Analisis QoS Tunneling pada Virtual Conference

Jonathan Joseph Liando[1], Indrastanti Ratna Widiasari[2]

[1,2]Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Satya Wacana, Jl. Dr. O. Notohamidjodjo Blotongan, Sidorejo, Kota Salatiga
[1]liandonathan@gmail.com
[2]indrastanti@gmail.com

Abstrak

Komunikasi menjadi bagian dari teknologi informasi yang mengalami banyak perubahan dan penyesuaian terutama semenjak pandemi COVID-19. Media komunikasi yang sering digunakan pun pada situasi ini seperti Zoom dan Google Meet juga mengalami hal serupa. Salah satu hal yang sering terjadi ketika menggunakan layanan *Virtual Conference* adalah adanya ketidakstabilan jaringan. Penelitian ini mencoba menggunakan *Tunneling* sebagai penyelesaian terhadap masalah ketidakstabilan jaringan karena *Tunneling* menggunakan jalur yang terisolasi. untuk memastikan stabilnya jaringan dalam sebuah aplikasi *Virtual Conference* diperlukan analisis untuk melihat performa jaringan yang dipakai. Penelitian ini menggunakan QoS sebagai metode untuk mengukur kestabilan performa dari suatu jaringan dengan melihat empat indikator, *Throughput, Packet loss, Delay, jitter*. Dari hasil perhitungan yang dilakukan menggunakan tiga jenis *Tunneling Protocol* yaitu GRE, IPSEC, dan PPTP sebagai perbandingan. Dari hasil perhitungan yang dilakukan menggunakan tiga jenis Tunneling Protokol yaitu GRE, IPSEC, dan PPTP sebagai perbandingan. Kesimpulan yang didapatkan adalah Tunneling Protokol PPTP menjadi *Tunneling* Protokol yang bagus untuk dialukannya *Tunneling* pada aplikasi *Virtual Conference* dengan nilai Throughput Google Meet 92.58Kbps dan Zoom 75.5Kbps, Packet Loss Google Meet 0.19% dan Zoom 0.13%, delay Google Meet 0.009s dan Zoom 0.008s, Jitter Google Meet 0.8s dan Zoom 0.008s.

Kata kunci: Tunneling, QoS, GRE, IPSEC, PPTP

Abstract

As one part in information technology, communication always going through a lot of changes even since COVID-19 began. A few platform such Zoom, Google meet which we often use also had a lot of changes. One of problem that we often face is network instability. In this article Tunneling being used to solve the problem which is network instability because tunneling using isolated track to transfer packet. To ensure the network stability using tunneling in virtual conference application analysis is required. this article uses QoS as a method to measure the stability of a network performance by looking at four indicator which is; Throughput, Packet loss, Delay and Jitter. Fourth indicator is testing in three different Tunneling Protocol which is GRE, IPSEC, PPT. the result is PPTP being the most stable Tunneling Protocol to run a virtual Meeting app. The result is Throughput Google Meet 92.58Kbps and Zoom 75.5Kbps, Packet Loss Google Meet 0.19% and Zoom 0.13%, delay Google Meet 0.009s and Zoom 0.008s, Jitter Google Meet 0.8s and Zoom 0.008s.

***Keyword**: Tunneling, QoS, GRE, IPSEC, PPTP*

1. PENDAHULUAN

COVID-19 mulai masuk ke Indonesia pada tanggal 12 Maret 2020, hal ini membuat masyarakat Indonesia harus beradaptasi dengan keadaan yang terjadi. Salah satu bentuk penyesuaian yang dilakukan adalah dengan melakukan kegiatan dari rumah atau *Work From home* (WFH) [1]. Bidang pendidikan menjadi salah satu bidang yang perubahannya sangat

DOI: 10.34128/jsi.v8i2.402 *Received:11 Mei 2022*
Accepted: 2 September 2022

dirasakan. Hal ini terlihat dari banyaknya artikel yang membahas tentang kualitas pembelajaran daring, analisis kepuasan peserta didik dalam mengikuti pembelajaran daring. [2]–[4].
masalah yang sering terjadi ketika menggunakan aplikasi virtual conference adalah adanya ketidakstabilan dalam performa jaringan yang digunakan [5]. Salah satu cara yang bisa digunakan untuk mengatasi masalah tersebut dengan menggunakan *tunneling* [6]. *Tunneling* adalah salah satu protokol jaringan yang digunakan untuk melakukan transfer data tanpa adanya hambatan antara jaringan satu dan lainnya [7]. Beberapa protokol jaringan yang sering digunakan di antaranya adalah *Generic Routing Encapsulation* (GRE)*, Internet Protocol Security* (IPSec), *Point to Point* Protocol (PPTP)[8]. GRE *Tunneling* merupakan sebuah *tunneling protocol* yang dikembangkan oleh Cisco yang memiliki kemampuan untuk membawa berbagai jenis protokol beralamatkan komunikasi selain paket yang memiliki alamat IP pada jaringan *point to point* [9], [10]. IPsec merupakan protokol yang pengamanan transmisi datagram yang bersifat *end to end* dalam sebuah *internetwork* berbasis TCP/IP. IPsec memiliki cara kerja melakukan enkripsi data pada lapisan yang sama dengan paket TCP kemudian menggunakan teknik tunneling untuk mentransmisikan paket tersebut melalui jaringan publik [11], [12]. PPPT merupakan *tunneling protocol* yang memungkinkan mengirim dan menerima data berbasis *client server.* Pada penerapannya terdapat beberapa hal yang harus dilakukan pada saat melakukan konfigurasi PPTP seperti menentukan *network security protocol* kemudian data tersebut ditransmisi dan dienkripsi menggunakan *Microsoft Point-to-point Encryption* (MPPE) [13], [14].

Beberapa penelitian yang telah dilakukan memiliki katiannya dengan penelitian ini seperti pada penelitian Ikhwan dan Amalina, [15] mencoba membandingkan PPPT dan *Layer Two Tunneling Protocol* (L2TP) dengan tujuan mengetahui performa PPTP dan L2TP jika diterapkan untuk jalur layanan *File Transfer Protocol* (FTP). Dalam pembahasannya setiap topologi akan diberikan beban dengan jumlah tertentu untuk diukur performanya menggunakan parameter QoS. Kesimpulan yang didapat adalah PPTP bisa menjadi solusi yang tepat untuk menggantikan L2TP.

Penelitian selanjutnya Arifin dan Wardhani, [10] mencoba mengimplementasikan GRE *Tunnel* pada Perangkat Metro-E Nokia. Dalam pembahasannya penelitian ini menggunakan topologi Ring dan Mesh sebagai model penelitian. Kesimpulan yang didapat adalah implementasi GRE pada perangkat Nokia berjalan dengan baik karena memiliki nilai *Throughput* yang tinggi dan total *delay* yang rendah.

Penelitian selanjutnya Firmansyah et al, [16], menerapkan *Protocol Internet Security Association and Key Management Protocol (*ISAKMP) ke dalam IPSec VPN yang digunakan untuk menyelesaikan masalah keamanan dan keutuhan paket yang ditransmisikan melalui jaringan *tunneling*. Kesimpulan dari penelitian yang dilakukan adalah penerapan *Protocol* ISAKMP berjalan dengan baik, performa yang dihasilkan juga memiliki nilai *Time To Live* yang lebih rendah.

Penelitian selanjutnya Yusril dan Setyawan, [17] membahas tentang penerapan *tunneling* untuk melihat kinerja HTTP *dan Hypertext Transfer Protocol Secure* (HTTPS) pada *video streaming.* Hasil penelitian yang didapatkan setelah mengukur performa protokol HTTP dan HTTPS menggunakan empat parameter QoS throughput, jitter, packet loss, delay adalah protokol HTTP memiliki nilai yang tinggi pada parameter delay dibandingkan HTTPS yaitu 24.17s.

Penelitian ini bertujuan untuk mencoba menerapkan *tunneling protocol* sebagai jalur alternatif untuk menggunakan aplikasi *virtual conference* yang kemudian akan dilakukan analisis QOS untuk mengukur performa setiap *tunneling protocol* yang diuji coba.

Adapun pembeda Penelitian dan penelitian yang lain. Yaitu belum ada penelitian yang membandingkan performa GRE, IPSEC dan PPTP sebagai tunneling protocol pada aplikasi

virtual conference. Selain itu beberapa referensi yang terdapat dalam penelitian fokus ke perbandingan antara *tunneling protocol*, atau menerapkan *tunneling protocol* ke dalam studi kasus yang dikaji. Hal tersebut yang menjadi pembeda dan kenapa penelitian ini dilakukan.

2. TINJAUAN PUSTAKA

2.1 Quality of Service

Quality of Service (QoS) digunakan untuk mengukur suatu jaringan apakah berjalan dengan baik atau tidak dengan melihat nilai dari empat parameter yang ada yaitu *throughput, packet loss, delay, jitter* [18]. Adapun perhitungan dan standar kategori menurut *Telecommunication and Internet Protocol Harmonization Over Network* (TIPHON) yang tersedia pada tabel 1 – 4 dan pada persamaan 1 – 4.

Tabel 1. Throughput

Kategori	*Throughput* (bps)
Sangat Bagus	100
Bagus	75
Sedang	50
Jelek	25

$$Throughput = \frac{\text{Jumlah Paket data yang dikirm}}{\text{waktu pengiriman data}} \quad (1)$$

Throughput adalah kecepatan transfer data yang diukur dalam satuan *bit per second* (bps). Throughput didapatkan dengan cara membagi jumlah paket yang masuk dengan durasi pengukuran yang dilakukan[18]. Hasil yang didapatkan kemudian dicocokkan dengan kategori berdasarkan standar TIPHON pada tabel 1. Jika hasil yang diperolah adalah 122bps maka nilai Throughput yang diperoleh adalah sangat bagus.

Tabel 2. Packet Loss

Kategori	*Packet loss*
Sangat Bagus	0%
Bagus	3%
Sedang	15%
Jelek	25%

$$Packet\ loss = \frac{(\text{paket dikirim} - \text{paket diterima})}{\text{paket dikirim}} \times 100\% \quad (2)$$

Packet loss merupakan jumlah total paket yang tidak sampai ke destination[19]. Perhitungan Packet Loss membutuhkan 2 jenis data, yaitu paket yang dikirim dan paket yang diterima. Kedua data tersebut dapat ditemukan dengan melihat isi paket tcp.analysis.lost_segment. Sama seperti Throughput hasil yang didapatkan kemudian dicocokkan dengan tabel 2.

Tabel 3. Delay

Kategori	*Delay (*ms)
Sangat Bagus	<150

Bagus	150 – 300
Sedang	300 – 450
Jelek	>450

$$Delay = \frac{\text{Total delay}}{\text{Total paket yang diterima}} \quad (3)$$

Delay merupakan total rata–rata waktu yang diperlukan paket dari *source* menuju *destination* yang didapatkan dengan mengurangi total jumlah waktu untuk setiap paket yang dikirimkan [18]. Hasil perhitungan tersebut kemudian dicocokkan hasilnya dicocokkan dengan tabel 3.

Tabel 4. Jitter

Kategori	***Jitter* (ms)**
Sangat Bagus	0
Bagus	0 – 75
Sedang	75 – 125
Jelek3.	125 – 225

$$Jitter = \frac{\text{Total variasi delay}}{\text{Total paket yang diterima}-1} \quad (4)$$

Jitter merupakan variasi *delay* selama transmisi paket berlangsung[18]. Jitter Sama seperti delay, diperlukan nilai total untuk dapat melakukan perhitungan jitter, nilai yang diperlukan total variasi delay yang bisa didapatkan dengan mengurangi nilai keseluruhan delay dua dengan nilai keseluruhan delay kemudian dibagi dengan total paket yang diterima.

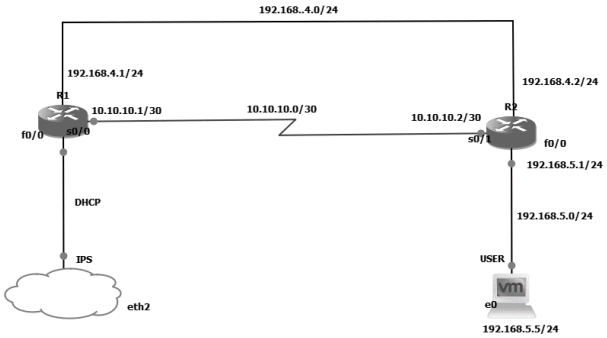
3. METODE PENELITIAN

Terdapat beberapa tahapan yang dilakukan agar penelitian ini dapat berjalan dengan baik. Berikut tahapan penelitian yang dilakukan

Gambar 1. Tahapan Penelitian

3.1 Perancangan, pembuatan topologi dan konfigurasi tunneling

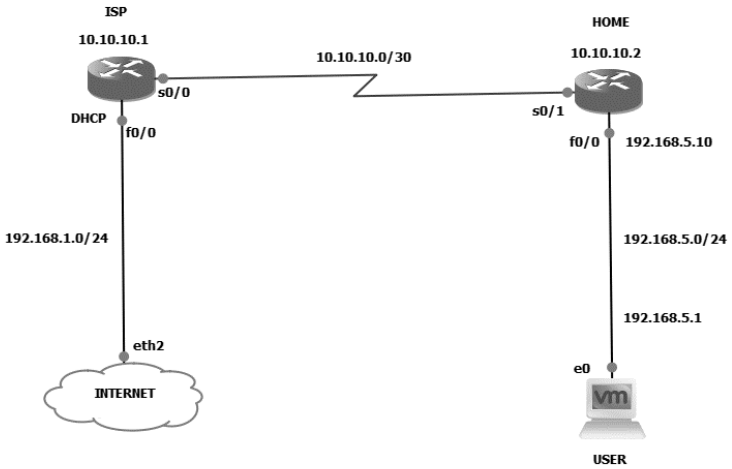
topologi jaringan dibuat menggunakan aplikasi emulator *Graphical Network Simulator* 3 (GNS 3) untuk melakukan simulasi jaringan yang terhubung dengan *Virtual Machine*



Workstation (VMware) 16. Masing – masing protokol memiliki topologi sendiri seperti pada Gambar 2 – Gambar 4.

Gambar 2. Topologi Protokol GRE Tunneling

Pada gambar 2, terdapat User yang terhubung dengan ISP melalui *router* R2 menggunakan IP 192.168.5.0/24. Kemudian pada *Router* terdapat percabangan jalur yaitu jalur serial yang menggunakan IP 10.10.10.0/30 dan jalur *Tunnel* yang menggunakan IP 192.168.4.0/24. *Router* R1 terhubung dengan ISP menggunakan IP DHCP. Protokol *Routing* yang digunakan adalah OSPF dengan alamat jaringan yang dikonfigurasi adalah 192.168.4.0/24 yang merupakan alamat jaringan *tunnel* selanjutnya melakukan konfigurasi NAT untuk menghubungkan internet dengan jaringan virtual yang dibuat di dalam GNS 3. Yang terakhir adalah melakukan konfigurasi GRE tunneling pada topologi tersebut

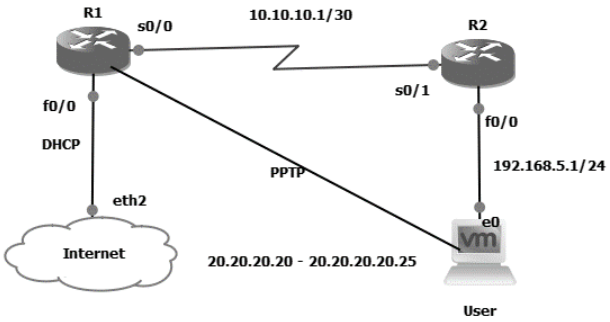


Gambar 3. Topologi Protokol IPSEC

Pada gambar 3, User terhubung dengan Router HOME dengan IP 192.168.5.0/24 dilanjutkan dengan kedua router yang terhubung dengan IP 10.10.10.0/30. *Router* ISP terhubung dengan INTERNET menggunakan IP 192.168.1.0/24. Protokol *Routing* yang digunakan adalah OSPF dengan alamat jaringan yang dikonfigurasi adalah 10.10.10.0/30 yang merupakan alamat jaringan *serial* selanjutnya melakukan konfigurasi NAT untuk menghubungkan internet dengan jaringan virtual yang dibuat di dalam GNS 3. Setelah itu barulah konfigurasi IPsec untuk topologi protokol IPsec dimulai. Dalam penerapannya IPSEC dibagi menjadi 2, yaitu IPSEC yang menggunakan

p-ISSN: 2460-173X
e-ISSN: 2598-5841

Transport mode, atau *Tunneling mode*, penelitian menggunakan transport mode. *Transport mode* dipilih karena memiliki proses enkripsi yang lebih sedikit dibandingkan *Tunneling mode.*



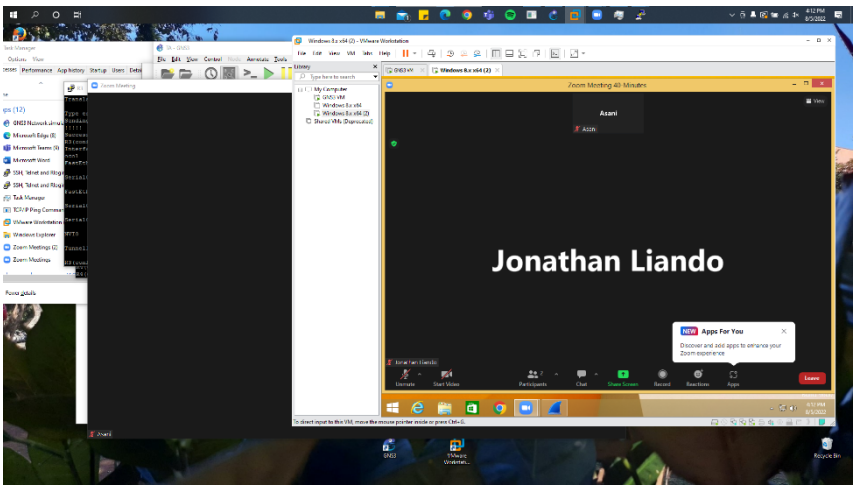
Penelitian ini menggunakan OSPF sebagai protokol *routing.* OSPF dipilih karena memiliki kemampuan untuk menentukan jalur tercepat untuk mengirimkan paket dari pengirim ke penerima.

Gambar 4. Topologi Protokol PPTP

Pada gambar 4, user terhubung dengan R2 menggunakan alamat 192.168.5.1/24. Lalu dihubungkan ke R1 melalui 10.10.10.1/30 lalu R1 terhubung dengan Internet menggunakan DHCP. konfigurasi VPDN dibagi menjadi 2 bagian, konfigurasi PTPP dan konfigurasi *Virtual template*. Pada bagian awal konfigurasi adalah pengaktifan *Virtual Private Dialup Networking*, membuat nama VPDN, mengaktifkan *Accept Dialin* agar dapat menerima koneksi yang masuk, kemudian memilih PPTP sebagai protokol yang digunakan, menentukan IP yang dibagikan ke *user* yang terakhir membuat *username* dan *password*. Setelah itu masuk ke bagian konfigurasi *Virtual Template*. Pada bagian ini fokus utama konfigurasi adalah membuat enkripsi yang dipakai. Setelah itu mengaktifkan Microsoft *Point to Point Encryption* atau MPPE 128. Yang terakhir adalah memasukkan alamat IP ke dalam *virtual interface*, dalam penelitian ini tidak ada alamat IP yang secara khusus diberikan untuk *virtual interface.* \

3.2 Analisis QoS

Proses analisis dilakukan dengan menambahkan bandwith sebesar 512Kb/s dengan tujuan untuk dapat membatas transfer data untuk setiap tunneling protocol menjalankan aplikasi Zoom dan Google Meet secara bergantian untuk mendapatkan data berupa *packet data, time, Delay*.



p-ISSN: 2460-173X
e-ISSN: 2598-5841

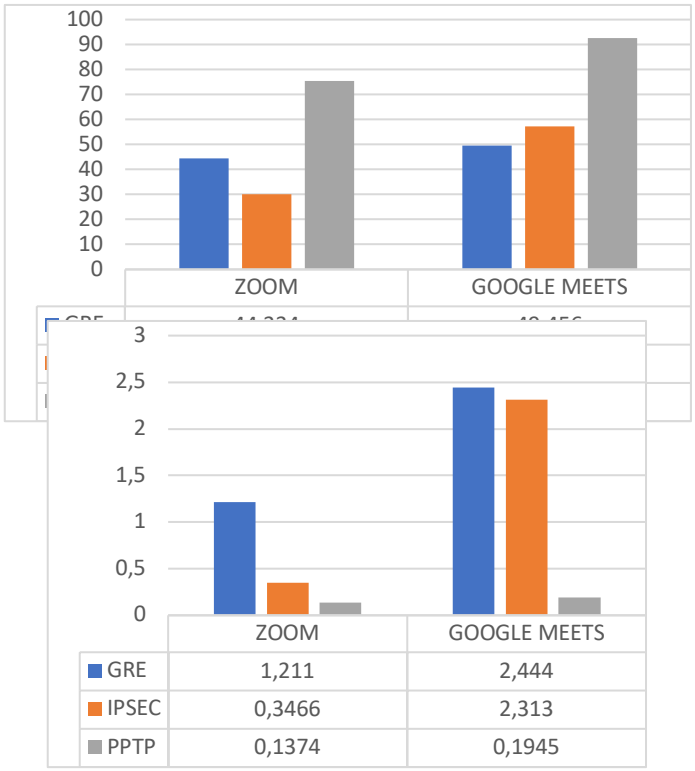
Gambar 5. Proses pengambilan data menggunakan topologi IPsec

Pada gambar 5, proses pengambilan data dilakukan. Durasi pengamatan yang dilakukan, yaitu selama 10 menit untuk setiap topologi yang di uji coba, Selama proses berlangsung, paket yang transmisikan direkam menggunakan aplikasi *wireshark* dengan Jenis paket yang akan di amati adalah *Transmission Control Protocol* (TCP).

4. HASIL DAN PEMBAHASAN

Berdasarkan hasil perhitungan menggunakan standar TIPHON, didapatkan hasil berupa nilai Throughput, Packet Loss, Delay dan jitter yang tersaji pada Gambar 5 – Gambar 8

Gambar 6. Hasil Perhitungan Throughput

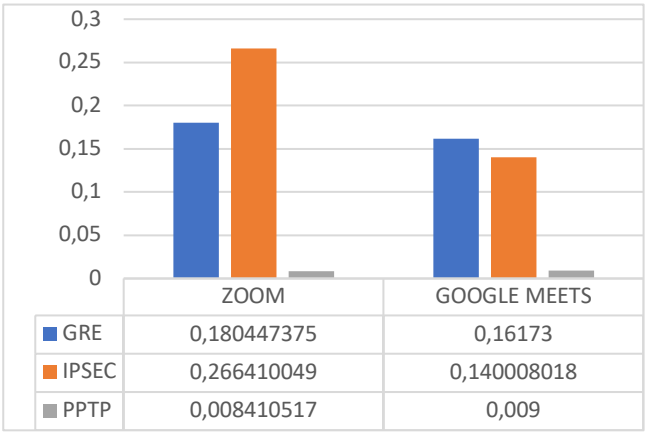


Hasil *Throughput* yang didapatkan berdasarkan gambar 6 adalah, Untuk model *Tunneling* GRE nilai yang didapatkan adalah sebesar 49.4Kbps untuk Meet dan 44.4Kbps untuk Zoom sedangkan untuk IPSEC didapatkan nilai 57.1Kbps untuk Zoom dan 30Kbps untuk Meet. Sedangkan untuk PPTP hasil yang didapatkan adalah 92.5Kbps dan 75.5Kbps untuk Google Meet dan Zoom. Dengan standar yang digunakan untuk mengukur kualitas Throughput jaringan adalah untuk protocol GRE predikat yang didapat adalah Jelek, protocol IPSEC mendapatkan predikat sedang untuk aplikasi Google Meet dan jelek untuk aplikasi Zoom, protocol PPTP mendapatkan predikat bagus untuk aplikasi Zoom dan sangat bagus untuk aplikasi Zoom.

Gambar 7. Hasil Perhitungan Packet Loss

Hasil perhitungan *Packet Loss* GRE, IPSEC, PPTP pada gambar 7 adalah *Packet Loss* yang dimiliki IPSEC untuk Google Meet adalah 2.31% dengan indikator sangat bagus. Sedangkan untuk Zoom nilai yang didapatkan adalah 0.34% dengan indikator sangat bagus. Sedangkan untuk GRE nilai yang didapatkan adalah 2.4% persen untuk Google Meet dan 1.21% persen untuk Zoom. Kedua nilai yang didapatkan GRE masuk dalam kategori sangat bagus. Sedangkan untuk PPTP nilai yang didapatkan adalah 0.13% dan 0.19% untuk Google *Meet* dan Zoom dengan kategori sangat bagus.

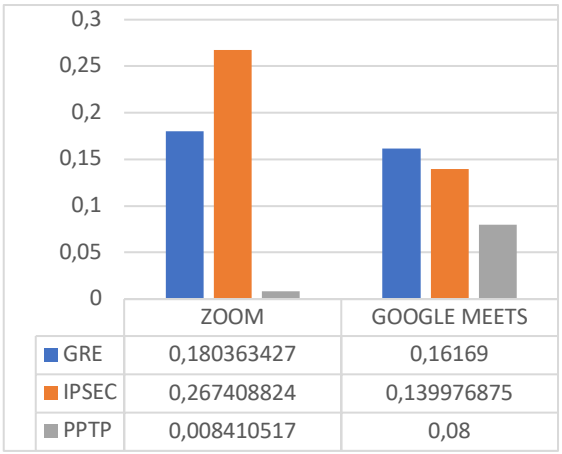
p-ISSN: 2460-173X
e-ISSN: 2598-5841



	ZOOM	GOOGLE MEETS
GRE	0,180447375	0,16173
IPSEC	0,266410049	0,140008018
PPTP	0,008410517	0,009

Gambar 8. Hasil Perhitungan Delay

Berikut Hasil yang didapatkan pada gambar 8, nilai *delay* yang dimiliki IPSEC untuk Google Meet memiliki angka yang tertinggi dengan nilai 0.14 dengan predikat sangat bagus, selanjutnya untuk Zoom nilai yang didapatkan adalah 0.26 dengan predikat sangat bagus. Sedangkan untuk GRE nilai yang didapatkan untuk Zoom dan Google Meet adalah 0.18 dan 0.16 Sedangkan untuk PPTP nilai yang didapatkan adalah 0.008 dan 0.009 untuk Google Meet dan Zoom dengan predikat sangat bagus.



	ZOOM	GOOGLE MEETS
GRE	0,180363427	0,16169
IPSEC	0,267408824	0,139976875
PPTP	0,008410517	0,08

Gambar 9. Hasil perhitungan Jitter

Pada gambar 9, hasil yang didapatkan adalah GRE untuk aplikasi Zoom dan Google Meet adalah 0.18 dan 0.16 dengan predikat bagus. Sedangkan untuk IPSEC untuk aplikasi Zoom dan Google adalah 0.26 dan 0.13, Sedangkan untuk PPTP nilai yang didapatkan adalah 0.008 dan 0.08 untuk Google Meet dan Zoom dengan predikat bagus.

5. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan dapat disimpulkan bahwa GRE, IPsec dan PPTP bisa digunakan sebagai *tunneling protocol* untuk menjalankan aplikasi virtual meeting dengan *tunneling protocol* yang direkomendasikan adalah PPTP. PPTP dipilih karena memiliki nilai throughput yang paling tinggi yaitu sebesar 75.56Kb/s untuk Zoom dan 92.58Kb/s untuk Google Meet, berdasarkan Standar TIPHON nilai throguhput yang dimiliki PPTP adalah Sangat Bagus. Hal ini juga diikuti dengan nilai dari packet loss yaitu 0.13% untuk Zoom, 0.19 untuk Google Meet, selanjutnya nilai delay yang didapatkan adalah 0.008 untuk Zoom dan 0.009 untuk Google Meet, selanjutnya nilai jitter yang didapatkan adalah 0.008 untuk Zoom dan 0.8 untuk Google

Meet Ketiga kategori tersebut mendapatkan predikat sangat bagus berdasarkan standar TIPHON. Dari segi keamanan, PPTP juga memiliki nilai lebih karena memiliki konsep client server.

DAFTAR PUSTAKA

[1] J. A. Dewantara and T. H. Nurgiansah, "Efektivitas Pembelajaran Daring di Masa Pandemi COVID 19 Bagi Mahasiswa Universitas PGRI Yogyakarta," *Jurnal Basicedu*, vol. 5, no. 1, pp. 367–375, Dec. 2020.

[2] F. Arkiang, "ANALISIS PEMBELAJARAN DARING SELAMA PANDEMI COVID-19 DI DAERAH 3T (NUSA TENGGARA TIMUR)," *Jurnal Pendidikan*, vol. 12, no. 1, pp. 57–64, 2021.

[3] T. Andriyanih, "Analisis kualitas layanan RA Manbaul Hikmah dimasa pandemi Covid-19 dengan metode IPA dan CSI Analysis of RA Manbaul Hikmah's service quality during the Covid-19 pandemic using the IPA and CSI methods," *JSI : Jurnal Sains Indonesia*, vol. 2, no. 3, pp. 141–152, 2021.

[4] Ilmadi, G. Sastro, R. Saefullah, D. N. Sari, and D. Wijawa, "ANALISIS KEPUASAN PESERTA DIDIK DALAM PEMBELAJARAN JARAK JAUH DI MASA PANDEMI COVID-19 (Studi Kasus: SMP Mater Dei Kota Tangerang Selatan)," *Indonesian Journal of Science*, vol. 2, no. 2, pp. 41–51, 2020.

[5] L. Hakim, "Pemilihan Platform Media Pembelajaran Online Pada Masa New Normal," *Justek : Jurnal Sains dan Teknologi*, vol. 3, no. 2, p. 27, Nov. 2020.

[6] D. Simion, M. Ursuleanu, A. Graur, A. Potorac, and A. Lavric, "Efficiency Consideration for Data Packets Encryption within Wireless VPN Tunneling for Video Streaming," *International Journal of Computer Communication and Control*, vol. 8, no. 1, pp. 136–145, 2013.

[7] N. Jain and A. Payal, "Performance Comparison Between Different Tunneling Techniques Using Different Routing Protocols," *Wireless Personal Communications*, vol. 123, no. 2, pp. 1395–1441, Mar. 2022.

[8] S. Jahan, M. S. Rahman, and S. Saha, "Application specific tunneling protocol selection for Virtual Private Networks," in *In Proc,International Conference on Networking, Systems and Security,* 2017, no. October, pp. 39–44.

[9] M. R. Efendi, E. A. Hamidi, and A. Saepulloh, "Implementasi GRE Tunneling Menggunakan Open vSwitch Pada Jaringan Kampus," *TELKA: Jurnal Telekomunikasi, Elektronika, Komputasi, dan Kontrol*, vol. 3, no. 2, pp. 103–111, 2017.

[10] R. M. Arifin, E. D. Wardhani, and S. BETA, "Implementasi Tunnel GRE pada Jaringan Ring dan Mesh Perangkat Metro-E Nokia," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, vol. 10, no. 3, pp. 204–213, 2021.

[11] A. H. M. Permana, N. Widiyasono, and A. Rahmatulloh, "Perbandingan Algoritma Pada Teknologi Virtual Private Network (VPN) IPSec Terhadap Kecepatan Transfer Data," *SISTEMASI: Jurnal Sistem Informasi*, vol. 9, no. 2, pp. 259–273, 2020.

[12] M. Arif and A. S. Budiman, "Interkoneksi Site-to-Site dan Remote Access Menggunakan Virtual Private Network dan IP Security," *JSI : Jurna l Sistem Informasi*, vol. 12, no. 1, pp. 1856–1866, 2020.

[13] W. K. Halawa and K. J. D. Lase, "ANALISIS PERBANDINGAN VPN PPTP DAN EOIP MENGGUNAKAN METODE AQM," *INFACT : Jurnal Sains dan Komputer*, vol. 6, no. 1, pp. 39–48, 2021.

[14] A. P. Pamungkas, M. R. Putra, and M. Hafizh, "Jurnal KomtekInfo Analisis Jaringan VPN Menggunakan PPTP dan L2TP Berbasis Mikrotik pada Diskominfo Kabupaten Muko Muko," *Jurnal KomtekInfo*, vol. 8, no. 3, pp. 189–194, 2021.

[15] S. Ikhwan and A. Amalina, "Analisis Jaringan VPN Menggunakan PPTP dan L2TP," *Jurnal Infotel*, vol. 9, no. 3, pp. 1–7, 2017.

[16] Firmansyah, M. Wahyudi, and R. A. Purnama, "Analisis Performa Site to Site IP Security Virtual Private Network (VPN) Menggunakan Algoritma Enkripsi ISAKMP," *JUITA : Jurnal Informatika*, vol. 7, no. 2, p. 129, 2019.
[17] M. Y. H. Setyawan, "VIRTUALISASI KINERJA HTTP DAN HTTPS PADA VIDEO STREAMING MELALUI TUNNELING," *Jurnal Teknik Informatika*, vol. 13, no. 3, pp. 10–15, 2021.
[18] F. Wulansari, R. Munadi, and R. Mayasari, "Analisis Jaringan MPLS-TE Fast Reroute Menggunakan Metode QoS Diffserv Berbasis Server OpenIMSCore," vol. 2016, no. Sentika, pp. 18–19, 2016.
[19] I. D. Amiza and S. Soim, "Implementasi dan Analisis Quality of Service (QoS) pada OpenMeetings dengan Virtual Private Network (VPN)," vol. 05, no. 04, pp. 19–27, 2020.

Biodata Penulis

Jonathan Joseph Liando**,** Lahir di kota Tangerang pada tahun 1999. Sejak kecil penulis pertama menempuh pendidikan di Kabupaten Kepualan Sangihe, Sulawesi Utara. Kemudian melanjutkan perkuliahan S1 Teknik Informatika di Universitas Kristen Satya Wacana Salatiga dengan konsentrasi yang dipilih adalah *Network Engineering*

Indrastanti Ratna Widiasari, Lahir di kota Sukoharjo pada tahun 1978. Pendidikan terakhir yang ditempuh adalah pendidikan doktoral Teknik Elektro Universitas Gajah Mada. Penulis bekerja sebagai Dosen progam studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Satya Wacana. Beberapa mata kuliah yang diajarkan kepada mahasiswa adalah Teknologi Jaringan, Cisco Certification Network Associate 1 (CCNA 1). Selain menjadi dosen, penulis juga menjadi editorial untuk jurnal aiti UKSW.