Perbandingan *Virtual Private Network* Protokol Menggunakan *Point to Point Tunnel Protocol* dan *OpenVPN*

Henki Bayu Seta[1)], Muhammad Ridwan[2)], Theresia Wati[3)]
Universitas Pembangunan Nasional "Veteran" Jakarta
Jl. Rs. Fatmawati Pondok Labu Jakarta Selatan, (021) 7656971 Ext 231
e-mail: henkiseta@gmail.com, m.ridwan@y7mail.com, theresia_waty@yahoo.com

Abstrak

Dengan semakin ketergantungannya user kepada teknologi internet tentu harus diimbangi dengan ketersediaan internet yang memadai dan handal, berbagai masalah justru muncul ketika internet tidak menjamin keamanan yang maksimal tanpa adanya metode-metode tertentu karena internet sendiri terbuka untuk umum, siapapun dapat mengakses didalamnya, untuk itu maka kerahasiaan serta autentifikasi atas informasi yang dikirim atau yang diterimapun bersifat terbuka. Sebelum mengimplementasikan Virtual Private Network (VPN) perlu dilakukan perbandingan antar protokol terutama protokol PPTP dan OpenVPN. Metode penelitian yang digunakan metode Network Development Life Cycle (NDLC) untuk mengimplementasikan konsep VPN beserta penerapan QoS. Perbandingan dilakukan dengan parameter kecepatan dan keamanan data pada saat dikirim maupun diterima. Hasil penelitian didapat kedua protokol memiliki kelebihan dan kekurangan masing-masing. Pada sisi kecepatan PPTP lebih unggul ketimbang OpenVPN, sedangkan pada sisi keamanan OpenVPN memiliki keamanan yang lebih baik ketimbang PPTP.

Kata kunci: *Virtual Private Network, Mikrotik, PPTP protocol, OpenVPN, NDLC*

1. Pendahuluan

VPN merupakan suatu jaringan *private* yang mempergunakan sarana jaringan komunikasi publik yaitu internet dengan memakai *tunneling protocol* sebagai prosedur pengamanannya. VPN merupakan suatu jaringan komunikasi lokal yang terhubung melalui media jaringan publik, infrastruktur publik yang paling banyak digunakan adalah jaringan internet. Didalam VPN terdapat perpaduan teknologi *tunneling* dan enkripsi yang membuat VPN menjadi teknologi yang handal untuk mengatasi permasalahan keamanan didalam jaringan. Dalam implementasinya, VPN menggunakan *Site-to-site* untuk menghubungkan antara 2 tempat yang letaknya berjauhan, seperti kantor pusat dengan kantor cabang atau suatu perusahaan dengan perusahaan mitra kerjanya. Implementasi VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, supplier atau pelanggan) disebut ekstranet. Sedangkan bila VPN digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis intranet *site-to-site* VPN [1].

Penelitian ini disusun berdasarkan beberapa penelitian sebelumnya, diantaranya penelitian yang berjudul "Perancangan dan Implementasi Jaringan *Virtual Private Network* menggunakan PPTP (*Point to Point Tunneling Protocol*) pada PT. Mega Tirta Alami. Pada penelitian ini dibangun VPN dengan menggunakan metode PPTP (*Point to Point Tunneling Protocol*) untuk membangun jaringan VPN di PT.Mega Tirta Alami. Penggunaan PPTP dikarenakan metode ini menggunakan protokol yang mengizinkan hubungan *point to point* yang melewati jaringan IP. Hasil yang didapatkan dalam pembangunan VPN di PT.Mega Tirta Alami adalah jaringan VPN dapat menghubungkan antara *Branch*-1 dan *Branch*-2 dengan *Head office*, pembangunan VPN dapat memberikan keamanan dengan adanya enkripsi disetiap komunikasi data. Dengan menggunakan metode PPTP pembangunan VPN di PT.Mega Tirta Alami dapat memberikan keamanan dengan adanya enkripsi disetiap komunikasi data dan memberikan *username* dan *password* sebagai pengenal untuk setiap *branch* [2].

Penelitian yang dilakukan oleh Muhammad Taufik Roseno mengenai analisis perbandingan protokol yang berjudul "Analisis Perbandingan Protokol *Virtual Private Network* (VPN) – PPTP, L2TP, IPSec – sebagai dasar perancangan VPN pada Politeknik Negeri Sriwijaya Palembang". Dari sisi keamanan, IPSec memiliki fungsi keamanan yang paling lengkap dibandingkan dengan protokol PPTP dan L2TP karena memiki protokol enkripsi dan otentikasi yang lebih baik. Sedangkan protokol PPTP dan

L2TP tidak menyediakan fungsi data sendiri tetapi hanya bergantung pada protokol yang melaluinya untuk menyediakan fungsi keamanan. Dari sisi performansi, PPTP dan L2TP memiliki performansi yang lebih baik dibandingkan dengan IPSec jika berjalan pada jaringan TCP/IP, sedangkan dari sisi interoperability, L2TP dapat bekerja lebih baik dengan sistem dari vendor lain dibandingkan protokol PPTP dan IPSec [3].

Penelitian yang dilakukan oleh Joko Triyono dkk, "Analisis Perbandingan Kinerja Jaringan VPN Berbasis Mikrotik Menggunakan Protokol PPTP dan L2TP Sebagai Media Transfer Data". Hasil penelitian menunjukkan kecepatan transfer dan waktu tempuh *upload* atau *download* pada jaringan VPN masih sangat dipengaruhi oleh ukuran dan jenis file yang dikirimkan. Dari 3 kali percobaan dapat diasumsikan bahwa nilai rata-rata kecepatan transfer dan waktu tempuh jaringan VPN-PPTP memiliki prosentase 50% atau hampir 2 kali lipat lebih baik daripada VPN-L2TP. Disamping itu, penggunaan VPN-PPTP dalam melakukan live *video streaming*, *video on demand*, dan proses pengiriman data dalam bentuk *video* lebih layak digunakan dibanding menggunakan VPN-L2TP [4].

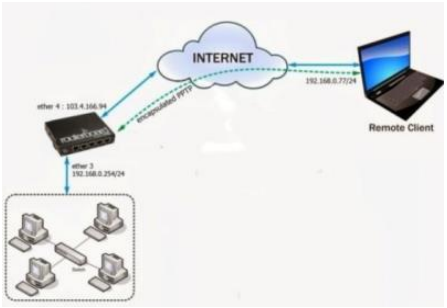
Berdasarkan penelitian-penelitian tersebut, maka penelitian ini akan melakukan perbandingan untuk pengujian jaringan pada jaringan VPN menggunakan teknologi PPTP dan OpenVPN. Penelitian ini akan menjawab mengenai VPN dengan protokol apa yang mampu memberikan fitur keamanan dan kestabilan yang baik serta kebutuhan *user* seperti apa yang dapat dipenuhi oleh OpenVPN maupun PPTP. Penelitian ini menggunakan Mikrotik RouterOS bertujuan untuk membandingkan VPN dengan menggunakan protokol PPTP dan OpenVPN untuk melihat protokol mana yang lebih unggul dari segi keamanan dan *throughput* yang dihasilkan untuk digunakan sesuai dengan kebutuhan *user*. Sebelum mengimplementasikan VPN yang harus dilakukan adalah mempelajari dan melakukan analisis protokol OpenVPN dan PPTP agar dapat menjadi bahan pertimbangan dalam melakukan perancangan VPN.

2. Metode Penelitian

Penulis melakukan pendekatan pengembangan sistem dengan menggunakan metode *Network Development Life Cycle* (NDLC) untuk mengimplementasikan konsep VPN beserta penerapan QoS. NDLC mempunyai beberapa alur kerja dalam mengembangkan suatu sistem jaringan.

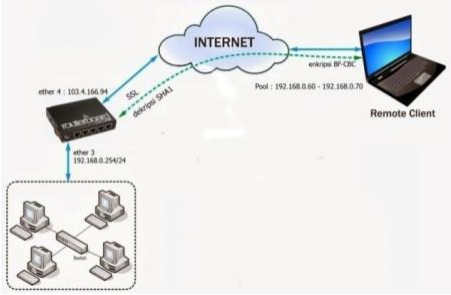
Tahapan penelitian yang dilakukan penulis adalah melakukan analisa (mengidentifikasi sistem yang berjalan), desain (membuat gambar desain topologi jaringan interkoneksi yang telah dibangun), simulasi prototipe (mensimulasikan kinerja VPN melalui aplikasi *Packet Tracer* untuk memiliki adanya gambaran tentang implementasi yang akan dibuat nantinya), implementasi (menerapkan semua yang telah direncanakan dan dirancang sebelumnya), *monitoring* (memonitor lalu lintas data yang digunakan pada *interface* VPN beserta pengaruhnya terhadap *host* lain ketika terhubung dalam satu jaringan, jika ditemukan kendala pada sistem dalam tahapan *monitoring* ini maka kembali akan dilakukan tahap analisis untuk mengetahui permasalahan yang terjadi), Uji Coba (melakukan uji coba jaringan VPN yang telah dibuat sebelumnya, baik uji coba pada protokol PPTP maupun OpenVPN, ketika semua berjalan dengan baik maka akan dilanjutkan pada tahap selanjutnya, jika terjadi kendala maka akan kembali pada tahap analisis demi memecahkan permasalahan yang ada) dan manajemen (membuat dan mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *reliability* terjaga).

Untuk melihat protokol mana yang lebih unggul dari segi keamanan dan *throughput* yang dihasilkan sesuai dengan kebutuhan *user*, penulis menggunakan topologi dengan menggunakan PPTP dan topologi dengan menggunakan OpenVPN.



Gambar 1. Topologi dengan menggunakan PPTP

Penulis menggunakan IP 192.168.0.77 untuk digunakan pada sisi *client* PPTP yang terkoneksi dengan VPN, ketika VPN terbentuk IP maka secara otomatis *client* yang terkoneksi menggunakan IP 192.168.0.77, hal ini sudah terdapat pada konfigurasi PPTP di sisi mikrotik.



Gambar 2. Topologi dengan menggunakan OpenVPN

Secara umum topologi baik PPTP maupun OpenVPN tidak memiliki perbedaan secara fisik, akan tetapi perbedaan hanya terdapat pada *policy* yang diterapkan, pada OpenVPN terdapat *policy* yang sedikit lebih kompleks karena menggunakan SSL sebagai *security* yang membutuhkan *certificate authority*, selain itu pula pada OpenVPN menggunakan *blowfish* pada enkripsinya serta SHA pada proses dekripsinya sedangkan pada PPTP hanya menggunakan GRE sebagai proses enkapsulasinya.

3. Hasil dan Pembahasan

Pengambilan data dilakukan dengan menggunakan jaringan sederhana pada setiap konfigurasi jaringan yang diujikan. Untuk melakukan uji coba terhadap dua Protokol VPN menggunakan topologi jaringan yang sama, yaitu menggunakan *Netbook* sebagai *client*, Mikrotik *Router* RB750, *Switch* 3Com 3CBLUG16A dan sebuah PC sebagai *Server*. PC *Server* terhubung langsung ke *Switch*, sedangkan *Switch* terhubung langsung dengan Mikrotik *Router* RB750 pada ethernet 3, untuk dapat diakses dari luar jaringan atau melalui *public*, maka dibutuhkan akses *public* yang terhubung dengan Mikrotik *Router* RB750 pada ethernet 1 yang merupakan *port* untuk WAN.

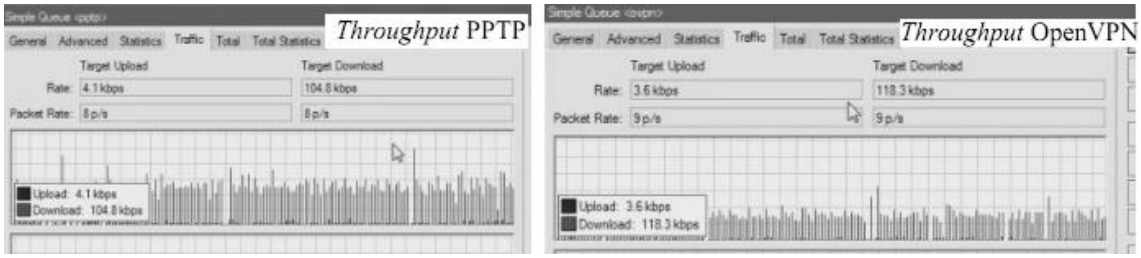
Dalam perancangan sistem jaringan VPN menggunakan PPTP maupun OpenVPN ini penulis membuat sebuah simulasi yang akan diterapkan pada prakteknya nanti, untuk mempresentasikan topologi jaringan berjalan dengan baik atau tidak. Perancangan atau pembuatan simulasi prototipe ini bertujuan untuk:

a. Mengurangi resiko kegagalan saat proses perancangan dan implementasi sistem jaringan VPN dengan PPTP maupun OpenVPN yang sebenarnya.
b. Untuk menjamin bahwa kegagalan atau kesalahan yang terjadi pada waktu proses perancangan, pembangunan dan implementasi tidak mengganggu dan mempengaruhi lingkungan sistem yang sebenarnya.

Pengambilan data diambil pada saat PC *client* terkoneksi dengan VPN dengan menggunakan OpenVPN maupun PPTP yang terhubung dengan *server* VPN yaitu sebuah Mikrotik. Untuk mengetahui seberapa besar t*hroughput* yang dihasilkan penulis melakukan percobaan dengan mengirimkan data berupa video dengan format MP4 sebesar 21 MB dan file berupa suara berformat MP3 sebesar 4 MB. selanjutnya data yang dikirim melalui VPN akan tertangkap oleh perangkat lunak Wireshark dan trafmeter dimana nanti akan terlihat seberapa besar *throughput* yang dihasilkan ketika menggunakan PPTP maupun *throughput* yang dihasilkan menggunakan OpenVPN, serta waktu yang diperlukan untuk melakukan *transfer* suatu file baik berupa video maupun audio. Pengujian dilakukan pada akses internet dengan *bandwidth dedicated* 6 MBPS memiliki kecepatan *download* sebesar 5859 kbps dan kecepatan *upload* 5226 kbps, akses internet ini memiliki ping sebesar 19ms, hasil pengujian bisa saja berbeda jika menggunakan akses internet yang berbeda pula.

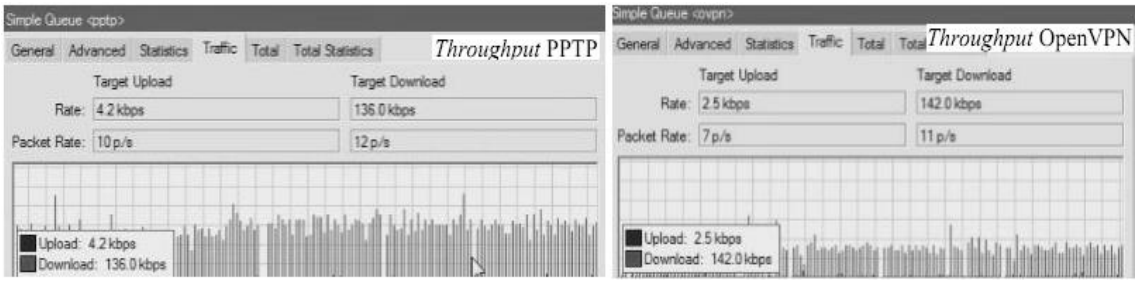
3.1. Analisa Perbandingan dengan data berupa Video

Pada perbandingan dengan data berupa video, *client* VPN akan melakukan *streaming*, pengujian dilakukan sebanyak tiga kali dengan video yang berbeda dan *frame rate* yang berbeda pula. Video pertama berekstensi MP4 dengan *frame rate* sebesar 25 fps, *client* melakukan *streaming* terhadap *file* video tersebut. Pengujian pertama menggunakan PPTP dari hasil pengujian pada *streaming file* tersebut, didapat *throughput* sebesar 68.6 kbps. Selanjutnya penulis mencoba melakukan *streaming* dengan menggunakan OpenVPN, dengan *file* yang sama pada pengujian sebelumnya didapat *throughput* sebesar 118.3 kbps.



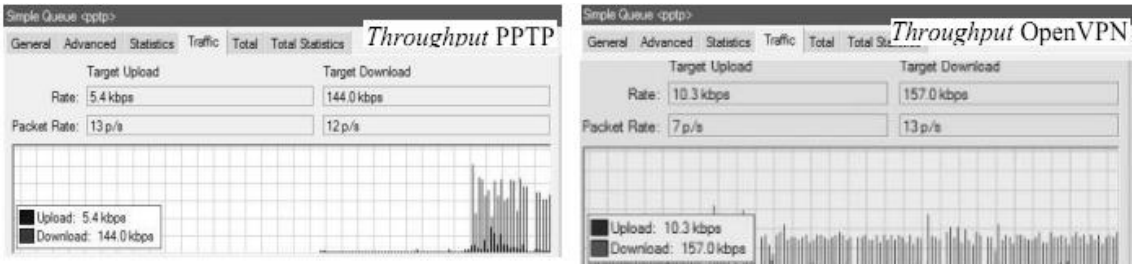
Gambar 3. Hasil Pengujian *Streaming Video* I dengan PPTP dan OpenVPN

Video kedua berekstensi MP4 dengan *frame rate* sebesar 23.97 fps, *client* melakukan *streaming* terhadap *file video* tersebut. Pengujian pertama menggunakan PPTP dari hasil pengujian pada *streaming file* tersebut, didapat *throughput* sebesar 136.0 kbps. Selanjutnya penulis mencoba melakukan *streaming* dengan menggunakan OpenVPN, dengan *file* yang sama pada pengujian sebelumnya didapat *troughput* sebesar 142.0 kbps.



Gambar 4. Hasil Pengujian *Streaming Video* I dengan PPTP dan OpenVPN

Selanjutnya pada pengujian terakhir dilakukan pengujian pada video dengan format MP4 dengan *Frame Rate* sebesar 29.97 fps. Pengujian pertama menggunakan PPTP. Dari hasil pengujian pada *streaming file* tersebut, didapat *throughput* sebesar 144.0 kbps. Selanjutnya penulis mencoba melakukan *streaming* dengan menggunakan OpenVPN, dengan *file* yang sama pada pengujian sebelumnya didapat *throughput* sebesar 157.0 kbps.



Gambar 5. Hasil Pengujian *Streaming Video* I dengan PPTP dan OpenVPN

Dari ketiga hasil pengujian diatas dengan *video* yang berbeda pula juga didapat secara keseluruhan *throughput* yang didapat pada VPN menggunakan protokol PPTP terlihat relatif lebih kecil dibandingkan dengan menggunakan OpenVPN baik pada pengujian pertama, kedua, maupun ketiga, hal ini dikarenakan OpenVPN memiliki proses enkripsi dan dekripsi yang lebih kompleks dibanding dengan PPTP, sehingga membutuhkan *resource* yang lebih besar. Berikut tabel hasil rangkuman dari pengujian diatas.

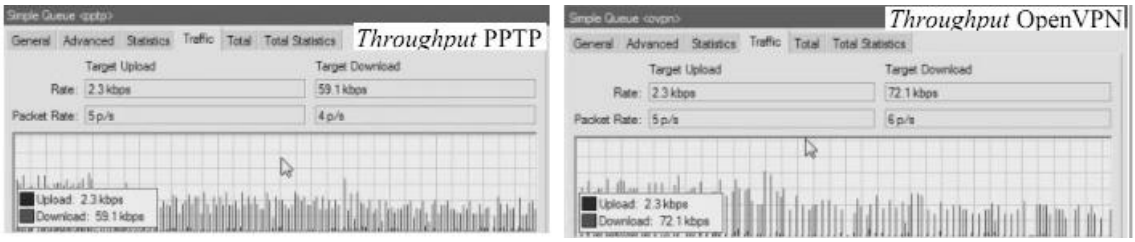
Tabel 1. Data *Throughput Streaming File Video*

No	Pengujian	*Throughput* (kbps)	
		PPTP	OpenVPN
1	Video I ()	104.8	118.3
2	Video II ()	136.6	142.0
3	Video III ()	144.0	157.0
Rata – rata Pengujian		128.5	139.1

3.2 Analisa Perbandingan data berupa Audio

Pada pengujian selanjutnya dilakukan pengujian perbandingan data berupa audio berformat MP3. Pengujian dilakukan sebanyak tiga kali dengan file audio yang berbeda serta ukuran *file* serta *bitrate* yang berbeda. *Bitrate* adalah istilah yang digunakan untuk menggambarkan jumlah data yang diolah dalam jumlah waktu tertentu. Tergantung dari konteksnya, pengukuran umum dari *bitrate* biasanya menggunakan istilah *kilobyte* per *second* (kbps) dan *Megabyte* per *second* (Mbps).

File audio yang pertama berformat MP3 dengan ukuran *file* 3 MB, memiliki *bitrate* sebesar 128 kbps. Pengujian pertama menggunakan protokol PPTP dari hasil pengujian pada *streaming file* audio tersebut, didapat *throughput* sebesar 59.1 kbps. Selanjutnya penulis mencoba melakukan *streaming* dengan menggunakan OpenVPN, dengan *file* yang sama pada pengujian sebelumnya didapat *throughput* sebesar 72.1 kbps.



Gambar 6. Hasil Pengujian Streaming Audio I dengan PPTP dan OpenVPN

File audio kedua yang akan diuji tetap berekstensi MP3 dengan ukuran *file* sebesar 928kb, memiliki *bitrate* sebesar 96 kbps. Seperti pada pengujian sebelumnya, pengujian pertama menggunakan protokol PPTP dari hasil pengujian pada *streaming file* audio tersebut, didapat *throughput* sebesar 74.2 kbps. Selanjutnya penulis mencoba melakukan *streaming* dengan menggunakan OpenVPN, dengan *file* yang sama pada pengujian sebelumnya didapat *throughput* sebesar 96.4 kbps.

File audio yang terakhir tetap pada format MP3 dengan ukuran *file* 3.6MB dengan *bitrate* sebesar 40 kbps. Pada pengujian terakhir ini tetap seperti pengujian sebelumnya, pertama pengujian dilakukan menggunakan protokol PPTP, dari pengujian tersebut didapat *throughput* sebesar 58.6 kbps.

Dari ketiga pengujian audio diatas terlihat tidak jauh berbeda dengan pengujian menggunakan *streaming video* seperti pengujian sebelumnya, tetap didapat secara keseluruhan OpenVPN membutuhkan t*hroughput* yang sedikit lebih banyak dibanding dengan PPTP, selain itu juga *bitrate* suatu *file* berpengaruh terhadap *throughput* yang dihasilkan. seperti contoh terlihat pada pengujian pertama dan kedua, jika dibandingkan *throughput* kedua *file* audio tersebut berbeda, semakin kecil *bitrate* suatu *file* audio semakin kecil pula *throughput* yang dihasilkan. Hal ini membuktikan tidak semata-mata hanya Protokol yang berpengaruh terhadap *throughput* akan tetapi hal-hal lain seperti *bitrate*-pun juga berpengaruh.

Tabel 2. Data *Throughput Streaming File* Audio

No	Pengujian	*Throughput* (kbps)	
		PPTP	OpenVPN
1	Audio I ()	59.1	72.1
2	Audio II ()	74.2	96.4
3	Audio III ()	58.6	81.6
Rata – rata Pengujian		63.97	83.37

Kembali terlihat pada tabel percobaan diatas, *throughput* lebih besar terdapat pada OpenVPN, sama seperti pengujian sebelumnya, hal ini dikarenakan oleh protokol SSL yang terdapat pada OpenVPN, akan tetapi *throughput* yang dihasilkan oleh PPTP maupun OpenVPN terlihat lebih kecil dari pengujian sebelumnya, hal ini dikarenakan *file* audio yang tidak sebesar *file* video seperti pengujian diatas

3.2 Analisa Perbandingan *Security*

Pada PPTP menggunakan protokol GRE (*Generic Routing Encapsulation*) atau IP *tunneling* (IP *encapsulation*) adalah teknik enkapsulasi *packet* IP di dalam *packet* IP. Lebih mudahnya, dengan GRE kita bisa menciptakan "terowongan" yang tentu udah terenkapsulasi sebagai jalur data khusus untuk meneruskan sebuah paket melalui jaringan komputer, baik itu jaringan komputer pribadi ataupun publik.

Pada OpenVPN terdapat pengamanan yang lebih *secure*, OpenVPN menggunakan SSL sebagai pengamannya, inilah sebabnya OpenVPN membutuhkan *Certificate Authority* (CA). Akan tetapi VPN dengan protokol OpenVPN tidak dapat ter*capture* dengan baik pada aplikasi wireshark, hal ini dikarenakan *security* yang digunakan pada OpenVPN jauh lebih baik ketimbang PPTP yaitu menggunakan SSL, berbeda jika dibandingkan dengan protokol PPTP, pada protokol PPTP terlihat dengan jelas ketika koneksi PPTP mulai dibentuk terbukti langsung ter*capture* GRE.

4. Simpulan

Setelah melakukan pengujian sebanyak tiga kali dengan menggunakan *video* yang berbeda, didapatkan suatu kesimpulan bahwa secara keseluruhan *throughput* yang didapat pada VPN menggunakan protokol PPTP terlihat relatif lebih kecil dibandingkan dengan VPN menggunakan OpenVPN. Hal ini dikarenakan OpenVPN memiliki proses enkripsi dan dekripsi yang lebih kompleks dibanding dengan PPTP sehingga membutuhkan *resource* yang lebih besar dibanding dengan PPTP.

Berdasarkan ketiga pengujian audio yang telah dilakukan didapatkan suatu kesimpulan bahwa OpenVPN membutuhkan *throughput* yang sedikit lebih banyak dibanding dengan PPTP, selain itu juga *bitrate* suatu *file* berpengaruh terhadap *throughput* yang dihasilkan. seperti contoh terlihat pada pengujian pertama dan kedua, jika dibandingkan *throughput* kedua *file* audio tersebut berbeda, semakin kecil *bitrate* suatu *file* audio semakin kecil pula *throughput* yang dihasilkan. Hal ini membuktikan tidak semata-mata hanya protokol yang berpengaruh terhadap *throughput* akan tetapi hal-hal lain seperti *bitrate*-pun juga berpengaruh. hal ini dikarenakan oleh protokol SSL yang terdapat pada OpenVPN, akan tetapi *throughput* yang dihasilkan oleh PPTP maupun OpenVPN terlihat lebih kecil dari pengujian sebelumnya, hal ini dikarenakan *file* audio yang tidak sebesar *file* video seperti pengujian diatas

Berdasarkan hasil pengujian dalam sisi *security*, *security* yang terdapat pada OpenVPN jauh lebih baik ketimbang PPTP yaitu menggunakan SSL, bahkan aplikasi wireshark sekalipun tidak dapat meng*capture*, berbeda jika dibandingkan dengan PPTP, pada PPTP terlihat dengan jelas ketika koneksi PPTP dimulai langsung ter*capture* GRE.

Daftar Pustaka

[1] Albert Suwandhi, Juni Erpin. Analisa Sistem Pengaman Data Jaringan Berbasis VPN. STMIK IBBI

[2] Jisnu Adi Widjaya. Perancangan dan Implementasi Jaringan *Virtual Private Network* menggunakan PPTP (*Point To Point Tunnelling Protocol*) pada PT. Mega Tirta Alami. Universitas Muhammadiyah Surakarta. 2013

[3] Muhammad Taufik Roseno. Analisis Perbandingan Protokol Virtual Private Network (VPN) – PPTP, L2TP, IPSEC – sebagai Dasar Perancangan VPN pada Politeknik Negeri Sriwijaya Palembang.

[4] Joko Triyono, Rr. Yuliana Rachmawati K, Fahmi Dhimas Irnawan. Analisis Perbandingan Kinerja Jaringan VPN Berbasis Mikrotik Menggunakan Protokol PPTP dan L2TP Sebagai Media Transfer Data. Institut Sains & Teknologi AKPRIND Yogyakarta. 2014

[5] Sandy Indra Jaya, Rissal Efendi, Noor Miyono. Pemanfaatan Point-to-Point Tunneling Protocol (PPTP) pada Virtual Private Network dalam Akses File Server. *Jurnal Teknologi Informasi-Aiti*. 2012. Vol.9.No.2: 101-200.

[6] I Made Mustika Kerta Astawa, Claudia Dwi Amanda. Pengamanan Jalur Komunikasi Internet Menggunakan PPTP (*Point-to-Point Tunnelling Protocol*). *Prosiding SeTISI Seminar Teknik Informatika dan Sistem Informasi.* 2013. Hal 24-28.

[7] Jimmy, Handriyanto, Handy Sulianto. Analisis dan Pemodelan Remote Access VPN dengan Aplikasi OpenVPN pada PT. Garmindo Utama Jaya. Jakarta Binus University. 2011

[8] Muhammad Ridwan. Analisa dan Perbandingan Layanan Virtual Private Network (VPN) Menggunakan Protokol Point To Point Tunneling Protocol (PPTP) dengan OpenVPN Berbasis Mikrotik. Universitas Pembangunan Nasional "Veteran" Jakarta. 2014.