Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.110-123
ISSN : -

Perbandingan Performa VPN Menggunakan PPTP Dan SSTP Over SSL Dengan Metode *Quality of Service*

Moezes Rasuanda[1], Haeruddin[2]
Sistem Informasi, Fakultas Ilmu Komputer, Universitas Internasional Batam, Sei Ladi, Jl. Gajah Mada, Baloi Permai, Kec. Sekupang, Kota Batam, Kepulauan Riau 29442
Email : moezes@uib.ac.id, haeruddini@uib.ac.id

Abstrak

Dengan majunya perkembangan teknologi begitu juga dengan keamanannya yang sudah seharusnya ditingkatkan. Maka dari itu banyak cara untuk para pengguna meningkatkan keamanan jaringan internet mereka sendiri, dikarenakan tingkat keamanan dari sebuah jaringan sangat lah penting untuk pengguna terhadap data-data yang melintas di jaringan tersebut, seperti perbankan, perusahaan besar, instansi pemerintah dan banyak lagi pengguna yang sangat membutuhkan keamanan jaringan mereka karena segala proses transaksi serta proses kerja berlangsung secara online sehingga menjadi titik tumpu penting nya sebuah keamanan jaringan tersebut. Banyak cara untuk mengamankan sebuah jaringan salah satunya adalah menggunakan VPN, salah satu cara yang mudah dan paling banyak digunakan oleh pengguna untuk mengamankan jaringan mereka, dan tidak hanya satu jenis namun VPN mempunyai banyak jenis atau bisa dibilang protokol, diantara lainnya ada PPTP, L2TP, IPSec, IKEv2, MPLS, SSTP, SSL-VPN. Dan Tujuan dari penelitian ini adalah untuk menguji serta membandingkan performa dari kedua protokol VPN yang sudah ditentukan yaitu protokol PPTP dan SSL, dengan menggunakan metode Quality of Service yang dimana metode ini adalah cara untuk mengukur seberapa baiknya jaringan tersebut dan juga memastikan pengguna mendapatkan qualitas dari servis yang terbaik.

Kata kunci: VPN, Virtual Private Network, PPTP, SSL-VPN, Networking

Abstract

Technology advancement requires high level of security. There are multiple ways for user to improve network security because network security is highly crucial for users with data streaming within the network. Some users of network security are banks, large enterprises, government agencies and other users requiring high network security due to enormous amount of transaction and work-related processes being executed online. Therefore, this becomes important support of network security. Among the ways to secure network is by using VPN which is an easy and commonly used way by users to secure their network. VPN has many types or protocol namely PPTP, L2TP, IPSec, IKEv2, MPLS, SSTP and SSL-VPN. This research is aimed to evaluate and compare performance of two predetermined VPN protocols which are PPTP and SSL protocol using a method called Quality of Service. The method acts as a measure of how well a certain network is, as well as to ensure users achieve best quality and available performance.

Keyword: *VPN, Virtual Private Network, PPTP, SSL-VPN, Networking*

I. PENDAHULUAN

Dengan cepatnya perkembangan didunia teknologi dengan segala kemudahan dan keuntungannya banyak bidang-bidang pekerjaan yang menggunakan jaringan internet sebagai sarana dalam proses kerja, sehingga apapun proses tersebut berketergantungan dengan internet, dengan digunakannya internet didalam bidang pekerjaan dan lainnya sangat membantu memudahkan pekerjaan, mempersingkat waktu pekerjaan, serta

banyak keuntungan lainnya namun tidak luput dari kekurangan, banyak juga kekurangan yang terdapat pada sebuah jaringan internet, salah satunya adalah masalah keamanan.

Keamanan sangat mempengaruhi sebuah jaringan, dikarenakan jaringan yang digunakan untuk proses bekerja adalah salah satu jalur dimana pengiriman data, transaksi data, pengambilan data dan banyak hal-hal penting yang berlalu lintas di sebuah jaringan, dengan tingkat keamanan yang sangat rendah dapat membuat suatu jaringan sangat rentan dari serangan-serangan diluar jaringan tersebut, serangan seperti pencurian data, pengiriman virus, pemalsuan identitas dan banyak hal merugikan lainnya.

Maka dari itu keamanan menjadi poin penting dari pembuatan sebuah jaringan, dengan adanya VPN atau Virtual Private Network ini sangat membantu pengguna untuk mengamankan sebuah jaringan, maka tujuan penulis melakukan penelitian ini untuk mencari metode yang cocok untuk beberapa pengguna agar para pengguna memiliki keamanan jaringan yang sesuai dengan kebutuhan agar memiliki jaringan yang baik.

Penulis menggunakan metode Quality of Service untuk membandingkan performa dari dua jenis protokol VPN yang sudah dipilih yaitu protokol PPTP dan SSL, yang dimana keduanya mempunyai kelebihan dan kekurangannya masing-masing, namun dengan digunakannya QoS atau Quality of Service ini mempermudah penulis untuk menentukan perbandingan apa saja yang menjadi pertimbangan performa dari kedua protokol, ini adalah beberapa parameter yang digunakan untuk mengukur menggunakan Qos: Packet Loss, Delay, Througput. Dengan digunakannya metode ini pastinya menjadi patokan dari kemampuan tiap VPN yang di teliti, sehingga membantu banyak pihak untuk mengetahui tiap performa dari tiap protokol-protokol yang ada.

Menurut penjelasan diatas yang dimana menjadikan latar belakang penulis menjadikan topik "**PERBANDINGAN PERFORMA VPN MENGGUNAKAN PPTP DAN SSTP OVER SSL DENGAN METODE QUALITY OF SERVICE**" menjadi topik skripsi. Yang dimana penulis akan mencoba untuk membandingkan performa dari satu protokol dengan protokol lainnya

Sesuai dengan latar belakang yang telah dijelaskan diatas maka penulis akan merumuskan beberapa masalah yang akan dibuat didalam laporan ini ialah:

1. Bagaimana mengukur performa dari protokol PPTP dan SSL dengan Quality of Service?
2. Bagaimana membangun kedua protokol dengan persyaratan-persyaratan yan dibutuhkan?

Penelitian yang dituju dengan topik "Perbandingan Performa VPN menggunakan PPTP dan SSTP Over SSL Dengan Metode Quality of Service" yang memiliki tujuan:

1. Membandingkan performa dari protokol-protokol VPN yang ada sehingga membantu para pengguna nantinya untuk memilih lebih tepat.
2. Memberikan persepsi yang berbeda dari kedua protokol tersebut agar dapat bermafaat bagi pembaca.

.

II. LANDASAN TEORI

A. Tinjauan Pustaka

"Perbandingan performansi jaringan VPN metode PPTP dengan metode IPS" adalah salah satu judul jurnal yang ditulis oleh (Nugroho, 2014) membahas tentang sebuah Analisa yang membandingkan dua protokol untuk diuji performa jaringan dari kedua protokol dalam mengatasi masalah yang terjadi.

Jadi saat sebuah komunikasi yang terjadi dari titik A ke titik B terjadi didalam dunia internet pastinya akan melewati jaringan umum atau publik, sebuah ilustrasi saat seorang pengemudi yang

berpergian dari kota A ke kota B pastinya akan melalui jalanan umum, yang dimana rentan terjadi banyak masalah, begitu juga dengan sistem jaringan yang mengantarkan paket dari titik A ke titik B, maka dari itu VPN sangat berperan penting untuk mengamankan atau membuatkan jalur pribadi untuk paket yang akan diantar tersebut sehingga terhindar dari berbagai ancaman, menurut (Supriyono, 2015) yang membahas tentang Penerapan jaringan Virtual Private Network Untuk Keamanan Komunikasi Data.

Penggunaan VPN dapat meminimalisir biaya dalam memberikan keamanan dari sebuah jaringan, misalkan sebuah perusahaan yang ingin datanya diamanakan tidak perlu membuat jaringan sendiri yang memakan biaya yang tergolong besar, cukup memasang jaringan publik biasa yang hanya tinggal diterapkan VPN didalamnya, sehingga tidak memakan banyak biaya dengan membeli kabel dan device lainnya yang membuat biaya operasional sangat tinggi,

banyak keuntungan dari penerapan VPN didalam jaringan bukan hanya biaya namun management, yang dimana user dengan mudah mengontrol atau mengkonfigurasi jaringan yang telah diamankan tersebut tnapa memakan waktu serta biaya yang tinggi. Menurut (Sakiwan, 2012) Kajian VPN lapan dan pemanfaatannya dalam mendukung pengembangan Government.

Menurut jurnal yang ditulis oleh (Triyono, 2014) yang berjudul Analisis Perbandingan Kinerja Jaringan VPN Berbasis Mikrotik Menggunakan Protokol PPTP dan L2TP Sebagai Media Transfer Data, yang mengatakan bahwa sifat dari VPN tersebut yang nyatanya tidak terlihat makanya bisa dikatakan sebagai sistem tunneling yang pada kenyataanya sistem ini tidak benar-benar tersembunyi seperti didalam terowongan, namun hanya tidak menghiraukan tujuan lain, hanya focus ke titik yang dikonfigurasikan, ada beberapa fungsi dari VPN tersebut:

1. Intergritas Data, keakurasian data yang dikirim dipastikan tidak ada perubahan selama masa pengiriman.
2. Enkripsi, keamanan data yang dikirim dipastikan tidak akan diganggu oleh pihak ketiga.
3. Autentikasi Sumber Data, kepastian data memang dari sumber pengirim, bukan pihak ketiga yang mencoba memalsukan paket.

B. Landasan Teori

Dalam membuat sebuah perbandingan antara satu VPN dengan VPN yang lain, peneliti menaruh landasan teori. Yang dimana landasan teori yang isinya tentang sekumpulan teori tentang penelitian yang nantinya dapat memperkuat teori dari penelitian ini. Ini adalah beberapa teori yang akan dipakai dalam penelitian adalah sebagai berikut:

1. Keamanan Jaringan

Keamanan jaringan didefinisikan sebagai sebuah implementasi dari keamananp, kebijakan, serta proses dalam mencegah sebuah jalan masuk atau akses untuk masuk tanpa izin ke dalam sebuah jaringan atau sumber daya data untuk melakukan perubahan, pencurian, perusakan data atau sumberdaya. (Marti widya sari, 2015) VPN merupakan salah satu metode untuk mengamankan sebuah jaringan dari berbagai jenis gangguan dari luar sebuah jaringan.

VPN atau Virtual Private Network yang membuat jaringan public menjadi privat adalah salah satu cara yang efektif untuk mengamankan jaringan-jaringan. VPN mulai banyak digunakan dikarenakan perusahaan-perusahaan besar mulai mengembangkan jaringan bisnis mereka sehingga keamanan jaringan menjadi faktor penting untuk mengamankan jaringan mereka agar bisa terus terhubung secara local dengan cabang atau anakan perusahaan yang lokasinya jauh dari pusat, sehingga dengan menggunakan VPN dapat membuat jaringan public menjadi private sehingga kecil kemungkinan adanya pihak lain untuk dapat mengakses tanpa izin untuk merubah, mencuri, merusak data atau

sumberdaya. Dengan VPN dapat mengecilkan anggaran dari perusahaan untuk tidak membangun jaringan pribadi sendiri yang akan memakan biaya yang cukup banyak, cukup dengan jaringan public yang dilapisi dengan VPN sehingga hanya yang memiliki akses saja yang dapat mengakses dengan mudah sebuah jaringan tersebut. Tidak hanya sebuah perusahaan menggunakan VPN, dikalangan pemerintahan juga menggunakan VPN dikarenakan sumber daya data yang terdapat memiliki tingkat sensitifitas yang tinggi, sehingga tidak boleh diakses oleh sembarang orang.

Dengan adanya VPN maka keamanan sebuah jarigan menjadi lebih terjamin sehingga pengguna tidak perlu khawatir untuk mengakses data keluar dan masuk, karena sekalipun ada pengguna lain mengakses jaringan public yang sama namun pengguna tersebut berada diluar dari VPN maka tidak bisa mengakses sumber daya data dari pengguna utama yang menaruh VPN didalam jaringan tersebut, karena VPN membuat jaringan sendiri didalam jaringan tersebut.

2. Quality Of Service

Quality of Service adalah salah satu metode untuk mengukur qualitas dari seberapa baik sebuah jaringan tersebut yang menggunakan beberapa standar atau beberapa patokan yaitu delay, packet loss, jitter, throughput menurut (Lubis & Pinem, 2014). Agar dapat mengetahui standar qualitas dari jaringan tersebut, serta karakteristik dari sebuah layanan tersebut sehingga pengguna memperoleh jaringan yang sesuai dengan yang diharapkan oleh pengguna.

Quality of Service memiliki beberapa parameter untuk mengukur kualitas setra karakteristik jaringan tersebut:

Delay: Merupakan waktu yang dibutuhkan sebuah paket untuk bisa sampai ketujuan dengan mengantri serta memilih jalur-jalur untuk bisa sampai ketujuan, rumusnya adalah waktu jeda antara paket pertama dan terakhir dibagi total paket yang diterima.

Packet loss: Merupakan paket yang hilang atau paket yang tertunda dikarenakan banyak faktor, misalkan penurunan jaringan atau melebihi batas standarisasi dari jaringan tersebut, rumusnya adalah paket yang dikirim dikurang paket yan diterima dibagi paket yang dikirim dikali seratus persen

Jitter: Merupakan variasi delay yang terjadi akibat panjang antrian serta pengolahan data dan dalam waktu pengiriman paket, jitter terjadi akibat paket data yang berbeda-beda mengalami waktu penundaan yang berbeda-beda, rumus menghitungnya adalah total variasi delay dibagi total paket yang diterima dikurang satu.

Throughput: Ukuran seberapa cepat kita mengirim data melalu jaringan, yang diukur dalam bps (bit per second) Throughput ialah jumpah kedatangan paket yang berhasil tiba ditujuan, rumusnya ialah data yang diterima dibagi antara paket pertama dan paket terakhir dikali delapan per seribu Kbps.

Sebagaimana dengan sebutannya Quality of Service mempunyai beberapa fungsi untuk memberikan pelayanan yang berkualitas, ini adalah beberapa fungsi dan kegunaannya:

Memberikan performa yang maksimal atau prioritas untuk aplikasi yang kritis didalam jaringan, serta aplikasi-aplikasi yang sensitif seperti video dan pesan suara.

Memaksimalkann pemakaian investasi jaringan yang sudah berjalan

Memberikan kendali penuh untuk mengelola jaringan serta menggunakan fungsi-fungsi jaringan dengan maksimal.

3. Jaringan Komputer

Jaringan ialah sebuah sistem yang didalamnya perangkat lunak, perangkat keras, media berkomunikasi yang dimana dibutuhkan untuk menyatukan beberapa sistem komputer dan perangkat lainnya menurut (Sharon & Supardi, 2014) Jaringan mempunyai peran yang penting karena memiliki beberapa alasan dan kegunaan. Pertama, jaringan komputer memudahkan dalam melakukan sebuah bisnis sehingga tidak memakan waktu serta lebih fleksibel. Kedua jaringan mempermudah sebuah kegiatan dalam

memberikan data, membagi data, meminta data dari komputer lain ke komputer lain. Ketiga jaringan komputer memudahkan beberapa orang dalam berbagi data realtime yang sedang dikerjakan. Dan yang terakhir, jaringan komputer memudahkan beberapa pekerjaan yang seharusnya diadakan pertemuan menjadi tidak harus karna bisa melakukan pertemuan online.

4. Jenis-Jenis Jaringan Komputer

Menurut (Wongkar et al., 2015) dalam jurnal yang ditulisnya dengan judul Analisa Implementasi Jaringan Internet Dengan Menggabungkan Jaringan LAN Dan WLAN, jenis-jenis jaringan terdapat beberapa jenis, penulis mengambil contoh 4 yang paling sering digunakan:

a) Wireless Local Area Network ialah satu jenis jaringan yan tidak menggunakan kabel sebagai penghubung router dengan device pengguna, dengan hanya memancarkan sinyal radio yang menjangkau sesuai kemampuan alat dengan tingkat kecepatan yang sangat tergantung dengan jarak dari router dengan device pengguna serta penghalang yang dapat menghambat sinyal sehingga dapat mengurangi besar kecil frekuensinya, WLAN sangat efektif dan banyak digunakan dikarenakan dapat menghemat alat seperti kabel yang dibutuhkan dalam jenis jaringan LAN, dikarenakan dapat tersambung dengan banyak device namun tetap terdapat limit agar penggunaan jaringan bisa terpakai dengan baik.
b) LAN atau Local Area Network merupakan jenis jaringan yang lumayan banyak digunakan selain WLAN dikarenakan kecepatannya sangat stabil dibanding WLAN, karena jaringan yang menggunakan LAN tidak bergantung dengan sinyal, melainkan menggunakan kabel, jadi saat satu device terhubung dengan satu router menggunakan jenis jaringan ini maka tidak ada yang bisa menghambat kecepatan jaringan dari jenis ini kecuali kerusakan kabel atau device tersebut, jenis jaringan ini masih banyak digunakan diperkantoran serta dibeberapa warung internet dikarenakan kecepatannya yang stabil, namun jenis jaringan ini memakan alat, jadi apabila ada sepuluh device yang harus tersambung maka pengguna harus menyiapkan switch untuk dapat menyambungkan semua device dengan baik.
c) WAN atau Wide Area Network adalah jenis jaringan dengan jangkauan yang cukup luas seperti menghubungkan satu wilayah dengan wilayah lainnya serta negara dengan negara lainnya, jenis jaringan ini sangat luas cakupannya, dan WAN biasa digunakan untuk mencakup program-program yang terus berjalan dibeberapa negara-negara yang berbeda.
d) PAN atau Personal Area Network salah satu jenis jaringan yang paling sering digunakan dikarenakan jenis jaringan ini selalu ada disekitar kita, contohnya menyambungkan komputer dengan wireless mouse, dengan bluetooth atau bisa juga denga portable hotspot menggunakan smartphone atau komputer.

5. Jenis-jenis VPN

Menurut (Yusron Aulia, 2016) bahwa VPN adalah salah satu metode untuk mengamankan sebuah jaringan yang dimana menggunakan jaringan publik namun dengan koneksi pribadi, serta VPN juga memberikan solusi untuk meringankan biaya-biaya operasional. Dengan menggunakan sistem tunneling, VPN memiliki beberapa jenis metode, seperti:

a. PPTP (Point to Point Tunneling Protocol), salah satu jenis VPN yang mempunyai konfigurasi yang mudah, yang dimana proses nya membungkus data dan dikirimkan melalui tunneling lalu dikirimkan melalui jaringan internet publik. VPN jenis PPTP beroperasi pada port 1723 dan memakai IP protokol

47/GRE untuk pemrosesan enkapsulasi paket data.

b. SSTP (Secure Socket Tunneling Protocol), salah satu jenis VPN yang serupa dengan PPTP namum mempunyai beberapa kelebihan dan untuk memanfaatkan VPN ini secara maksimal adalah dengan memberikan sertifikat SSL pada masing-masing perangkat. Dan VPN ini menggunakan port 443.
c. L2TP (Layer Two Tunneling Protocol), adalah jenis VPN yang dimana adalah modifikasi dari VPN PPTP yang dimana VPN ini menambahkan lapisan kedua untuk mengotentikasi PPP dan LAC, dan VPN ini menggunakan port 1701.
d. OpenVPN, salah satu jenis VPN yang mudah digunakan dan mempunyai tingkat keamanan yang secure, dan jenis VPN ini juga membutuhkan serfikasi pada setiap perangkat sama dengan jenis VPN SSTP, dan menggunakan UDP port 1194.

6. Topologi Jaringan

Menurut jurnal dengan judul Implementasi Tools Network Mapper pada Lokal Area Network bahwa topologi jaringan adalah jenis-jenis atau suatu cara untuk menghubungkan suatau device dengan device lainnya sehingga terbentuklah sebuah jaringan, topologi jaringan sendiri memiliki beberapa jenis-jenis atau arsitekturnya sendiri:

1. Topologi Bintang, adalah topologi yang dimana semua perangkat terhubung langsung ke konsentrartor.
2. Topologi Cincin, adalah topologi yang sambung menyambung tanpa putus seperti bentuk cincin.
3. Topologi Bus, adalah topologi yang dimana satu kabel lurus ditarik dan setiap perangkat terhubung kekabel tersebut.
4. Topologi Campuran, adalah gabungan dari masing-masing topologi sesuai dengan kebutuhan pengguna.

Diatas adalah beberapa jenis topologi yang sering dijumpai atau sering digunakan pada pembuatan jaringan dengan skala yang cukup banyak digunakan menurut (Ginta, 2013).

7. Teknologi Tunneling

Teknologi Tunneling adalah teknologi jaringan yang dimana dikatakan tunneling dikarenakan tugasnya hanya satu jalur, tidak untuk mampir-mampir di titik-titik didalam jaringan, bisa dikatakan sebagai Point-to-Point¬. Dikarenakan tugas tunneling ini bertugas untuk fokus mengantar suatu paket dari asal ke tujuan, namun yang sebenarnya sistem ini tidak benar benar berada didalam sebuah tunnel melainkan tetap berada di jaringan publik tapi tidak menghiraukan paket-paket lain yang berada pada jaringan tersebut, sehingga terlihat seperti tunneling dan sebaliknya juga paket lain tidak bisa sembarangan masuk kedalam sistem ini dikarenakan sistem ini memiliki alamat yaitu IP yang sudah terdaftar dari asal ke tujuan yang dimana memiliki tingkat enkripsi yang baik, sistem inilah yang membuat VPN menjadi salah satu opsi untuk keamanan dalam penggunaan sebuah jaringan, menurut (Afrianto & Setiawan, 2013).

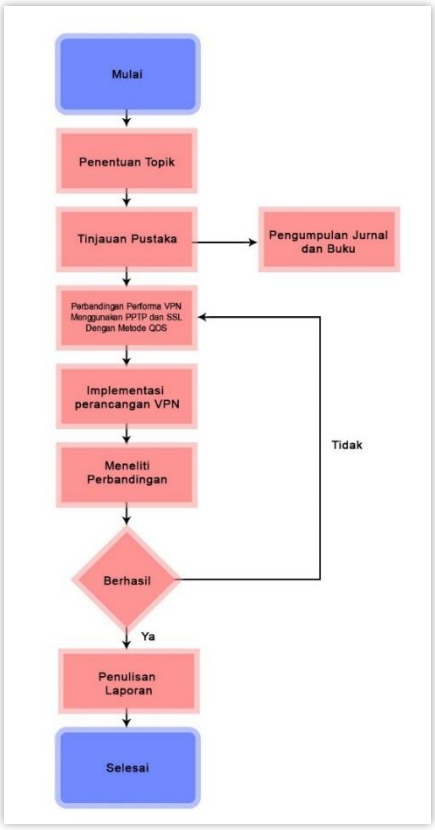
8. Network Development Life Cycle (NDLC)

NDLC atau Network Development Life Cycle ialah sebuah metode penelitian yang lumayan sering digunakan dalam beberapa penilitian yang dimana metode ini sangat mudah diterapkan serta dipahami. Disebabkan metode ini sangat berfungsi untuk mengembangkan serta merancang jaringan untuk dapat bisa diketahui statistik dan kinerja jaringannya. Dari hasil pengembangan serta perancangan tersebut dapat kembali dianalisa untuk melakukan perbaikan, perubahan, serta peningkatan jaringan serta desain dan skemanya, dan meningkatkan keamanan serta manajemen penggunaanya. Menurut (Kurniawan, Nurfajar, Dwi, & Yunan, 2016).

III. METODE PENELITIAN

A. Alur Penelitian

Alur penelitian ialah langkah-langkah yang dilakukan oleh penulis agar penelitian berjalan sesuai dengan alur yang teratur, mulai dari tahapan awal perancangan hingga penyelesaian, berikut adalah alur dan tahapan dari penelitian:



Gambar 1. Alur Penelitian

Dibawah ini adalah beberapa penjelasan tentang alur-alur dari diagram yang ada di atas:

1. Penentuan topik adalah dimana penulis menentukan topik untuk diteliti dan dicari rincian-rincian materinya agar bisa dijadikan karya ilmiah yang akan penulis buat.
2. Setelah menentukan topi yang dipilih maka selanjutnya penulis akan mengumpulkan informasi serta data-data yang menjelaskan tetnagn topik tersebut untuk dijadikan landasan teori, langkah ini adalah langkah yang paling penting dikarenakan landasan teori lah yang memperkuat karya ilmiah.
3. Langkah selanjutnya adalah Analisa, dimana penulis melakukan Analisa pada karya ilmiah yang ditulis sehingga penulis dapat merumuskan permasalahan yang ada sehingga nan
4. Kemudian langkah selanjutnya ialah implementasi, yang dimana penulis merancang sistem yang menjadi landasan proyek dari karya ilmiah tersebut agar dapat berjalan dengan baik.
5. Tahap selanjutnya adalah pemantauan dari pengalaman sistem yang sudah dirancang, agar penulis dapat melihat perbandingan dari sistem yang sedang berjalan.
6. Selanjutanya apabila terjadi masalah didalam proses pemantauan, penulis akan mengulang ke tahap Analisa untuk memperbaiki masalah yang ada, namun jika tidak terjadi masalah maka penulis akan melanjutkan karya ilmiah ketahap selanjutnya.
7. Selanjutanya atau tahap paling akhir ialah penulisan laporan, tahap dimana penulis merangkum semua nya untuk dijadikan sebuah laporan atas karya ilmiah yang diteliti.

B. Analisa Permasalahan

Dengan majunya perkembangan teknologi dalam dunia bisnis dan lainnya maka semakin dibutuhkan juga inovasi serta pembaharuan dari segala jenis aspek, salah satunya adalah internet. yang dimana internet menjadi salah kebutuhan pokok dalam menjalankan apapun di era sekarang, terutam dalam topik yang sedang penulis teliti ini ialah tentang keamanan jaringan, yang dimana internet juga memiliki kekurangan dalam bidangnya.

Dengan pesatnya penggunaan internet didalam bidang bisnis dan lainnya, membuat internet menjadi kebutuhan pokok yang dimana semuanya bergantung penuh pada internet, yang dimana internet sangay memudahkan serta mempersingkat waktu kerja, namun disisi lain internet juga memiliki kekurangan yaitu dari segi keamanan juga, banyak pihak-pihak dan oknum-oknum yang tidak suka atau mau mencari keuntungan diatas kerugian orang lain, maka dari itu VPN menjadi salah satu opsi untuk mengamankan internet yang

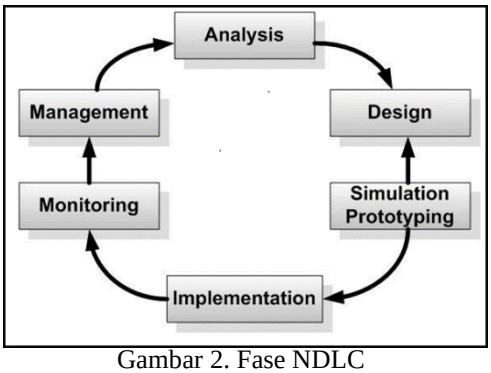
pengguna miliki, VPN mengamankan jaringan internet yang digunakan dengan cara memfokuskan paket yang diantar melalui jaringan local untuk dapat sampai ketujuan tanpa terganggu atau menggangu paket lain yang berada pada lokal yang, VPN juga mengenkripsikan paket yang diantar dari semula hingga tujuan dan memastikan paket yang diantar sesuai dari awal mula

Dengan adanya VPN didalam jaringan internet yang digunakan oleh pengguna pastinya akan memberikan kesan yang aman dalam proses melakukan bisnis serta kerjasama antar pihak tanpa merasa khawatir akan serangan-serangan yang terjadi dari luar lingkup jaringan.

C. Analisa Perancangan

Dalam penelitian "Perbandingan Performa VPN Menggunakan PPTP Dan SSTP Over SSL Dengan Metode Quality Of Service" penulis menggunakan cara Network Development Life Cycle sebagai metode penulisan. Agar proyek yang telah di modifikasi sedemikian rupa dapat terarah dengan baik sesuai dengan tujuan yang diinginkan, NDLC ialah sebuah metode yang dimana memiliki siklus atau tahapan pada sebuah sistematis perancangan sistem pada jaringan komputer.

Didalam metode NDLC ini terdapat 6 langkah yang dapat dilihat pada gambar di bawah:



Gambar 2. Fase NDLC

Terdapat beberapa penjelasan yang dirangkum terhadap tahapan-tahapan pada gambit diatas:

1. Analysis

Tahapan awal dari metode ini ialah Analisa yang dimana tahapan ini mencari masahal yang ada, dan juga mencari kebutuhan apa saja yang diperlukan untuk menjalankan penulisan ini, dengan melakukan survey, wawancara dan lainnya.

2. Design

Tahapan selanjutnya ialaha Desain yang dimana tahapan ini ialah tahapan dimana percangan jaringan dari infrastrukturnya serta perancangan sistem yang akan dibuat, tahapan infrastruktur ini akan dilakukan dengan merancang sebaik mungkin sistem serta jaringannya agar nantinya dapat memaksimalkan karya ilmiah yang dibuat.

3. Simulation

Simulasi ialah tahapan awal dimana setelah sistem serta jaringan dibangun nantinya akan diuji dulu sementara untuk melihat kinerja pada awal pengecekan agar bisa dilihat apakah sistem sudah berjalan dengan baik.

4. Implementation

Tahapan selanjutnya ini adalah tahapan yang penting dikarenakan sistem yang sudah dirancang akan diterapkan semuanya agar menjadi sistem yang utuh, agar bisa dipastikan bahwa rancangan sistem ini berhasil,

5. Monitoring

Tahapan selanjutnya ini ialah melakukan pemantauan dari sistem yang sudah diimplementasikan pada tahapan sebelumnya yang dimana tahapan ini ialah tahapan yang juga penting karena pada tahapan inilah dimana masalah serta kekurangan dari sistem yang telah dirancang terlihat, agar dapat diperbaharui lagi kedepannya agar menjadi sistem yang baik.

6. Management

Tahapan terakhir ini ialah tahapan dimana setelah semua berjalan dengan baik akan dibutuhkan penanganan berkala pada sistem yang dimana sistem pastinya akan selalu butuh pemantauan serta pembaharuan setiap masanya, agar sistem yang telah dibuat tersebut menjadi sistem yang bisa terus berguna.

Didalam merancang sistem perbandingan VPN ini, penulis telah melakukan pertimbangan serta Analisa untuk dapat bisa membangan penelitian tentang perbandingan VPN ini, berikut ini adalah anilsa yang dibutuhkan:

1. **Analisa Kebutuhan Perangkat Keras**

Untuk bisa merancang sistem perbandingan VPN ini, penulis membutuhkan beberapa komponen serta perangkat untuk melengkapi kebutuhan sistem agar dapat berjalan dengan baik:

- Remote Client (personal computer) Remote client atau sebuah komputer yang menjadi tempat untuk mengontrol serta melakukan proses dari router ke router.
- Router Router adalah sebuah alat yang dapat menghubungkan beberapa alat untuk dapat tersambung keinternet serta dapat mengirimkan paket data melalui internet atau jaringan lainnya yang melalui sebuah proses yaitu routing:

2. **Analisa Kebutuhan Perangkat Lunak**

Tidak hanya membutuhkan perangkat keras, dalam melakukan penelitian ini penulis juga membuthkan perangkat lunak untuk melengkapi pembuatan sistem ini.

- Aplikasi winbox, tempat melakukan konfigurasi router mikrotik.
- Wireshark aplikasi untuk mengukur serta memenuhi persyartan Quality of Service.

III. IMPLEMENTASI

A. Analysis

Untuk merancang sebuah sistem, sangat dibutuhkan satu tahap yang dinamakan analisis, pada permulaan untuk merancang sebuah sistem agar penelitian yang dirancang akan dapat berjalan dengan baik, penulis melakukan penelitian terhadap dua protokol yang akan di uji.

Dengan meneliti terlebih dahuhlu penulis memperoleh informasi tentang kelebihan dan kekurangan dari kedua protokol tersebut, maka penulis mencoba untuk menguji sendiri dengan metode yang penulis gunakan, dikarenakan tingkat kebutuhan dari pengguna terhadap kedua protokol sangat berbeda, karena dari kedua protokolo mempunyai kelebihan nya masing-masing, serta kekurangan yang juga bisa menjadi masalah dalam penggunaan dikemudian harinya. Penulis juga menelita bahwa tingkat keamanan juga berbeda dan ketersediaan disetiap perangkat juga terbatas dari salah satu protokol, dikarenakan itu penulis akan mengimplementasikan agar bisa meneliti hasil fakta dari dua protokol tersebut agar bisa menjadi acuan dikemudian harinya.

Dikarenakan keamanan menjadi peran yang penting dalam dunia internet sekarang, sebab data yang disimpan, diperoleh, diubah, diakses adalah data-data yang penting sehingga menjadi akan sangat riskan apabila jaringan internet yang didalamnya adalah data-data yang privasi tidak diberikan keamanan yang baik, akan sangat mudah untuk orang-orang yang mengerti tentang jaringan untuk bisa masuk mengambil, merubah serta merusak data yang ada didalamnya.

B. Design

Kemudian setelah data-data anilisa yang sudah diperoleh penulispun melakukan tahapan desain, tahapam dimana penulis akan merancang sistem yang akan dibuat perbandingannya dengan menggunakan beberapa perangkat keras yang sudah dicantumkan pada bab 3.3 Analisa Kebutuhan Perangkat Keras.

C. Simulation

Kemudian setelah sistem dirancang dan dibuat, lalu penulis meneruskan untuk disimulasikan sistem yang telah dirancang dan dibuat tersebut, proses ini dilaksanakan agar penulis dapat melihat kinerja dari sistem yang sudah dirancang tersebut agar selanjutnya dapat dijadikan referensi pada saat tahap implementasi

Untuk mensimulisasikannya, penulis memakai perangkat lunak WinBox untuk melakukan konfigurasi pada kedua router yang nantinya akan dijadikan Server dan Client untuk dapat menjalankan sistem

VPN dibutuhkan kedua ini agar metode pengukuran performa bisa diukur dikarenakan adanya timbal balik dari pihak client dan server. Dengan terjadinya tahap simulasi ini akan bisa menjadi referensi untuk diimplementasikan menjadi sistem yang lebih baik lagi.

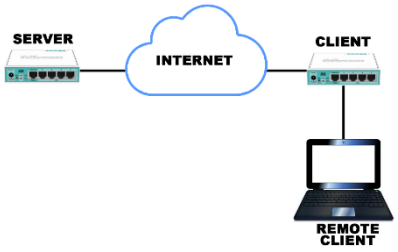
D. Implementation

Dengan berjalan baiknya tahapan simulasi, lalu penulis melanjutkan tahapan implementasi Perbandingan Performan VPN Menggunakan PPTP dan SSTP Over SSL Dengan Metode Quality of Service.

Dalam tahapan ini penulis melakukan konfigurasi pada dua jenis protokol VPN ini dengan melakukan konfigurasi dengan menggunakan aplikasi WinBox, dibawah ini akan diberikan gambar serta tahapan yang akan diurai dalam proses implementasi:

1. Konfigurasi VPN

Langkah pertama yang harus dilakukan untuk melakukan konfigurasi jaringan ialah mengetahui terlebih dahulu apa yang harus dibuat, desain seperti apa yang mau di buat atau topologinya seperti apa, disini penulis menggunakan topologi yang standar.



Gambar 3 Desain Topologi

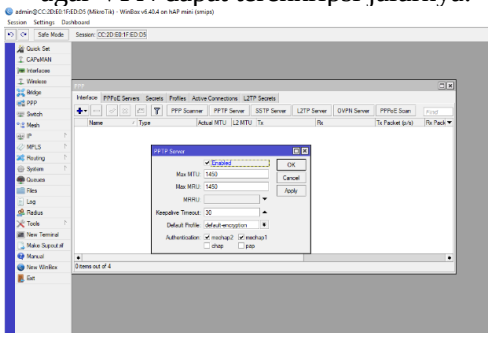
Gambar diatas menjadi patokan untuk membuat penulis untuk melakukan konfigurasi kedua protokol, router server terhubung dengan internet begitu juga dengan router client yang terhubung langsung dengan pc yang akan mengontrol client, langkah-langkah nya akan dijabarkan dibawah:

2. Konfigurasi PPTP

a. Sebelum melakukan konfigurasi pada router A, pastikan router telah siap dan dalam kondisi hidup, pastikan juga kabel LAN terpasang dengan baik pada router dan tidak mengalami kerusakan atau masalah, sebelum masuk ke tahap selanjutnya ada baiknya untuk melakukan reset router untuk melakukan konfigurasi awal, dikarenakan adanya konfigurasi default.

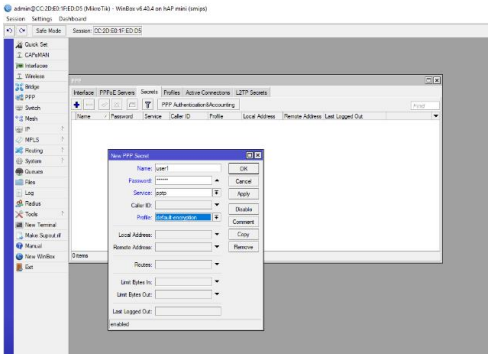
Gambar 4 Tampilan awal sebelum konfigurasi Router A/Server

b. Tahapan selanjutnya ialah melakukan konfigurasi PPTP Server, terletak pada menu PPP lalu pilih tab Interface dan ada menu PPTP Server. Akan terbuka jendela PPTP Server, centang kolom Enabled untuk mengaktifkan PPTP Servernya, lalu patsikan Default Profile pada mode default-encryption agar VPN dapat terenkripsi jalurnya.



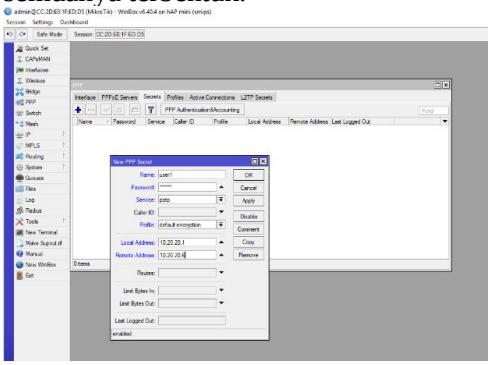
Gambar 5 Konfigurasi PPTP Server

c. Kemudian konfigurasi Secret, dimana tahap ini adalah tahap untuk memberikan atau membuat user dan pass untuk nantinya sebagai autentikasi untuk client bisa terhubung pada server, serta mengkonfigurasikan service pada menu pptp dan profile default-encryption.



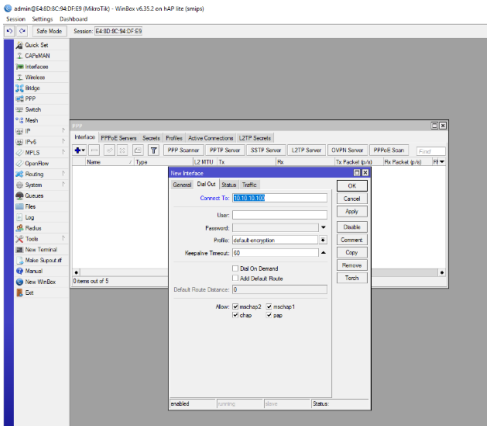
Gambar 6 Konfigurasi Secret

d. Masih pada tabel yang sama yaitu PPP Secret, selanjutnya adalah memberikan Address pada local yang dimana IP tersebut terpasang di router tersebut atau router server, lalu masukan juga remote address yang dimana ip ini yang nantinya akan diberi kepada client setelah semuanya terbentuk.



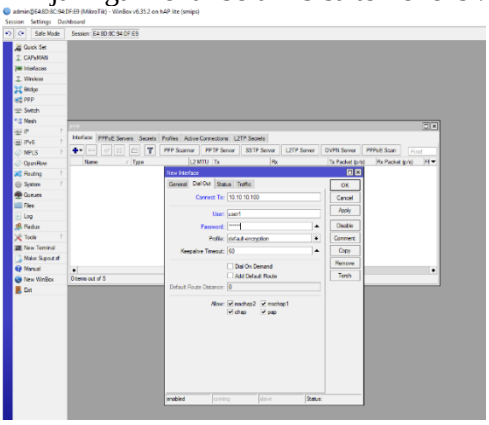
Gambar 7 Konfigurasi IP pada Secret

e. Setelah tahap diatas selesai pastinya konfigurasi PPTP Server sudah selesai, langkah selanjutanya ialah konfigurasi di router Client atau router B, langkah pertama yang dilakukan adalah menambahkan PPTP Client lalu isi set semuanya pada jendela New Interface, pilih tab Dial out lalu set Connect to dengan memasukan ip public router A.



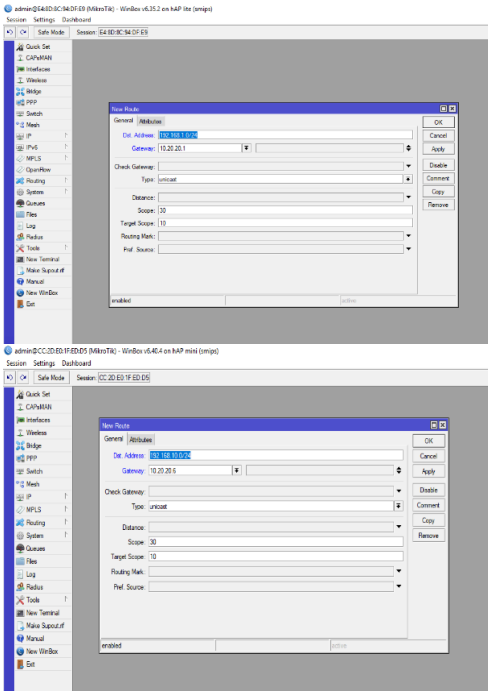
Gambar 8 Konfigurasi IP server pada Router B/Client

f. Lalu masukan user dan password sesuai dengan yang dikonfigurasikan pada router server pada tahap sebelumnya dan pastikan agar sesuai dengan router server agar bisa terkoneksi, lalu pastikan profile tetap pada default-encryption. Pada tahap ini VPN pada router server dan router client sudah terbentuk, namun pada jaringan lokal belum bisa terkoneksi.



Gambar 9 Konfigurasi User dan Password

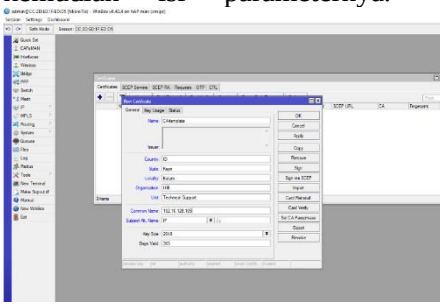
g. Agar bisa saling terkoneksi antara router server dengan router client perlu ditambahkan routing static pada kedua router, masuk pada menu IP lalu pilih Routes dan terdapat satu IP yang bertanda bendera yang muncul dikarenakan konfigurasi sebelumnya, lalu tambahkan IP baru pada label Dst. Address dan Gateway, tahap ini dilakukan pada kedua router, server dan client.



Gambar 10 Konfigurasi penambahan IP Static pada router B dan A

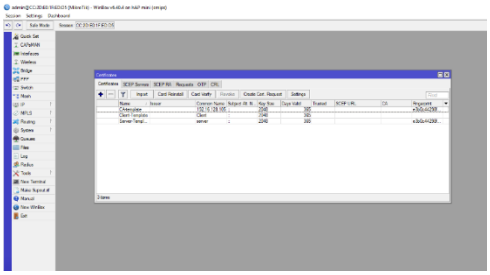
h. Setelah VPN PPTP sudah terbuat dan sudah bisa digunakan maka mulai lah pada tahap pengujian performa dengan mengukur jitter, delay, packet loss, throughput

3. Konfigurasi SSTP dengan sertifikasi SSL
   a) Tahapan pertama adalah membuat sertifikat SSL pada router server apabila tidak mempunyai OS Linux, pada menu System pilih Certificates lalu pilih New Certificate, kemudian isi parameternya.



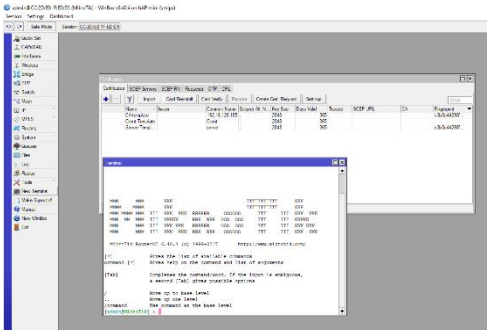
Gambar Pembuatan Sertifikat SSL

   b) Penulis akan membuat tiga sertifikat SSL disini, yang pertama Certificate Authority, Certificate Server an Certificate Client.



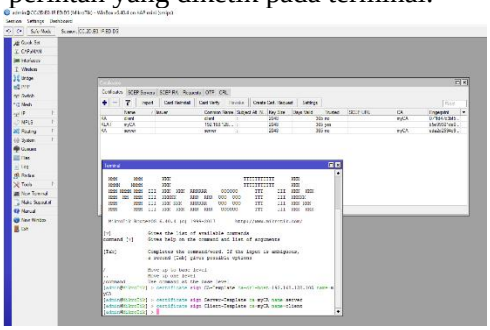
Gambar 4.10 Tiga sertifikat SSL Non-Signed

   c) Setelah membuat sertifikat-sertifikat yang diperlukan lalu tahapan selanjutnya ialah melakukan self-signing untuk mengesahkan sertifikat-sertifikat yang sudah dibuat sebelumnya. Caranya dengan masuk ke menu terminal.



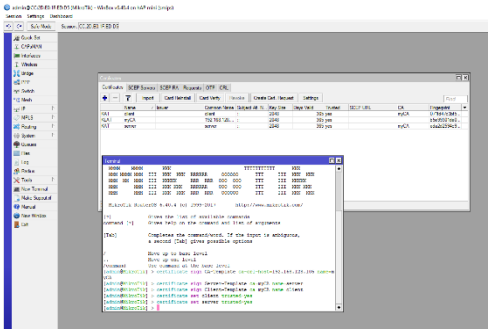
Gambar 4.11 Menu terminal untuk konfigurasi via CLI

   d) Lalu ketikan command-command untuk menandatangani sertifikat, besar kecil huruf mempengaruhi perintah yang diketik pada terminal.



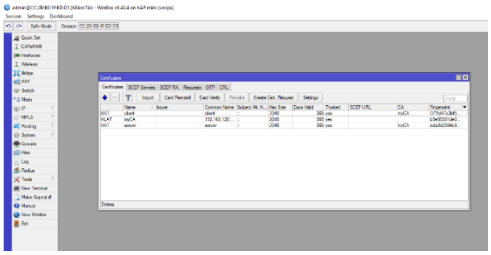
Gambar 4.12 Command self-signing pada terminal

   e) Setelah melakukan self-signing maka akan muncul flag atau tanda pada kiri nama sertifikat, seperti gambar dibawah.



Gambar 4.13 konfigurasi Trusted pada terminal

f) Apabila sertifikat tidak terdapat tanda T atau Trusted maka perlu melakukan command lagi seperti dibawah ini.



Gambar 4.14 Tiga Sertifikat SSL Signed

g) Jika tahapan-tahapan diatas sudah dilakukan dengan benar maka pastinya sertifikat sudah bisa digunakan untuk router client, letak sertifikat akan berada pada menu Files dan tinggal di import pada router client

4. Monitoring

Setelah semua proses dari implementasi selesai maka pastinya sistem akan sudah bisa digunakan, dan pada tahapan ini penulis akan melakukan pemantauan lebih lagi terhadap sistem untuk memastikan sistem bejalan dengan baik.
Pada tahapan ini penulis melakukan pemantauan terhadap perangkat keras seperti router dan kabel LAN serta koneksi internet, untuk memastikan proses penggunaan sistem berjalan dengan baik, dan sesuai dengan yang diinginkan.

5. Manajemen

Tahapan ini adalah tahapan dimana sistem akan di manage, agar kedepannya saat sistem ingin digunakan untuk kegunaan lainnya agar dapat dipastikan bahwa sistem berjalan sesuai dengan kebutuhan
Penulis juga memberikan arahan atau panduan yang terarah langsung kepada penggunga sistem kedepannya, agar mengetahui tetntang bagaimana sistem ini dapat digunakan dengan baik sesuai dengan rancangan. baik dan benar.

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Menurut hasil penelitian yang dilaksanakan oleh penulis dengan topil "Perbandingan Performa VPN Menggunakan PPTP dan SSTP Over SSL Dengan Metode Quality of Service", maka penulis menarik kesimpulan bahwa kedua protokol mempunyai kelebihan dibidangnya masing-masing, serta juga memiliki kekurangan masing-masing, dan ini adalah beberapa manfaat:

1. VPN PPTP memiliki kelebihan dimana mendukung semua sistem operasi desktop dan seluler, setup konfigurasi sederhana, dan memiliki kecepatan yang baik. Dan memiliki kekurangan dimana mudah untuk diblokir oleh ISP, tingkat enkripsi tidak begitu tinggi.
2. VPN SSTP memiliki kelebihan dimana mampu menembus firewall, dan terdukung penuh oleh sistem operasi Windows. Sedangkan kekurangan dari VPN ini ialah tidak bisa melakukan backdoor, dan sementara masih terfungsi hanya pada platform Windows.

B. Saran

Didalam penelitian dalam membandingan dua jenis pengamanan jaringan tersebut, penulis memberikan sarang kepada pengembang-pengembang lainnya untuk dapat bisa melakukan penelitian lainnya:

1. Meneliti lebih dalam tentang kedua protokol agar bisa menjadi acuan untuk pengguna lain.
2. Memberikan perbandingan yang lebih akurat kembali tentang beberapa jenis VPN lainnya.

DAFTAR PUSTAKA

Afrianto, I., & Setiawan, E. B. (2013). KAJIAN VIRTUAL PRIVATE NETWORK (VPN) SEBAGAI SISTEM PENGAMANAN (Studi Kasus Jaringan Komputer Unikom). Majalah Ilmiah UNIKOM, 12(1), 43–52.

Ginta. (2013). ISSN : 1858-2680, 9(2).

Kosasi, S. (2015). Perancangan E-learning untuk Meningkatkan Motivasi Belajar Guru dan Siswa, (September).

Lubis, R. S., & Pinem, M. (2014). ANALISIS QUALITY OF SERVICE (QoS) JARINGAN, 7(3), 131–136.

Nugroho, I. (2014). PERBANDINGAN PERFORMANSI JARINGAN VIRTUAL PRIVATE NETWORK METODE POINT TO POINT TUNNELING PROTOCOL (PPTP) DENGAN METODE INTERNET PROTOCOL SECURITY, 1–9.

Sakiwan. (2012). KAJIAN VIRTUAL PRIVATE NETWORK (VPN) LAPAN DAN PEMANFAATANNYA DALAM MENDUKUNG PENGEMBANGAN E-GOVERNMENT, 145–152.

Sharon, D., & Supardi, R. (2014). MEMBANGUN JARINGAN WIRELESS LOCAL AREA NETWORK (WLAN), 10(1), 35–41.

Supriyono, H. (2015). Penerapan jaringan.

Triyono, J. (2014). Jurnal JARKOM Vol . 1 No . 2 Januari 2014 ISSN : 2338-6312 Jurnal JARKOM Vol . 1 No . 2 Januari 2014 ISSN : 2338-6312, 1(2), 112–121.

Wongkar, S., Sinsuw, A., Najoan, X., Studi, P., Informatika, T., Teknik, F., & Ratulangi, U. S. (2015). Analisa Implementasi Jaringan Internet Dengan Menggabungkan Jaringan LAN Dan WLAN Di Desa Kawangkoan Bawah Wilayah Amurang II, 4(6), 62–68.

Yusron Aulia, A. (2016). ANALISIS PERBANDINGAN VIRTUAL PRIVATE NETWORK (VPN).