

Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet Di atas VPN

Akbar Rachmawan

D3 Manajemen Informatika, Fakultas Teknik, Universitas Negeri Surabaya
Email: rachmawanakbar4@gmail.com

Agus Prihanto, S.T.,M.Kom

Jurusan Teknik Informatika, Fakultas Teknik, Universitas Negeri Surabaya
Email: agusprihanto@unesa.ac.id

Abstrak

Perkembangan jaringan komputer sangat pesat. Jaringan komputer sudah menjadi hal mendasar dalam semua bidang. Hal ini dapat dilihat dari mayoritas orang-orang di dunia sudah pernah mengakses internet. Ide pembuatan jaringan pribadi atau Virtual Private Network, adalah sebagai suatu keuntungan dari suatu infrastruktur dalam jaringan komunikasi terbuka (internet). Tunneling VPN pada layer 2 ada metode tunneling PPTP dengan L2TP.

Dari latar belakang diatas, penulis memunculkan gagasan untuk membuat perbandingan antara protokol tunneling PPTP dan L2TP untuk mengetahui bagaimana perbandingan mekanisme kerja kedua tunneling dilihat dari keamanan apa saja yang digunakan sebagai algoritma autentikasi dan enkripsi pada saat komunikasi data. Dari penelitian yang dilakukan menunjukkan bahwa pada saat autentikasi, L2TP memerlukan waktu sedikit lebih lama dibandingkan dengan PPTP. Hal itu dikarenakan L2TP dapat dipadukan dengan IPSec sehingga memungkinkan keamanan yang lebih tinggi daripada tunneling PPTP. Namun, untuk performa kedua tunneling, PPTP sedikit lebih unggul dalam hal kecepatan transfer data daripada L2TP. Nilai delay PPTP lebih kecil dibandingkan L2TP, serta nilai throughput lebih besar daripada L2TP.

Kata kunci : Virtual Private Network, PPTP, L2TP, Delay, Throughput.

Abstract

The development of computer networks is very rapid. Computer networks have become fundamental in all areas. This can be seen from the majority of people in the world have access internet. The idea of creating a private network or Virtual Private Network, is as an advantage of an infrastructure in an open communication network (internet). Tunneling VPN on layer 2 is a PPTP tunneling method with L2TP.

From the above background, the authors come up with the idea of making comparison between PPTP and L2TP tunneling protocols to find out how the comparison mechanism of the tunneling work is seen from what security is used as authentication and encryption algorithm during data communication. From the research conducted shows that at the time of authentication, L2TP takes a little longer than the PPTP. That's because L2TP can be integrated with IPSec to enable higher security than PPTP tunneling. However, for both tunneling performance, PPTP is slightly superior in terms of data transfer rate than L2TP. The value of PPTP delay is smaller than L2TP, and the throughput value is greater than L2TP.

Keywords: Virtual Private Network, PPTP, L2TP, Delay, Throughput.

PENDAHULUAN

Dengan semakin banyaknya metode VPN saat ini memungkinkan kurang tepatnya pemilihan metode yang digunakan oleh perusahaan-perusahaan besar dalam mengelola jaringan intranet untuk perusahaannya. Dari latar belakang ini, penulis mencoba untuk melakukan sebuah penelitian yaitu membandingkan beberapa metode VPN dengan tujuan untuk mengetahui dan menganalisa beberapa metode dari VPN sehingga untuk kedepannya dapat dijadikan acuan dalam pemilihan tipe VPN entah untuk jaringan intranet dalam skala kecil maupun untuk intranet dalam skala yang lebih besar. Kemudian bagaimanakah langkah yang dapat dilakukan? Sistem *Virtual Private Network* atau VPN dapat membantu sebuah

perusahaan saling terkoneksi, karena VPN dapat menghubungkan beberapa *client site* melalui jaringan publik. Dengan VPN maka perusahaan tidak perlu membangun jaringan sendiri. Cukup terhubung dengan jaringan publik contohnya internet.

Dalam VPN terdapat protokol *tunneling* yang mana merupakan proses mengirim paket ke komputer pada jaringan *private* dengan menggunakan jaringan lain seperti internet. *Network routers* yang berada diluar jaringan *private* tidak dapat mengakses komputer yang berada jaringan *private*. Bagaimanapun, *tunneling* memungkinkan *routing network* untuk mengalirkan data ke komputer perantara, seperti *server* yang dikoneksikan ke *routing network* dan jaringan

private. Keduanya, *client* dan *server*, menggunakan *tunneling* untuk mengamankan paket ke komputer pada jaringan *private* dengan menggunakan *routers* yang hanya mengetahui alamat dari jaringan *private server* perantara.

Untuk membangun sebuah *tunnel*, diperlukan sebuah protokol pengaturnya sehingga *tunnel* secara logika ini dapat berjalan dengan baik bagaikan koneksi *point-to-point* sungguhan. Saat ini, tersedia banyak sekali protokol pembuat *tunnel* yang bisa digunakan seperti PPTP, dan L2TP.

KAJIAN PUSTAKA

Tunneling

Tunneling adalah dasar dari VPN untuk membuat suatu jaringan *private* melalui jaringan internet. *Tunneling* juga merupakan enkapsulasi suatu protokol kedalam paket protokol. *Tunneling* menggunakan satu jaringan untuk mengirim datanya melalui koneksi jaringan lain. *Tunneling* ini bekerja dengan mengenkapsulasi protokol jaringan dalam paket yang dibawa oleh jaringan publik.

OSPF (Open Shortest Path First)

OSPF adalah sebuah protokol *routing* otomatis (*Dynamic Routing*) yang mampu menjaga, mengatur, dan mendistribusikan informasi *routing* antar *network* mengikuti setiap perubahan jaringan secara dinamis. Menurut Mulyana, OSPF adalah protokol *routing link-state* yang akan mengirimkan *Link-State Advertisement (LSA)* ke semua router dengan area hierarkis yang sama.

Routing

Routing adalah proses untuk memilih jalur (*path*) yang harus dilalui oleh paket (Rohiman, 2011). Jalur yang baik tergantung pada beban jaringan, panjang *datagram*, *type of service requested* dan pola trafik. Pada umumnya skema *routing* hanya mempertimbangkan jalur terpendek (*the shortest path*).

Layer 2 Tunneling Protocol (L2TP)

Layer 2 Tunneling Protocol adalah *protocol tunneling* yang digunakan untuk mendukung *Virtual Private Network* (saputro, 2010). L2TP juga merupakan *tunnel* standar dari satu router ke router lain atau dari *client* ke *host gateway* melewati *Network Access Server (NAS) ISP* yang dianalisa terlebih dahulu oleh *server NAS ISP* dan jika proses autentikasi berhasil maka ISP akan membuat saluran dari *client* ke *host gateway* secara *Point-to-Point*. L2TP merupakan basis dan kombinasi dari protokol L2F dari *Cisco system* dan PPTP dari Microsoft (Stiawan, 2005).

Point To Point Tunneling Protocol (PPTP)

PPTP merupakan protokol jaringan yang memungkinkan pengamanan *transfer data remote klien* ke *server* pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP (Prihanto, 2015).

IPSec

IPSec telah dikembangkan untuk menyediakan layanan keamanan pada jaringan IP. Dua layanan utama yang disediakan oleh IPSec adalah enkripsi dan autentikasi secara per paket. IPSec juga menyediakan layanan lain seperti proteksi terhadap serangan replay (Shea, 2000).

Virtual Private Network

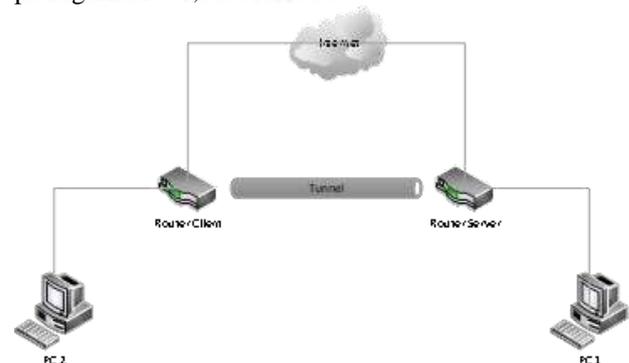
Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan local. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada didalam LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik.

Performa Network

Beberapa gangguan yang terjadi pada *wireless* sangat sering terjadi dan terkadang sulit untuk dihindari. Gangguan-gangguan tersebut secara tidak langsung dapat menurunkan kinerja suatu jaringan. Sebuah jaringan yang baik dapat diketahui berdasarkan parameter yang mempengaruhi performa jaringan tersebut (Sofana, 2011).

METODE PERANCANGAN NETWORK

Pada tahap ini dibahas mengenai analisa perancangan VPN *tunneling*, baik itu menggunakan protokol PPTP maupun protokol L2TP. Dalam analisa perancangan VPN ini nantinya akan terbagi menjadi beberapa bagian, yaitu PC 1, PC 2 dan *network ISP/Internet*. PC 2 akan mengakses PC 1 untuk keperluan *file transfer* melalui *network ISP/Internet* yang bertindak sebagai penyedia layanan internet. Kemudian untuk perancangan VPN PPTP dan L2TP secara umum dapat dilihat pada gambar 3.1,



Gambar 1 Topologi PPTP dan L2TP

Topologi diatas merupakan acuan yang akan digunakan oleh penulis dalam membuat topologi untuk tunneling PPTP dan L2TP pada tugas akhir ini. Internet pada topologi diatas akan digantikan dengan Cloud OSPF yang menggunakan 3 buah router.

Kebutuhan Sistem

Kebutuhan sistem yang digunakan dalam perancangan tugas akhir ini terdiri dari perangkat keras dan perangkat lunak agar dalam penulisan tugas akhir ini dapat berjalan dengan baik. Berikut ini adalah daftar perangkat-perangkat yang digunakan antara lain :

1) Perangkat Keras

Perangkat keras yang dibutuhkan penulis dalam pembuatan tugas akhir ini adalah satu buah laptop dengan spesifikasi berikut ini:

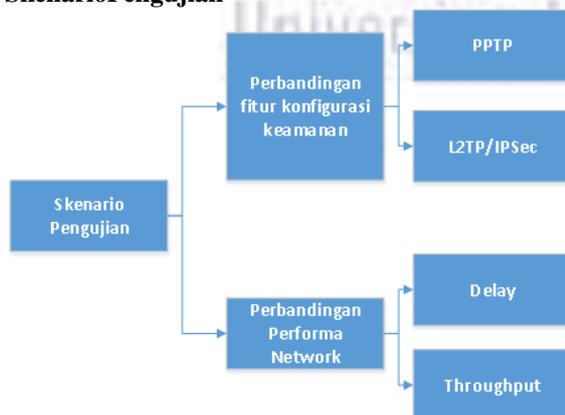
- Sistem Operasi : Windows 7 Ultimate 64-bit
- RAM : 6.00 GB
- Processor : Intel(R) Core(TM) i3-3217U CPU @ 1.80GHz

2) Perangkat Lunak

Penulis juga membutuhkan beberapa perangkat lunak untuk melakukan simulasi dan sniffing paket saat simulasi. Berikut ini adalah daftar kebutuhan perangkat lunak:

- Windows XP Professional Edition Service Pack 3
- GNS3 v.1.4.6
- Virtual Box v.5.1.18
- Winbox v.3.1
- Mikrotik RouterOS v.5.20
- FileZilla Server v.0.9.40 (FTP Server)
- FileZilla Client v.3.0.10 (FTP Client)
- Wireshark v.1.12.2

Skenario Pengujian



Gambar 2. Bagan Skenario Pengujian

Setelah merancang topologi untuk L2TP dan PPTP, tahap selanjutnya adalah skenario pengujian yang akan dilakukan dengan tahap-tahap Perbandingan Hasil Pengujian

Pada tahap ini, pengambilan data akan dilakukan setelah proses *sniffing* menggunakan perangkat lunak wireshark. *Sniffing* ini nantinya akan dilakukan di ethernet *server*. Dan pengambilan data dilakukan dalam beberapa waktu, diantaranya :

- 1) L2TP/PPTP *client* melakukan *dial* VPN ke L2TP/PPTP *server*.
- 2) L2TP/PPTP *client* melakukan *transfer* file dari L2TP/PPTP *server*.

Data untuk perbandingan keamanan kedua protokol *tunneling* nantinya diambil dari banyaknya fitur keamanan yang dikonfigurasi pada masing-masing protokol.

HASIL DAN PEMBAHASAN

Implementasi

1. Konfigurasi Router Cloud OSPF
 - a) Konfigurasi IP Address
 - b) Menambahkan OSPF Network
2. Konfigurasi Router Server (PPTP dan L2TP)
 - a) Konfigurasi IP Address
 - b) Konfigurasi Firewall NAT
 - c) DHCP Server
 - d) Static Routing
 - e) Konfigurasi PPTP dan L2TP Server
 - f) Konfigurasi IPSec Router Server L2TP
3. Konfigurasi Router Client (PPTP dan L2TP)
 - a) Konfigurasi IP Address
 - b) Konfigurasi Firewall NAT
 - c) DHCP Server
 - d) Static Routing
 - e) Konfigurasi PPTP dan L2TP Client
 - f) Konfigurasi IPSec Router Client L2TP
4. Konfigurasi PC 1 (PPTP dan L2TP)
 - a) Renew IP Address
 - b) Instalasi Wireshark
 - c) Instalasi dan Konfigurasi FileZilla Server
5. Konfigurasi PC 2 (PPTP dan L2TP)
 - a) Renew IP Address
 - b) Instalasi FileZilla Client

Hasil Pengujian

Dari hasil konfigurasi yang telah dilakukan diawal, dapat diambil beberapa data yang dapat dijadikan sebagai pembanding antara PPTP dengan L2TP/IPSec dalam hal keamanan. Berikut ini adalah hasil dari perbandingan fitur keamanan kedua *tunneling*,

Tabel 1 Hasil Perbandingan Fitur Keamanan PPTP dan L2TP

Fitur	PPTP	L2TP
Enkripsi 128-bit	√	√
Enkripsi 256-bit	-	√
Waktu inisialisasi	Cepat	Lambat
IPSec	-	√
Pap	√	√
Chap	√	√
Mschap1	√	√
Mschap2	√	√
3des	-	√
sha-1	-	√

Pada kedua protokol ini memiliki waktu untuk inialisasi yang berbeda pada saat client dial-up ke server. Pada protokol PPTP waktu inialisasi cukup cepat dibandingkan protokol L2TP. Berikut ini adalah nilai waktu inialisasi kedua protokol,

Tabel 2. Rata-rata Waktu Inisialisasi

Uji Ke-	PPTP	L2TP
1	6.96 s	13.24 s
2	6.68 s	13.88 s
3	5.77 s	13.54 s
4	6.59 s	14.19 s
5	6.85 s	14.67 s
Rata-rata	6.57 s	13.90 s

PERBANDINGAN PERFORMA NETWORK

a) Nilai Rata-rata *Delay* PPTP pada saat transfer file

Berikut ini adalah hasil perhitungan *delay* untuk PPTP,

Tabel 3. Rata-rata delay pada saat transfer file

File	Simulasi	Implementasi
1	272.124105/ms	2.862023/ms
2	894.93636/ms	2.773505/ms
3	805.16287/ms	2.643134/ms
4	859.06902/ms	2.593978/ms
5	567.39659/ms	2.612187/ms
Rata-rata <i>delay</i>	679.73779 /ms	2.696965/ms

b) Nilai Rata-rata *Delay* L2TP pada saat transfer file

Berikut ini adalah hasil perhitungan *delay* untuk L2TP,

Tabel 4. Rata-rata delay L2TP pada saat transfer file

File	Simulasi	Implementasi
1	781.15961/ms	3.152687/ms
2	933.22295/ms	3.776592/ms
3	908.38786/ms	2.78863/ms
4	886.12099/ms	2.929584/ms
5	943.75857/ms	2.63303/ms
Rata-rata <i>delay</i>	890.529996/ms	3.056105/ms

Untuk memperoleh nilai *throughput* dengan menggunakan wireshark tidak serumit menghitung *delay*. Setelah paket-paket tertangkap oleh wireshark, pilih menu *Statistics* lalu pilih *Summary*, lalu akan muncul kotak dialog Wireshark: *Summary* yang menampilkan beberapa data dari hasil *monitoring* jaringan dan data yang terdapat pada bagian paling bawah (Avg. Mbit/sec) itulah besar *throughput* yang didapatkan,

Tabel 5. Rata-rata *throughput* PPTP pada saat transfer file

File	Simulasi	Implementasi
1	4.125	5.601
2	4.200	4.234
3	4.721	5.254
4	4.498	4.612
5	4.234	2.584
Rata-rata Throughput	4.3556 Mbit/sec	4.457 Mbit/sec

Tabel 6. Rata-rata *throughput* L2TP pada saat transfer file

File	Simulasi	Implementasi
1	3.532	5.754
2	4.125	3.912
3	4.311	3.439
4	4.103	3.865
5	4.321	2.594

Rata-rata Throughput	4.0784 Mbit/sec	3.9128 Mbit/sec
-----------------------------	-----------------	-----------------

Perbandingan Hasil Pengujian

Dari hasil pengambilan data diatas, maka dapat diambil perbandingan secara menyeluruh mulai dari perbandingan delay dan throughput saat implementasi serta fitur keamanan dari kedua tunneling. Berikut adalah tabel perbandingannya,

Tabel 7. Hasil Perbandingan

Data	PPTP	L2TP
Rata-rata <i>delay</i>	2.696965/ms	3.056105/ms
Rata-rata <i>throughput</i>	4.457 Mbit/sec	3.9128 Mbit/sec
Enkripsi	128-bit	256-bit
Autentikasi	Pap, chap, mschap1, mschap2	Pap, chap, mschap1, mschap2, sha1
Fitur IPSec	Tidak <i>Support</i>	<i>Support</i>
Rata-rata Waktu Inisialisasi	6.57 s (Cepat)	13.90 s (Lambat)

KESIMPULAN dan SARAN

Simpulan

Dari hasil penelitian ini, dapat disimpulkan bahwa:

- 1) Fitur keamanan yang digunakan oleh tunneling L2TP sedikit lebih unggul daripada keamanan yang digunakan pada PPTP. L2TP dapat dipadukan dengan IPSec sedangkan PPTP tidak dapat dipadukan dengan keamanan tambahan yaitu IPSec
- 2) Nilai *throughput* PPTP lebih besar dibandingkan dengan L2TP/IPSec karena autentikasi dan enkripsi yang digunakan tidak sebanyak dan serumit L2TP/IPSec. L2TP/IPSec memiliki *delay* sedikit lebih lama dan memiliki *throughput* yang lebih kecil daripada PPTP.

Saran

Penelitian ini masih sebatas perbandingan antara dua protokol tunneling yaitu PPTP dan L2TP/IPSec dalam keperluan file transfer. Diharapkan pada penelitian selanjutnya dapat menambahkan berbagai macam protokol tunneling lain seperti OpenVPN, IKEv2, dan SSTP, serta perbandingan dalam keperluan hal yang lain.

DAFTAR PUSTAKA

Agus, M. (2008). *Mengenal Wifi, Hotspot, LAN, dan Sharing Internet*. Jakarta: Gramedia.

Ansoni, Fadli Ghalib. 2014. *Perbandingan QoS VPN Protokol PPTP dan L2TP Untuk Layanan Video Streaming*.

King, Todd., dan Diane Barret. 2005. *Computer Networking Illuminated*. Canada: Jones and Barlett Publisher.

Madcoms. (2010). *Panduan Lengkap Microsoft Server 2008*. Madiun: Andi Publisher.

Prihanto, A. (2015). Modul Jaringan Komputer. *Modul Praktikum Jaringan Komputer*.

Rohiman, A. (2011, 5 22). *Pengertian Routing, Tabel Routing dan Protocol Routing*. Diambil kembali dari catatan teknis: <http://www.catatanteknisi.com/2011/05/pengertian-routing-tabel-routing.html>

Shea, Richard. 2000. *L2TP Implementation and Operation*. Addison-Wesley Professional.

Siregar, Edison. (2010). *Langsung Praktik Mengelola Jaringan Lebih Efektif dan Efisien*. Yogyakarta: Andi Publisher.

Stiawan, Deris. (2005). *Sistem Keamanan Komputer*. Jakarta: Elex Media Komputindo.

Syafrizal, Melwin. (2005). *Pengantar Jaringan Komputer*. Yogyakarta: Andi Publisher.

Web, C. (2014, Juni 19) *Pengertian Tunneling*. Diambil kembali dari gaptex: <http://gaptex.com/pengertian-tunneling/>.

Web, C. *IP Security*. Diambil kembali dari wikipedia: https://id.wikipedia.org/wiki/IP_Security.