Analisa Perbandingan Pengaruh Penggunaan Protokol *Tunneling IP Security* dengan Protokol *Tunneling Layer 2 Tunneling Protocol* terhadap *Quality of Services* Pada Jaringan *Virtual Private Network*

Haza Taufano* , Linna Oktaviana Sari , MT**
*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: hazataufano@gmail.com

ABSTRACT

Internet Protocol Security (IPSec) and Layer 2 Tunneling Protocol (L2TP) is a security protocol on the VPN is used to improve the security of an Internet network. Comparison of the use of these protocols may affect network performance or Quality of Services (QoS). The QoS measurement parameters measured by delay, jitter, throughput and packet loss. Network modeling scenarios using the bus topology model. Results of this study was to compare the performance of each protocol which is VPN IPSec and L2TP by measuring the QoS performance without using the protocol as a benchmark to compare their effects on QoS by using the tunneling protocol.

Keywords : Virtual Private Network, IPSec, L2TP, Quality of Services

1. PENDAHULUAN

Saat ini jaminan keamaan dalam mengakses internet menjadi salah satu faktor yang utama, terutama ketika ingin melakukan pertukaran data penting yang hanya boleh diakses oleh orang-orang tertentu saja, namun hal ini tidak dapat diberikan pada jaringan internet yang bersifat publik. Dengan munculnya permasalahan tersebut maka dibentuk sebuah jaringan yang dimana jaringan tersebut seolah-olah adalah jaringan privat tetapi berada di dalam jaringan publik, Teknologi tersebut dinamakan *Virtual Private Network* (VPN).

Keamanan data dan ketertutupan transmisi data dari akses yang tidak berhak dalam transmisinya pada internet menjadi standar utama dalam VPN, sehingga dalam VPN selalu disertakan akan fitur utama yaitu enkripsi dan *tunneling*.

Tunneling adalah metode untuk melakukan transfer data dari satu jaringan ke jaringan lain dengan memanfaatkan jaringan internet secara terselubung. Disebut *tunnel* atau saluran karena aplikasi yang memanfaatkan tunnel hanya melihat dua end point atau ujung, sehingga paket yang lewat pada *tunnel* hanya akan melakukan satu kali lompatan atau *hop*. Data yang akan ditransfer dapat berupa frame (atau paket) dari protokol yang lain (Faizal, 2009).

Pada penelitian ini, akan dianalisa perbandingan penggunaan protokol *Tunneling* IPSec dengan L2TP pada pemodelan jaringan VPN terhadap paramater QoS, sehingga dapat diketahui seperti apa pengaruh penggunaan protokol *Tunneling* tersebut terhadap QoS jaringan VPN.

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

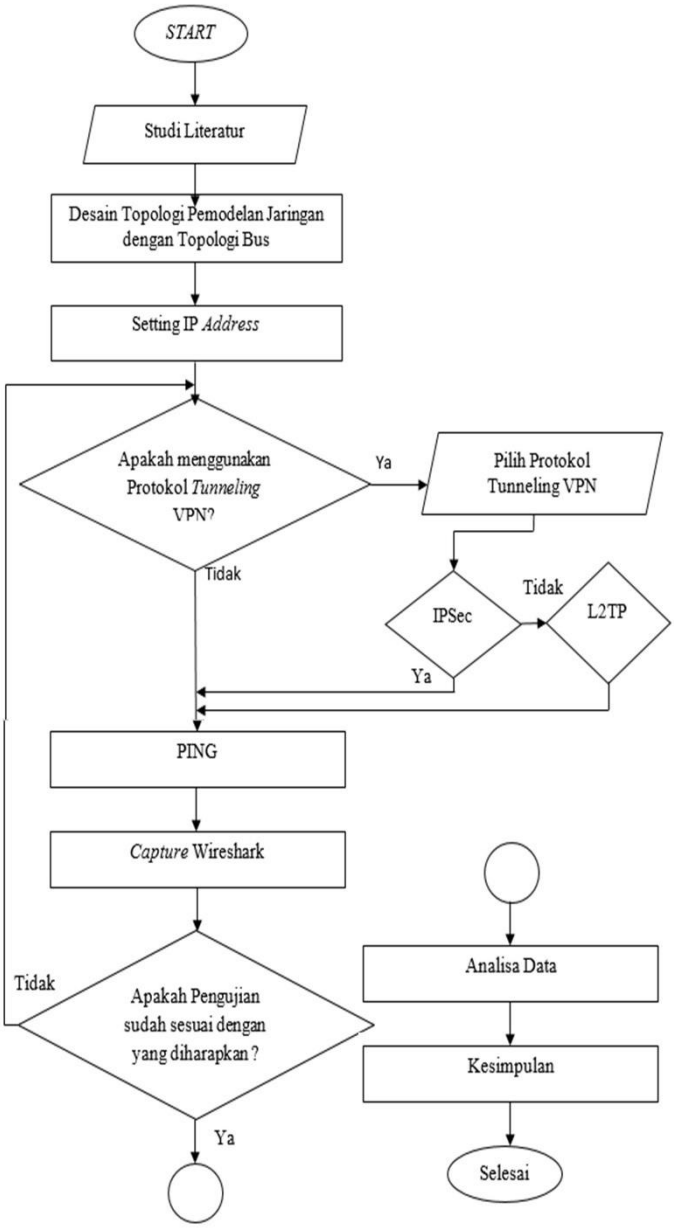
Adapun alat yang digunakan dalam melakukan penelitian ini adalah:

1. *Hardware* :
   Laptop Sony Vaio SVE 1412CVP dengan spesifikasi,
   - Prosesor : Intel Core i5 ~2,5 GHz (4 CPUs) 64 bit
   - *Memory* : DDR3 PC 12800 4 GB
   - ROM : 500 GB
   - *Graphic Card* : AMD Radeon HD 7550 1 GB
   - Operating System : Windows 10

2. *Software* :
   - GNS3 versi 1.3.11.
   - Wireshark versi 1.12.4
   - IOS Image Router Cisco Operating System c2691

2.2 PROSEDUR PENELITIAN

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



Gambar 1. *Flowchart* Penelitian

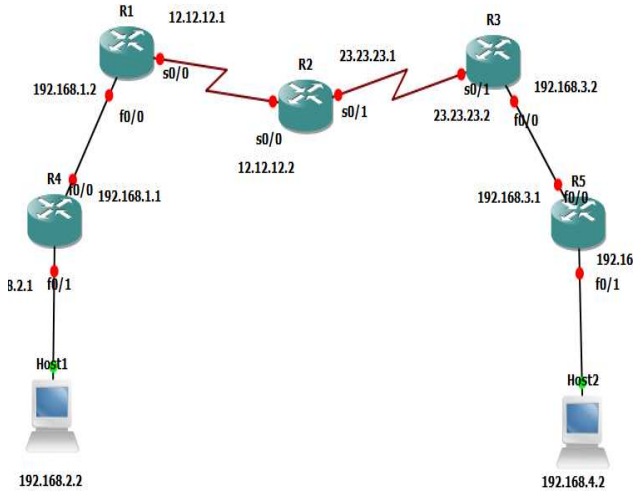
2.2.1 Studi Literatur

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 literatur dapat dilihat model topologi jaringan yang akan dirancang untuk melakukan penelitian ini, topologi yang digunakan yaitu topologi bus yang dapat dilihat pada gambar dibawah ini



Gambar 2. Pemodelan Jaringan VPN yang digunakan dalam penelitian

Router yang digunakan adalah router cisco c2691 dengan 2 *router* berperan sebagai *Provider Rdge* (PE) dan 2 *router* yang lain sebagai *Customer Edge* (CE) sementara 1 router sisanya bertindak sebagai *router* ISP. Router c2691 diemulasi di laptop dengan pengaturan RAM sebesar 256 MB pada tiap routernya, sehingga banyaknya router yang dapat disimulasikan tergantung oleh RAM pada PC yang akan digunakan untuk melakukan simulasi.

Tiap router yang terhubung menggunakan kabel serial pada tiap router *provider* nya dan kabel *fastethernet* pada setiap *router edge* dan kabel *serial* pada koneksi antar *router. Router cisco c2691* dipilih karena sudah mempunyai fitur *tunneling* dan enkripsi untuk membentuk *Virtual Private Network.*

2.2.3 Pengalokasian *IP Address*

Pengalokasian sebuah IP Address untuk setiap interface pada jaringan harus direncanakan dengan baik agar dapat menghubungkan *router* dan efisien dalam penggunaan sumber daya berupa IP Address. Dibawah ini merupakan tabel pengalokasian *ip address* untuk tiap topologi jaringan yang akan dimodelkan.

Tabel 1.Pengalokasian IP *Address* tanpa menggunakan VPN dan menggunakan protokol VPN IPSec

Source	Interface	IP Address	Subnet Mask	Default Gateway	Destination
R1	s0/0	12.12.12.1	255.0.0.0	-	R2
	f0/0	192.168.1.2	255.255.255.0	-	R4
R2	s0/0	12.12.12.2	255.0.0.0	-	R1
	s0/1	23.23.23.1	255.0.0.0	-	R3
R3	s0/1	23.23.23.2	255.0.0.0	-	R2
	f0/0	192.168.3.2	255.255.255.0	-	R5
R4	f0/0	192.168.1.3	255.255.255.0	-	R3
	f0/1	192.168.2.1	255.255.255.0	-	Host 1
R5	f0/0	192.168.1.1	255.255.255.0	-	R3
	f0/1	192.168.4.1	255.255.255.0	-	Host 2
Host 1	NIC	192.168.2.2	255.255.255.0	192.168.2.1	R4
Host 2	NIC	192.168.4.2	255.255.255.0	192.168.4.1	R5

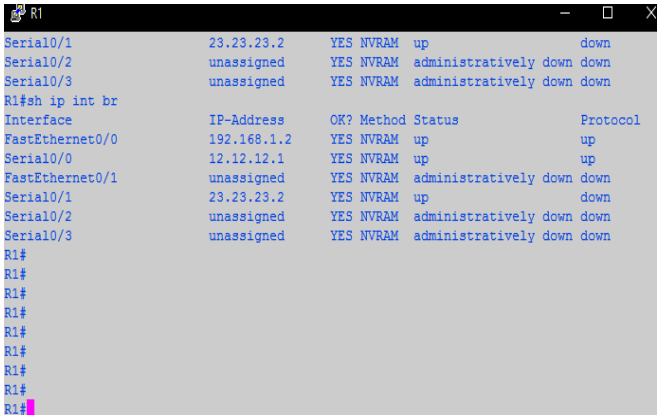
Pengalokasian IP *Address* pada protokol *tunneling* L2TP sedikit berbeda pada *interface* router yang berada di *provider edge* yaitu pada R1

dan R3 tidak berikan IP *Address* pada *interface fastethernet* f0/0 karena untuk membentuk *tunnel xconnect* pada konfigurasi L2TP, IP *Address* harus ditiadakan agar terbentuk seakan-akan berada dijaringan lokal. Tabel distribusi IP *Address* nya dapat dilihat dibawah ini

Tabel 2.Pengalokasian IP *Address* menggunakan protokol VPN L2TP

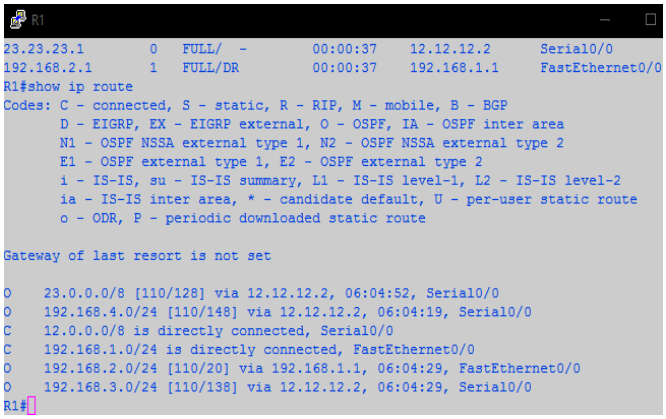
Source	Interface	IP Address	Subnet Mask	Default Gateway	Destination
R1	s0/0	12.12.12.1	255.0.0.0	-	R2
	f0/0	-	-	-	R4
R2	s0/0	12.12.12.2	255.0.0.0	-	R1
	s0/1	23.23.23.1	255.0.0.0	-	R3
R3	s0/1	23.23.23.2	255.0.0.0	-	R2
	f0/0	-	-	-	R5
R4	f0/0	192.168.1.3	255.255.255.0	-	R3
	f0/1	192.168.2.1	255.255.255.0	-	Host 1
R5	f0/0	192.168.1.1	255.255.255.0	-	R3
	f0/1	192.168.4.1	255.255.255.0	-	Host 2
Host 1	NIC	192.168.2.2	255.255.255.0	192.168.2.1	R4
Host 2	NIC	192.168.4.2	255.255.255.0	192.168.4.1	R5

Setelah *router* dikonfigurasi dengan IP *Address* sesuai dengan tabel 1 dan 2 pada masing-masing *router* maka setelah itu mengkonfigurasi *routing protocol* yaitu dengan menggunakan *routing protocol* OSPF. Pada gambar 3 dapat dilihat pada *router* R1 untuk memastikan IP Address pada R1 sudah sesuai dengan Tabel diatas dengan menggunakan perintah "*show ip interface brief*".



Gambar 3. Hasil konfigurasi IP *Address* R1

Terlihat pada gambar diatas bahwa IP *Address* sudah sesuai dengan *interface* yang terdapat pada tabel 1. Pada gambar 4 dibawah ini dapat dilihat bahwa *router* R1 telah dikonfigurasi *routing protocol* OSPF dengan perintah "*show ip route*"



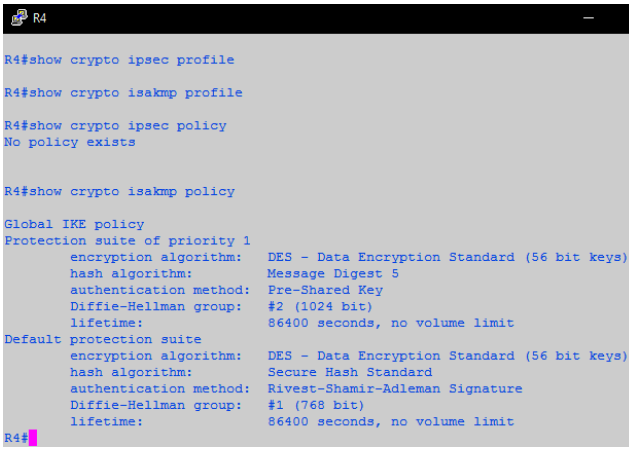
Gambar 4. Tampilan Perintah "*show ip route*" Pada *Router* R1

Pada gambar 4 terlihat tiap-tiap *router* telah terhubung dengan R1. Kode "C" menunjukkan bahwa perangkat dengan IP *address* tertentu telah terhubung secara langsung ke perangkat *router* R1, sedangkan kode "O" menandakan bagwa perangkat dengan IP *address* tertentu telah terhubung dengan *router* R1 melalui *routing protocol* OSPF.

2.2.4 Konfigurasi IPSecurity VPN

Setelah rancangan jaringan, pengalokasian IP *address*, dan konfigurasi *routing protocol* telah dilaksanakan sesuai dengan tabel 1 dan koneksi antara Host 1 dan Host 2 telah dapat dilakukan yang dapat dibuktikan dengan melakukan ping dari Host 1 ke Host 2 dan sebaliknya, protokol IPSec dapat dikonfigurasi melalui R4 dan R5.

Pada gambar 5 dibawah ini dapat dilihat algoritma enkripsi yang digunakan yaitu DES 56 bit.



Gambar 5. Algoritma Enkripsi yang digunakan pada IPSec

2.2.5 Konfigurasi L2TP VPN

Pada L2TP konfigurasinya sedikit berbeda dengan IPSec, yaitu untuk membuat koneksi antara Host 1 dan Host 2 pada gambar 1, router R4 dan router R5 ip *address* harus berada dalam 1 subnet yang dapat dilihat pada tabel 2, dengan menggunakan perintah xconnect pada router R1 dan router R3.

Sehingga terbentuk tunnel dengan menggunakan otentikasi berupa password, sehingga hanya R4 dan R5 saja yang terhubung secara lokal dengan tiap paket dienkapsulasi dengan l2tpv3.

3. PENGUJIAN

Pengujian ini membandingkan performansi tiap protokol VPN yang diuji yaitu protokol IPSec dan L2TP dengan cara mengukur kinerja QoS tanpa menggunakan protokol tersebut sebagai acuan untuk membandingkan pengaruhnya dengan menggunakan protokol tersebut.

Langkah yang dilakukan yaitu dengan melakukan pengiriman paket ICMP (ping) dan melakukan *capture* menggunakan *software wireshark* dari Host1 ke Host2 dengan variasi ukuran paketnya adalah 100 *bytes,* 200 *bytes,* 500 *bytes,* 1000 *bytes* selama 15 menit.

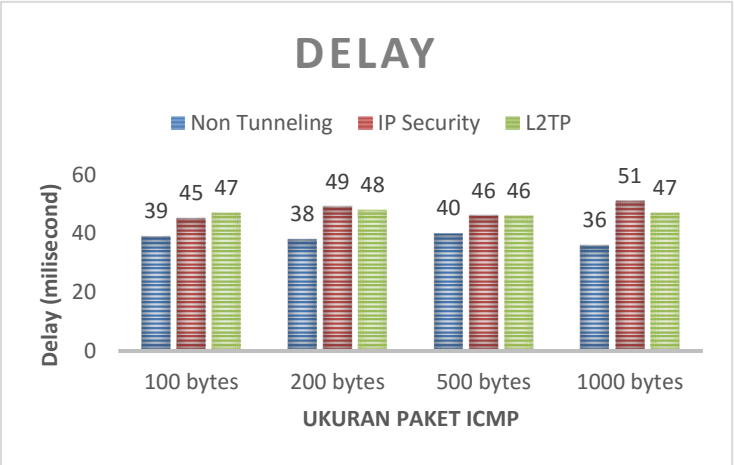
Parameter QoS yang diukur yaitu *delay, jitter, throughput, packet loss.*

3.1 Delay

Hasil pengujian *delay* didapat dari melakukan *capture* jaringan menggunakan *wireshark*. Kemudian hasil *capture* diolah ke dalam *excel* sehingga pengukuran delay dapat dilihat pada tabel 3 dibawah ini.

Tabel 3. Hasil Perbandingan Perhitungan Delay (millisecond)

ICMP PACKETS	Non Tunneling	IP Security	L2TP
100 bytes	39 ms	45 ms	47 ms
200 bytes	38 ms	49 ms	48 ms
500 bytes	40 ms	46 ms	46 ms
1000 bytes	36 ms	51 ms	47 ms
Rata-rata	38.25 ms	47.75 ms	47 ms



Gambar 6. Grafik Perbandingan Pengukuran *delay* pada penggunaan IPSec, L2TP, dan *Non tunneling,*

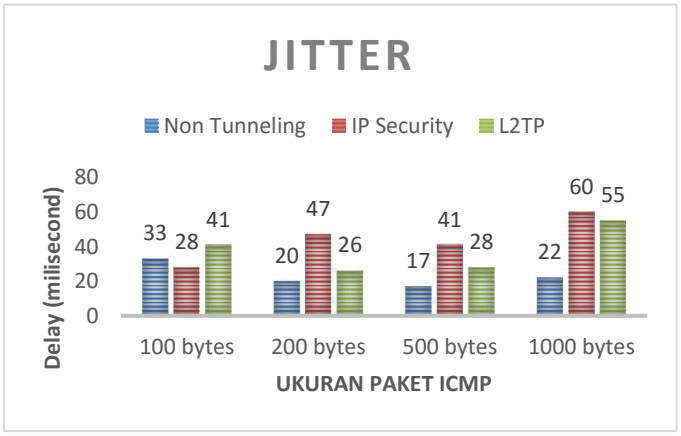
Pada gambar 6 dapat dilihat *Delay* yang didapat ketika tidak menggunakan protokol *tunneling* VPN lebih baik dibanding dengan menggunakan protokol IPSec dan L2TP. Namun selisih perbandingan delay dengan tidak menggunakan *protokol tunneling* hanya sekitar 6 ms hingga 15 ms terhadap IPSec, dan 8 ms hingga 11 ms terhadap L2TP. Tentunya perbedaan tersebut sangat kecil sehingga dapat diabaikan karena *delay* yang didapat masih dalam kategori sangat bagus.

3.2 Jitter

Hasil pengukuran jitter didapat dari pengukuran wireshark yang kemudian diolah hingga dapat dilihat pada tabel 4 dibawah ini.

Tabel 3. Hasil Perbandingan Perhitungan *jitter* (millisecond)

ICMP PACKET	Non Tunneling	IP Security	L2TP
100 bytes	33 ms	28 ms	41 ms
200 bytes	20 ms	47 ms	26 ms
500 bytes	17 ms	41 ms	28 ms
1000 bytes	22 ms	60 ms	55 ms
Rata-rata	23 ms	44 ms	37.5 ms



Gambar 7. Grafik Perbandingan Pengukuran *jitter* pada penggunaan IPSec, L2TP, dan *Non tunneling,*

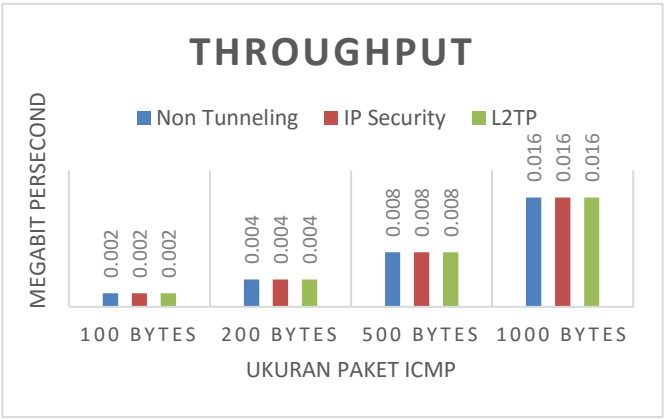
Pada gambar 7 terlihat Pengujian *Jitter* yang didapat ketika tidak menggunakan protokol *tunneling* VPN lebih baik dibanding dengan menggunakan protokol IPSec dan L2TP pada pengujian dengan ukuran paket ICMP 200, 500, dan 1000 *bytes.* Namun pada pengujian 100 *bytes* IPSec memiliki *jitter* yang lebih baik. Selisih perbandingan *jitter* dengan tidak menggunakan *protocol tunneling* sekitar 24 ms hingga 38 ms terhadap IPSec, dan 6 ms hingga 33 ms terhadap L2TP.Tentunya perbedaan tersebut kecil sehingga dapat diabaikan karena *jitter* yang didapat pada semua pengujian rata-rata masih dalam kategori bagus.

3.3 Throughput

Pengukuran *throughput* didapat langsung dari *software Wireshark* yang dapat dilihat pada tabel 4 dibawah ini

Tabel 3. Hasil Perbandingan Perhitungan *throughput* (Mbps)

ICMP PACKET	Non Tunneling	IP Security	L2TP
100 bytes	0.002	0.002	0.002
200 bytes	0.004	0.004	0.004
500 bytes	0.008	0.008	0.008
1000 bytes	0.016	0.016	0.016



Gambar 8. Grafik Perbandingan Pengukuran *throughput* pada penggunaan IPSec, L2TP, dan *Non tunneling,*

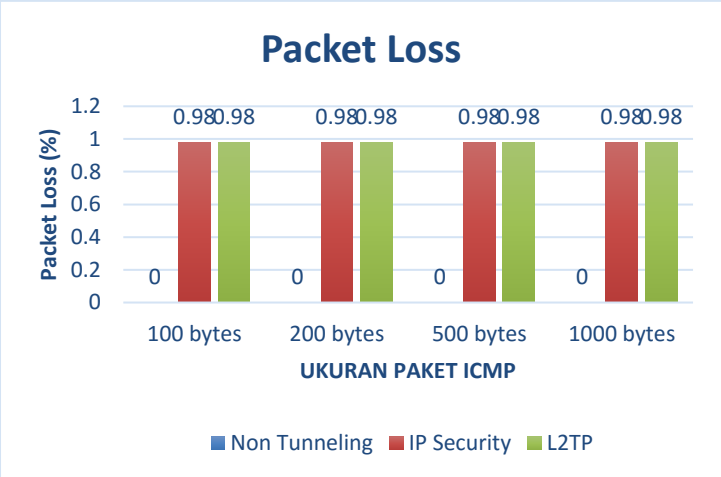
Pada *throughput* yang didapat pada semua pengujian yaitu sama pada tiap protokol-protokol *tunneling* dan juga sama pada waktu tidak menggunakan protokol *tunneling.* Dikarenakan panjang paket dan ukuran paket yang digunakan yaitu sama besar sehingga *throughput* yang didapat juga sama besar.

3.4 Packet Loss

Packet loss yang didapat dari data pengukuran *wireshark* dan pengamatan langsung saat pengujian dilakukan dapat dilihat pada tabel 4 dibawah ini

Tabel 3. Hasil Perbandingan Perhitungan *Packet Loss* (%)

ICMP PACKET	Non Tunneling	IP Security	L2TP
100 bytes	0 %	0.98 %	0.98 %
200 bytes	0 %	0.98 %	0.98 %
500 bytes	0 %	0.98 %	0.98 %
1000 bytes	0 %	0.98 %	0.98 %



Gambar 8. Grafik Perbandingan Pengukuran *packet loss* pada penggunaan IPSec, L2TP, dan *Non tunneling,*

Pada gambar 8 dapat dilihat pengukuran *packet loss* pada grafik yaitu saat tanpa menggunakan protokol *tunneling, packet loss* bernilai 0%. Sedangkan pada pengujian menggunakan kedua protokol *tunneling*, nilai packet loss yang didapat yaitu 0.98%.

Nilai *packet loss* yang masih dibawah 3% menunjukkan bahwa penggunaan kedua protokol *tunneling* VPN ini masih dalam kategori Bagus.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Dari hasil analisa dan pengujian yang dilakukan, dapat disimpulkan yaitu Penggunaan protokol *tunneling* VPN IPSec maupun L2TP menyebabkan terjadinya penurunan QoS.

Penurunan QoS yang terjadi sangat kecil untuk konfigurasi jaringan yang sama, sehingga pada dasarnya penggunaan protokol *tunneling* VPN IPSec maupun L2TP tidak membebani performa dari jaringan yang menggunakan protokol *tunneling* VPN *IPSecurity* maupun L2TP

4.2 Saran

Dalam melakukan simulasi perancangan jaringan menggunakan *software* GNS3, salah satu aspek yang utama yaitu hardware PC yang digunakan untuk melakukan simulasi harus memiliki spesifikasi yang tinggi.

DAFTAR PUSTAKA

Firmansyah, Firman. 2009. *Analisa Pengaruh Enkripsi Terhadap QoS Pada GRE/IPSEC VPN Untuk Implementasi IP-BASED Video Thelephony.* Universitas Indonesia, Jakarta.

Lisa Kristiana, Lita Lidyawati, Abdissalam Rido. (2012). "*Evaluasi Performansi MPLS VPN Dengan Simulator GNS3*". Jurusan Teknik Informatika, Jurusan Teknik Elektro, Institut Teknologi Nasional, Bandung.

Roseno, Muhammad. 2010. *Analisis Perbandingan Protokol Virtual Private Network (VPN) – PPTP, L2TP, IPSEC – Sebagai Dasar Perancangan VPN Pada Politeknik Negeri Sriwijaya Palembang.* Politeknik Negeri Sriwijaya, Palembang.

Sofana, Iwan(2010). Cisco CCNA dan Jaringan Komputer. Bandung :Informatika.

Wendy, aris dan Ahmad SS Ramadhana. *Membangun VPN Linux Secara Cepat.* Penerbit Andi. Yogyakarta. 2005