ANALISA DAN PERANCANGAN JARINGAN BERBASIS VPN PADA PT. FINROLL

Johan Muliadi Kerta; David Wennoris; Tonny Gunawan; Erny

[1]Jurusan Sistem Informasi, Fakultas Ilmu Komputer, Bina Nusantara University,
Jln. KH Syahdan 9 Kemanggisan Jakarta,
johanmk@binus.ac.id

ABSTRACT

Along with the development of the company to run operations such as data communication and perform other transactions to relations and vice versa, PT Finroll just uses the public network such as sending email to their partners. Data information is not safe in public because it can be tapped or intercepted by unauthorized person. With the Virtual Private Network (VPN), PT Finroll can do business in secure environment to their partners. The methodologies used in this research are data collection that was started by surveying, interviewing, and analyzing the current network topology, performance and design requirements that support network design. From these results, PT Finroll can increase productivity and performance from competition in their business. In addition, with this research company has a better ability to increase their competitiveness in present and the future.

Keywords: *public network, data security, VPN*

ABSTRAK

Seiring dengan perkembangan perusahaan dalam menjalankan kegiatan operasional seperti melakukan transaksi data dan lainnya dari PT Finroll ke perusahaan relasinya maupun sebaliknya, hanya menggunakan jalur public, yaitu salah satunya melalui email. Data informasi tidak aman berada di jaringan public karena dapat disadap oleh pihak yang tidak berkepentingan. Dengan adanya Virtual Private Network (VPN), maka PT Finroll dapat menjalankan bisnis dengan pihak relasinya dalam melakukan hubungan secara private di dalam jaringan public dengan koneksi yang ekonomis dan keamanan data yang terjamin. Metodologi yang digunakan adalah metode pengumpulan data yang dimulai dengan melakukan survey, wawancara, dan melakukan analisis topology jaringan saat ini, kinerja dan kebutuhan yang mendukung perancangan jaringan. Dari hasil penelitian ini, PT Finroll dapat meningkatkan produktivitas dan kinerja dalam perusahaan untuk dapat bersaing dalam dunia bisnis yang semakin ketat. Selain itu, dengan penelitian ini perusahaan memiliki kemampuan untuk dapat meningkatkan daya saingnya yang lebih baik untuk saat ini maupun yang akan datang.

Kata kunci: *jaringan public, keamanan data, VPN*

PENDAHULUAN

Teknologi yang semakin berkembang menimbulkan masalah dari segi keamanan data terutama jika dikirim melalui jaringan public seperti Internet. Dengan masalah tersebut, maka pengguna Internet berusaha mengamankan apa yang dikirim dimana hanya pihak yang berkepentingan yang dapat mengakses data tersebut misalnya dengan password. Seiring berjalannya waktu, password tetap tidak membuat data dan informasi aman berada di jalur public tersebut. Dengan permasalahan ini maka dibutuhkan sebuah mekanisme jaringan dimana jaringan tersebut seolah-olah merupakan jaringan private atau pribadi namun tetap berjalan pada jaringan public. Teknologi tersebut dinamakan Virtual Private Network (VPN). Dengan menggunakan VPN maka data informasi tersebut akan lebih aman berada di jaringan public karena disembunyikan atau terenkripsi sehingga user lain tidak mengetahui data atau informasi tersebut.

PT. Finroll merupakan perusahaan yang bergerak dalam bidang IT solution yang sedang mengembangkan sayapnya menjadi penyedia jasa informasi mengenai saham maupun finance. Selama ini, untuk melakukan transaksi data dan lainnya ke perusahaan relasinya maupun sebaliknya, PT. Finroll menggunakan email melalui internet. Seperti diketahui, data informasi tersebut kurang aman berada di jalur public, apalagi jika data yang bersifat rahasia dan pribadi. Dengan adanya VPN maka PT. Finroll dapat menjalankan bisnis dengan pihak relasinya untuk melakukan hubungan secara private di dalam jaringan public.

Ruang Lingkup penelitian ini meliputi analisa jaringan yang saat ini berjalan dan yang akan diusulkan pada PT. Finroll dan relasinya tetapi lebih dikhususkan pada PT. Finroll. Selanjutnya hasil penelitian ini akan memberikan usulan solusi perancangan VPN melalui jalur *tunneling point-to-point* dengan menggunakan protocol PPTP untuk koneksi antar perusahaan. Sedangkan tipe perancangan VPN yang akan dibahas berupa Remote Access VPN.

METODE

Metodologi yang digunakan dalam penelitian ini adalah dengan melakukan studi kepustakaan mengenai teknologi VPN dari jenis, keuntungan, kelemahan, dan teori-teori yang mendukung, melakukan wawancara kepada staff IT PT. Finroll untuk mendapatkan informasi yang berguna untuk penelitian ini, kemudian melakukan observasi dan survei terhadap jaringan perusahaan pada Millenium Danamata Group (MDG) untuk mendapatkan informasi yang berguna dalam perancangan remote access VPN. Setelah itu menetapkan solusi yang dipakai serta menentukan teknologi yang dipakai beserta alasan pemilihan teknologi tersebut. Tahap selanjutnya adalah dengan merancang jaringan remote access VPN berdasarkan hasil analisa serta perangkat keras/hardware yang dipakai pada masing-masing perusahaan. Dan pada akhirnya mengevaluasi jaringan remote access VPN baik itu dari segi bandwith yang dipakai, traffic antar perusahaan, encryption yang dipakai serta proses tunneling remote access VPN yang digunakan

HASIL DAN PEMBAHASAN

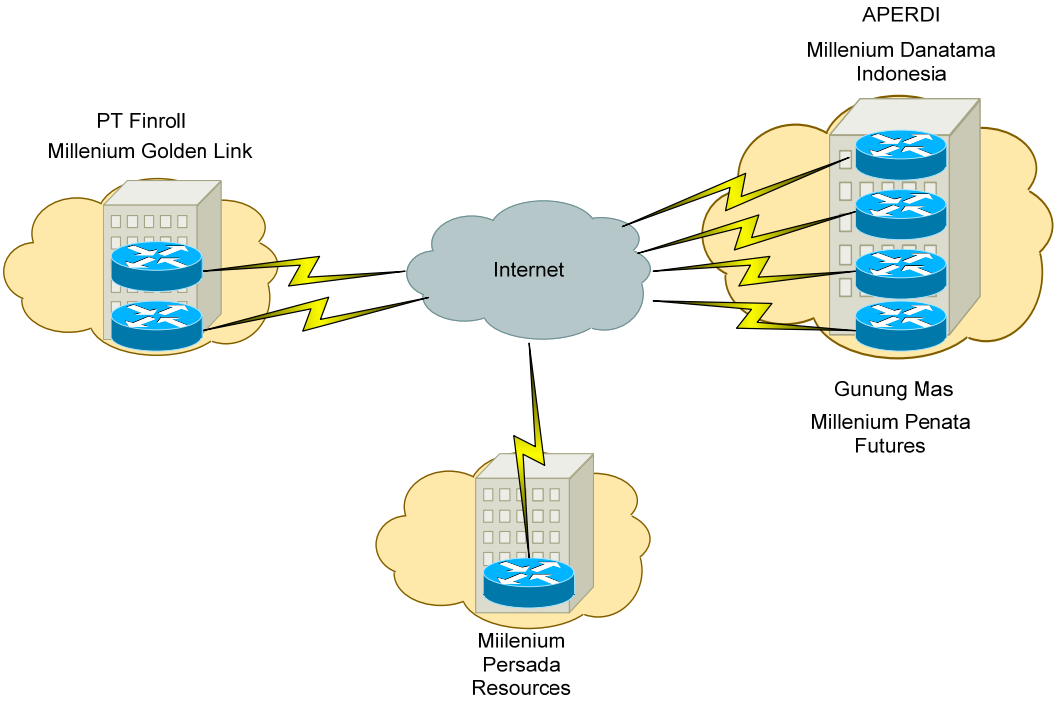
PT. Finroll merupakan salah satu anggota dalam asosiasi Millenium Danatama Group (MDG). Atas pemenuhan kebutuhan dari PT. Finroll yang hanya ingin membentuk jaringan VPN dengan relasi bisnisnya yang tertentu saja (tetapi masih dalam lingkup anggota MDG), maka dari itu sistem yang

akan dianalisis adalah sistem yang sedang berjalan pada ketujuh anak perusahaan Millenium Danatama Group (MDG), yaitu :

1. PT. Finroll
2. APERDI
3. Millenium Danatama Indonesia (MDI)
4. Millenium Penata Futures (MPF)
5. Millenium Golden Link (MGL)
6. Gunung Mas
7. Millenium Persada Resources (MPR)

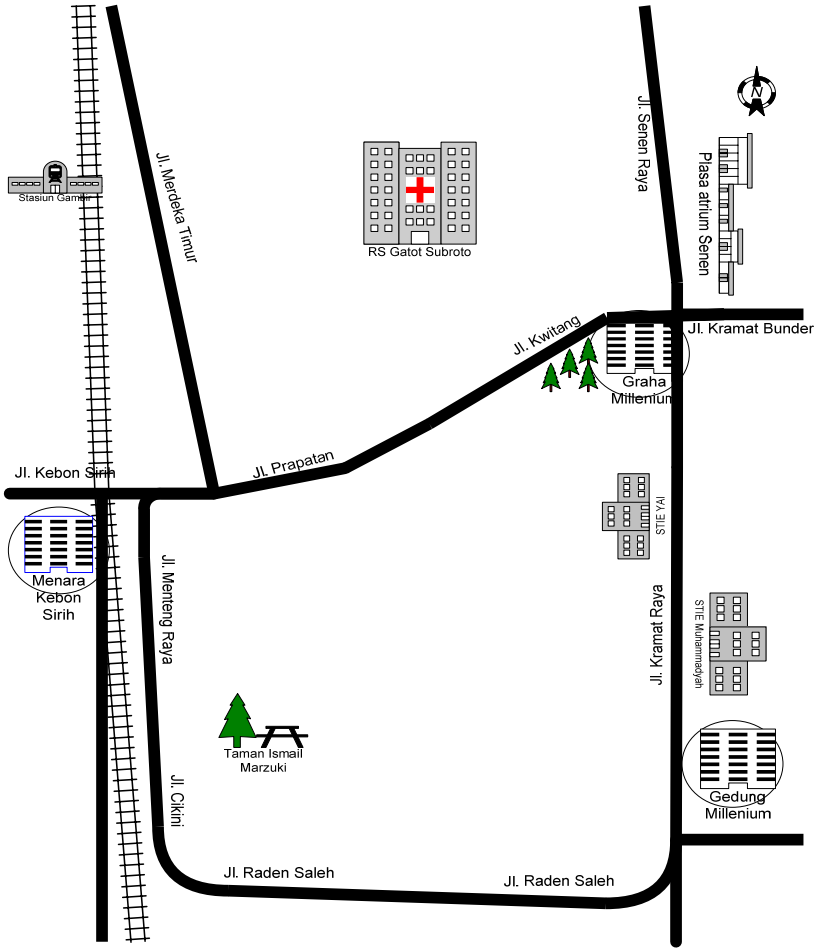
dimana ketujuh perusahaan tersebut bernaung di dalam satu group, yaitu Millenium Danatama Group (MDG). Berikut pertama-tama akan dibahas terlebih dahulu mengenai sejarah MDG lalu kemudian dilanjutkan dengan pembahasan lebih detil mengenai ketujuh anak perusahaan MDG yang menjadi objek utama dalam penelitian ini.

Berikut adalah gambaran umum jaringan yang saat ini sedang berjalan pada ketujuh anak perusahaan Millenium Danatama Group :



Gambar 1. Topologi Milenium Danatama Group

Pada ketujuh perusahaan tersebut menggunakan mikrotik sebagai routernya. Mikrotik yang dipakai pada ketujuh perusahaan merupakan PC router yang diinstal software mikrotik. Untuk koneksi internet perusahaan di atas menggunakan koneksi wireless dimana MPR yang terletak di Gedung Millenium menggunakan jasa ISP PT Jasnita Telekomindo. APERDI, MDI, MPF, serta Gunung Mas terletak di Menara Kebon Sirih. PT. Finroll dan MGL terletak di Graha Millenium. Keenam perusahaan yang berada pada kedua gedung tersebut menggunakan jasa ISP Biznet Networks. MPF dan APERDI mendapatkan bandwitdh 512 Kbps dan PT. Finroll, MGL, MDI, MPR, Gunung Mas mendapatkan 256 Kbps dari ISP.



Gambar 2 Denah Ketujuh Lokasi Perusahaan

Selama ini, untuk melakukan transaksi data dan lainnya dari PT. Finroll ke perusahaan relasinya maupun sebaliknya hanya menggunakan jalur public yaitu Internet. Internet memiliki kekurangan dalam segi keamanan yang kurang baik. Berdasarkan kondisi tersebut, permasalahan yang dihadapi jaringan perusahaan saat ini adalah permasalahan keamanan. Akibat dari permasalahan keamanan tersebut dapat menimbulkan beberapa masalah, antara lain :

- Proses transaksi data yang selama ini dilakukan pada PT. Finroll dan relasinya dapat disadap oleh pihak luar karena menggunakan jalur public.
- PT. Finroll sulit mendapatkan jalur yang aman untuk melakukan komunikasi ke perusahaan relasinya. PT. Finroll biasanya menggunakan aplikasi yahoo messenger untuk berkomunikasi.

Karena PT. Finroll menggunakan jaringan public untuk melakukan transfer data ke perusahaan relasinya, maka proses transfer data antar perusahaan menjadi tidak aman. Banyak alternatif yang ada untuk memecahkan masalah tersebut, salah satunya yaitu menggunakan encryption email. Proses ini sama sekali tidak memerlukan biaya Karena softwarenya gratis dan mudah didapat. Tetapi dengan menggunakan encryption email, PT. Finroll tidak dapat terhubung dengan jaringan internal perusahaan relasinya sehingga tidak dapat melakukan hubungan misalnya chatting antar LAN. Oleh karena itu, disarankan membuat sebuah jalur private antara PT. Finroll dengan perusahaan relasinya agar data yang dikirimkan tidak diketahui oleh pihak yang tidak diinginkan. Dengan adanya jalur private, maka proses pengiriman data dapat melalui file sharing. Jalur private hanya dibuat untuk pengiriman data yang terjadi pada PT. Finroll ke perusahaan relasinya yang berada di gedung yang berbeda sedangkan untuk MGL yang berada di gedung yang sama dengan PT. Finroll, dilakukan proses routing biasa

dengan cara menghubungkan antara jaringan perusahaan dengan router masing-masing dengan kabel UTP karena jarak yang antara dua perusahaan tersebut masih bisa ditempuh oleh kabel UTP

Beberapa alternatif jalur private yang ada antara lain :

Pembuatan jalur *private* dengan media kabel
Pembuatan jalur *private* dengan media kabel memerlukan biaya yang sangat mahal karena letak dari tiga gedung untuk ketujuh anak perusahaan MDG jauh sehingga membutuhkan waktu yang lama untuk menghubungkan jaringan perusahaaan satu sama lain.

Pembuatan jalur *private* dengan media *wireless*
Pembuatan jalur *private* dengan media *wireless* memerlukan biaya yang mahal karena faktor perbedaan ketinggian gedung yang berbeda. Seperti gedung Graha Millenium yang berlantai 3 dengan Menara Kebon Sirih yang berlantai 29.

Pembuatan jalur *private* dengan media internet yaitu dengan *tunneling* VPN.
Pembuatan jalur *private* dengan media internet memerlukan biaya yang murah dan waktu yang singkat.

Dari beberapa pertimbangan di atas maka dipilih jaringan yang berbasis VPN, walaupun jaringan VPN ini memiliki kekurangan dari segi kecepatan pengiriman data dibandingkan alternatif lainnya seperti WAN. Biasanya PT. Finroll melakukan proses pengiriman data seperti file-file dokumen, program-program, poster-poster dalam bentuk JPEG sebesar ±10 MB via *email*. Karena data yang dikirimkan dari PT. Finroll relatif kecil ukurannya, maka PT. Finroll memerlukan *bandwidth* 128 Kbps dimana *bandwidth* tersebut dibagikan untuk lima jalur *tunneling.* PT. Finroll mendapatkan *bandwidth* 256 Kbps dari ISP maka *bandwidth* untuk proses VPN disarankan tidak dibuat *dedicated* sehingga jika proses pengiriman data melewati jalur *tunneling* membutuhkan kapasitas *bandwidth* kurang dari 128 Kbps maka sisa *bandwidth* dapat dipakai untuk kebutuhan yang lain. Adapun kerugian yang terjadi jika tidak men*dedicated bandwidth* pada proses VPN yaitu jika ada proses di luar jalur VPN (contoh: *download* dalam jumlah besar) yang membutuhkan *bandwidth* maksimal sehingga tidak ada *bandwidth* yang tersisa untuk jalur VPN. Beberapa keuntungan yang diperoleh dari pengimplementasian *remote access* VPN ini adalah :

1. Mengurangi biaya implementasi jaringan dibandingkan dengan penggunaan WAN karena *remote access* VPN menggunakan media internet sehingga tidak membutuhkan kabel (WAN). Penggunaan kabel akan membutuhkan biaya produksi yang sangat besar. Semakin jauh jarak yang diinginkan, semakin meningkat pula biaya produksinya.
2. Menyediakan keamanan transaksi yang dilakukan PT. Finroll karena VPN menggunakan teknologi *tunneling* untuk mengirim data melalui jaringan *public* yang tidak aman. Selain itu VPN juga menggunakan *authentication*, *encapsulation*, dan *encryption* untuk memastikan keamanan dan *integritas* dari pengiriman data. Kemudahan untuk melakukan hubungan antara jaringan PT. Finroll dan perusahaan relasinya baik itu melalui *software-software* yang mendukung seperti *pony chat*, *vpress chat*.

Namun *remote access* VPN memiliki kekurangan dalam hal *bandwidth* karena ada *bandwidth* yang terpakai untuk proses pembentukan jalur tunnel. Jalur tunnel akan selalu terbentuk baik ada atau tidaknya pengiriman data yang berlangsung antar PT. Finroll dengan relasinya.

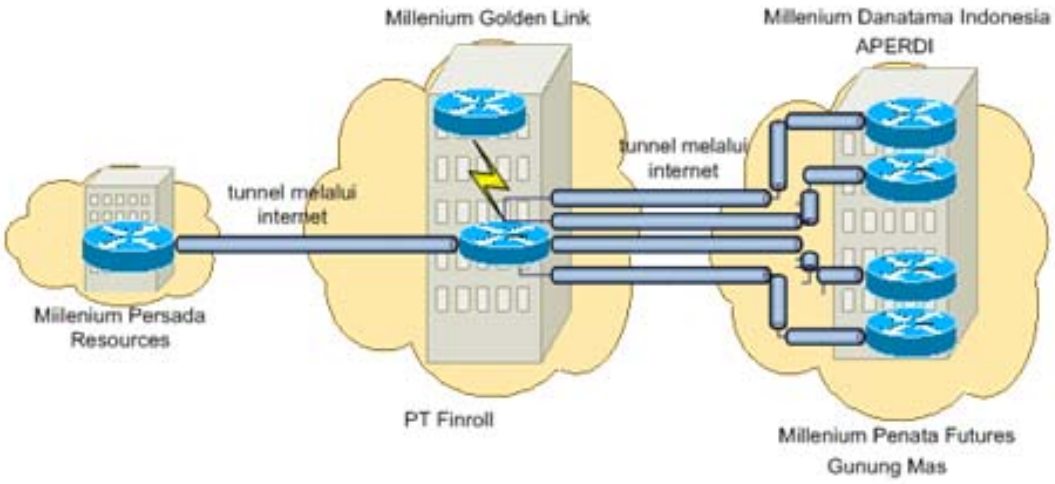
Dalam perancangan ini, dipilih PPTP sebagai *protocol* yang digunakan untuk perancangan jaringan *remote access* VPN pada PT. Finroll. PPTP menggunakan *protocol GRE* (*Generic Routing Encapsulation*) untuk proses *encapsulation, protocol* MPPE (*Microsoft Point-to-Point Encryption*) untuk proses *encryption,* dan menggunakan *protocol* MS-CHAP2 (*Microsoft Challenge-Handshake Authentication Protocol* 2) untuk proses *authentication*. Beberapa pertimbangan-pertimbangan dalam

memilih *protocol* ini antara lain :

1. *Protocol* PPTP sudah ada pada *mikrotik* ketujuh perusahaan tersebut sehingga tidak perlu menyiapkan sebuah komputer yang digunakan sebagai *server* VPN.
2. PPTP lebih efisien dalam proses pengiriman data dalam jumlah besar dibandingkan dengan *protocol* IPSec.
3. PPTP mendukung *multiple routing protocol* sehingga lebih mudah untuk perusahaan yang memiliki *routing protocol* lebih dari satu.
4. Koneksi *point-to-point* dapat membatasi hubungan antar perusahaan sehingga perusahaan yang tidak berwenang tidak dapat mengakses jaringan perusahaan sedangkan jika koneksi *point-to-multipoint* apabila ada proses pengiriman data antar dua jaringan perusahaan, maka jaringan perusahaan yang tidak terlibat tetapi masih dalam satu jaringan dapat mengetahui adanya pengiriman data yang terjadi.

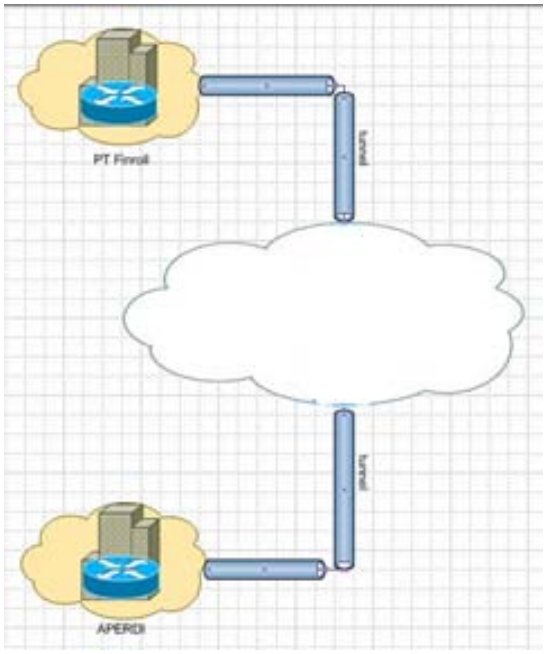
Rancangan Jaringan VPN

Untuk menghubungkan jaringan PT. Finroll dan perusahaan relasinya maka perlu adanya proses *tunneling* antar perusahaan tersebut. Karena proses PPTP merupakan proses *client-server* maka proses *tunneling* hanya terjadi antara dua perusahaan saja. Karena ada lima perusahaan yang akan dihubungkan dengan PT. Finroll, maka diperlukan adanya lima proses *tunnel*. Topologi jaringan VPN yang ditinjau dari PT. Finroll dapat dilihat pada halaman berikut, dimana pada gambar terdapat lima proses *tunneling* yang bersumber dari PT. Finroll menuju ke perusahaan relasinya. Pertama-tama, kelima perusahaan relasi akan melakukan proses *dial-up* ke PT. Finroll untuk membentuk *tunnel*. Setelah *tunnel*nya terbentuk, proses *dial-up* yang dilakukan perusahaan lain itu akan bersifat permanen.



Gambar 3. Topologi jaringan VPN

Pada halaman berikut ini merupakan gambar dari salah satu proses *tunneling* VPN, yaitu antara PT. Finroll dan APERDI.



Gambar 4. Proses *tunneling* antara PT. Finroll dan APERDI

Gambar di atas menggambarkan proses *tunneling* yang menghubungkan antara PT. Finroll dengan salah satu relasinya yaitu APERDI. *Tunneling* akan meng*encapsulate* dan meng*encyrpt* setiap data paket yang akan dikirim ke jaringan *internal* masing-masing perusahaan. APERDI akan melakukan proses *dial* IP *public* ke PT. Finroll sebagai proses *authentication* awal. Setelah melakukan proses tersebut maka dibentuk sebuah jalur *tunnel* antara kedua perusahaan tersebut dengan menggunakan IP *virtual*. Setelah jalur terbentuk maka data yang melewati jalur tersebut akan di*encapsulate* dan di*encrypt*.

Dalam penelitian ini belum dilakukan implementasi secara langsung pada jaringan PT. Finroll dan relasinya, maka dibuat sebuah rancangan simulasi jaringan VPN untuk melihat perbedaan *bandwidth* dan proses *encrypt* data yang terjadi. Beberapa peralatan yang dibutuhkan untuk menjalankan simulasi VPN ini antara lain :

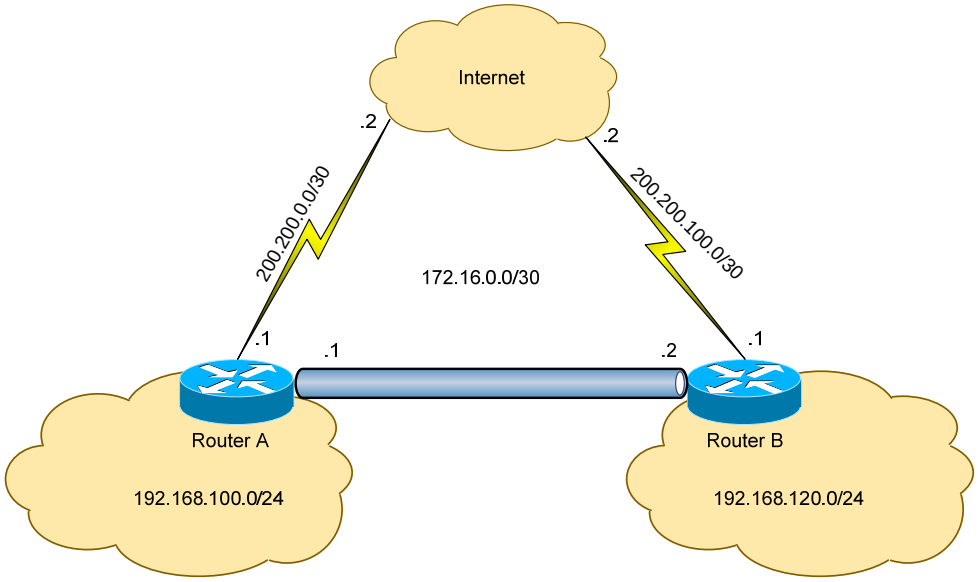
1. 5 buah komputer yang terdiri dari :
   - 2 buah PC *router* yang diinstal *Operating System Mikrotik*.
   - 1 buah PC *router* yang diinstal *Operating System Windows Server* 2003.
   - 2 buah komputer *client* yang *Operating System Windows XP service pack* 2.
2. 5 buah LAN Card yang terdiri dari :
   - 2 buah LAN *card* masing-masing pada 2 PC *router* yang diinstal *MikrotikOS*.
   - 2 buah LAN *card* masing-masing pada 1 PC *router* yang diinstal *Windows Server* 2003.
3. 1 buah LAN *card* masing-masing pada 2 buah komputer *client* yang diinstal *Windows XP Service pack* II.
4. Kabel *unshielded twisted pair* (UTP) yang bertipe *cross* untuk menghubungan semua komputernya.

Topologi *logical* dari simulasi rancangan jaringan VPN sebagaimana seperti yang telah diusulkan :

Gambar 5. Topologi *logical* simulasi jaringan VPN

PC *router* yang berada di tengah bertujuan untuk sebagai *router* penghubung sehingga terlihat bahwa pada Router A dan Router B merupakan dua jaringan yang berbeda satu sama lainnya.

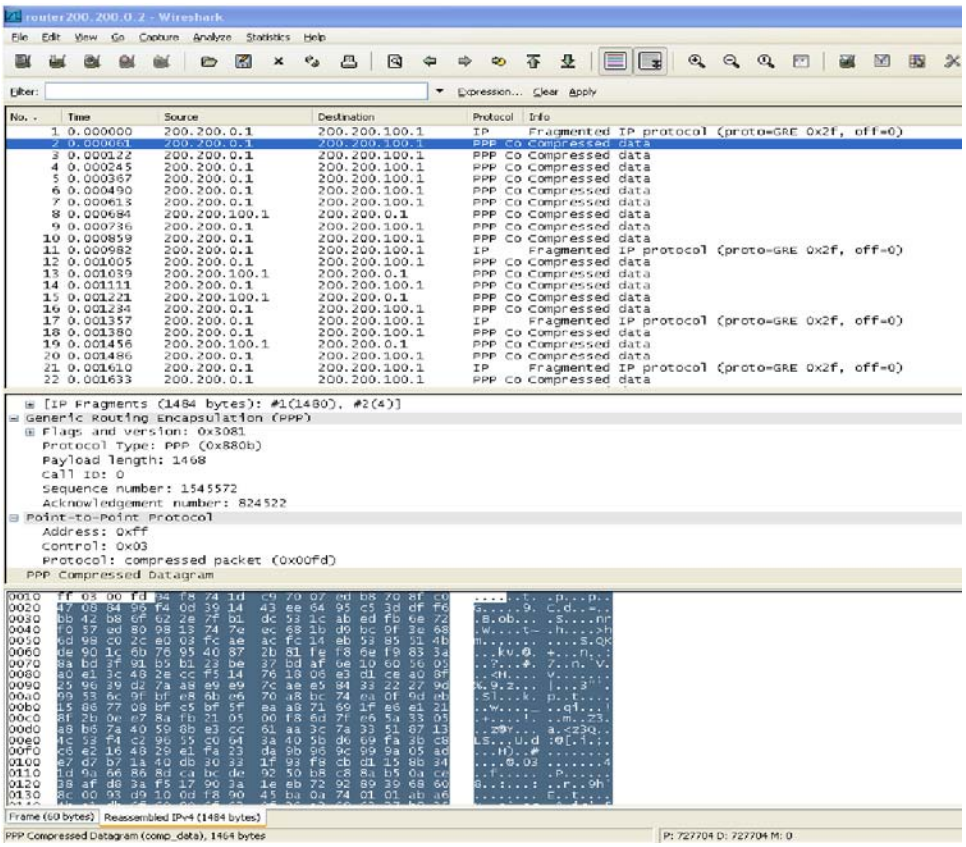
Proses *tunneling* ini diawali di Router A yang bertindak sebagai *server*. Router A akan membuat dua buah IP virtual yaitu IP *virtual* untuk Router A yaitu 172.16.0.1 dan IP *virtual* untuk Router B yaitu 172.16.0.2. Masing-masing IP *virtual* tersebut akan menjadi alamat untuk proses *tunneling* pada Router A dan Router B. Setelah itu, Router A dan Router B akan melakukan proses *authentication* dengan cara Router B melakukan proses *dial* ke IP public Router A. Setelah *tunnel* terhubung, maka jaringan *internal* masing-masing harus membuat *static route* untuk menghubungkan IP *virtual* dengan IP *gateway* jaringan *internal*.



Gambar 6. Proses *tunneling* pada Router A dan Router B

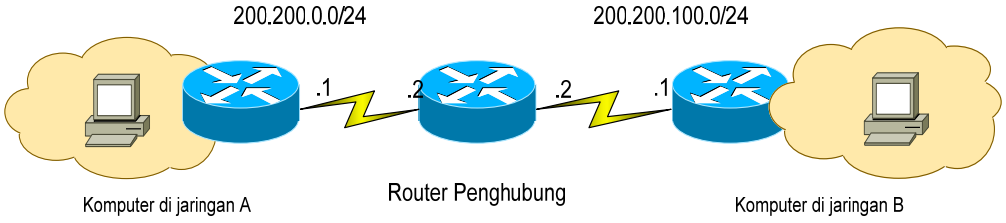
Setelah proses VPN berjalan, maka dilakukan proses pengiriman data dari jaringan *internal* Router A ke jaringan *internal* Router B. Data yang dikirimkan merupakan data *multimedia* sebesar 240 MB.

Berikut merupakan hasil *capture* bahwa data yang dikirimkan tidak dapat ditemukan pada jaringan *router* penghubung.



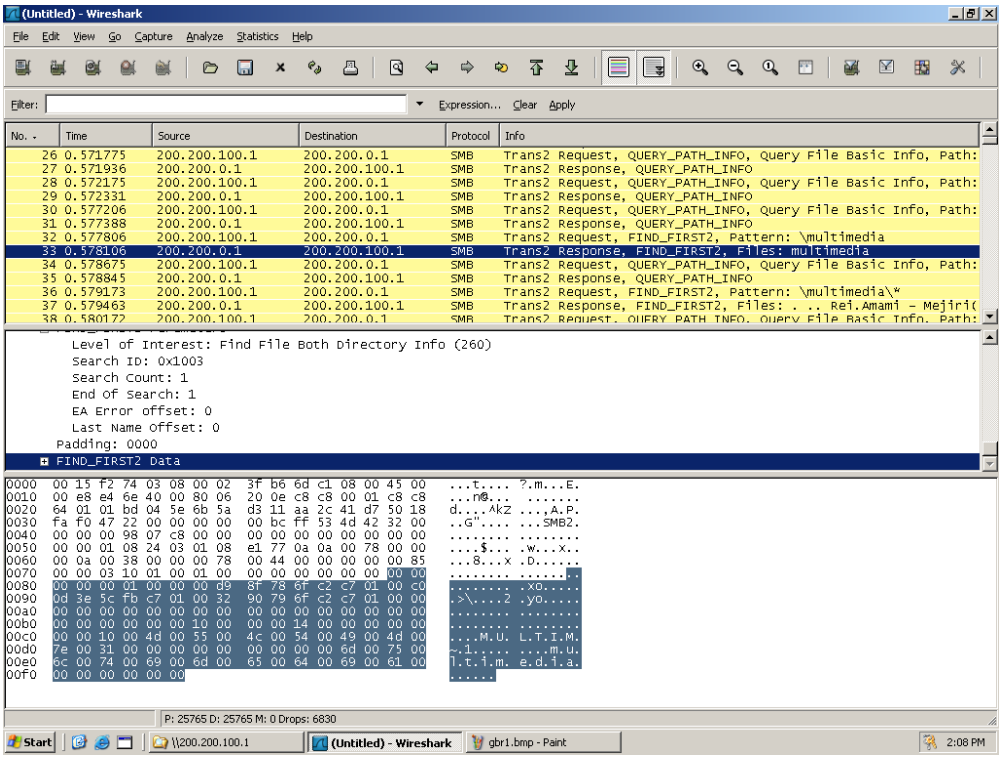
Gambar 7. Hasil *encapsulation* data VPN dengan *wireshark*

Dalam hal ini juga dilakukan proses pengiriman data pada jaringan A ke jaringan B tanpa melalui proses VPN melainkan secara langsung melalui proses *point-to-point*. Untuk melakukan proses ini maka *router* harus disetting agar IP *private* pada jaringan *internal*nya tersebut bisa berkomunikasi dengan IP *public* dengan memakai *Network Address Translation* (NAT). Pada halaman berikut adalah topologinya :



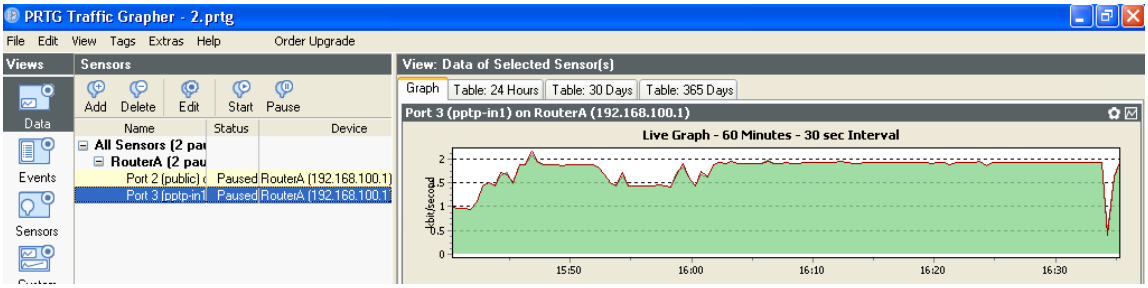
Gambar 8. Topologi jaringan *point-to-point*

Pada topologi di atas komputer A akan mengirimkan data ke komputer B. *Wireshack* akan diinstal pada komputer penghubung yang berperan sebagai *internet*. Berikut ini merupakan hasil *capture* data yang dikirim ditemukan pada jaringan *router* penghubung.



Gambar 9. Hasil *capture* data tanpa VPN dengan menggunakan *wireshark*

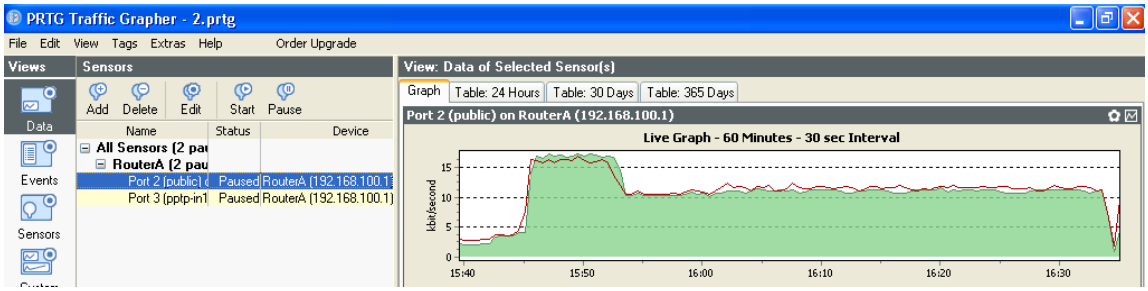
Berdasarkan hasil *monitoring* pengiriman data dari komputer *client* pada jaringan A ke komputer *client* pada jaringan B, komputer *client* A Karena melalui proses *tunnel* akan memakan *transfer rate* yang lebih kecil dibandingkan dengan melalui jalur *point-to-point*. Hal ini Karena data yang dikirim sudah di*encapsulate* dan di*encrypt* sehingga memakan *transfer rate* yang kecil.



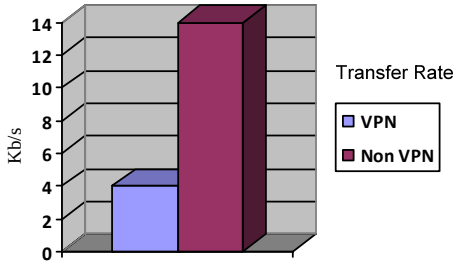
Gambar 10. Hasil *capture* simulasi jalur VPN menggunakan PRTG

Pada gambar terlihat bahwa *transfer rate* yang dipakai untuk pembuatan proses jalur *tunnel* PPTP adalah 0,5 Kbps. Jadi jika tidak terdapat proses transaksi data dan komunikasi maka membutuhkan 0,5 Kbps untuk pembuatan jalur *tunnel*.

Berdasarkan hasil *monitoring* pengiriman data dari komputer *client* A ke komputer *client* B, *client* A yang tanpa melalui proses *tunnel* akan memakan *transfer rate* yang lebih besar dibandingkan melalui proses *tunnel* PPTP. Hal ini Karena karena tidak adanya proses *encapsulation* dan proses *encrypt* sehingga memakan *transfer rate* yang lebih besar.



Gambar 11. Hasil *capture* simulasi jalur non VPN menggunakan PRTG



Gambar 12. Perbandingan *transfer rate* jalur VPN dan non VPN

Pada grafik melalui VPN, dapat dilihat pada grafik bahwa *transfer rate* yang kecil yaitu 4 kbit/sec dan dengan *interval* 30 detik. Sedangkan pada grafik tanpa VPN, dapat dilihat pada grafik bahwa *transfer rate* yang lebih besar yaitu 14 kbit/sec dengan *interval* 30 detik.

Perbandingan antara jaringan VPN dan *frame relay* dalam hal ini akan dibandingkan antara jaringan VPN dan *frame relay*. Perbandingan dapat dilihat pada tabel di bawah ini:

Tabel 1. Tabel perbandingan jaringan VPN dan *Frame Relay*

Perbandingan (dari segi)	**VPN**	***Frame relay***
Biaya	Relatif lebih murah	Relatif lebih mahal
Konektivitas	tidak mendukung QoS	mendukung QoS

1. Segi Biaya
   Seperti yang kita ketahui VPN menggunakan jaringan internet untuk pembuatan jalurnya sehingga memerlukan biaya yang relatif murah. Pembuatan *frame relay* memerlukan jasa penyedia jalur yang biasanya diberikan oleh ISP sehingga memerlukan biaya relatif mahal.

2. Segi konektivitas
   Seperti yang kita ketahui VPN tidak mendukung *Quality of Service* (QoS) sehingga kepastian jalur yang terhubung tidak terjamin lain halnya dengan *frame relay* mendukung *Quality of Service* (QoS).

SIMPULAN

Simpulan yang dapat diambil dari penelitian ini adalah *Remote access* VPN dapat membantu PT. Finroll untuk membuat jalur dan komunikasi yang lebih aman dengan kelima perusahaan relasinya dengan proses *encrypt* pada setiap pengiriman datanya. Penggunaan *internet* sebagai media pembuatan jalur *tunnel* merupakan cara yang efisien karena tidak memerlukan biaya tambahan untuk proses pembuatan jalur *tunnel* dan pengiriman datanya. PT. Finroll menggunakan *mikrotik* untuk proses *routing* pada jaringan *internal*nya, baik untuk mendapatkan *internet* dan *management bandwidth* sehingga tidak memerlukan *device* tambahan untuk VPN *gateway* maka lebih hemat dalam pengeluaran biaya untuk proses pembuatan *tunnel* antara PT. Finroll dan relasinya. Proses jalur *tunnel* tidak memerlukan *transfer rate* yang besar sehingga pemakaian *transfer rate* pada PT Finroll relatif kecil untuk proses *tunnel* tersebut.

Semakin berkembangnya teknologi informasi maka otomatis sebuah jaringan pun semakin lama akan semakin besar. Oleh sebab itu diperlukan *hardware upgrade* pada PC *router* sehingga dapat menjalankan proses dengan sebagaimana mestinya. Perlu dibuat sebuah domain *server* untuk menampung data-data yang dikirimkan baik dari PT. Finroll sendiri maupun relasinya sehingga dapat mempermudah komunikasi. Adanya penambahan aplikasi LAN *messenger* pada PT. Finroll dan relasinya dapat mempermudah komunikasi. Disarankan membuat sebuah jalur alternative baik itu dengan PC *router* ataupun dengan *router* karena apabila PC *router* utama sedang dilakukan *maintainance*, maka koneksi *internet* dan jalur *tunnel* pada PT. Finroll dapat terus berjalan.

DAFTAR PUSTAKA

Sukmawan, B. (2000). *Metoda Enkripsi Blowfish*. http://www.bimacipta.com/blowfish.htm

Davis, C. R. (2001). *IPSec: Securing VPNS*. USA: McGraw-Hill.

Downs, K., Spanier, S., Ford, M. Stevenson, T., Lew, H.K. (1998). *Internetworking Technologies Handbook*, 2nd *edition*. Indianapolis: Macmillan Technical Publishing..

Gupta, M.. (2003). *Building a Virtual Private Network.* USA: Premier Press.

Lammle, T. (2004). *CCNA™ Cisco Certified Network Associate STUDY GUIDE*. Jakarta: PT. Elex Media Komputindo.

Lukas, J. (2006). Jaringan Komputer. Yogyakarta: Graha Ilmu.

Mikrotik Indonesia (2007), *Mikrotik RouterOS V2.9 Reference Manual* http://www.mikrotik.com/testdocs/ros/2.9/

Paessler Bandwidth Management Software (2007). *Monitor and Manage bandwidth with PRTG*. http://www.paessler.com/prtg

Perlmutter, B., & Zarkower, J. (1999). *Virtual Private Networking: A View From The Trenches.* New Jersey: Prentice Hall.

Stallings, W. (2003). *Cryptography and Network Security*: *Principles and Practice, 3rd edition.* New Jersey: Prentice Hall.