InComTech: Jurnal Telekomunikasi dan Komputer
vol.15, no.1, April 2025, 01-12
http://publikasi.mercubuana.ac.id/index.php/Incomtech
P-ISSN: 2085-4811 E-ISSN: 2579-6089

Komparasi *Quality of Service* Protokol Virtual Private Network Menggunakan PPTP, L2TP, SSTP, dan OpenVPN

Febrian Wahyu Christanto*, Cahya Krisna Angga Riski

Program Studi S1 Teknik Informatika,, Universitas Semarang
Jl. Arteri Soekarno-Hatta, Tlogosari, Kota Semarang, Jawa Tengah 50196, Indonesia
*Email Penulis Koresponden: febrian.wahyu.christanto@usm.ac.id

Abstrak **:**
Teknologi *internet* selalu berkembang serta mengalami kemajuan yang signifikan yang diikuti oleh peningkatan jumlah penggunanya. Sebuah survei APJII yang melibatkan 5.900 sampel selama periode Maret hingga 14 April 2020, sejumlah 64,8% (171,17) dari total penduduk Indonesia (264 juta jiwa) telah terhubung dengan jaringan *internet*. Perkembangan internet diikuti pula dengan perkembangan layanan keamanan seperti *Virtual Private Network* (VPN). *Virtual Private Network* (VPN) merupakan layanan jaringan dalam proses transaksi data menggunakan enkripsi antara dua atau lebih pengguna jaringan yang terdefinisi. VPN memiliki empat metode yaitu PPTP, L2TP, SSTP, dan OpenVPN. Penelitian ini akan melakukan komparasi *Quality of Service* (QoS) pada keempat metode VPN dalam pengiriman paket data. Percobaan dilakukan dengan pengiriman paket data. Pada metode PPTP dan L2TP membutuhkan waktu pengiriman data rata-rata 100 ms, sedangkan metode SSTP dan OpenVPN membutuhkan waktu rata-rata 2 ms. Nilai indeks QoS *Packet Loss* pada OpenVPN sebesar 0% dengan kategori memuaskan. Untuk hasil *Delay* rata – rata sebesar 0 ms dengan kategori memuaskan. Nilai *Jitter* 17 ms bernilai bagus, sedangkan untuk nilai *Trounghput* dari keempat metode VPN didapatkan hasil bahwa OpenVPN *Server* rata – rata mempunyai nilai sebesar 3,428 Mbps dengan kategori memuaskan. Dari data pengujian yang didapatkan hasil bahwa OpenVPN mempunyai QoS terbaik dalam pengiriman paket data di dalam VPN.

Kata Kunci*:*
Network Development Life Cycle (NDLC);
Mikrotik*;*
Virtual Private Network (VPN);
Quality of Service

Riwayat Artikel:
Diserahkan 25 September 2023
Direvisi 15 Agustus 2024
Diterima 06 Desember 2024

DOI:
10.22441/incomtech.v15i1.23250

1. PENDAHULUAN

Teknologi *internet* selalu berkembang serta mengalami kemajuan yang signifikan yang diikuti oleh peningkatan jumlah penggunanya [1] [2] [3]. Sebuah survei APJII yang melibatkan 5.900 sampel selama periode Maret hingga 14 April 2020, sejumlah 64,8% (171,17) dari total penduduk Indonesia (264 juta jiwa) telah terhubung dengan jaringan *internet*. Angka tersebut bertumbuh 10,12%. Menurut wilayah geografisnya, Jawa merupakan daerah dengan pengguna *internet* terbesar, yakni 55%. Selanjutnya Sumatera 21%, Papua 10%, dan Kalimantan 9%. Hal ini membuktikan bahwa *internet* sangat dibutuhkan masyarakat luas dan tentunya akan semakin bertambah penggunanya setiap tahun [4].

Perkembangan *internet* diikuti pula dengan perkembangan layanan keamanan seperti *Virtual Private Network* (VPN) yang merupakan teknologi yang memungkinkan terbentuknya sebuah jaringan data *private* pada jaringan publik dengan menerapkan autentikasi dan enkripsi sehingga akses terhadap jaringan tersebut hanya dapat dilakukan oleh pihak- pihak tertentu. Pada VPN terdapat banyak protokol untuk mendukung keamanan data. Salah satu protokol yang dapat digunakan untuk pengembangan VPN adalah *Internet Protocol Security* (IPSec) dan OpenSSL [5] [6] [7].

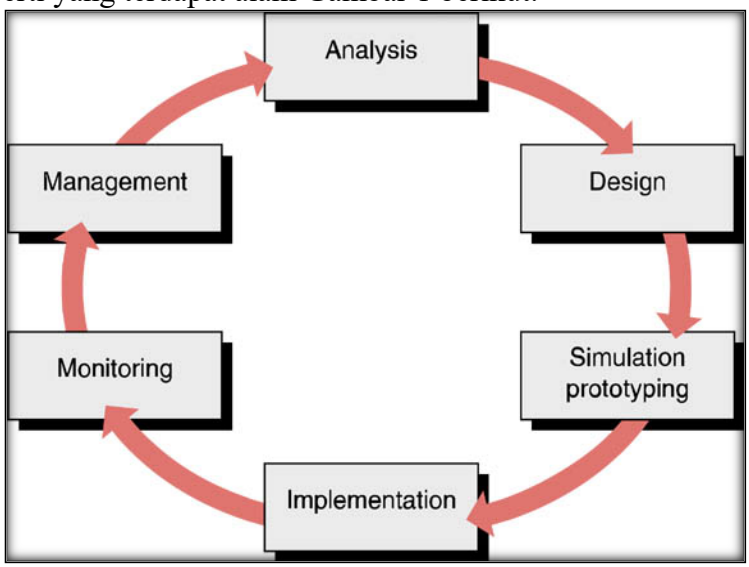
IPSec/IPv6 telah dirancang untuk memastikan privasi dan komunikasi aman *End-to-End* melalui jaringan publik. Sedangkan OpenSSL telah diimplementasikan pada *platform* apa pun untuk mengautentikasi data yang ditransfer dengan akses ke *internet* dengan menggunakan alamat IP statis atau dinamis [8] [9].

Salah satu cara untuk meminimalkan adanya serangan keamanan dari luar yaitu dengan memanfaatkan *Virtual Private Network* (VPN) [10] [11]. Penelitian yang pernah dilakukan dalam analisa perbandingan protokol VPN sebagai pedoman dalam penelitian ini antara lain adalah analisa dan perbandingan SSTP dan PPTP dengan hasil PPTP mempunyai keunggulan dalam hal QoS daripada SSTP, sedangkan SSTP unggul dalam kecepatan transfer *file* dan *download* [12]. Penggunaan algoritma *Logistic Regression, Support Vector Machine, Naïve Bayes, K-Nearest Neighbour, Random Forest* (RF) *Classifier*, dan *Gradient Boosting Tree* (GBT) *Classifier* dapat dilakukan untuk mendeteksi suatu jaringan VPN dan non VPN. Hasil dari penelitian ini membuktikan *Random Forest* (RF) *Classifier* dan *Gradient Boosting Tree* (GBT) *Classifier* mempunyai tingkat keakuratan mencapai 90% [13]. Penelitian-penelitian lainnya mengkomparasikan protokol PPTP dan L2TP dengan hasil L2TP dipadu dengan IPSec adalah solusi VPN paling komprehensif [14] [15].

State of the art yang ditawarkan dari penelitian ini adalah perbandingan *Quality of Service* (QoS) menggunakan empat protokol PPTP, L2TP, SSTP, dan OpenVPN. QoS akan mempermudah menentukan pertimbangan performa dalam penerapan jaringan VPN. Perbandingan yang digunakan untuk mengukur QoS yaitu *Throughput, Delay, Packet Loss*, dan *Jitter*. Selain itu, dilakukan juga perbandingan kecepatan transfer dan *download file* dari masing-masing protokol VPN pada Mikrotik *Router* OS dan *monitoring* perjalanan data akan dilakukan dengan *tools* Wireshark. Diharapkan dari penelitian ini dapat menjadi bahan pertimbangan *administrator* jaringan dan akademisi dalam melakukan perancangan dan implementasi VPN.

2. METODE

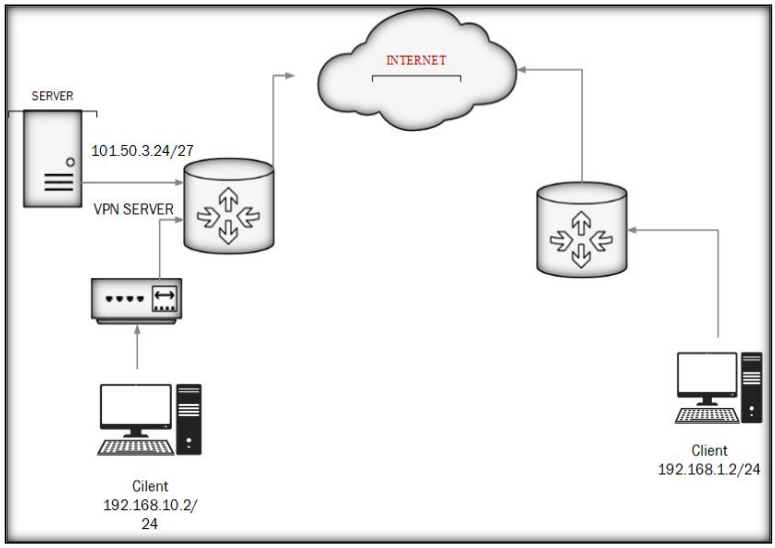
Metode penelitian yang digunakan adalah *Network Development Life Cycle* (NDLC). Metodologi berisi langkah demi langkah untuk analisis dan desain jaringan seperti yang terdapat alam Gambar 1 berikut.



Gambar 1. *Network Development Life Cycle* (NDLC) [9]

Tahap pertama pada metode ini adalah *Analysis*. Analisa dilakukan untuk mengidentifikasi yang dibutuhkan pengguna jaringan dan menganalisis kebutuhan seperti peralatan berupa perangkat *Router* Mikrotik serta perangkat lain untuk implementasi VPN.

Tahap selanjutnya adalah *Design* yang dilakukan dengan gambar topologi jaringan interkoneksi yang akan dibangun. Diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan penelitian. Topologi jaringan yang akan dibangun terdapat di dalam Gambar 2 berikut.



Gambar 2. Topologi Jaringan VPN

Selain itu desain akses data, desain tata *layout* pengkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang penelitian yang akan dibangun.

Pada tahap *Simulation Prototyping* dilakukan untuk melihat kinerja awal dari jaringan. Simulasi dari hasil analisis dari metode PPTP, L2TP, SSTP, dan OpenVPN pada *server* Mikrotik yang akan digunakan dalam implementasi penelitian ini.

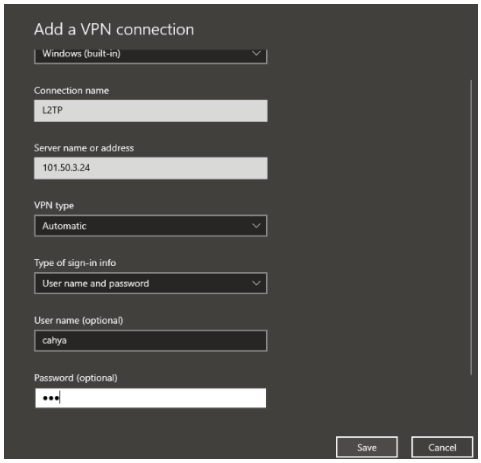
Tahap selanjutnya adalah *Implementation* yaitu tahapan menguji hasil simulasi dan memantau hasil kinerja perbandingan VPN berdasarkan performanya [16]. *Monitoring* merupakan tahapan memantau jaringan komputer dan komunikasi hasil implementasi agar berjalan sesuai dengan tujuan penelitian. Pengujian terhadap *Quality of Service* (QoS) antar protokol dan pengujian terhadap keamanan jaringan dilakukan pula dalam tahapan ini [17].

Tahapan terakhir adalah *Management* atau pengaturan. Salah satu yang menjadi perhatian khusus adalah masalah *policy* atau kebijakan yang perlu dikelola untuk mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dengan unsur *reliability* yang terjaga.

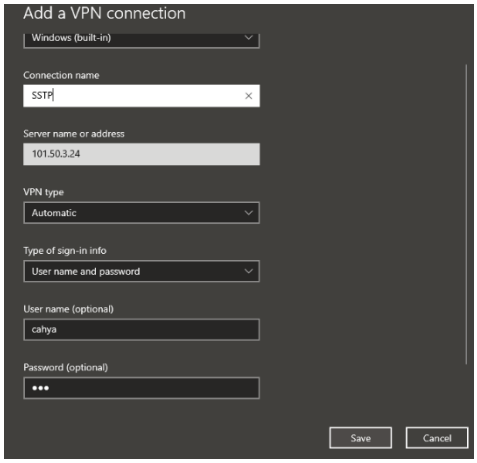
3. HASIL DAN PEMBAHASAN

Hasil dan pembahasan yang dicapai merupakan implementasi dari metode *Network Development Life Cycle* (NDLC) yang telah direncanakan. Implementasi komparasi VPN menggunakan metode PPTP, L2TP, SSTP, dan OpenVPN dilakukan untuk mendapatkan analisa perbandingan terbaik yang merupakan tujuan dalam penelitian ini. Sebelum koneksi terbentuk, maka dibutuhkan *static routing* terlebih dahulu agar jaringan lokal dapat terhubung satu sama lain dengan *internet*. Berikut dalam Gambar 3 sampai dengan Gambar 6 adalah pembentukan koneksi VPN yang dibangun dari keempat metode tersebut.

Gambar 3. Koneksi PPTP



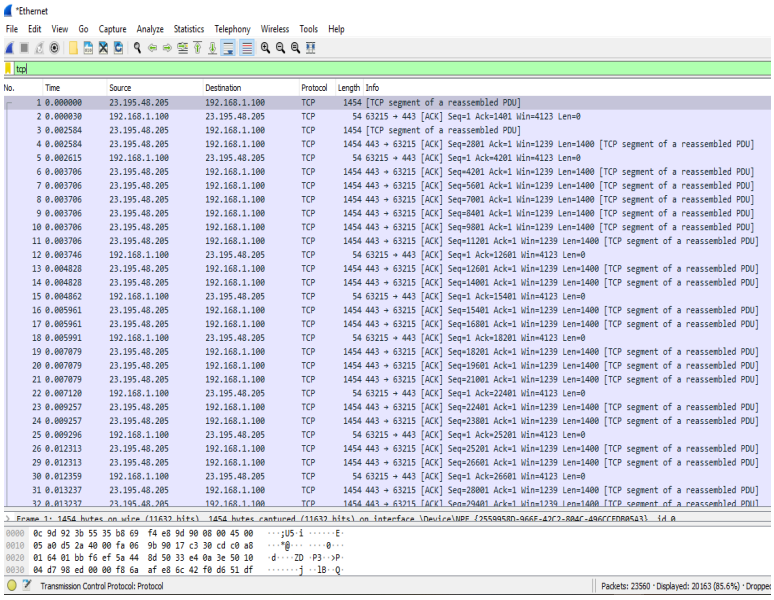
Gambar 4. Koneksi L2TP



Gambar 5. Koneksi SSTP

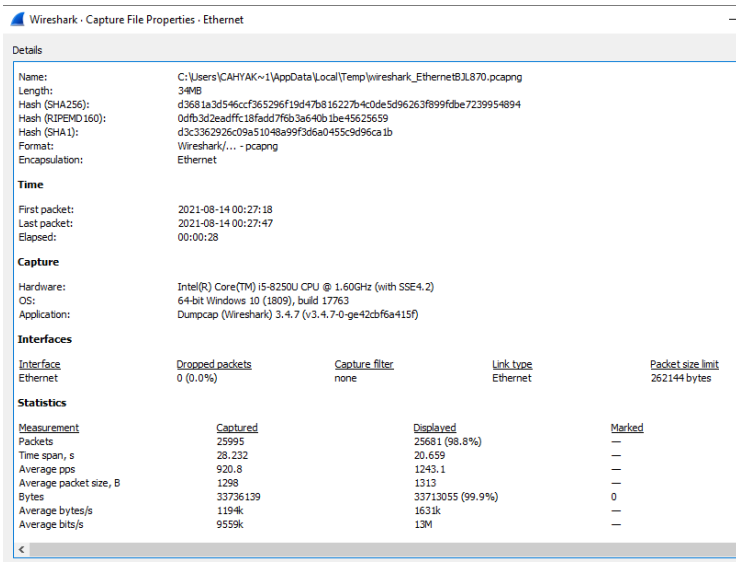
Gambar 6. Koneksi OpenVPN

Analisa akses data dilakukan menggunakan *tools monitoring* jaringan. Pengujian dilakukan sebanyak 10 kali dengan lama waktu masing-masing 15 detik (1 menit per 1 kali pengujian). Hasil pengujian terhadap akses data terdapat dalam Gambar 7 berikut.



Gambar 7. Pengujian Akses Data

Selama *streaming* pengujian untuk setiap metode VPN selalu dilakukan proses *capture file* untuk menambah *source* dalam analisis komparasi. Hal ini dilakukan agar hasil yang didapatkan nantinya dapat lebih valid sesuai dengan tujuan penelitian. Hasil *capture file* data pengujian terdapat di dalam Gambar 8 berikut.



Gambar 8. *Capture File* Data Pengujian

Pengujian VPN lainnya dilakukan pada PC *client* menggunakan 4 (empat) parameter QoS yaitu *Throughput, Delay, Packet Loss*, dan *Jitter* [3]. Hasil perhitungan rata-rata pengujian parameter QoS pada keempat metode VPN terdapat pada Tabel 1 berikut.

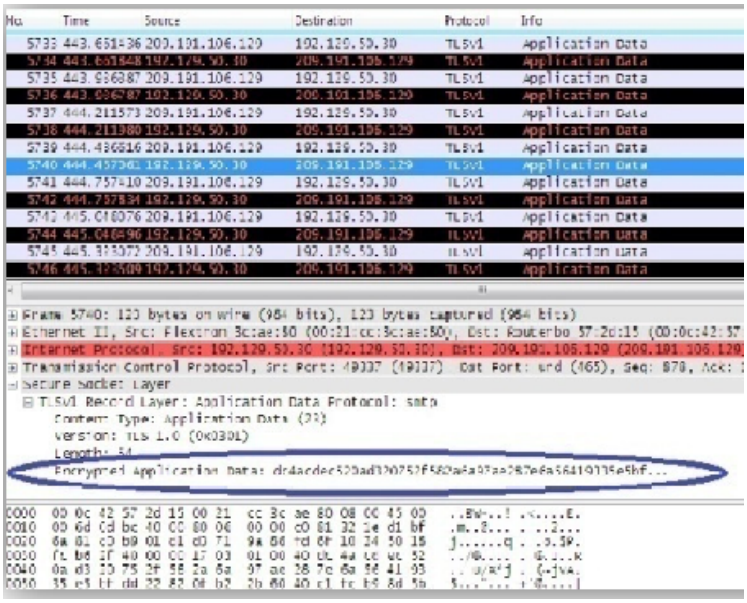
Tabel 1. Perbandingan QoS PPTP, L2TP, SSTP, dan OpenVPN

NO	PROTOKOL							
	PPTP				L2TP			
	ROUGH	DELAY	PACKET LOSS	JITTER	THROUGHPUT	DELAY	PACKET LOSS	JITTER
1	898	7.004	0.02%	11.646	2658	4.525	0.82%	4.525
2	5579	0.884	0.03%	1.748	1131	7.303	0.38%	7.303
3	1500	4.414	0.00%	8.725	1351	59.163	0.36%	110.374
4	3567	1.703	0.00%	3.349	1689	4.705	0.37%	8.896
5	2180	2.7	0.49%	5.17	805	9.303	1.41%	18.16
6	5853	0.924	0.01%	4.296	1169	6.548	0.68%	27.686
7	565	11.278	0.00%	23.373	524	14.042	0.94%	5.111
8	3613	1.591	0.02%	118.026	2623	2.75	0.66%	12.205
9	3957	1.229	0.03%	29.843	1125	6.248	0.25%	18.049
10	4039	1.396	0.00%	14.094	852	9.223	0.19%	15.849
JML	31751	33	0.006	220	13926	124	0.061	228
RATA	3428	3	0	23	1252	13	0	25

	PROTOKOL							
	SSTP				Open VPN			
NO	THROUGHPUT	DELAY	PACKET LOSS	JITTER	THROUGHPUT	DELAY	PACKET LOSS	JITTER
1	1093	5.132	0.22%	7.303	3207	0.01	0%	23.9
2	1770	24.312	0.38%	110.374	1689	0.12	0%	22.533
3	1499	2.811	0.36%	8.896	805	0.01	0%	12.654
4	1870	11.013	0.37%	18.16	1169	0.01	0%	18.2
5	1138	9.728	1.41%	12.139	1544	0.01	0%	17.2
6	1544	6.882	0.60%	12.783	259	0.01	0%	9.3
7	259	4.521	0.75%	22.686	2548	0.01	0%	20.3
8	2548	4.997	1.75%	5.111	677	0.01	0%	10.4
9	677	4.287	0.70%	12.205	5853	0.05	0%	28.3
10	833	6.756	0.68%	16.049	565	0.01	0%	10.1
JML	13230	80	0.072	226	18315	0	0	172.887
RATA	1349	8	0	24	1679	0	0	17

Perbandingan QoS pada Tabel 1 menjelaskan perhitungan metode-metode VPN dengan standar perhitungan TIPHON. Kondisi *Throughput* dari masing-masing protokol menunjukkan perbedaan, yakni PPTP 3428 kbps, L2TP 1252kbps, SSTP 1349 kbps, dan OpenVPN 1679 kbps. Hal ini menunjukkan bahwa *Throughput* PPTP lebih baik dibandingkan dengan *Throughput* metode lainnya karena *Throughput* PPTP lebih besar. Nilai rata-rata *Delay* dari PPTP berjumlah 3 ms, L2TP 13 ms, SSTP 8ms, dan sedangkan nilai rata-rata *Delay* dari OpenVPN berjumlah 0 ms. Metode OpenVPN masuk dalam kategori *latency* "sangat bagus". Maka, dapat diketahui bahwa *Delay* dari OpenVPN lebih baik dibanding dari metode VPN lainnya karena nilai *Delay* OpenVPN lebih kecil. *Paket Loss* keempat metode masuk dalam indeks 4, yaitu "*perfect"*. Nilai *Packet Loss* dari PPTP sebanyak 0.006%, L2TP sebanyak 0.061%, SSTP adalah sebanyak 0.72%, sedangkan nilai *Packet Loss* dari OpenVPN sebanyak 0%. Hal ini berarti *Packet Loss* Protokol OpenVPN lebih baik karena nilai *Packet Loss* OpenVPN lebih kecil. Kondisi *Jitter* dari masing-masing protokol menunjukkan perbedaan yang tidak terlalu signifikan. Keempat metode VPN masuk kedalam indeks 3 "bagus" dengan nilai PPTP 23 ms, L2TP 25 ms, SSTP 23 ms, dan OpenVPN dengan 17 ms. Dari nilai parameter hasil pengujian QoS tersebut didapatkan data bahwa metode OpenVPN mempunyai QoS terhadap akses data yang lebih efektif dibandingkan metode VPN lainnya.

Pengujian terhadap *packet sniffing* atau besar kecilnya resiko atas penyadapan data diimplementasikan pula dalam penelitian ini. Hal ini dilakukan dengan cara melakukan *sniffing* dari luar jaringan dan dilakukan *monitoring* menggunakan *tools* jaringan.

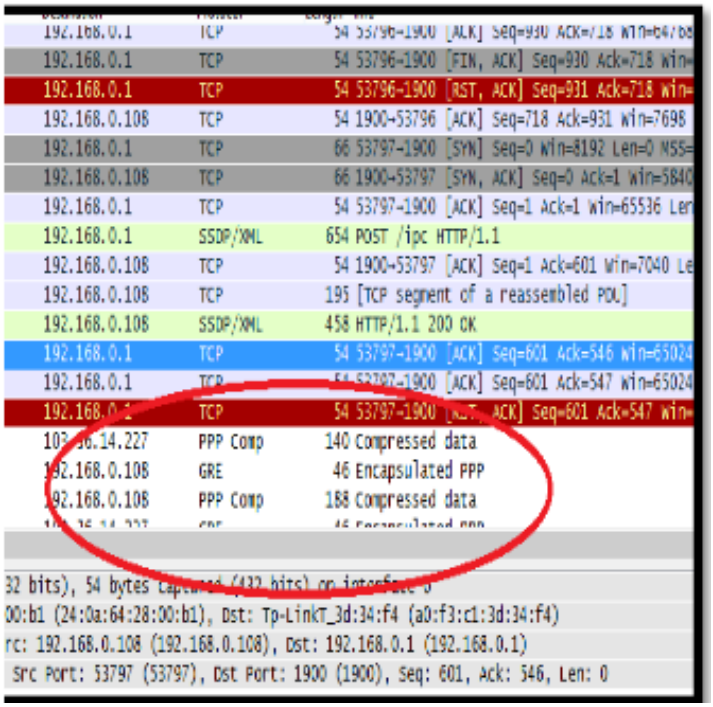


Gambar 9. *Packet Sniffing* Terhadap PPTP

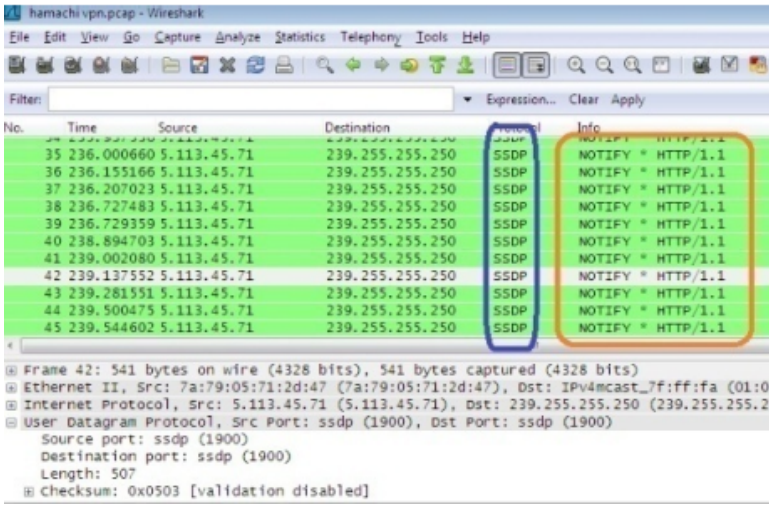
PC *client* pada Gambar 9 mencoba melakukan koneksi ke alamat IP 209.191.106.129, sedangkan pada kolom protokol yang terlihat adalah protokol TLSv1 (*Transport Layer Security version* 1.0). TLS merupakan bagian dari protokol SSL (*Secure Socket Layer*) dan pada hasil tersebut terlihat bahwa data terenkripsi (*Encrypted Application Data*). Sedangkan pada Gambar 10 dilakukan proses *packet sniffing* pada metode L2TP yang hanya menunjukkan aktivitas *tunnel*

VPN hal itu ditunjukkan pada kolom info yaitu *Encapsulated* PPP dan *Compressed* Data sehingga proses *sniffing* berikutnya menggunakan fasilitas *follow* TCP *stream* sudah tidak dapat dilakukan.

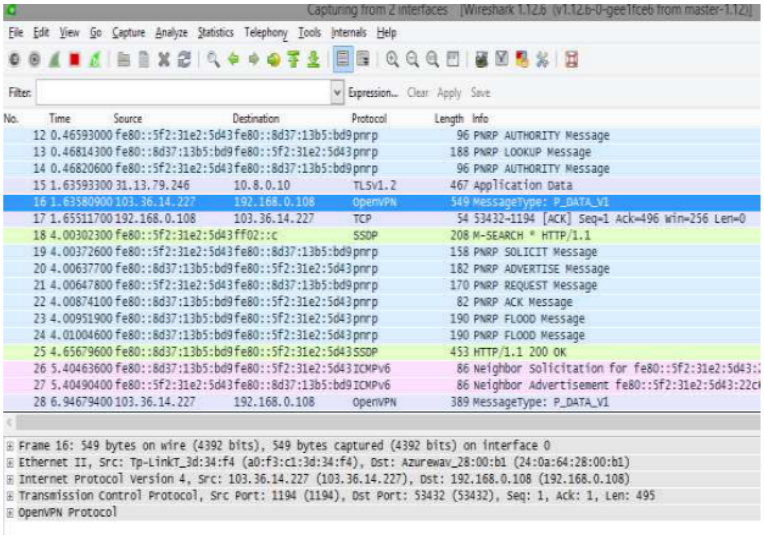
Pada hasil pengujian VPN dengan SSTP pada Gambar 11, tidak dapat dilihat informasi pertukaran data yang dilakukan antara *server* dan *client*. Selain itu yang muncul adalah protokol SSDP (*Simple Service Dicovery Protocol*). Protokol SSDP dapat menemukan perangkat *plug and play* dengan UPnP (*Universal Plug and Play*). SSDP menggunakan alamat *unicast* dan *multicast* (239.255.255.250). SSDP adalah seperti protokol HTTP (*Hypertext Transfer Protocol*) dan bekerja dengan metode *Notify* dan *M-Search*. SSDP menggunakan metode *Notify* HTTP untuk mengumumkan pembentukan atau penarikan informasi ke grup *multicast*.



Gambar 10. *Packet Sniffing* Terhadap L2TP

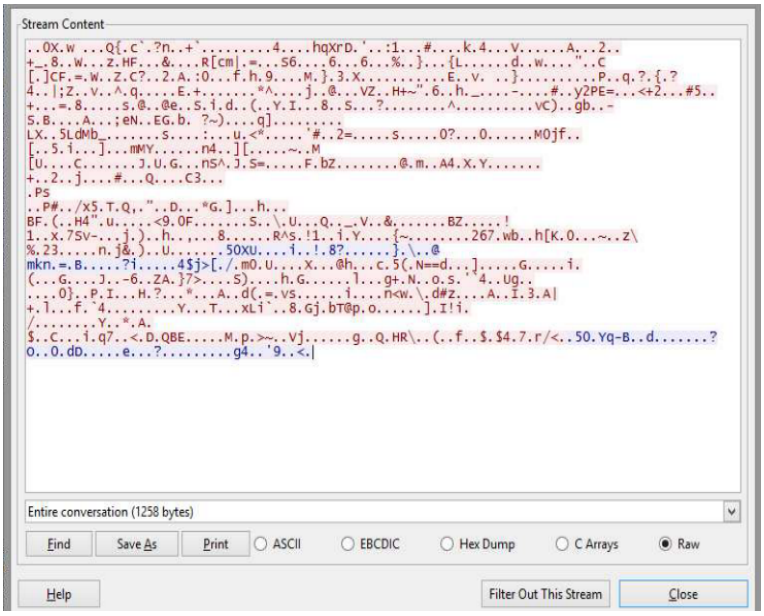


Gambar 11. *Packet Sniffing* Terhadap SSTP



Gambar 12. *Packet Sniffing* Terhadap OpenVPN

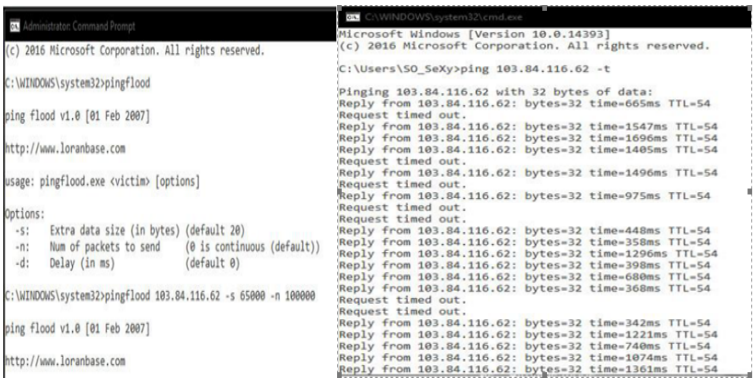
Pengujian *sniffing* pada Gambar 12 dilakukan pula pada metode OpenVPN Client yang mencoba untuk terhubung dengan VPN *Server*. Hasil *sniffing* pada jaringan OpenVPN terlihat dengan jelas kegiatan OpenVPN dengan ditunjukkan bagian protokol bertuliskan OpenVPN, sedangkan hasil *sniffing* tidak jelas atau acak seperti menunjukkan enkripsi pada OpenVPN berjalan dengan baik seperti yang terdapat di dalam Gambar 13 dibawah ini.



Gambar 13. *Packet Sniffing* Terhadap OpenVPN

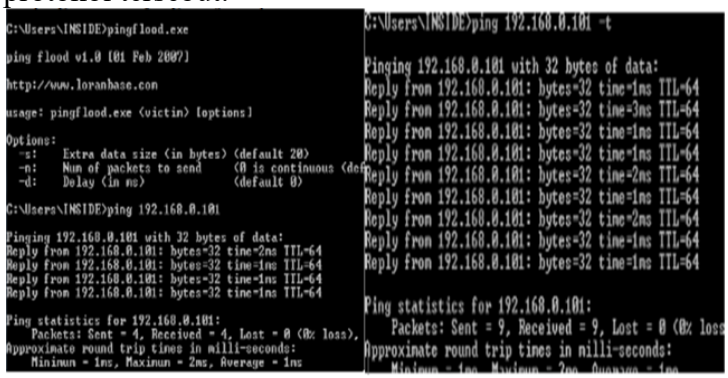
Dari pengujian *sniffing* terhadap keempat metode VPN didapatkan hasil bahwa metode PPTP dan L2TP memiliki kesamaan yaitu masih bisa dilihat dari paket data dan alamat IP yang dikirimkan. Sedangkan untuk metode SSTP pengiriman data lebih baik karena di dukung oleh protokol SSDP untuk keamanan dalam proses pengiriman data. Metode OpenVPN memiliki tingkat enkripsi yang paling baik dengan otentikasi menggunakan sertifikat.

Komparasi metode VPN dilakukan kembali dengan memberikan serangan *Denial of Service* (DoS) terhadap keempat metode tersebut. Hasil dari pengujian terdapat dalam Gambar 14 berikut.



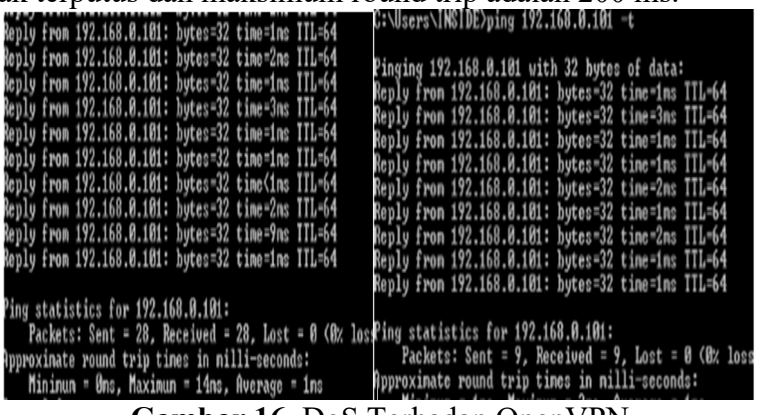
Gambar 14. DoS Terhadap PPTP dan L2TP

Berdasarkan percobaan pada Gambar 14 diatas dengan mengirimakan paket data sebesar 25kb dari 1000 paket ke *Server* yang mengakibatkan aktivitas *Server* menjadi lambat sehingga banyak terjadi Request Time Out. Saat percobaan tersebut dijalankan, waktu pengiriman data berada di antara angka 100 ms sampai 300 ms untuk kedua protokol tersebut.



Gambar 15. DoS Terhadap SSTP

Setelah dilakukan pengujian serangan DoS pada SSTP seperti pada Gambar 15 dengan mengirimkan 1000 paket data sebesar 25 kb dan didapatkan hasil bahwa jaringan tidak terputus dan maksimum round trip adalah 200 ms.



Gambar 16. DoS Terhadap OpenVPN

Pengujian yang dilakukan pada Gambar 16 adalah dengan membanjiri server VPN yang menggunakan OpenVPN dengan 1000 paket data sebesar masing-masing 25 kb. Data yang diperoleh untuk perjalanan pulang pergi paket rata-rata masih dalam batas wajar.

Percobaan DoS pada metode PPTP dan L2TP didapatkan untuk pengiriman paket data cepat dengan waktu 100 ms, sedangkan pada metode SSTP memerlukan waktu 200ms, dan untuk metode OpenVPN memerlukan waktu sebesar 100 ms untuk 1000 paket yang dikirimkan. Percobaan DoS keempat metode tersebut mempunyai perbandingan waktu tipis dalam mengirimkan data dari dan ke *server*.

4. KESIMPULAN

Penelitian komparasi *Quality of Service* (QoS) metode VPN yang telah dilakukan mendapatkan hasil bahwa OpenVPN lebih baik dari metode VPN yang lainnya. Dari pengujian *Troughput* yaitu kecepatan transfer *file* memang kecepatan OpenVPN yang hanya mencapai 1.679 kbps atau lebih rendah 48% daripada PPTP yang mencapai 3.428 kbps, tetapi dalam pengujian *Delay, Packet Loss*, dan *Jitter* OpenVPN masuk dalam indeks 4 yaitu *"perfect"*. Secara berturut OpenVPN menghasilkan 0 ms *Delay*, 0% *Packet Loss*, dan 17 ms *Jitter*. Pengujian keamanan jaringan terhadap serangan *sniffing* menghasilkan bahwa OpenVPN memiliki tingkat enkripsi yang lebih baik dengan otentikasi menggunakan sertifikat keamanan. Pengujian lain yang dilakukan yaitu pengujian serangan *Denial of Service* (DoS) dengan membanjiri 1000 paket yang masing-masing paket sebesar 25 kb ke *server*, OpenVPN hanya membutuhkan waktu 100 ms dalam mengirimkan data walau dalam keadaan jaringan yang sedang diserang oleh DoS.

Penelitian selanjutnya akan lebih baik ditambahkan peningkatan sistem keamanan VPN dengan mengaktifkan fitur IPSec yang terdapat pada *router* sehingga lalu linta data akan lebih terjamin, kerahasiaan, dan keamanannya karena penerapan keamanan berlapis pada jaringan VPN.

REFERENSI

[1] J. L. Putra, L. Indriyani, and Y. Angraini, "Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna," *IJCIT (Indonesian J. Comput. Inf. Technol.*, vol. 3, no. 2, pp. 260–267, 2018.

[2] R. Saibi, Kurniabudi, and A. Rahim, "Analisa dan Perancangan Jaringan Komputer Menggunakan Metode Virtual Local Area Network (VLAN) (Studi Kasus: Diskominfo Provinsi Jambi)," *J. Ilm. Media Process.*, vol. 9, no. 2, pp. 185–195, 2014.

[3] S. Surono, F. W. Christanto, and C. Maulana, "Uji Komparasi Quality of Service Antara Metode Routing dan VLAN pada Distribusi Paket Data Jaringan Internet," *JPRT (Pengembangan Rekayasa dan Teknol.*, vol. 16, no. 2, pp. 183–190, 2020.

[4] Y. Pratomo, "Survei Pengguna Internet APJII 2019-Q2 2020: Ada Kenaikan 25,5 Juta Pengguna Internet Baru di RI," *Buletin APJII*, vol. 74, Jakarta, pp. 1–10, Nov-2019.

[5] I. Melyana and T. Indriyani, "Analisa Quality Of Service Dan Implementasi Voice Over Internet Protocol Dengan Menggunakan IPSEC VPN," *Integer J.*, vol. 1, no. 2, pp. 53–66, 2016.

[6] A. H. M. Permana, N. Widiyasono, and A. Rahmatulloh, "Perbandingan Algoritma Pada Virtual Private Network Ipsec Terhadap Kecepatan Data Transfer," *Sist. J. Sist. Inf.*, vol. 9, no. 2, pp. 259–273, 2020, doi: 10.32520/stmsi.v9i2.713.

[7] D. E. Kurniawan, H. Arif, N. Nelmiawati, and A. H. Tohari, "Implementation and analysis ipsec-vpn on cisco asa firewall using gns3 network simulator," in *1st International Conference on Advance and Scientific Innovation (ICASI)*, 2019, pp. 1–9, doi: 10.1088/1742-

6596/1175/1/012031.

[8] M. Juma, A. A. Monem, and K. Shaalan, "Hybrid End-to-End VPN Security Approach for Smart IoT Objects," *J. Netw. Comput. Appl.*, vol. 158, no. March, pp. 1–14, 2020, doi: 10.1016/j.jnca.2020.102598.

[9] Sugiyatno and P. D. Atika, "Virtual Private Network (VPN) Secure Socket Tunneling Protocol (SSTP) Menggunakan Raspberry Pi," *Inf. Syst. Educ. Prof.*, vol. 2, no. 2, pp. 155–166, 2018.

[10] C. Yin, "Application of Virtual Private Network Technology in University Network Information Security," *Journal of Physics: Conference Series*, *The 5th International Statistics Competition for Engineering Students (ISCE 2023)*, pp. 1-6, 2021.

[11] M. O. Akinsanya, C. C. Ekechi, and C. D. Okeke, "Virtual Private Networks (VPN): a Conceptual Review of Security Protocols and Their Application in Modern Networks," *Engineering Science & Technology J.*, vol. 5, no. 4, pp. 1452–1472, 2024.

[12] D. C. G. R. Saijuna, A. R. Himamunanto, and J. Jatmika, "Analisis Perbandingan Performa SSTP dan PPTP pada VPN," *J. Sains Dan ...*, vol. 1, no. 2, pp. 1–15, 2017, doi: https://doi.org/10.1233/jurnal%20infact.v1i2.191.

[13] S. Bagui, X. Fang, E. Kalaimannan, S. C. Bagui, and J. Sheehan, "Comparison of machine-learning algorithms for classification of VPN network traffic flow using time-related features," *J. Cyber Secur. Technol.*, vol. 1, no. 2, pp. 108–126, 2017, doi: 10.1080/23742917.2017.1321891.

[14] N. Musyaffa and M. Ryansyah, "Implementation of VPN Using Router MikroTik at Al-Basyariah Education Foundation Bogor," *J. Tek. Inform. C.I.T Medicom*, vol. 12, no. 2, pp. 49–55, 2020.

[15] P. Arora, P. R. Vemuganti, and P. Allani, "Comparison of VPN Protocols – IPSec , PPTP , and L2TP," Virginia, 2021.

[16] T. Rahman, S. Sumarna, and H. Nurdin, "Analisis Performa RouterOS MikroTik pada Jaringan Internet," *J. INOVTEK POLBENG - SERI Inform.*, vol. 5, no. 1, pp. 178–192, 2020, doi: 10.35314/isi.v5i1.1308.

[17] M. F. Adriant and I. Mardianto, "Implementasi Wireshark Untuk Penyadapan (Sniffing) Paket Data Jaringan," in *Seminar Nasional Cendekiawan*, 2015, pp. 224–228.