Analisa Perbandingan Pengaruh Penggunaan Protokol *Secure Soket Layer* (SSL) Dan Protokol *Point To Point Protocol* (PTTP) Terhadap *Quality Of Service* (QoS) Pada Jaringan *Vitual Private Network* (VPN)

Lamhot Raden Sitorus* , Linna Oktaviana Sari**
*Mahasiswa Program Studi Teknik Elektro S1, **Dosen Teknik Elektro
Jurusan Teknik Elektro Fakultas Teknik Universitas Riau
Kampus Binawidya Km 12,5 Simpang Baru Panam, Pekanbaru 28293
Email: lamhotr@gmail.com

ABSTRACT

Security Protocols Protocol Point-to-Point (PPTP) and Secure Socket Layer (SSL) are VPN security protocols that used to enhance the security of a network. The use of these protocols effect on performance network or Quality of Service (QoS). The QoS is measured using delay parameters, the jitter, throughput, and packet loss. Network testing scenario uses the topology bus. The results of this research is to compare the performance of each VPN protocols tested i.e. PPTP and SSL in a way of measuring the QoS performance without using the Protocol as a basis for comparing its effects by using VPN protocols.

Keywords : Virtual Private Network, PPTP, SSL, Quality of Services

1. Pendahuluan

Dengan semakin berkembangnya internet dan komunikasi memerlukan jaminan keamanan dalam mengakses internet, terutama ketika ingin melakukan pertukaran data penting. Tetapi teknologi internet tidak memberikan jaminan keamanan dalam pertukaran data dan informasi, karena internet adalah jaringan yang bersifat *public*. Dengan permasalahan tersebut maka *user* membuat sebuah jaringan dimana jaringan tersebut seolah-olah merupakan jaringan private tetapi berada di jaringan *public*. Teknologi tersebut dinamakan Virtual Private Network (VPN)

Teknologi VPN hadir sebagai salah satu solusi untuk mengamankan data yang di transfer memelalui jaringan internet. Teknologi ini memungkinkan data yang dikirim dibuat dalam bentuk ter-enkripsi dan hanya bisa dibaca ketika sudah di-dekripsikan kembali sehingga tidak bisa dengan mudah dikusasai oleh pihak ketiga. Keamanan data dan ketertutupan transmisi data dari akses yang tidak berhak dalam transmisinya pada internet menjadi standar utama dalam VPN.

Proses *enkripsi* dan *dekripsi* pada VPN membuat *delay* di dalam jaringan bertambah karena proses ini juga membutuhkan waktu. Keamanan data pada VPN pada akhirnya akan berpengaruh pada performansi QOS (*Quality of service*). Pada penelitian ini akan dianalisa perbandingan penggunaan protokol SSL (*Secure Soket Layer*) dan protokol PPTP dengan pemodelan jaringan VPN terhadap parameter QoS, sehingga dapat diketahui apa pengaruh penggunaan protokol VPN terhadap QoS.

2. Metode Pelaksanaan

Penelitian ini dilakukan melalui simulasi menggunakan perangkat lunak yang terdapat pada PC. *Software yang digunakan yaitu Graphical Network Simulator* (GNS3). GNS3 adalah *software* simulasi jaringan komputer berbasis GUI yang mirip dengan Cisco Packet Tracer. Namun pada GNS3 memungkinkan simulasi jaringan yang komplek, karena menggunakan *operating system* asli dari perangkat jaringan seperti cisco dan juniper. Sehingga kita berada kondisi lebih nyata dalam mengkonfigurasi *router* langsung.

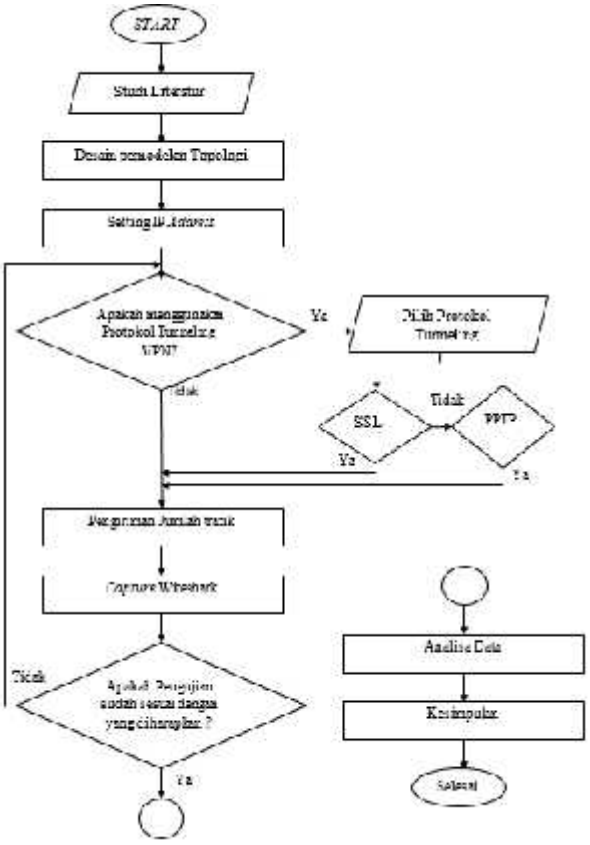
2.1 Alat yang Digunakan

Adapun alat yang digunakan dalam penelitian ini adalah:

1. Hardware :
   Laptop Toshiba Satelite L745
   - Prosesor :Intel® Core™ i5-2430 CPU @2.40Ghz (4CPUs)
   - Memory : DDR3 4 GB
   - ROM : 500 GB
   - Graphic Card :NVIDIA GeForce GT 525M 1GB
   - Operating System: Windows 10 Pro 64-bit
2. Software :
   - GNS3 versi 1.5.2.
   - Wireshark versi 2.0.3
   - Virtual Box
   - IOS Image Router Cisco Operating System c7200

2.2 Prosedur Penelitan

Tahapan-tahapan penelitian ini dapat dilihat pada flowchart dibawah ini :



Gambar 1 Flowchart penelitian

2.2.1 Studi Literatur

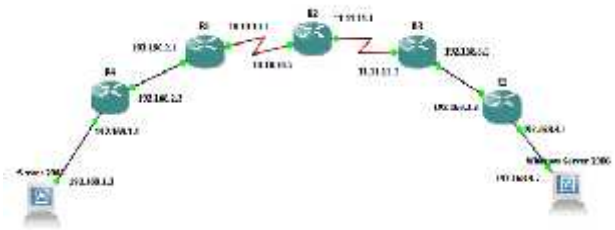
Studi literatur dilaksanakan dengan menggunakan beberapa cara, diantaranya :

1. Melakukan studi diperpustakaan dengan membaca buku dan skripsi yang berkaian dengan judul penelitian ini.
2. Mencari informasi melalui jurnal–jurnal terkait untuk mendapatkan referensi penelitian yang telah dilakukan sebelumnya sehingga dapat diketahi seperti apa alur penelitian yang akan dilakukan sehingga dapat dilihat korelasinya dengan penelitian sebelumnya.

2.2.2 Desain Topologi Pemodelan Jaringan

Setelah melakukan studi literature dilakukan pemodelan

jaringan yang akan digunakan dalam penelitian ini, topologi yang akan digunakan pada penelitian ini yaitu topologi bus seperti pada gambar dibawah ini :



Gambar 2. Desain topologi jaringan VPN

Dalam penelitian ini router yang digunakan adalah *router cisco* c7200 dengan koneksi menggunakan kabel *gigabitethernet* pada setiap *router edge* dan kabel *serial* pada koneksi antar *router*. Router c7200 diemulasi di laptop dengan pengaturan RAM sebesar 512 MB pada tiap routernya, sehingga banyaknya router yang dapat disimulasikan tergantung oleh RAM pada PC yang akan digunakan untuk melakukan simulasi. *Router cisco c7200* dipilih karena sudah mendukung *tunneling* dan enkripsi untuk membentuk *Virtual Private Network*.

2.2.3 Pengalokasian *IP Address*

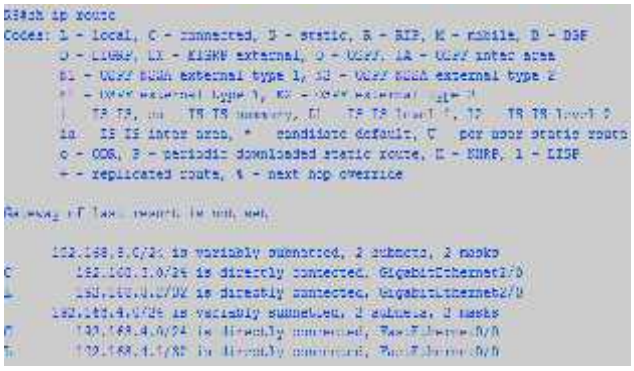
Pengalokasian ip adderess pada sebuah jaringan harus di rencanakan dengan baik supaya dapat menghubungkan router dengan baik dan efisien dalam penggunaan sumber daya yang terbatas yaitu ip address. Tabel dibawah menunjukkan pengalokasian ip address untuk setiap interface yang digunakan di topologi jaringan bus yang disimulasikan.

Tabel 1. Pengalokasian IP Address

Source	Interface	IP Address	Subnet Mask	Default Gateway	Destination
R1	g2/0	192.168.2.2	255.255.255.0		R4
	s1/0	10.10.10.1	255.0.0.0	-	R2
R2	s1/0	10.10.10.2	255.0.0.0.		R1
	s1/1	11.11.11.1	255.0.0.0.	-	R3
R3	g2/0	192.168.3.2	255.255.255.0		R5
	s1/0	11.11.11.2	255.0.0.0.	-	R2
R4	g2/0	192.168.2.1	255.255.255.0		R1
	f0/0	192.168.4.1	255.255.255.0	-	Host 1
R5	g2/0	192.168.3.1	255.255.255.0	-	R3
	f0/0	192.168.4.1	255.255.255.0		Host1
Host 1	NIC	192.168.4.2	255.255.255.0	192.168.4.1	R4
Host 2	NIC	192.168.4.2	255.255.255.0	192.168.4.1	R5

Pengalokasian *IP address* dipilih berdasarkan karakteristik *router*, dimana koneksi yang terdapat pada *interface* suatu *router* ke *router* lain harus berada pada *subnet mask* yang sama. Dapat dilihat contoh pada topologi *bus* pada *router* R1 *interface* s1/0 memiliki ip *address* 10.10.10.1 yang terhubung dengan *router* R2 melalui *interface* s0/0 dengan ip *address* 10.10.10.2, dimana kedua alamat ini berada pada satu *subnet*.

Setelah pengalamatan ip address selesai dilakukan,pada router kemudian dilakukan konfigurasi protokol *routing*. Pada penelitian ini dipakai protokol *routing ospf*. Pada gambar 3 dibawah ini dapat dilihat hasil konfigurasi protokol ospf dengan menggunakan command "*show ip router*"



Gambar 3 tampilan "show ip route" pada R5

Pada gambar 3 dapat dilihat bahwa semua router telah terhubung dengan R5. Kode "C" pada gambar menunjukkan bahwa ip address perangkat yang terhubung pada R1 terhubung secara langsung. Kode "O" menunjukkan bahwa ip address perangkat terhubung ke R5 melalui *routing protocol ospf*.

2.2.4 Konfigurasi PPTP

Setelah konfigurasi ip address dan konfigurasi protokol routing ospf selesai dilakukan sesuai dengan table dan gambar diatas dan koneksi antara host 1 dan host 2 sudah terhubung, selanjutnya dilakukan konfigurasi protokol VPN PPTP (*Point-to-point protocol*)pada R5 yang akan berfungsi sebagai router server.

Pada gambar 4 dibawah ini dapat dilihat bahwa protokol PPTP mengunakan enkripsi mppe 128 bit dan menggunakan tipe *authentication* ms-chap-v2

```
interface Virtual-Template1
 ip unnumbered GigabitEthernet2/0
 peer default ip address pool USER-POOL
 no keepalive
 ppp encrypt mppe 128
 ppp authentication ms-chap ms-chap-v2
```

Gambar 4. Algoritma enkripsi PPTP

2.2.5 Konfigurasi SSL

Konfigurasi protokol SSL dilakukan pada R5 yang juga akan berfungsi sebagai *router server*, konfigurasi ini dapat dilakukan dengan mengupload *software anyconnect* pada router yang akan dikonfigurasi, setelah *anyconnect* selesai diupload maka baru bisa dilakukan konfigurasi protokol SSL (*secure socket layer*)

Setelah konfigurasi selesai dilakukan maka untuk membentuk tunneling antara host 1 dan host 2, terlebih dahulu user melakukan install program *anyconnect* pada komputer pada yang digunakan. Dibawah ini merupakan tampilan *software* yang telah terhubung dengan *router server*

Gambar 5. Tampilan *anyconnect*

3. Pengujian

Pengujian ini dilakukan untuk membandingkan hasil performansi antar protokol yang diuji yaitu protokol PPTP dan protokol SSL, dengan mengukur QoS tanpa menggunakan kedua protokol tersebut sebagai dasar perbandingan untuk membandingan pengaruhnya dengan menggunakan kedua protokol tersebut.

Langkah untuk melakukan pengujian yaitu dengan mengirimkan paket ICMP dari host 1 ke host 2 dan melakukan capture dengan menggunakan software wireshark pada R1. Dengan variasi ukuran paket yang dikirimkan adalah sebesar 100 byte, 200 byte, 500 byte dan 1000 byte dengan pengukuran selama 15 menit.

Parameter QoS yang diukur pada pengujian ini yaitu *delay, jitter, throughput, packet loss*.

3.1 *Delay*

Hasil pengujian delay didapat dengan cara melakukan capture pada jaringan dengan menggunakan software wireshark, hasil capture kemudian diolah kedalam excel sehingga didapat ukuran delay seperti table 2 dibawah ini.

Tabel 2. Hasil perbandingan delay (millisecond)

ICMP Packet	Non Tunneling	PPTP	SSL
100 Byte	77 ms	79 ms	80 ms
200 Byte	80 ms	78 ms	81 ms
500 Byte	79 ms	79 ms	79 ms
1000 Byte	81 ms	81 ms	80 ms
Rata - rata	79.25 ms	79.25 ms	80 ms

Gambar 6. Grafik Perbandingan ukuran *delay* pada penggunaan *Non tunneling*, protokol PPTP dan SSL.

Pada gambar 6 terlihat perbandingan *delay* antara Non tunneling, protokol PPTP dan Protokol SSL. Perbandingan *delay* masing – masing tidak terlalu besar. Pada pengujian 100 dan 200 *byte* protokol SSL memiliki nilai *delay* yang lebih besar dibanding dengan *delay* PPTP. Pada pengujian 500 *byte non tunneling*, protokol PPTP dan protokol SSL memiliki *delay* yang sama sebesar 79 ms, sedangkan pada pengujian 1000 *byte delay* PPTP dan *non tunneling* sama dan protokol SSL berada dibawah PPTP dan *non tunneling*. Pengggunaan protokol Tunneling rata – rata memiliki *delay* yang sama dengan *non tunneling*.

3.2 *Jitter*

Hasil pengukuran jiiter didapat dengan melakukan capture pada jaringan dengan wireshark kemudian diolah sehingga didapat hasil seperti table 3 dibawah ini.

Tabel 3. Hasil perbandingan Jitter (millisecond)

ICMP Packet	Non Tuneneling	PPTP	SSL
100 Byte	38 ms	37 ms	50 ms
200 Byte	40 ms	42 ms	37 ms
500 Byte	40 ms	44 ms	46 ms
1000 byte	49 ms	45 ms	39 ms
Rata - rata	41.75 ms	42 ms	43 ms

Gambar 7. Grafik Perbandingan ukuran *Jitter* pada penggunaan *Non tunneling*, protokol PPTP dan SSL.

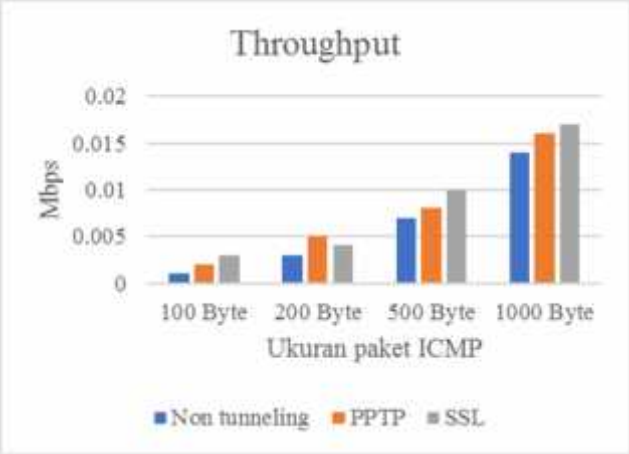
Pada gambar 7 terlihat perbandingan jitter antara *non tunnuling*, protokol PPTP dan protokol SSL. Pada pengujian 100 dan 500 *byte* protokol SSL memiliki *jitter* lebih besar daripada penggunaan prokokol PPTP sedangkan pada pengujian 200 *byte* PPTP memiliki nilai lebih besar dari pada SSL dan pada pada pengujian 1000 *byte non tunneling* memiliki *jitter* lebih besar dari pada penggunaan protokol PPTP maupun protokol SSL. Nilai *jitter* pada pengujian ini tidak memiliki perbedaan secara signifikan, PPTP memiliki nilai *jitter* yang lebih baik jika dibanding dengan protokol SSL.

3.3 *Throughput*

Throughput didapat dari pengukuran jaringan menggunakan *wireshark* dan hasil *troughput* didapat lansung dari *wireshark*. Dapat dilihat pada tabel 4 dibawah ini

Tabel 4. Hasil perbandingan *Throughput* (Mbps)

ICMP Packet	Non Tunneling	PPTP	SSL
100 Byte	0.001	0.002	0.003
200 Byte	0.003	0.005	0.004
500 Byte	0.007	0.008	0.01
1000 Byte	0.014	0.016	0.017
Rata - rata	0.00625	0.00775	0.0085



Gambar 8. Grafik Perbandingan ukuran *Throughput* pada penggunaan *Non tunneling*, protokol PPTP dan SSL.

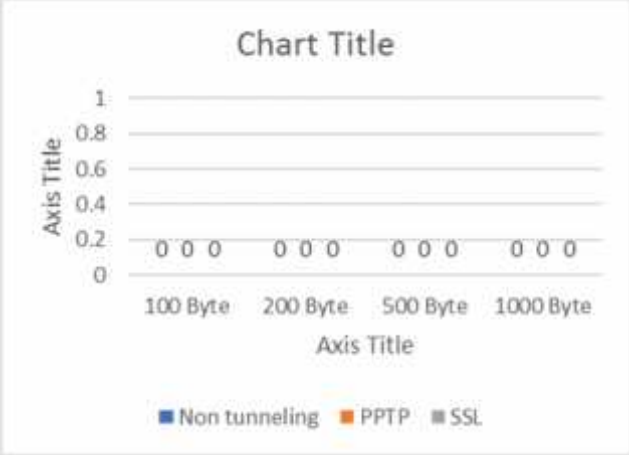
Pada gambar 8 terlihat perbandingan antara *throughput* pada *non tunneling*, protokol PPTP dan pada protokol SSL. Nilai *throughput* pada pengujian ini baik protokol tunneling maupun *non tunneling* hampir sama, bertambahnya jumlah ukuran paket *Throughput*nya juga semakin besar. Pemakaian protokol *tunneling* tidak menurunkan nilai *throughput* untuk berbagai macam ukuran paket. Nilai SSL lebih baik daripada PPTP.

3.4 *Packet Loss*

Packet loss yang didapat dari data pengukuran *wireshark* dan pengamatan langsung saat pengujian dilakukan dapat dilihat pada tabel 5 dibawah ini

Tabel 5. Hasil perbandingan *Packet Loss* (%)

	Non Tunneling	PPTP	SSL
100 Byte	0	0	0
200 Byte	0	0	0
500 Byte	0	0	0
1000 Byte	0	0	0
Rata - rata	0	0	0



Gambar 9. Grafik Perbandingan ukuran *Packet Loss* pada penggunaan *Non tunneling*, protokol PPTP dan SSL

Pada gambar 9 merupakan perbandingan packet loss pada non tunneling, protokol PPTP dan protokol SSL. Terlihat bahwa pada non tunneling, protokol PPTP dan protokol SSL paket loss nya tidak ada. Dapat dilihat bahwa penggunaan protokol PPTP dan Protokol SSL tidak berpengaruh pada paket loss pada pengujian ini.

4. Kesimplan dan Saran

4.1 Kesimpulan

Dari hasil analisa penguian protokol PPTP dan protokol SSL dapat disimpulkan bahwa penggunaan protokol tunneling VPN PPTP dan protokol SSL menurunkan performansi QoS jaringan

Penurunan QoS pada jaringan yang menggunakan protokol PPTP dan SSL tidak signifikan, sehingga pada dasarnya penggunakan protokol VPN tidak membebani performansi QoS pada suatu jaringan.

4.2 Saran

Untuk simulasi jaringan menggunakan software GNS3 sangat memerlukan hardware PC, untuk mendapatkan hasil yang lebih baik dan penambah penggunaan router dibutuhkan spesifikasi PC yang labih tinggi.

DAFTAR PUSTAKA

Ansoni, Fadloli Ghalib. 2014. Perbandingan QOS VPN protokol PPTP dan L2TP untuk Layanan video streaming. Universitas muhammadiya, Surakarta

Aprinaldi. Ruri. 2012. Implementasi dan Analisis VPN Protokol IPSec (*Internet Protocol Security*) Beserta VPN Protokol SSL (*Secure Socket Layer*). Universitas Telkom, Bandung

Hardani, Muhammad Salmon. 2009. Analisa Unjuk Kerja dan Quality of Service dari Aplikasi Secure video streaming pada jaringan berbasis VPN (Virtual Privat Network) Universitas Indonesia. Depok.

Rizal, Ferdy Agus.2012. Analisis Perbandingan Penerapan Protokol Tunneling SSL, L2TP, Dan PPTP Pada Layanan Voip Terhadap QoS (Quality of Service). Universitas Telkom. Bandung