JIKB
Jurnal Ilmu Komputer dan Bisnis

Jurnal Ilmu Komputer dan Bisnis (JIKB)
Mei-2022, Vol. XIII, No.1, hal.105-114
ISSN(P): 2087-3921; ISSN(E): 2598-9715

Analisa Penggunaan VPN L2TP dan SSTP di Masa Pandemi Covid-19

[1]Haeruddin, [2]Kelvin
[1,2]Universitas Internasional Batam

Alamat Surat
Email: haeruddin@uib.ac.id, 1831169.kelvin@uib.edu

Article History:
Diajukan: 27 Maret 2021; Direvisi: 15 April 2022; Diterima: 25 April 2022

ABSTRAK

COVID-19 merupakan sebuah virus yang telah berkembang menjadi pandemi global. Hal ini menyebabkan jutaan karyawan di seluruh dunia saat ini bekerja dari rumah. *Virtual Private Network (*VPN*)* dapat digunakan untuk memberikan karyawan akses data kantor dari rumah. Penelitian ini menganalisa perbedaan protokol VPN L2TP/IPsec dengan SSTP untuk memilih teknologi VPN yang cocok digunakan sesuai kebutuhan pengguna. Hal ini dilakukan dengan cara membangun jaringan VPN tersebut dengan parameter kebutuhan perangkat, QoS, keamanan, dan skalabilitas dengan menggunakan metode *Network Development Life Cycle (NDLC)*. Hasil dari penelitian ini menunjukkan bahwa kedua jenis VPN tersebut memiliki kelebihan dan kekurangannya masing-masing dari segi performa, keamanan dan skalabilitas. Hasil penelitian ini diharapkan dapat memberikan gambaran kepada pengguna untuk mempertimbangkan jenis VPN yang sesuai dengan kebutuhan.

Kata kunci: COVID-19*, IPsec, L2TP, NDLC, SSTP*

ABSTRACT

*COVID-19 is a virus have developed into a global pandemic. This has resulted in millions of employees around the world currently working from home. Virtual Private Network (*VPN*) can be used to provide employees access to office data from home. This study analyzes the differences between L2TP/IPsec and SSTP* VPN *protocols to choose a* VPN *technology that is suitable for use according to user needs. This is done by building the* VPN *network in according to the device requirements, QoS, security, and scalability parameters using Network Development Life Cycle (NDLC) method. The results of this study indicate that both types of* VPNs *have their respective advantages and disadvantages in terms of performance, security and scalability. The results of this study are expected to provide an overview for users to consider the type of* VPN *that suits their needs.*

Keywords: COVID-19, IPsec, L2TP, NDLC, SSTP

1. PENDAHULUAN

SARS-CoV-2 atau lebih sering disebut COVID-19 merupakan sebuah virus penyebab infeksi saluran pernafasan (Wang et al., 2020). Virus ini telah menyebar dengan cepat dan berkembang menjadi pandemi global, menciptakan krisis kesehatan masyarakat. Beberapa upaya telah dilakukan oleh pemerintahan di seluruh dunia untuk membatasi aktifitas ekonomi dan sosial yang bersifat non-esensial (Chun et al., 2020). Penularan virus dapat terjadi saat di tempat kerja maupun saat dalam perjalanan menuju tempat kerja. Resiko terpapar virus ini sangat bergantung terhadap jarak

https://doi.org/10.47927/jikb.v13i1.279

antar manusia dan sering kontak fisik dengan orang yang mungkin terinfeksi COVID-19. Untuk menjaga keselamatan para pekerja, maka *work from home (WFH)* diberlakukan.

Jutaan karyawan saat ini bekerja dari rumah di seluruh dunia. Sebelum pandemi para pekerja mengakses data perusahaan menggunakan jaringan lokal yang disediakan oleh perusahaan di kantor. Sehingga dimasa pandemi karyawan mengalami kesulitan mengakses data yang ada di kantor dari rumah mereka. Tidak semua perusahaan memiliki infrastruktur keamanan yang handal untuk mempublikasikan data melalui *server* di jaringan publik. Serangan siber seperti *denial-of-service*, malware komputer, atau akses yang tidak memiliki izin dapat menyebabkan kerusakan yang tidak dapat diperbaiki dan kerugian finansial (Sarker et al., 2020). Agar karyawan dapat mengakses data secara lokal layaknya mengakses data dari kantor, solusi utama yang dapat digunakan adalah penggunaan *Virtual Private Network (*VPN*).*

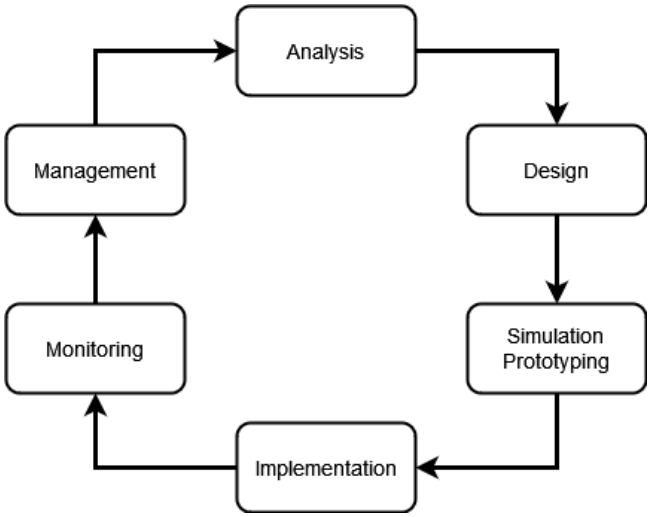
VPN dapat digunakan untuk membentuk jaringan privat yang memiliki keamanan tinggi antara dua perangkat melalui jaringan publik (Lukman & Mukhlishah, 2020; Skendzic & Kovacic, 2017; Xu & Ni, 2020). VPN memiliki keunggulan *tunneling* dan enkripsi yang menjamin kerahasiaan dan integritas selama proses transmisi data (Yang et al., 2019; Zhang et al., 2018). VPN memiliki beberapa jenis protokol *tunneling*, diantaranya adalah *Layer Two Tunneling Protocol (L2TP)* dan *Secure Socket Tunneling Protocol (SSTP)* (Bui et al., 2019).

Data yang ditransmisikan melalui L2TP/IPsec umumnya diautentikasi dua kali. Salah satu alasan mengapa L2TP merupakan protokol umum adalah bahwa tidak ada kerentanan yang diketahui (Aung & Thein, 2020). SSTP adalah protokol yang dikembangkan oleh *microsoft* dan merupakan kombinasi antara SSL dan TCP. Penggunaan SSL menjamin kerahasiaan dan integritas data saat transmisi (Farly et al., 2017). SSTP memanfaatkan PPP yang dienkapsulasi didalam HTTPS untuk mentransmisi lalu lintas jaringan (Bui et al., 2019).

Tujuan dari penelitian ini adalah bagaimana mengimplementasikan jaringan VPN L2TP/IPsec dan SSTP, serta menetukan protokol mana yang tepat untuk kebutuhan *WFH* di tinjau dari *QoS*, Keamanan, Skalabilitas, Biaya, Tingkat Kesulitan, dan Dukungan Perangkat.

2. METODE

Dalam melakukan peneltian ini penulis menggunakan metode *Network Development Life Cycle (NDLC)*. NDLC merupakan metode untuk mengembangkan dan mengimplementasikan sistem jaringan (Suharto & Irfan, 2019). NDLC terbagi menjadi 6 tahap namun pada penelitian ini, dikarenakan batasan masalah hanya sampai *monitoring* maka penulis hanya melaksanakan metode NDLC hingga metode ke 5 (Lihat Gambar 1), yaitu:



Gambar 1. *Network Development Life Cycle (NDLC)*

1. *Analysis*: Pada tahap ini dilakukan analisa terhadap permasalahan yang ada, kebutuhan jaringan, protokol yang akan digunakan, serta mentukan parameter yang akan digunakan, serta *hardware* dan *software* yang akan digunakan dan biaya yang implementasi VPN.
2. *Design*: berdasarkan data pada tahap sebelumnya, pada tahap ini penulis mendesain topologi yang sesuai untuk digunakan pada masing masing jenis VPN yaitu L2TP/IPsec dan SSTP.
3. *Implementation*: Pada tahap ini penulis akan melakukan implementasi desain topologi VPN yang sudah dibuat sebelumnya di *VirtualBox* meliputi menginstall dan konfigurasi sistem operasi *Host* dan *RouterOS*.
4. *Monitoring*: Pada tahap ini penulis akan melakukan pemantauan serta melakukan beberapa pengujian terhadap parameter yang sudah ditentukan sebelumnya untuk mendapatkan hasil perbandingan antara kedua VPN yaitu L2TP/IPsec dan SSTP. Tahapan dalam melakukan pemantauan dimulai dari *Packet Loss*, *Throughput*, Packet Analysis. Hasil dari pengujian tersebut akan dijabarkan menjadi empat parameter yaitu *Security*, *QoS*, dan *Scalability*.

3. HASIL DAN PEMBAHASAN

3.1 *Analysis*

Berikut adalah hasil analisa dari protokol VPN L2TP/IPsec dan SSTP

1. Cara Kerja VPN L2TP/IPsec dan SSTP

   L2TP/IPsec bekerja dengan mengenkapsulasi paket L2TP yang menggunakan *Password Authentication Protocol (PAP)* dalam IPsec untuk meningkatkan keamanan. L2TP/IPsec memanfaatkan UDP *port* 1701 untuk melakukan komunikasinya. Sedangkan SSTP bekerja dengan menggunakan PPP yang menggunakan authentikasi MS-CHAPv2 untuk membawa lalu lintas jaringan dan mengenkapsulasi paket PPP tersebut dalam HTTPS. SSTP memanfaatkan TCP *port* 443 untuk melakukan komunikasinya.

2. Kelebihan Serta Kekurangan VPN L2TP/IPsec dan SSTP

   L2TP/IPsec memiliki kelebihan yaitu sistem enkripsi dan keamanan yang kuat, enkapsulasi dan verifikasi dua kali, mudah dikonfigurasi, serta mendukung sistem operasi windows, Mac, Android, IOS, maupun Linux. Kekurangan L2TP/IPsec adalah performa yang lambat dikarenakan authentikasi dan enkripsi dua kali, *port* protokol L2TP dapat diblokir oleh *firewall*, sulit dikonfigurasi di perangkat yang menjalankan NAT *routers*.

   SSTP memiliki kelebihan yaitu dapat melewati *firewall* dikarenakan menggunakan SSL dengan *port* 443, sistem enkripsi dan keamanan yang kuat, mudah untuk dikonfigurasi, didukung oleh *microsoft* dan diintegrasi kedalam sistem operasi *Windows*, serta mendukung sistem operasi lain seperti *Mac*, *Android*, *IOS*, maupun *Linux* dengan konfigurasi atau *software* tambahan. Kekurangan SSTP adalah performa yang lambat dikarenakan enkripsi tingkat tinggi serta pihak ketiga tidak dapat mengaudit kerentanannya dikarenakan SSTP merupakan properti *Microsoft*.

3. Kebutuhan VPN L2TP/IPsec dan SSTP

   Perangkat yang perlu disediakan adalah *router* sebagai *server* mikrotik serta *client* yang dapat berupa *router* lainnya untuk jenis *Site-to-Site* dan/atau *client Host* yang mendukung sebagai *client* L2TP/IPsec maupun SSTP. IP publik yang akan digunakan sebagai IP VPN *Server*. Jika terdapat *firewall*, maka perlu mengizinkan UDP *port* 1701 agar L2TP dapat berfungsi. Sertifikat CA dan *Server Authentication* juga dibutukan

untuk mengkonfigurasi SSTP *Server*. Dan bagi *client* SSTP juga perlu untuk memasang sertifikat CA untuk dapat terhubung ke SSTP *Server*.

4. Perangkat Serta Kapasitas *User*

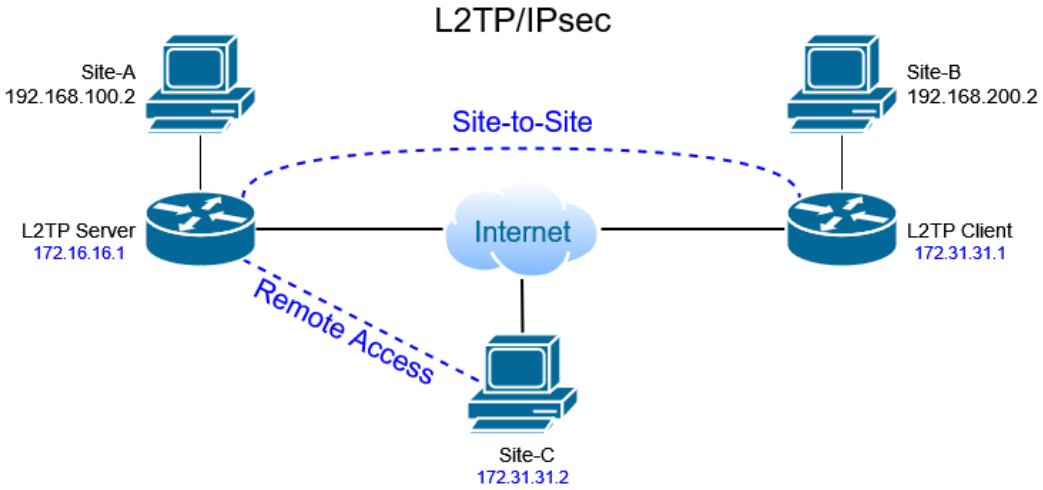
   Berikut adalah beberapa referensi perangkat yang dapat digunakan sebagai L2TP/IPsec *Server* maupun SSTP *Server*:

Tabel 1. Perbandingan Perangkat VPN

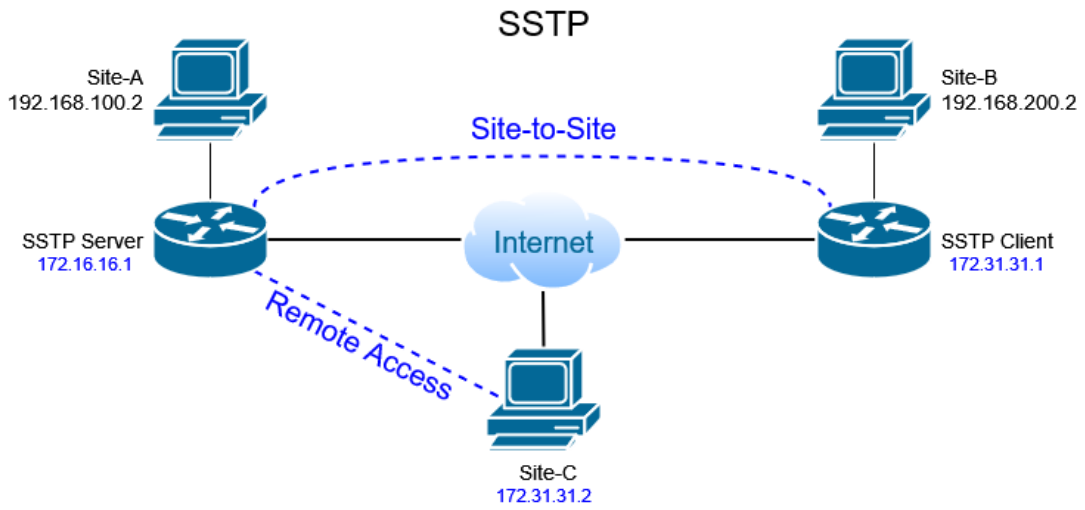
No	***Model / Product Code***	***Protokol VPN***	***Kapasitas User***	***Harga***
1	Mikrotik RB760iGS	L2TP/IPSec & SSTP	200	Rp1.045.000
2	Mikrotik RB4011iGS+RM	L2TP/IPsec & SSTP	500	Rp3.253.635
3	Mikrotik CCR1036-8G-2S+EM	L2TP/IPsec & SSTP	2500	Rp18.899.000
4	TP-Link TL-R600VPN	L2TP/IPsec	16	Rp915.000
5	Cisco RV340	L2TP/IPsec	50	Rp5.150.000

3.2 *Design*

Dengan hasil analisa yang telah dilakukan, selanjutnya penulis membuat rancangan topologi jaringan yang akan digunakan sebagai dasar pengujian yang terdiri dari L2TP/IPsec *Site-to-Site*, L2TP/IPsec *Remote Access*, SSTP *Site-to-Site*, dan SSTP *Remote Access*. Rancangan topologi ditunjukkan pada gambar dibawah ini:



Gambar 2. Topologi L2TP/IPsec *Site-to-Site* dan *Remote Access*



Gambar 3. Topologi SSTP *Site-to-Site* dan *Remote Access*

3.3 *Implementation*

Pada tahap implementasi penulis menggunakan *VirtualBox* sebagai *Test Bed Site-to-Site* yang di *install* dengan *VM Windows* 7 sebagai *Host* A dengan jaringan internal "LAN A", *VM RouterOS* 6.48.6 Long-term sebagai *Router* A dengan jaringan internal "internet" dan "LAN A", VM RouterOS 6.48.6 Long-term Sebagai *Router* B dengan jaringan internal "internet" dan "LAN B", dan VM Windows 7 sebagai *Host* B dengan jaringan internal "LAN B". Sedangkan untuk *Remote Access*, *VM Windows* 7 sebagai *Host* B dengan jaringan internal "internet" yang terhubung langsung ke *Router* A.

3.4 *Monitoring*

Pada tahap pemantauan penulis melakukan pengujian *transfer file* sebesar 5 MB dan menangkap lalu lintas jaringannya menggunakan *wireshark* yang akan digunakan sebagai dasar dari pengujian QoS. Parameter QoS terbagi menjadi empat yaitu *Delay*, *Jitter*, *Throughput*, dan *Packet Loss*. Ke empat parameter ini akan diuji di dua protokol VPN yang dikategorikan dalam dua jenis VPN dengan pengujian limitasi *bandwidth* 5 Mbps, 10 Mbps, 15 Mbps, dan 20 Mbps. Sedangkan untuk dasar pengujian *Security* penulis melakukan pengujian ICMP Ping dan menangkap lalu lintas jaringannya menggunakan *wireshark* kemudian menganalisa paket tersebut.

Berikut adalah hasil dari pengujian dari empat parameter QoS:

1. Hasil *Delay*

   Delay diukur dalam satuan *millisecond*. Dengan menganalisa hasilnya, penulis mengkategorikan masing-masing hasil sesuai dengan standard TIPHON.

Tabel 2. Tabel Perbandingan *Delay*

Protokol	***Jenis***	***Bandwidth***	***Delay***	***Indeks***	***Kategori***
L2TP	*Site-to-Site*	5 Mbps	3.869135	4	Sangat Bagus
		10 Mbps	1.868084	4	Sangat Bagus
		15 Mbps	1.175022	4	Sangat Bagus
		20 Mbps	0.881107	4	Sangat Bagus
	Remote Access	5 Mbps	2.232723	4	Sangat Bagus

Protokol	***Jenis***	***Bandwidth***	***Delay***	***Indeks***	***Kategori***
		10 Mbps	1.206035	4	Sangat Bagus
		15 Mbps	1.051938	4	Sangat Bagus
		20 Mbps	0.921878	4	Sangat Bagus
SSTP	*Site-to-Site*	5 Mbps	2.315580	4	Sangat Bagus
		10 Mbps	1.289159	4	Sangat Bagus
		15 Mbps	1.157977	4	Sangat Bagus
		20 Mbps	0.772595	4	Sangat Bagus
	Remote Access	5 Mbps	2.687634	4	Sangat Bagus
		10 Mbps	1.426459	4	Sangat Bagus
		15 Mbps	1.122768	4	Sangat Bagus
		20 Mbps	0.897506	4	Sangat Bagus

Dari hasil pengujian tersebut dapat dilihat bahwa VPN L2TP/IPsec dan SSTP jenis *Site-to-Site* dan *Remote Access* termasuk dalam kategori Sangat Bagus. Namun dapat dilihat bahwa L2TP/IPsec-*Remote Access* memiliki rata-rata *Delay* paling rendah, SSTP-*Site-to-Site* memiliki rata-rata *Delay* paling rendah ke dua, SSTP-*Remote Access* memiliki rata-rata *Delay* paling tinggi kedua, dan L2TP/IPsec-*Site-to-Site* memiliki rata-rata *Delay* paling tinggi.

2. Hasil *Jitter*

Jitter diukur dalam satuan *millisecond*. Dengan menganalisa hasilnya, penulis mengkategorikan masing-masing hasil sesuai dengan standard TIPHON.

Tabel 3. Tabel Perbandingan *Jitter*

Protokol	***Jenis***	***Bandwidth***	***Jitter***	***Indeks***	***Kategori***
L2TP	*Site-to-Site*	5 Mbps	3.870417	3	Bagus
		10 Mbps	1.868110	3	Bagus
		15 Mbps	1.175162	3	Bagus
		20 Mbps	0.952492	4	Sangat Bagus
	Remote Access	5 Mbps	2.113241	3	Bagus
		10 Mbps	1.250653	3	Bagus
		15 Mbps	1.098038	3	Bagus
		20 Mbps	0.921592	4	Sangat Bagus
SSTP	*Site-to-Site*	5 Mbps	2.367824	3	Bagus
		10 Mbps	1.292634	3	Bagus
		15 Mbps	1.213225	3	Bagus
		20 Mbps	0.772475	4	Sangat Bagus
	Remote Access	5 Mbps	2.740321	3	Bagus
		10 Mbps	1.478697	3	Bagus

Protokol	***Jenis***	***Bandwidth***	***Jitter***	***Indeks***	***Kategori***
		15 Mbps	1.170078	3	Bagus
		20 Mbps	0.947544	4	Sangat Bagus

Dari hasil pengujian tersebut dapat dilihat bahwa VPN L2TP/IPsec dan SSTP jenis *Site-to-Site* dan *Remote Access* termasuk dalam kategori Bagus untuk pengujian limitasi *bandwidth* 5 Mb, 10 Mb, dan 15Mb. Sedangkan untuk limitasi *bandwidth* 20 Mb termasuk dalam kategori Sangat Bagus. Namun dapat dilihat bahwa L2TP/IPsec-*Remote Access* memiliki rata-rata *Jitter* paling rendah, SSTP-*Site-to-Site* memiliki rata-rata *Jitter* paling rendah ke dua, SSTP-*Remote Access* memiliki rata-rata *Jitter* paling tinggi kedua, dan L2TP/IPsec-*Site-to-Site* memiliki rata-rata *Jitter* paling tinggi.

3. Hasil *Throughput*

Delay diukur dalam satuan Mbps. Dengan menganalisa hasilnya, penulis mengkategorikan masing-masing hasil sesuai dengan standard TIPHON.

Tabel 4. Tabel Perbandingan *Throughput*

Protokol	***Jenis***	***Bandwidth***	***Throughput / Persentase***	***Indeks***	***Kategori***
L2TP	*Site-to-Site*	5 Mbps	4.32/86.45	4	Sangat Bagus
		10 Mbps	9.18/91.76	4	Sangat Bagus
		15 Mbps	13.4/89.36	4	Sangat Bagus
		20 Mbps	19.26/77.04	4	Sangat Bagus
	Remote Access	5 Mbps	4.97/99.38	4	Sangat Bagus
		10 Mbps	9.53/95.29	4	Sangat Bagus
		15 Mbps	10.64/70.91	3	Bagus
		20 Mbps	15/75.02	3	Bagus
SSTP	*Site-to-Site*	5 Mbps	4.58/91.69	4	Sangat Bagus
		10 Mbps	8.94/89.4	4	Sangat Bagus
		15 Mbps	9.93/66.2	3	Bagus
		20 Mbps	11.47/57.37	4	Sangat Bagus
	Remote Access	5 Mbps	4.36/87.13	4	Sangat Bagus
		10 Mbps	8.17/81.75	4	Sangat Bagus
		15 Mbps	10.13/67.51	3	Bagus
		20 Mbps	12.34/61.72	3	Bagus

Dari hasil pengujian tersebut dapat dilihat bahwa VPN L2TP/IPsec jenis *Site-to-Site* termasuk dalam kategori Sangat Bagus untuk pengujian limitasi *bandwidth* 5 Mb, 10 Mb, 15 Mb, dan 20 Mb. SSTP jenis *Site to-Site* termasuk dalam kategori Sangat Bagus untuk pengujian limitasi *bandwidth* 5 Mb, 10 Mb, dan 15 Mb. Sedangkan untuk limitasi *bandwidth* 20 Mb termasuk dalam kategori Bagus. VPN L2TP/IPsec dan SSTP jenis *Remote Access* termasuk dalam kategori Sangat Bagus untuk pengujian limitasi *bandwidth* 5 Mb dan 10 Mb. Sedangkan untuk limitasi *bandwidth* 15 Mb dan 20 Mb

termasuk dalam kategori Bagus. Namun dapat dilihat bahwa L2TP/IPsec-*Site-to-Site* memiliki rata-rata *Throughput* paling tinggi, SSTP-*Site-to-Site* memiliki rata-rata *Throughput* paling tinggi ke dua, L2TP/IPsec-*Remote Access* memiliki rata-rata *Throughput* paling rendah kedua, dan SSTP-*Remote Access* memiliki rata-rata *Throughput* paling rendah.

4. Hasil *Packet Loss*

Delay diukur dalam satuan persen. Dengan menganalisa hasilnya, penulis mengkategorikan masing-masing hasil sesuai dengan standard TIPHON.

Tabel 5. Tabel Perbandingan *Packet Loss*

Protokol	***Jenis***	***Bandwidth***	***Packet Loss***	***Indeks***	***Kategori***
L2TP	*Site-to-Site*	5 Mbps	1.90%	3	Bagus
		10 Mbps	1.80%	3	Bagus
		15 Mbps	1.60%	3	Bagus
		20 Mbps	1.40%	3	Bagus
	Remote Access	5 Mbps	2.30%	3	Bagus
		10 Mbps	1.50%	3	Bagus
		15 Mbps	1.60%	3	Bagus
		20 Mbps	1.70%	3	Bagus
SSTP	*Site-to-Site*	5 Mbps	2.20%	3	Bagus
		10 Mbps	1.30%	3	Bagus
		15 Mbps	1.60%	3	Bagus
		20 Mbps	1.00%	3	Bagus
	Remote Access	5 Mbps	1.60%	3	Bagus
		10 Mbps	1.80%	3	Bagus
		15 Mbps	1.20%	3	Bagus
		20 Mbps	1.30%	3	Bagus

Dari hasil pengujian tersebut dapat dilihat bahwa VPN L2TP/IPsec dan SSTP jenis *Site-to-Site* dan *Remote Access* termasuk dalam kategori Bagus. Namun dapat dilihat bahwa SSTP-*Remote Access* memiliki rata-rata *Packet Loss* paling rendah, SSTP-*Site-to-Site* memiliki rata-rata *Packet Loss* paling rendah ke dua, L2TP/IPsec-*Site-to-Site* memiliki rata-rata *Packet Loss* paling tinggi kedua, dan L2TP/IPsec-*Remote Access* memiliki rata-rata *Packet Loss* paling tinggi.

Dari segi Security, L2TP menggunakan enkripsi IPsec yang terbaca sebagai paket *Encapsulating Security Payload (ESP)* di *wireshark*, sedangkan SSTP menggunakan enkripsi SSL/TLS yang terbaca sebagai paket TLSv1.2 di *wireshark*. Keduanya memiliki sistem enkripsi yang bagus sehingga paket ping yang dikirimkan oleh kedua *Host* tidak dapat dibaca oleh pihak lain melainkan hanya berupa informasi yang terenkripsi.

Tabel 6. Perbandingan Keamanan Protokol VPN

Protokol	***Jenis Paket***	***Hasil***
L2TP/IPsec	Encapsulating Security Payload (ESP)	Aman, Paket Ping Tidak Terbaca
SSTP	TLSv1.2	Aman, Paket Ping Tidak Terbaca

Skalabilitas pada protokol VPN L2TP/IPsec dan SSTP tergantung terhadap Jumlah *IP* yang tersedia pada *IP Pool* serta lisensi yang dimiliki. Dalam hal perangkat Mikrotik, lisensi *RouterOS Level* 1 dapat mendukung hingga 1 *user* L2TP dan/atau SSTP, lisensi *RouterOS Level* 3 dan *Level* 4 dapat mendukung hingga 20 *user* L2TP dan/atau SSTP, lisensi *RouterOS Level* 5 dapat mendukung hingga 500 *user* L2TP dan/atau SSTP, dan lisensi *RouterOS Level* 6 tidak memiliki limitasi *user* L2TP dan/atau SSTP.

4. SIMPULAN DAN SARAN

Berdasarkan hasil penelitian pada protokol VPN L2TP/IPsec dan SSTP dengan jenis *Site-to-Site* dan *Remote Access* dapat disimpulkan bahwa kompabilitas protokol VPN L2TP/IPsec lebih baik dikarenakan sudah tersedia secara *default* di banyak sistem operasi dibandingkan protokol VPN SSTP yang hanya tersedia secara *default* di sistem operasi *windows*. Sedangkan Indeks rata-rata QoS pada protokol VPN L2TP/IPsec lebih unggul daripada protokol VPN SSTP. Dalam hal sistem keamanan protokol VPN L2TP/IPsec dan SSTP cukup baik dikarenakan data sudah dienkripsi sehingga tidak dapat disadap oleh pihak lain, dan skalabilitas protokol VPN L2TP/IPsec dan SSTP cukup baik dikarenakan dapat melakukan penambahan jumlah *user* dengan menambah atau mengurangi jumlah IP *Address* pada IP *Pool* yang tersedia dan lisensi yang dimiliki serta kemudahan dalam konfigurasi bagi sisi *client*. Namun demikian dalam teknologi VPN masih terdapat protokol VPN seperti PPTP dan Open VPN yang dapat dijadikan perbandingan untuk penelitian berikutnya.

5. DAFTAR PUSTAKA

Aung, S. T., & Thein, T. (2020). Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks. *2020 IEEE Conference on Computer Applications (ICCA)*, 1–5.

Bui, T., Rao, S., Antikainen, M., & Aura, T. (2019). Client-Side Vulnerabilities in Commercial VPNs. *Nordic Conference on Secure IT Systems*, 103–119.

Chun, S. A., Li, A. C. Y., Toliyat, A., & Geller, J. (2020). Tracking Citizen's Concerns During COVID-19 Pandemic. *The 21st Annual International Conference on Digital Government Research*, 322–323.

Farly, K. A., Najoan, X. B. N., & Lumenta, A. S. M. (2017). Perancangan dan Implementasi VPN Server dengan menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Studi Kasus Kampus Universitas Sam Ratulangi. *Jurnal Teknik Informatika*, *11*(1).

Lukman, & Mukhlishah, A. (2020). 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). *Jurnal Teknologi Informasi*, *15*(2), 16–25.

Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model. *Symmetry*, *12*(5), 1–15.

Skendzic, A., & Kovacic, B. (2017). Open Source System OpenVPN in a Function of Virtual Private Network. *IOP Conference Series: Materials Science and Engineering*, *200*(1), 012065.

Suharto, A., & Irfan. (2019). Analisa dan Perancangan Sistem Jaringan Berbasis VLan Dengan Metode NDLC pada SMK Boedi Luhur. *Jurnal Teknologi Informasi ESIT*, *14*(3), 42–48.

Wang, C., Horby, P. W., Hayden, F. G., & Gao, G. F. (2020). A Novel Coronavirus Outbreak of Global Health Concern. *The Lancet*, *395*(10223), 470–473.

Xu, Z., & Ni, J. (2020). Research on Network Security of VPN Technology. *2020 International Conference on Information Science and Education (ICISE-IE)*, 539–542.

Yang, D., Wei, H., Zhu, Y., Li, P., & Tan, J. C. (2019). Virtual Private Cloud Based Power-Dispatching Automation System—Architecture and Application. *IEEE Transactions on Industrial Informatics*, *15*(3), 1756–1766.

Zhang, S., Li, A., Zhu, H., Sun, Q., Wang, M., & Zhang, Y. (2018). Research on the Protocols of VPN. *International Conference on Intelligent and Interactive Systems and Applications*, 554–559.