PERANCANGAN VIRTUAL PRIVATE NETWORK UNIVERSITAS SUMATERA SELATAN

Antoni Pratama Sakti[1], Syahril Rizal[2]
Fakultas Ilmu Komputer, Universitas Bina Darma
Email: antonipratama464@gmail.com [1], syahril.rizal@binadarma.ac.id [2]

ABSTRAK

Jaringan internet berperan untuk mempermudah publik berkomunikasi dan bertukar data dengan cepat dan murah. untuk menjaga kerahasiaan pada jaringan publik pada saat berkomunikasi dan bertukar data, Virtual Private Network adalah salah satu solusinya. Virtual Private Network juga digunakan untuk menghubungkan antar jaringan lokal dengan memanfaatkan jaringan internet publik dan membuat tunnel jaringan menjadi private. Virtual Private Network mempunyai protokol jaringan seperti Point to Point Tunneling Protocol, Layer 2 Tunneling Protocol, dan Open Virtual Private Network. Universitas Sumatera selatan adalah salah satu Universitas yang ada di Palembang, Pada saat ini Universitas Sumatera Selatan memiliki tiga kampus yang masing-masing memiliki lokasi yang berbeda. Saat ini setiap kampus dalam komunikasi dan pengiriman data melalui jaringan publik yang belum tentu aman dan tidak dapat terhubung secara langsung, masalah seperti ini menjadi hal yang serius bagi setiap kampus tersebut, Ini tentunya akan berdampak pada keamanan dalam komunikasi dan pengiriman data setiap kampus tersebut. Salah satu solusinya adalah dengan cara menggunakan Virtual Private Network (VPN). Untuk mengetahui protokol Virtual Private Network yang mana yang cocok untuk jaringan di Universitas Sumatera Selatan, dalam hal ini penulis akan membandingkan protokol Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), dan Open Virtual Private Network (OpenVPN) dari segi performansinya berdasarkan hasil pengujian hasil Quality of Service (QoS) menggunakan Parameter yang diukur meliputi Throughput, PacketLoss, dan Delay. Dalam penelitian ini penulis menggunakan metode Action Research. Sehingga dapat diketahui dan ditentukan protokol Virtual Private Network mana yang cocok untuk jaringan Virtual Private Network di Universitas Sumatera Selatan dan dapat menyediakan suatu jaringan private yang handal dan aman tetapi dapat berjalan pada jaringan publik seperti internet. Sehingga dalam komunikasi dan pengiriman data bisa dapat terhubung secara langsung dan berjalan dengan aman.

Kata kunci: *Virtual Private Network, Tunneling,* PPTP, L2TP, *OpenVPN*

ABSTRACT

The internet network plays a role in making it easier for the public to communicate and exchange data quickly and cheaply. To maintain confidentiality on public networks when communicating and exchanging data, a Virtual Private Network is one solution. Virtual Private Network are also used to connect between local networks by utilizing the public internet network and making network tunnels private. Virtual Private Network have network protocols such as Point to Point Tunneling Protocol, Layer 2 Tunneling Protocol and Open Virtual Private Network. The University of South Sumatra is one of the Universities in Palembang. Currently, the University of South Sumatera has three campuses, each of which has a different location. Currently every campus is communicating and sending data through public networks which are not necessarily safe and cannot be connected directly. So that communication and data transmission can be connected directly and run safely.

1. PENDAHULUAN

Jaringan internet berperan untuk mempermudah publik berkomunikasi dan bertukar data dengan cepat dan murah. Untuk menjaga kerahasiaan pada jaringan publik pada saat berkomunikasi dan bertukar data maka salah satu solusinya yaitu dengan menggunakan Virtual Private Network. Virtual Private Network juga digunakan untuk menghubungkan antar jaringan lokal yang dengan memanfaatkan jaringan internet publik dan membuat tunnel jaringan

menjadi *private*. *Virtual Private Network* mempunyai protokol jaringan seperti *Point-to- Point Tunneling Protocol* (PPTP), Layer 2 *Tunneling Protocol* (L2TP), dan *Open Virtual Private Network* (OpenVPN).

Pada saat ini Universitas Sumatera Selatan memiliki dua kampus yaitu kampus A yang terletak di JL. Letnan Murod No.55 Talang Ratu KM5 Palembang, kampus B yang terletak di JL. Jend. Sudirman, Pahlawan, Kec. Kemuning, Kota Palembang, Sumatera Selatan 30128. Dalam menjalankan aktivitas komunikasi dan pengiriman data, kecepatan dan keakuratan beserta keamanan dalam komunikasi dan pengiriman data dari setiap kampus sangat dibutuhkan, ini sangat memerlukan jaringan internet yang terintegrasi dengan baik agar dalam pelaksanaan aktivitas perusahaan berjalan dengan efisien. Saat ini setiap kampus dalam komunikasi dan pengiriman data melalui jaringan publik yang belum tentu aman dan tidak dapat terhubung secara langsung , masalah seperti ini menjadi hal yang serius bagi setiap kampus tersebut, Ini tentunya akan berdampak pada keamanan dan kemudahan dalam komunikasi dan pengiriman data setiap kampus tersebut. Oleh karena itu, penulis menuangkan ide unutk melakukan perancangan jaringan *Virtual Private Network* dengan membandingkan *protokol Virtual Private Network* terlebih dahulu, dalam hal ini penulis akan membandingkan *protokol Point-to-Point Tunneling Protocol* (PPTP), Layer 2 *Tunneling Protocol* (L2TP), dan *Open Virtual Private Network* (*OpenVPN*) dari segi performansinya berdasarkan hasil pengujian hasil *Quality of Service* (QoS) menggunakan Parameter yang diukur meliputi *Throughput*, *PacketLoss*, dan *Delay*. Sehingga dapat diketahui dan ditentukan protokol *Virtual Private Network* mana yang cocok untuk jaringan komputer di Universitas Sumatera Selatan.

Banyak penelitian yang membahas tentang virtual private network. [1], VPN merupakan suatu bentuk private internet yang melalui public network (internet), dengan menekankan pada keamanan data dan akses global melalui internet. [2], Virtual Private Network (VPN) memberi kemudahan untuk mengakses internet dimanapun dan kapanpun. [3], Informasi yang di kirimkan dari pusat ke cabang atau sebaliknya terkadang mengandung informasi yang sangat sensitif, penggunaan VPN akan memberikan rasa aman karena informasi yang dikirimkan melalui jalur VPN tidak akan terdeteksi oleh proses sniffing sekalipun. [4], Pemilihan produk VPN tersebut, perpustakaan mempertimbangkan aspek otentikasi yang kuat, enkripsi yang cukup kuat, memenuhi standar, integrasi dengan servis network bidang lain. [5], OpenVPN lebih unggul dari PPTP dari hasil pengujian keamanan.

METODOLOGI PENELITIAN

[1] H. A. Musril, "InfoTekJar : Jurnal Nasional Desain Virtual Private Network (VPN) Berbasis Open Shortest Path First (OSPF)," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 3, no. 2, pp. 187–192, 2019.

[2] M. D. Andini, "PENGGUNAAN APLIKASI VIRTUAL PRIVATE NETWORK (VPN) POINT TO POINT TUNNELING PROTOCOL (PPTP) DALAM MENGAKSES SITUS TERBLOKIR," *Junal Penelit. Huk.*, vol. 29, no. 2, pp. 148–166, 2020.

[3] S. A. Khoir, A. Yudhana, and S. Sunardi, "Implementasi GPS (Global Positioning System) Pada Presensi Berbasis Android DI BMT Insan Mandiri," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 4, no. 1, pp. 9–17, 2020, doi: 10.30645/j-sakti.v4i1.182.

[4] L. Umaroh and M. Rifauddin, "IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN)," *J. Dokumentasi dan Inf.*, vol. 9008, no. 21, pp. 193–201, 2020.

[5] P. Oktivasari and A. B. Utomo, "Analisa Virtual Private Network menggunakan OpenVPN dan Point to Point Tunneling Protocol," *J. Penelit. Komun. dan Opini Publik*, vol. 20, no. 2, pp. 185–202, 2016.

2.

2.1 Metode Penelitian

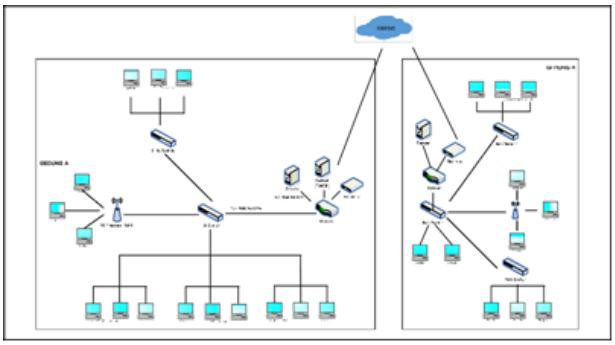
Metode pada penelitian ini menggunakan penelitian tindakan yang merupakan pendekatan kolabolatif untuk menyelidiki, menelaah atau mengkaji dan menemukan sesuatu, yang memungkinkan orang menggunakan tindakan yang sistematis untuk menyelesaikan suatu permasalahan. Metode penelitian tindakan terdiri dari beberapa tahapan yaitu dimulai dari Diagnosis, rencana tindakan, melakukan tindakan, evaluasi dan pembelajaran.

3. HASIL DAN PEMBAHASAN

3.1. Diagnosis

Pada tahap pertama peneliti mendiagnosis dan melakukan observasi pada jaringan LAN / Wi-Fi yang sudah diterapkan sebelumnya pada Universitas Sumatera Selatan. Berikut hasil diagnosis yang peneliti lakukan pada Universitas Sumatera Selatan.

a) Topologi Jaringan Komputer Berjalan
Universitas Sumatera Selatan menggunakan 2 tipe jaringan yaitu jaringan LAN dan *Nirkabel*, dimana jaringan internet di sebarkan pada beberapa titik, yaitu di ruang kepala, ruang dosen, ruang lab dan ruang *server*.



Gambar 1. Topologi Jaringan Komputer Universitas Sumatera Selatan

b) Analisis Permasalahan
Dapat dilihat pada gambar 1 setiap kampus dalam komunikasi dan pengiriman data melalui jaringan publik yang belum tentu aman dan tidak dapat terhubung secara langsung sehingga rentan terhadap serangan serangan yang biasa dilakukan oleh orang-orang yang tidak bertanggung jawab, masalah seperti ini menjadi hal yang serius bagi setiap kampus tersebut, Ini tentunya akan berdampak pada keamanan dalam komunikasi dan pengiriman data setiap kampus tersebut. Untuk memenuhi kebutuhan seperti menciptakan jalur komunikasi langsung antar kampus, digunakan teknologi yang dapat menjamin komunikasi data antar jaringan yang terpisah secara efisien dan aman, yaitu teknologi Virtual Private Network (VPN).

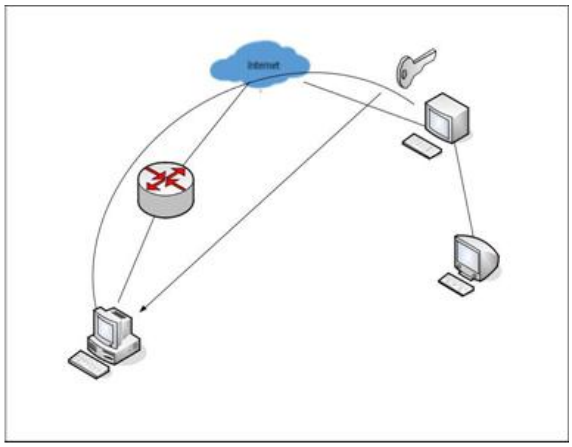
3.2. Rencana Tindakan (*Action Planning*)

Pada tahap ini dilakukan perencanaan berdasarkan pengumpulan data yang sudah diambil, maka peneliti akan merancang jaringan VPN Universitas Sumatera Selatan. Dengan adanya koneksi VPN maka komunikasi jaringan lokal dapat dimaksimalkan dengan keamanan yang lebih baik. Keamanan yang dimaksud adalah penggunaan account VPN, dimana account ini terdiri dari username dan password. Username dan password dapat dimiliki pihak-pihak yang diizinkan untuk melakukan koneksi tersebut.

a) Perencanaan VPN

Pada perencanaan VPN ini peneliti akan melakukan perbandingan dengan melakukan pengukuran Quality of Service (QoS) dari masing – masing VPN (Virtual Private Network), untuk mengetahui protokol VPN (Virtual Private Network) yang mana yang cocok untuk jaringan di Universitas Sumatera Selatan, dalam penelitian ini peneliti akan membandingkan protokol VPN antara lain *Point-to-Point Tunneling Protocol* (PPTP), *Layer 2 Tunneling Protocol* (L2TP), dan *Open Virtual Private Network* (OpenVPN). Dari ketiga teknologi tersebut dapat diukur segi performansinya berdasarkan hasil pengujian dari *Quality of Service* (QoS) menggunakan Parameter yang diukur meliputi *Bandwith*, *Throughput, Packet Loss,* dan *Delay*.

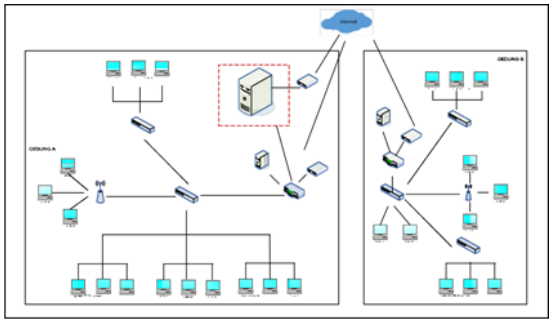
b) Perencanaan Topologi Jaringan VPN



Gambar 2. Topologi Sistem VPN

Dapat dilihat pada gambar 2 jaringan sistem VPN untuk pengkoneksian menggunakan media internet yang rentan terhadap serangan serangan yang biasa dilakukan oleh orang-orang yang tidak bertanggung jawab. Oleh karena itu sebelum client bisa terkoneksi pada server maka akan dilakukan proses otentikasi terlebih dahulu menggunakan key dan CA

c) Topologi jaringan VPN diusulkan



Gambar 3. Topologi Jaringan Sistem + VPN

Berdasarkan gambar 3 pemodelan di atas dapat dilihat bahwa VPN Server diletakkan pada Gedung A induk dari semua Router yang terhubung. Router Server VPN (RVPN) digunakan sebagai Server VPN ini bertugas menangani pengolahan, pendistribusian data dan manajemen bandwith secara terpusat, juga sebagai pintu gerbang menuju internet (gateway). Sehingga RVPN menjadi koordinator pada sistem jaringan IP VPN.

3.3. Melakukan Tindakan (Action Taking)

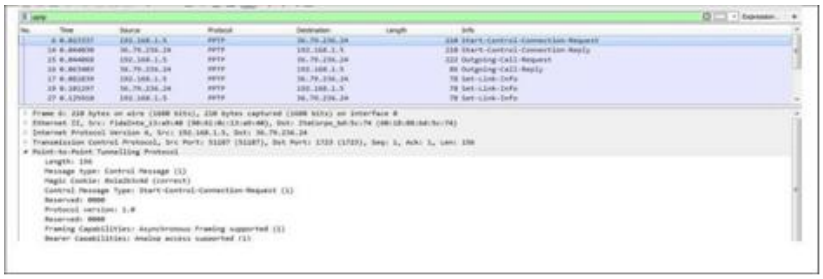
Tahapan ini merupakan tahapan penerapan instalasi jaringan VPN sesuai dengan topologi beserta perangkat yang direncanakan pada tahap sebelumnya. Dari tahapan ini dihasilkan instalasi jaringan VPN yang telah selesai dirancang.

3.4. Evaluasi

Pada tahap ini peneliti akan melakukan evaluasi dari hasil yang didapat. Untuk pengujian protokol VPN, dibutuhkan perangkat *software* dan *hardware* untuk mendukung dalam pengujian kinerja jaringan VPN dengan menggunakan protokol PPTP, L2TP dan OpenVPN berbasis Mikrotik. Untuk protokol PPTP, L2TP, dan OpenVPN pengambilan data dilakukan pada saat protokol PPTP, L2TP, dan OpenVPN client melakukan dial VPN ke PPTP, L2TP, dan OpenVPN server. Tujuan dari pengambilan data ini adalah melakukan pengamatan terhadap protokol PPTP, L2TP, dan OpenVPN dalam membangun sebuah tunnel VPN sebelum data streaming dapat dilewatkan melalui tunnel tersebut.

1) VPN PPTP

Peneliti mengambil data menggunakan aplikasi *wireshark* saat PPTP client membuat koneksi ke PPTP server, hasil didapatkan seperti gambar 4



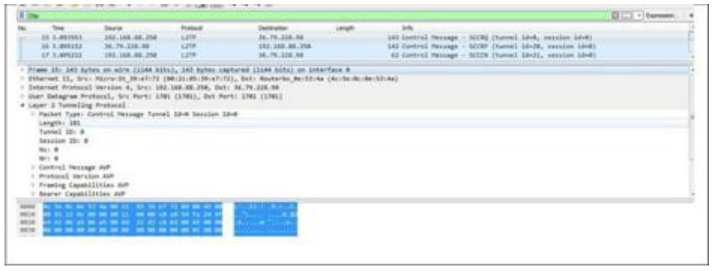
Gambar 4. *Tunnen* pada PPTP

Seperti terlihat pada gambar 4.1, terjadi pertukaran pesan antara PPTP client dengan PPTP server melalui koneksi TCP untuk membuat tunnel dengan urutan sebagai berikut :

a) PPTP client mengirim Start-Control-Connection-Request kepada PPTP server, permintaan untuk memulai session.
b) PPTP Server mengirim Start-Control-Connection-Reply kepada PPTP Client, untuk menjawab start session.
c) PPTP Client mengirim Outgoing-Call-Request kepada PPTP Server, permintaan untuk melakukan outgoing call.
d) PPTP Server mengirim Outgoing-Call-Reply kepada PPTP Client, respon dari server telah menerima Outgoing-Call-Request.
e) PPTP Client mengirim Set-Link-Info kepada PPTP server, permintaan untuk merubah setting koneksi antara client dan server.

2) VPN L2TP

Peneliti mengambil data menggunakan aplikasi wireshark saat L2TP client membuat koneksi ke L2TP server, hasil didapatkan seperti gambar 5



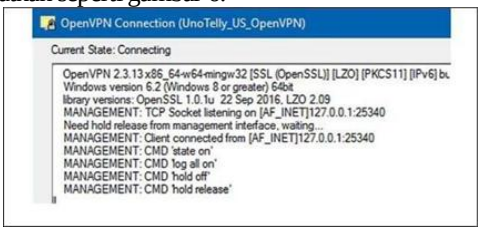
Gambar 5 Tunnel pada L2TP

Seperti terlihat pada gambar 5, terjadi pertukaran pesan antara L2TP client dengan L2TP server melalui koneksi TCP untuk membuat tunnel dengan urutan sebagai berikut :

a) L2TP Client mengirim SCCRQ (Start-Control-Connection-Request) ke L2TP Server, untuk menginisialisasi tunnel antara server dan client, untuk proses pembentukan tunnel.
b) L2TP Server mengirim SCCRP (Start-Control-Connection-Reply) ke L2TP Client, untuk mengindikasikan bahwa SCCRQ telah diterima dan pembentukan tunnel harus dilanjutkan. Dikirim sebagai balasan dari message SCCRQ yang dikirim oleh L2TP Client.
c) L2TP Client mengirim SCCCN (Start-Control-Connection-Connected) ke L2TP Server; dikirim sebagai balasan dari message SCCRP yang dikirim oleh L2TP Server mengindikasikan proses pembentukan tunnel telah selesai.

3) VPN OpenVPN

Peneliti mengambil data menggunakan aplikasi wireshark saat OpenVPN client membuat koneksi ke OpenVPN server, hasil didapatkan seperti gambar 6.

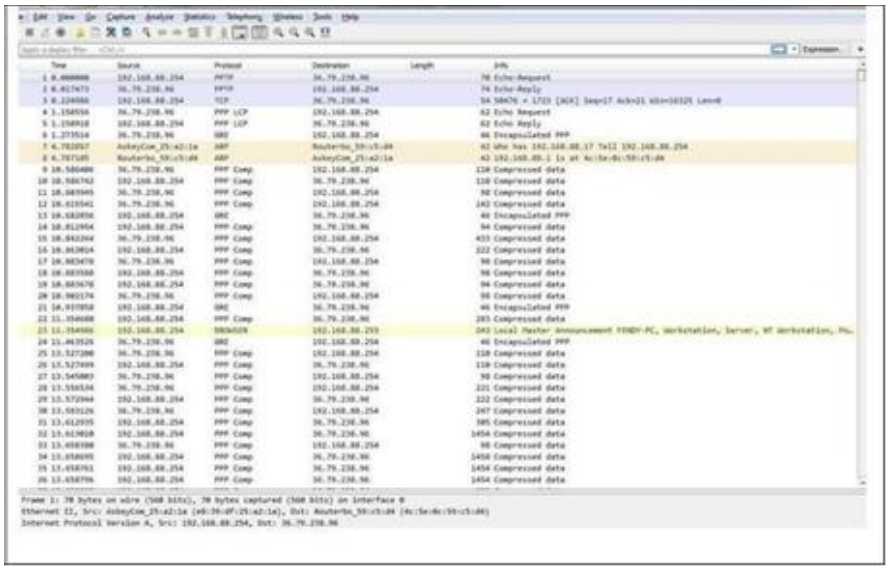


Gambar 6. *Tunnel* pada Open VPN

Seperti terlihat pada gambar 4.3, terjadi pertukaran pesan antara OpenVPN client dengan OpenVPN server melalui koneksi TCP untuk membuat tunnel dengan urutan sebagai berikut :

a) OpenVPN Client mengirim permintaan terhbung ke OpenVPN Server, untuk proses pembentukan tunnel antara server dan client
b) OpenVPN Server melakukan pengecekan dan memverifikasi fileconfig pada client yang berisi sertifikat dan key yang sesuai dengan VPN server, untuk melanjutkan pembentukan tunnel.
c) OpenVPN Client jika OpenVPN Server berhasil terkoneksi maka OpenVPN Client mendapat IP address baru untuk dapat mengakses jaringan atau resource yang berada dibelakang VPN server.

Pada hasil penelitian ini peneliti akan mengevaluasi dan membahas mengenai hasil analisa perbandingan antara tiga protokol yaitu PPTP, L2TP dan OpenVPN dengan membuat tunnel VPN melalui jaringan public, parameter yang diukur adalah besaran bandwidth dan ukuran video yang berbeda pada jaringan server dan client kemudian dianalisis berdasarkan QoS, seperti delay, throughput dan packet loss untuk mengetahui kinerja dari kedua protokol tersebut. Berikut adalah hasil rekam Wireshark :



Gambar 7. Hasil Rekam *Wireshark*

Hasil tersebut kemudian disaring file header hasil data PPTP yaitu PPP untuk mendapatkan file streaming yang direkam. Setelah disaring kemudian di-export dalam format CSV. File dari format CSV akan dibuka menggunakan Ms.Excel untuk dihitung berdasarkan rumus. Berikut adalah perhitungan delay, throughput, dan packet loss.

1) *Qos Delay*

Hasil delay dari streaming video antara 3 VPN menggunakan protokol PPTP, L2TP dan OpenVPN dengan satuan Second yang mempunyai ukuran video sebesar 10,502 MB, 21,28 MB dan 30,62 MB dengan bandwidth sebesar 128 Kbps, 256 Kbps dan 512 Kbps. Pada VPN dengan protokol PPTP, dengan bandwidth yang digunakan untuk streaming sebesar 128 Kbps dengan ukuran video sebesar 10,502 MB menghasilkan nilai delay sebesar 2,36 Second, ukuran video sebesar 21,28 MB menghasilkan nilai delay sebesar 3,365 Second.

Waktu delay rata – rata pada streaming video dengan perbedaan bandwidth dan ukuran video antara PPTP, L2TP dengan OpenVPN terdapat perbedaan. Pada bandwidth 128 Kbps L2TP memiliki selisih delay sebesar 0,123 Second lebih besar dibanding dengan PPTP sehingga PPTP mempunyai lebih baik dibandingkan dengan L2TP dalam segi delay. Kemudian untuk OpenVPN memiliki selisih delay dengan L2TP sebesar 0.11 Second lebih besar dibanding L2TP sehingga L2TP lebih baik dibandingkan OpenVPN.

2) *Qos Throughput*

Throughput merupakan jumlah total kedatangan paket yang diamati pada waktu interval tertentu. Nilai Throughput digunakan untuk menentukan kecepatan data. Hasil *throughput* dari *streaming* video antara 3 protokol VPN yaitu PPTP, L2TP dan OpenVPN dengan satuan *kilobits* per *second* (kbps) yang mempunyai ukuran video sebesar 10,502 MB, 21,28 MB dan 30,62 MB dengan bandwidth sebesar 128 Kbps, 256 Kbps dan 512 Kbps.

3) *Qos Loss Packet*

Packet loss merupakan jumlah paket yang hilang pada proses pengiriman. Hasil packet loss dari *streaming* video antara 3 protokol jaringan VPN dalam hitungan persen yang mempunyai ukuran video sebesar 10,502 MB, 21,28 MB dan 30,62 MB dengan bandwidth sebesar 128 Kbps, 256 Kbps dan 512

Kbps. Pada VPN dengan protokol PPTP, dengan bandwidth yang digunakan untuk streaming sebesar 128 Kbps dengan ukuran video sebesar 10,502 MB menghasilkan nilai packet loss sebesar 41,83 %, ukuran video sebesar 21,28 MB menghasilkan nilai packet loss sebesar 49,7 %.

3.5. *Learning* (Pembelajaran)

Dari hasil yang telah dilakukan mengenai perancangan VPN dengan melakukan perbandingan 3 protokol VPN. Konfigurasi router merupakan tahap awal dalam membuat keamanan. Didalam konfigurasi ini akan dihubungkan atau diintegrasikan dengan firewall agar lebih aman. Penambahan firewall dalam sistem merupakan cara untuk lebih mengamankan jaringan atau sistem yang telah dibuat agar user yang tidak berhak masuk dapat dicegah oleh firewall. Selanjutnya dengan menambahkan keamanan VPN didalam sistem dimana pada penambahan ini akan dikonfigurasi VPN (*Virtual Private Network*) yang merupakan metode untuk membentuk jaringan baru didalam jaringan yang sudah ada agar lebih aman. VPN juga dapat diterapkan untuk client yang dapat mengakses informasi yang biasanya hanya diizinkan di area tertentu. Dalam hal ini VPN diimplementasikan menggunakan PPTP dimana VPN yang dilakukan di network yang sudah melewati multi Hop router atau melewati internet.

4. KESIMPULAN

Menurut hasil penelitian yang dilaksanakan oleh penulis dengan judul "Perancangan Virtual Private Network Universitas Sumatera Selatan", maka penulis menarik kesimpulan bahwa ketiga protokol mempunyai kelebihan di bidangnya masing-masing, serta juga memiliki kekurangan masing-masing, dan ini adalah beberapa manfaat:

a) Protokol VPN PPTP memiliki kelebihan dari semua percobaan, PPTP memiliki perbandingan yang lebih baik dibandingkan L2TP dan OpenVPN.
b) Pengujian dilakukan pada sistem operasi Windows, untuk pengujian pada sistem operasi lainnya kemungkinan mendapatkan hasil yang berbeda dari ke 3 protokol yaitu VPN PPTP, L2TP dan OpenVPN.

DAFTAR PUSTAKA

[1] H. A. Musril, "InfoTekJar : Jurnal Nasional Desain Virtual Private Network (VPN) Berbasis Open Shortest Path First (OSPF)," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 3, no. 2, pp. 187–192, 2019.

[2] M. D. Andini, "PENGGUNAAN APLIKASI VIRTUAL PRIVATE NETWORK (VPN) POINT TO POINT TUNNELING PROTOCOL (PPTP) DALAM MENGAKSES SITUS TERBLOKIR," *Junal Penelit. Huk.*, vol. 29, no. 2, pp. 148–166, 2020.

[3] S. A. Khoir, A. Yudhana, and S. Sunardi, "Implementasi GPS (Global Positioning System) Pada Presensi Berbasis Android DI BMT Insan Mandiri," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 4, no. 1, pp. 9–17, 2020, doi: 10.30645/j-sakti.v4i1.182.

[4] L. Umaroh and M. Rifauddin, "IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN)," *J. Dokumentasi dan Inf.*, vol. 9008, no. 21, pp. 193–201, 2020.

[5] P. Oktivasari and A. B. Utomo, "Analisa Virtual Private Network menggunakan OpenVPN dan Point to Point Tunneling Protocol," *J. Penelit. Komun. dan Opini Publik*, vol. 20, no. 2, pp. 185–202, 2016.