berdasarkan tabel TIPHON memiliki kedudukan yang sama yaitu masuk pada kategori Sangat Bagus dengan angka presentase 0% artinya tidak ada data yang hilang pada saat proses transmisi data yang berlangsung. Semakin kecil nilai packet loss maka akan semakin baik kualitas keutuhan paket data yang dikirim dan diterima.
3. Jaringan dengan metode SSTP pada pengujian 1 lebih unggul dengan nilai delay yang lebih kecil dari L2TP+IPSec. Nilai pengujian SSTP 14.9219787 ms dan nilai L2TP+IPSec 15.3199236 ms. Sedangkan pada pengujian 2 L2TP+IPSec lebih unggul dengan nilai lebih kecil yaitu 4.42344006 ms dibandingkan dengan SSTP dengan nilai 4.61684209 ms. Kedua metode tersebut memiliki selisih yang terbilang cukup kecil. Nilai kedua metode ini dalam parameter QoS berdasarkan tabel TIPHON memiliki kedudukan yang sama yaitu masuk pada kategori Sangat Bagus dengan besar delay <150. Semakin kecil nilai delay maka akan semakin cepat pengiriman paket data pada jaringan.
4. Jaringan dengan metode L2TP+IPSec pada pengujian 1 lebih unggul dengan nilai jitter yang lebih kecil dari SSTP. Nilai pengujian SSTP 0.000301551 ms dan nilai L2TP+IPSec 0.000161821 ms. Sedangkan pada pengujian 2 SSTP lebih unggul dengan nilai lebih kecil yaitu 0.000106479 ms dibandingkan dengan L2TP+IPSec dengan nilai 0.000444307 ms. Pada pengujian jitter dengan metode SSTP semakin banyaknya transmisi data yang berjalan maka nilai jitter semakin menurun berarti performa jaringan akan lebih baik ketika banyaknya lalu lintas jaringan yang terjadi. Sedangkan pada pengujian jitter metode L2TP + IPSec semakin banyaknya transmisi data yang berjalan maka nilai jitter akan semakin naik yang berarti performa jaringan akan menurun. Nilai kedua metode ini dalam parameter QoS berdasarkan tabel TIPHON memiliki kedudukan yang sama yaitu masuk pada kategori Bagus dengan besar jitter 0-75 ms. Semakin kecil nilai jitter maka akan semakin cepat pengiriman paket data pada jaringan.

Kedua metode jaringan ini memiliki kelebihan dan kekurangan yang berbeda beda namun dari beberapa parameter yang diukur penulis menyimpulkan bahwa metode L2TP+IPSec lebih baik jika dibandingkan dengan SSTP. Dapat dilihat melalui parameter troughput yang diukur memiliki jumlah paket yang dikirim dan diterima lebih banyak dalam waktu 5 menit. Kemudian parameter delay L2TP+IPSec juga lebih unggul dilihat dari total delay yang dihasilkan memiliki nilai yang lebih kecil, artinya semakin berat beban kinerja jaringan yang di jalankan maka delay akan semakin kecil dan semakin cepat pula kualitas jaringan yang ada. Dan Meskipun nilai troughput, packet loss, delay dan jitter L2TP + IPsec lebih besar atau lebih kecil dari pada SSTP namun jika di lihat mengunakan wireshark bahwa jumlah paket yang dikirim pada satuan waktu yang sama dibanding SSTP, L2TP+IPSec lebih banyak mengirimkan paket yang diterima tanpa adanya paket yang hilang ketika transmisi data berlangsung.

REFERENSI

[1] Sugiyatno, S., & Atika, P. D. Virtual Private Network (VPN) Secure Socket Tunneling Protocol (SSTP) Menggunakan Raspberry Pi. *INFORMATION SYSTEM FOR EDUCATORS AND PROFESSIONALS*, *2*(2), 2018, hal.155-166.

[2] Prasetyo, E., Hamzah, A., & Sutanta, E. Analisa Quality Of Service (QOS) Kinerja Point to Point Protocol Over Ethernet (PPPOE) DAN POINT TO POINT TUNNELING PROTOCOL (PPTP). *Jurnal Jarkom*, *4*(1), 2017.

[3] Sari, Linna Oktaviana. "Analisa Perbandingan Pengaruh Penggunaan Protokol Tunneling IP Security dengan Protokol Tunneling Layer 2 Tunneling Protocol terhadap Quality Of Services pada Jaringan Virtual Private Network." *Jurnal Online Mahasiswa Fakultas Teknik Universitas Riau* 4.1: 1-7

[4] Herlambang, Moch Linto, and Catur L. Azis. "Panduan Lengkap Menguasai Router Masa Depan Menggunakan Mikrotik RouterOS." *Yogyakarta: ANDI Publisher*, 2008.

[5] Teorikomputer.com. Jenis-jenis Mikrotik Pada Jaringan. http://www.teorikomputer.com/2016/10/jenis-jenis-mikrotik-pada-jaringan.ht ml diakses tanggal 2 september 2019

[6] Thomas.Tom. Network Security Firt-Step Yogyakarta. Andi Yogyakarta, 2005.

[7] Iswara, G.S., Periyadi, and Ismail, S.J.I. Implementasi Protokol SSTP dalam Membangun Server VPN Menggunakan Konfigurasi Routing dan Remote Access untuk Access Client pada Windows Server, 2008.

[8] Microsoft TechNet "MS-SSTP: Secure Socket Tunneling Protocol (SSTP)".2015.

[9] Juniper Network, Inc. Volume 5: Virtual Private Network. Relese 6.1.0, Rev. 03.1194 Nort Mathilda Avenue Sunnyvale, CA 94089.USA, 2019.

[10] Musjad A., Naufal R., Fatin D., Anang M. VPN Cisco & Mikrotik. Jakarta: Pesantren Network IDN, 2017.

[11] I.P.A.E.P. Handbook Jaringan Komputer Teori dan Praktik Berbasis Open Souce. Bandung : INFORMATIKA, 2015.

[12] TIPHON. *Telecomminications and Internet Protocol Harmonization Over Network (TIPHON) General aspects Quality of Service (QoS).* Jurnal 1, 1999.

[13] Yanto. Analisis QoS (Quality of Service) pada jaringan Internet (Study Kasus Fakultas Teknik Untan) : Pontianak, 2013.

[14] Cyberlink.co.id. Apa itu Winbox. http://cyberlink.co.id/blog/apa-itu-winbox/Diakses tanggal 2 september 2019.

[15] Wireshark FAQ. Diakses tanggal 2 september 2019.