PERANCANGAN VIRTUAL PRIVATE NETWORK DENGAN SERVER LINUX PADA PT. DHARMA GUNA SAKTI

Siswa Trihadi[1]; Frenky Budianto[2]; Wirriyanto Arifin[3]

[1, 2, 3] Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Bina Nusantara,
Jln. K.H. Syahdan No.9, Palmerah, Jakarta Barat 11480

ABSTRACT

Purpose of this research is to analyze and design a network between head and branch office, and company mobile *user*, which can be used to increase performance and effectiveness of company in doing their business process. There were 3 main methods used in this research, which were: library study, analysis, and design method. Library study method was done by searching theoretical sources, knowledge, and other information from books, articles in library, and internet pages. Analysis method was done by doing an observation on company network, and an interview to acquire description of current business process and identify problems which can be solved by using a network technology. Meanwhile, the design method was done by making a topology network diagram, and determining elements needed to design a VPN technology, then suggesting a configuration system, and testing to know whether the suggested system could run well or not. The result is that network between the head and branch office, and the mobile *user* can be connected successfully using a VPN technology. In conclusion, with the connected network between the head and branch office can create a centralization of company database, and a suggested VPN network has run well by encapsulating data packages had been sent.

Keywords: *network, Virtual Private Network (VPN), library study, analysis, design*

ABSTRAK

Tujuan penulisan ini adalah untuk menganalisis dan merancang suatu jaringan antara kantor pusat dengan kantor cabang, serta mobile user pada perusahaan yang dapat dimanfaatkan untuk meningkatkan kinerja dan efektifitas perusahaan dalam melaksanakan proses bisnisnya. Metode yang digunakan dalam penulisan penelitian ini meliputi tiga bagian pokok, yaitu: studi pustaka, analisis, dan perancangan. Metode pustaka dilakukan dengan mencari sumber-sumber teori, pengetahuan dan informasi lainnya dari buku, artikel di perpustakaan, dan halaman internet. Metode analisis dilakukan dengan melakukan observasi terhadap jaringan perusahaan, dan melakukan wawancara untuk memperoleh gambaran proses bisnis yang sedang berjalan, serta mengidentifikasi permasalahan yang dapat dibantu dengan menggunakan teknologi jaringan. Sementara itu, metode perancangan dilakukan dengan membuat diagram topologi jaringan, serta menentukan elemen-elemen yang dibutuhkan untuk merancang teknologi VPN, kemudian memberikan usulan konfigurasi sistem, dan melakukan testing untuk mengetahui sistem yang diusulkan dapat berjalan dengan baik atau tidak. Hasilnya adalah jaringan antara kantor pusat dengan kantor cabang, serta mobile user berhasil dihubungkan dengan menggunakan teknologi VPN. Kesimpulannya adalah dengan terhubungnya jaringan antar kantor cabang dapat menciptakan sentralisasi database pada perusahaan dan rancangan VPN yang diusulkan telah berjalan dengan baik dengan melakukan enkapsulasi pada paket-paket data yang dikirim.

Kata Kunci: *jaringan, Virtual Private Network (VPN), studi pustaka, analisis, perancangan*

PENDAHULUAN

Latar Belakang

Peranan dari teknologi jaringan komputer akan semakin penting, terutama bagi perusahaan yang memiliki banyak cabang. Oleh karena itu, suatu sistem jaringan komputer dibutuhkan untuk menyediakan

pelayanan aliran informasi yang terjadi antara jaringan komputer kantor pusat dengan kantor cabang yang letaknya berjauhan. Dalam melakukan komunikasi dan pengolahan informasi antara kantor pusat dengan kantor cabang yang tersebar di lokasi-lokasi yang terpisah, dibutuhkan suatu jaringan *internet*, sehingga jaringan yang berbeda tadi terhubung dalam satu sistem jaringan komputer. Namun, jaringan *internet* merupakan jaringan yang bebas dan dapat diakses oleh siapa saja, sehingga belum terjamin keamanannya.

Teknologi yang dapat membantu mengatasi masalah keamanan jaringan *internet* adalah teknologi *Virtual Private Network* (VPN). Dengan adanya VPN, hubungan yang dilakukan antara kantor pusat dan kantor cabang menjadi lebih ekonomis. Selain itu, koneksi VPN tidak terbatas hanya pada hubungan antara kantor pusat dan cabang saja, tetapi juga memberikan jaminan keamanan dan reabilitas yang hampir sama dengan jaringan pribadi. Penggunaan VPN menjamin keamanan yang tinggi karena koneksi dengan VPN dilakukan dengan peralatan yang menerapkan metode autentikasi, yang berfungsi untuk memberi identitas kepada pemakai dan data yang dikirimkan lewat VPN dienkripsikan.

Penulisan penelitian ini dibatasi pada hal-hal sebagai berikut. Pertama, melakukan analisis jaringan komputer pada PT Dharma Guna Sakti, yang mencakup topologi jaringan, spesifikasi perangkat keras yang ada, dan hal-hal lainnya yang berhubungan. Kedua, memberikan usulan solusi perancangan VPN menggunakan PC-*based* VPN dengan Sistem Operasi Linux Fedora Core 6 dan perangkat lunak, yang dibutuhkan untuk menghubungkan antara kantor pusat dengan kantor cabang dan *mobile user*. Ketiga, tipe perancangan VPN yang akan dibahas adalah. *remote access* VPN dengan protokol *tunneling* L2TP/IPSec. Keempat, pembahasan lainnya mengenai tipe enkripsi data, autentikasi, dan konfigurasi yang diperlukan untuk merancang sebuah teknologi VPN.

Tujuan dari penulisan penelitian adalah menganalisis jaringan komputer pada PT Dharma Guna Sakti dan merancang sebuah jaringan, sehingga kantor cabang dan *mobile user* dapat melakukan koneksi ke kantor pusat dengan menggunakan teknologi *Virtual Private Network*.

Sedangkan manfaat dari penulisan penelitian ini adalah menghubungkan jaringan komputer antara kantor pusat dengan kantor cabang serta menyediakan akses bagi *user* yang berada di luar kantor (*mobile user*) untuk mengakses jaringan kantor pusat, sehingga dapat meningkatkan kinerja dan efektifitas perusahaan dari penggunaan sektor jaringan komputer dan jaringan *internet*.

Metode

Metode Pustaka

Metode pustaka dilakukan dengan mencari sumber-sumber teori, pengetahuan, dan informasi lainnya yang berkaitan dengan penelitian, baik berupa buku, artikel di perpustakaan, dan halaman *internet*.

Metode Analisis

Metode analisis ini dilakukan melalui 3 tahapan, yaitu: melakukan observasi untuk mengumpulkan data dan informasi; melakukan wawancara dengan pihak-pihak yang bersangkutan untuk memperoleh data dan informasi yang dibutuhkan; serta menetapkan usulan solusi dengan menggunakan teknologi VPN untuk menghubungkan kantor pusat dengan kantor cabang dan *mobile user*.

Metode Perancangan

Metode perancangan dilakukan melalui 4 tahapan, yaitu: pembuatan diagram topologi jaringan dengan menggunakan alat bantu pemodelan seperti *Microsoft Office Visio*; menentukan elemen-elemen yang dibutuhkan dalam merancang sebuah teknologi VPN; memberikan usulan konfigurasi sistem pada VPN *server* yang akan dibangun pada perusahaan sesuai dengan elemen-elemen VPN yang telah ditentukan; serta melakukan *testing* koneksi dengan mengirimkan paket-paket ICMP dan menggunakan tool *sniffer*.

Tinjauan Pustaka

Definisi Jaringan Komputer

Dengan berkembangnya teknologi komputer dan komunikasi, suatu model komputer tunggal yang melayani seluruh kebutuhan akan tugas-tugas komputasi suatu organisasi kini telah digantikan dengan

sekumpulan komputer yang terpisah-pisah, tetapi saling berhubungan dalam melaksanakan tugasnya. Sistem ini disebut dengan jaringan komputer (Tanenbaum, 2003).

Virtual Private Network (VPN)

Virtual Private Network adalah perkembangan dari sebuah jaringan lokal intranet melalui jaringan publik yang menjamin keamanan dan efektifitas biaya di antara kedua hubungan jaringan (Gupta, 2003). Dengan adanya VPN, komputer-komputer yang tersebar secara geografis dapat di-*manage* menjadi sebuah *single-network* yang dapat saling berhubungan satu sama lainnya.

Elemen-Elemen *Virtual Private Network*

Untuk membangun teknologi VPN, diperlukan 6 elemen yang berperan penting pada setiap masing-masing fungsinya, yaitu perangkat keras VPN, perangkat lunak VPN, infrastruktur keamanan pada organisasi, dukungan infrastruktur S*ervice Provider*, jaringan publik, dan *tunnels* (Gupta, 2003).

Perangkat Keras VPN

Perangkat keras VPN terdiri dari sebagai berikut. Pertama adalah VPN *Server*. Ini adalah sebuah perangkat jaringan yang menjalankan perangkat lunak *server*. Fungsi-fungsi utama pada VPN *servers* yaitu: menerima *request* dari koneksi VPN, melakukan negosiasi kebutuhan koneksi dan parameter, melakukan autentikasi dan otorisasi pada VPN *clients*, menerima data dari *client* atau meneruskan *request* data yang dilakukan *client*, serta berlaku sebagai titik akhir (*end point*) pada VPN *tunnel* dan koneksi. Yang kedua adalah VPN *Client*. Ini adalah mesin lokal maupun jarak jauh yang melakukan sebuah koneksi VPN pada sebuah VPN *server*, dan melakukan *login* pada sebuah jaringan jarak jauh setelah diautentikasi pada VPN *server*, yang kemudian dapat melakukan komunikasi.

Perangkat Lunak VPN

Perangkat Lunak VPN terdiri dari sebagai berikut. Pertama adalah VPN *server*. Mesin apapun yang memiliki *Network Operating System* yang digunakan untuk melayani *request* dari VPN *client*. Microsoft Windows 2000, Windows NT, Novell Net Ware, dan Linux. Kedua adalah VPN *client*. Semua komputer jaringan apapun yang menghasilkan permintaan ke VPN *server*. Yang ketiga adalah aplikasi dan peralatan (*tools*) VPN *Management*.

Infrastruktur Keamanan Jaringan pada Perusahaan

Infrastruktur keamanan VPN biasanya terdiri dari kombinasi dari beberapa mekanisme, yaitu *firewall*, *Network Address Translation* (NAT), autentikasi *server* dan *database*, arsitektur *Authentication, Authorization and Accounting* (AAA), dan protokol IPSec.

Dukungan Infrastruktur S*ervice Provider*

Infrastruktur *Service Provider* merupakan suatu batas pada akses antara intranet perusahaan dengan jaringan publik.

Jaringan Publik

Jaringan Publik terdiri dari: POTS (*Plain Old Telephone Service*). POTS merupakan standar layanan jaringan telepon yang digunakan pada perumahan maupun perkantoran; PSTN (*Public Switched Telephone Network*). Contohnya adalah: ADSL, DSL, ISDN, FDDI, *Frame Relay*, dan ATM; serta *internet*.

Tunnels

Tunnels merupakan hubungan *point-to-point* secara *virtual* yang melewati jaringan publik seperti *internet*.

Tipe *Virtual Private Network* (VPN)

Virtual Private Network (VPN) terdiri dari 3 tipe, yakni: *Remote Acces* VPN, *Site To Site* VPN, dan *Extranet* VPN.

Remote Acces VPN

Remote Access VPN adalah koneksi *user-to-LAN* yang memungkinkan para *user* melakukan koneksi ke jaringan LAN perusahaan dari tempat yang berbeda di mana dia berada.

Site To Site VPN

Pada tipe ini digunakan untuk mengembangkan LAN suatu perusahaan ke gedung atau tempat yang lain. Tipe VPN ini dikoneksikan secara aktif sepanjang waktu (24 jam).

Extranet VPN

Extranet VPN memungkinkan koneksi yang aman dengan relasi bisnis, pemasok atau pelanggan untuk tujuan *e-commerce*. *Extranet* VPN merupakan extensi dari intranet VPN dengan tambahan *firewall* untuk melindungi jaringan internal perusahaan.

Komponen Keamanan VPN

Untuk keamanan VPN terdiri dari 4 komponen, yakni: Autentikasi *User*, Kendali Akses, Enkripsi, dan *Public Key Infrastructure* (PKI).

Autentikasi *User*

Autentikasi adalah proses dalam rangka validasi *user* pada saat memasuki sistem. Nama dan *password* dari pengguna diperiksa melalui proses yang memeriksa langsung daftar para *user*, yang diberikan hak untuk memasuki sistem.

Kendali Akses

Kendali akses (*acces control*) memliki kemampuan untuk memberikan akses (seperti hak terhadap *server*, direktori, dan file) yang berbeda kepada setiap *user* atau *group* tertentu dalam jaringan komputer lokal (*private network*) atau *remote access*.

Enkripsi

Enkripsi merupakan proses untuk mengubah, menyandikan atau mengkodekan sebuah pesan (informasi), sehingga tidak dapat dilihat atau dibaca tanpa menggunakan kunci pembuka.

Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) adalah teknologi lanjutan, yang pada akhirnya menjadi standar IETF (*Internet Engineering Task Force*). Sasaran PKI adalah menyediakan dasar untuk sistem yang akan mendukung berbagai layanan keamanan, sepeti integritas data, kerahasiaan data, dan autentikasi *user*.

Tunneling

Tunneling adalah dasar dari VPN untuk membuat suatu jaringan *private* melalui jaringan *internet* yang merupakan proses pengambilan semua paket data, dan mengenkapsulasinya dengan paket lain sebelum mengirimnya melalui sebuah jaringan (Thomas, 2004: 283).

Protokol *Tunneling*

***Point-to-Point Tunneling Protocol* (PPTP)**

Point to Point Tunneling Protocol (PPTP) beroperasi pada *Layer* 2 pada model referensi OSI dan didasarkan pada standar *Point to Point Protocol* (PPP) untuk jaringan *dial-up* yang memungkinkan semua pengguna dengan PPP *client* menggunakan ISP untuk terkoneksi ke *internet*. PPTP adalah sebuah protokol atau perangkat kebutuhan komunikasi yang memungkinkan korporasi untuk mengembangkan *corporate network* nya melalui *tunnel* pribadi pada *internet* publik (Thomas, 2004: 162).

Layer 2 Tunneling Protocol

L2TP adalah suatu standar yang dikembangkan oleh *Internet Engineering Task Force* (IETF) (RFC 2661) pada *layer* 2, yang merupakan kombinasi dari keunggulan-keunggulan fitur dari protokol L2F (dikembangkan oleh Cisco) dan PPTP (dikembangkan oleh Microsoft), yang didukung oleh vendor-vendor seperti: Ascend, Cisco, IBM, Microsoft, dan 3Com. Untuk mendapatkan tingkat keamanan yang lebih baik, L2TP dapat dikombinasikan dengan protokol *tunneling* IPSec pada *layer* 3 (Gupta, 2003).

IP Security (IPSec)

IPSec merupakan suatu standar keamanan komunikasi melalui jalur *internet* dengan autentikasi dan enkripsi untuk semua paket IP yang lewat pada *data stream* (Gupta, 2003). IPSec menyediakan keamanan pada *layer* 3 OSI yaitu *network layer*. IPSec menawarkan 3 layanan utama, yaitu: *authentication and data integrity*, *confidentiality*, dan *key management*.

Layanan autentikasi, *data integrity* dan *confidentialy* pada IPSec disediakan oleh 2 protokol utama IPSec yaitu: *Authentication Header* (AH) dan *Encapsulapted Security Payload* (ESP).

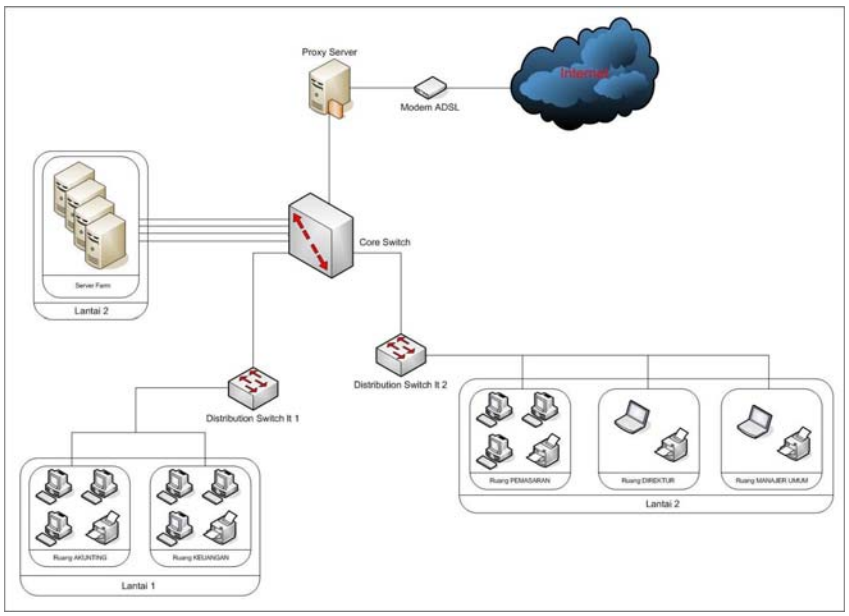
Protokol L2TP *over* IPSec (L2TP/IPSec)

Untuk dapat memenuhi kebutuhan keamanan pada L2TP, maka harus dilakukan implementasi keamanan dengan menggunakan protokol IPSec tipe *transport*, atau lebih dikenal dengan protokol L2TP *over* IPSec (L2TP/IPSec). Sehingga paket-paket data yang dikirimkan oleh protokol L2TP ini akan dienkapsulasi oleh protokol IPSec. Dengan pendekatan ini, paket-paket data pada L2TP ditukar melalui *User Datagram Protocol* (*port* 1701). Lalu, *Encapsulating Security Payload* (ESP) pada IPSec melindungi UDP *payload*, untuk memastikan komunikasi yang aman. Protokol ESP digunakan untuk menyediakan layanan *confidentiality*, keabsahan data yang asli dan lalu lintas yang terbatas pada aliran data yang bersifat rahasia. Untuk menyediakan kebutuhan *key management*, protokol IPSec menyediakan *Internet Key Exchange* (IKE) yang dapat memenuhi kebutuhan autentikasi dan melakukan perjanjian antara 2 komputer, yang disebut *Security Association* (SA). Autentikasi dan perjanjian antara 2 komputer tersebut disimpan pada sebuah *digital certificate* yang harus dimiliki oleh *server* maupun *client*.

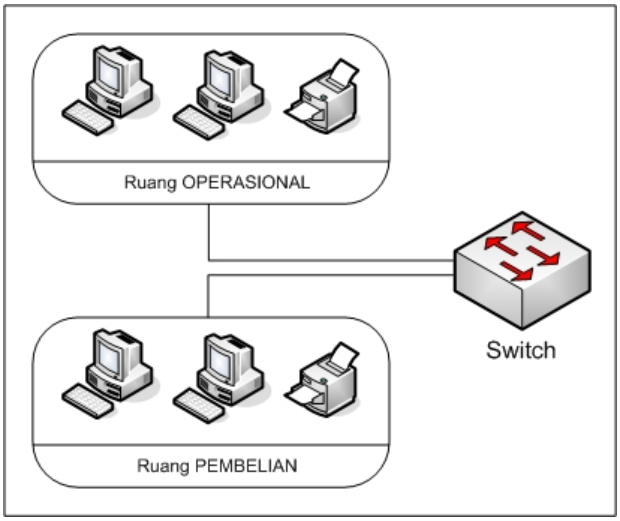
PEMBAHASAN

Analisis Sistem pada Perusahaan

PT Dharma Guna Sakti memiliki 2 jaringan lokal (LAN) yang terletak pada kantor pusat (Gambar 1) dan kantor cabang (Gambar 2).



Gambar 1 Topologi Umum Jaringan Kantor Pusat PT Darma Guna Sakti



Gambar 2 Topologi Umum Jaringan Kantor Cabang PT Dharma Guna Sakti

Penggunaan Aplikasi pada Perusahaan

Untuk membantu pengolahan data keuangan dan pembuatan laporan keuangan yang berjalan di perusahaan, PT Dharma Guna Sakti menggunakan *software* aplikasi keuangan Accurate. *Software* Accurate yang digunakan perusahaan saat ini adalah Accurate versi 3.2 *Deluxe*.

Analisis Permasalahan

Analisis permasalahan terdiri dari hal-hal sebagai berikut. Pertama, *order* dari pelanggan diterima oleh manajer operasional atau bagian pemasaran, kemudian dicek ketersediaan truk. Jika truk tersedia, maka *order* akan diterima. Bila truk tidak tersedia, maka *order* akan ditangguhkan dahulu atau ditolak langsung. Kedua, manajer operasional akan menerbitkan surat jalan, yang ditujukan kepada supir truk sebagai bukti bahwa truk dikeluarkan/dijalankan karena adanya *order* dari pelanggan. Kemudian diberitahukan kepada pelanggan tentang nomor polisi truk yang akan disewa oleh pelanggan. Ketiga, bila itu *order* untuk aktivitas ekspor, maka akan disertakan surat *Delivery Order* (DO) untuk pengambilan kontainer kosong (surat DO kontainer) di terminal kontainer yang telah ditentukan oleh pelanggan. Surat DO untuk pengambilan kontainer kosong ini biasanya dikirimkan melalui mesin *facsimile* kepada Manajer Operasional oleh

pelanggan sendiri, beserta surat DO barang. Keempat, surat DO barang ini bertujuan sebagai surat perintah kepada petugas gudang (gudang milik pelanggan), untuk melakukan pengisian kontainer kosong tersebut dengan barang yang dimiliki pelanggan di gudang, yang telah ditentukan oleh pelanggan tersebut.

Kelima, setelah kontainer terisi dengan barang, maka kontainer tersebut akan dibawa ke Pelabuhan Tanjung Priok untuk dilakukan aktivitas ekspor. Keenam, untuk *order* dengan aktivitas impor akan disertakan dengan dokumen-dokumen pengambilan kontainer impor (yang biasanya dilakukan oleh marketing perusahaan dan staf dari pelanggan). Truk akan langsung mengambil kontainer dari kapal (di Pelabuhan Tanjung Priok), yang kemudian isinya akan dibongkar di gudang milik pelanggan yang telah ditentukan. Ketujuh, kontainer yang telah kosong akan dikembalikan kepada pemilik kontainer berdasarkan surat perintah DO yang diberikan oleh pelanggan. Kedelapan, dari semua proses tersebut, maka dokumen-dokumen yang ada dibawa oleh supir, yang nantinya diserahkan kepada manajer operasional, yang kemudian akan didokumentasikan. Kesembilan, semua dokumen-dokumen dari hasil aktivitas tersebut nantinya akan dikirimkan oleh staf operasional kepada staf keuangan untuk diolah lebih lanjut, sehingga menjadi bukti transaksi hasil penjualan perusahaan dan *invoice* sebagai surat tagihan pembayaran oleh pelanggan.

Permasalahan yang Dihadapi

Dalam penelitian, ada beberapa masalah yang dihadapi seperti sebagai berikut. Pertama, dokumen transaksi yang ada di kantor cabang harus dikirim ke kantor pusat dengan menggunakan jalan darat. Akan tetapi, dengan terbatasnya karyawan dan waktu, maka sering terjadi penumpukan dokumen transaksi di kantor cabang. Hal ini menghambat pekerjaan yang ada pada kantor pusat. Kedua, belum adanya jalur komunikasi langsung antar komputer yang berada di kantor pusat dengan kantor cabang, sehingga arus informasi data dari kantor cabang ke kantor pusat ataupun sebaliknya belum terbentuk. Ketiga, kebutuhan kantor cabang menggunakan *software* Accurate untuk melakukan sentralisasi dan pengawasan data secara langsung. Keempat, belum tersedianya koneksi jaringan ke kantor pusat bagi *mobile user* untuk mengakses maupun mengirimkan data. Kebutuhan koneksi ke jaringan pusat bagi *mobile user* ini seperti direktur, manajer umum, dan manajer bagian yang ingin senantiasa melakukan pemeriksaan laporan keuangan pada perusahaan.

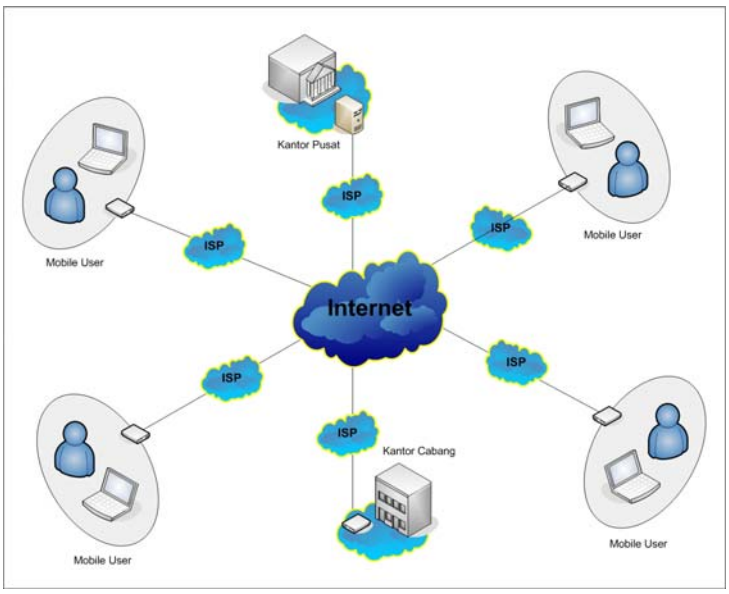
Usulan Pemecahan Masalah

Untuk menciptakan jalur komunikasi langsung antara kantor pusat dan kantor cabang, digunakan teknologi yang dapat menjamin komunikasi data antar jaringan yang terpisah secara efisien dan aman, yaitu teknologi *Virtual Private Network* (VPN). Tipe teknologi VPN yang diusulkan dengan pertimbangan kebutuhan pada PT Dharma Guna Sakti adalah *remote access* VPN. Dengan usulan ini, pada kantor pusat akan dibangun sebuah VPN *server*, yang akan melayani hubungan dari kantor cabang maupun *mobile user*.

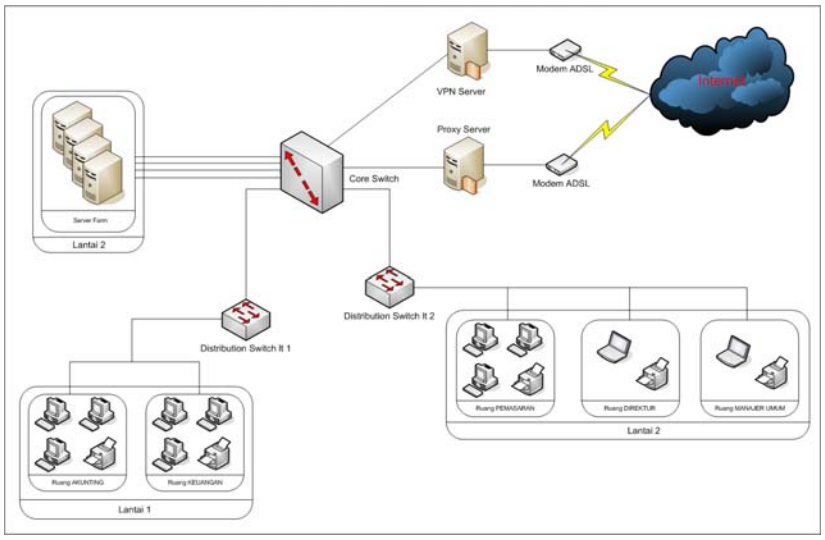
Dengan perancangan VPN pada PT Dharma Guna Sakti, ketika komputer kantor cabang maupun *mobile user* yang berada di luar kantor pusat ingin terhubung dengan kantor pusat, harus melakukan *dial-in* pada VPN *server* di kantor pusat terlebih dahulu. Setelah proses autentikasi berhasil, kemudian VPN *server* akan menempatkan *user* yang melakukan *dial-in* pada jaringan lokal kantor pusat, sehingga kantor cabang dan *mobile user* dapat mengakses *database* Accurate pada komputer yang telah di-*install* aplikasi *client* sebelumnya. Dengan demikian, dokumen yang biasanya dikirim melalui jalan darat dapat dengan segera di-*input* pada *database server* Accurate di kantor pusat, dan direktur, manajer umum maupun manajer bagian dapat selalu memeriksa keuangan perusahaan ketika berada di luar kantor.

Usulan Solusi Perancangan VPN

Software-based VPN dengan sistem operasi Linux merupakan solusi yang paling tepat untuk perusahaan, karena memiliki fungsionalitas baik dan tidak memerlukan biaya untuk membeli sistem operasi maupun perangkat lunak yang menunjang kebutuhan sebuah VPN *server*, serta tidak perlu membayar setiap lisensi *client* yang akan terhubung dengan VPN *server*. Gambar 3 menunjukkan usulan solusi koneksi jaringan antara kantor pusat dengan kantor cabang dan *mobile user*. Sedangkan usulan konfigurasi sistemnya dapat dilihat pada Gambar 4.



Gambar 3 Usulan Solusi Koneksi Jaringan pada Perusahaan



Gambar 4 Topologi Jaringan Kantor Pusat dengan VPN *Server*

Pemilihan *Internet Service Provider* (ISP)

Perancangan VPN pada perusahaan menggunakan layanan *internet* ADSL dari *service provider* Speedy Telkom, dengan *bandwidth* sebesar 128 Kbps.

Pemilihan Perangkat Keras VPN

Untuk perancangan VPN pada perusahaan, akan digunakan perangkat keras VPN berbasis PC.

Pemilihan Perangkat Lunak VPN

Perangkat lunak yang akan digunakan terdiri dari: sistem operasi Linux Fedora Core 6, Openswan untuk implementasi protokol IPSec, xl2tpd untuk implementasi protokol L2TP, dan open SSL untuk membuat *digital certificate*.

Pemilihan Protokol *Tunneling*

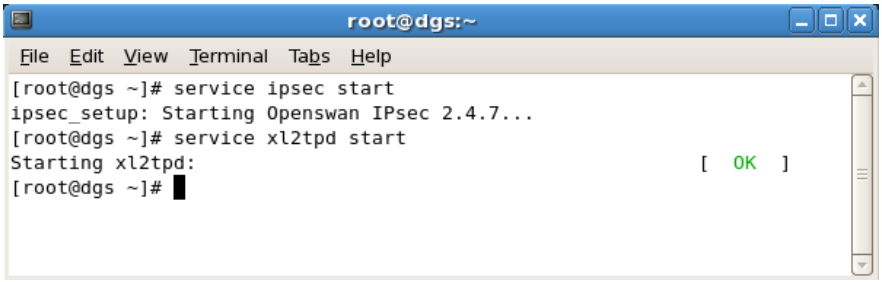
Perancangan VPN pada perusahaan akan dipilih protokol *tunneling* L2TP/IPSec.

Pemilihan Protokol Autentikasi

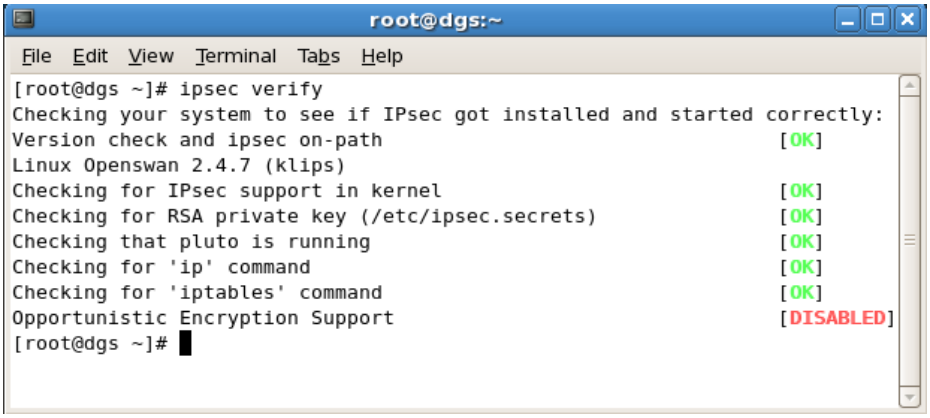
Untuk pemilihan protokol autentikasi didasarkan pada protokol *tunneling* yang telah dipilih sebelumnya. Pada L2TP/IPSec, protokol autentikasi dijalankan oleh *Internet Key Exchange* (IKE) pada IPSec.

Tes Koneksi

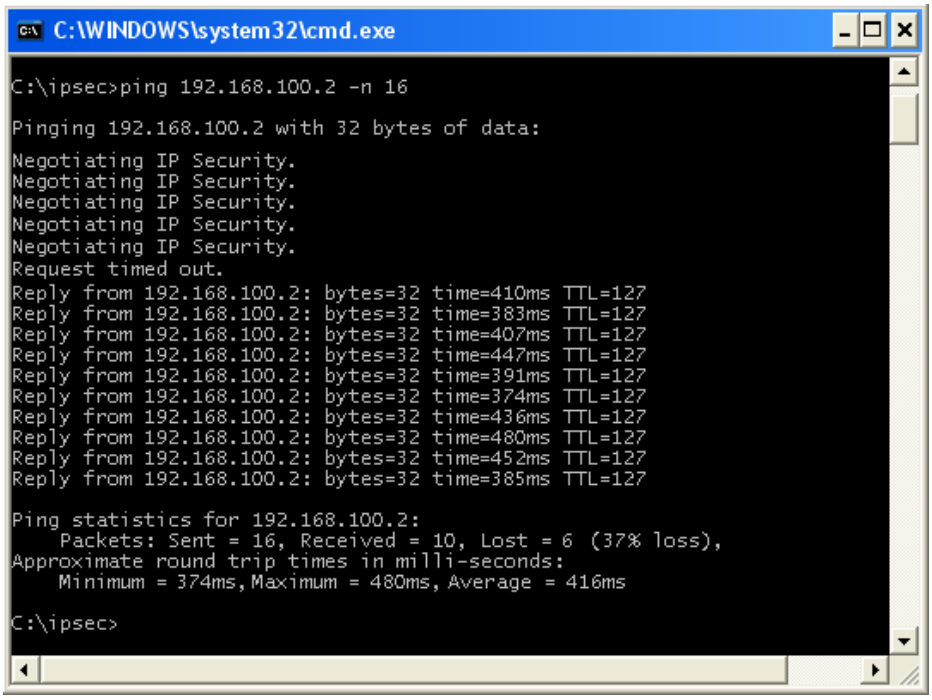
Gambar 5 menunjukkan pengujian koneksi pada saat *service* IPSec dan xl2tpd pada VPN *Server*. Sedangkan Gambar 6 menunjukkan status modul *service* IPSec yang berhasil di-*install* dan dijalankan. Gambar 7 menunjukkan proses pengiriman paket yang dilakukan dari VPN *client* menuju *database* di belakang VPN *server* dengan IP *address* 192.168.100.2, serta dapat dilihat proses negosiasi keamanan dengan melakukan proses autentikasi terlebih dahulu.



Gambar 5 Menjalankan *Service* IPSec dan xl2tpd pada VPN *Server*



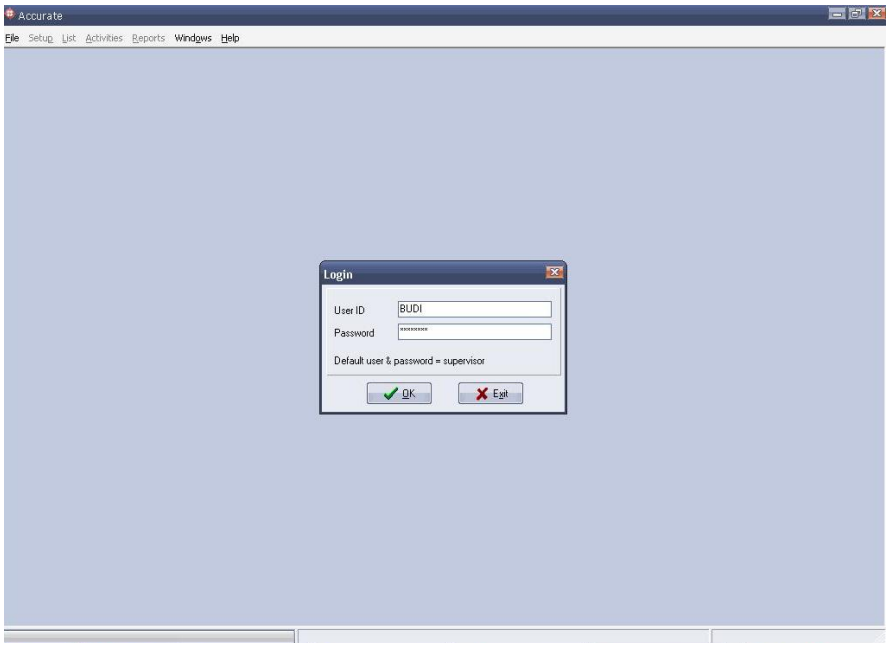
Gambar 6 Status Modul *Service* IPSec yang Berhasil Di-*install* dan Dijalankan



Gambar 7 Proses Pengiriman Paket ICMP Menuju *Database* di Belakang VPN *Server*

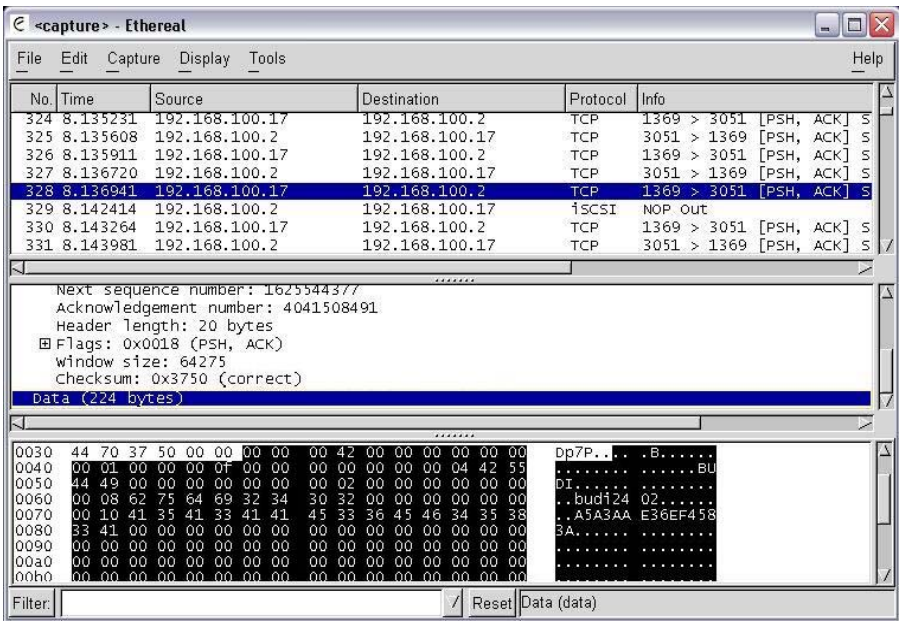
Tes *Sniffing* Paket

Percobaan yang dilakukan adalah dengan melakukan *sniffing* paket data sebelum menjalankan VPN. Pada percobaan ini, *user* dengan IP *address* 192.168.100.17 akan melakukan koneksi pada *database* Accurate, dengan IP *address* 192.168.100.2. Pada Gambar 8, ditunjukkan sebuah layar *login* Accurate dengan menggunakan *user*ID BUDI dan *password* budi2402.



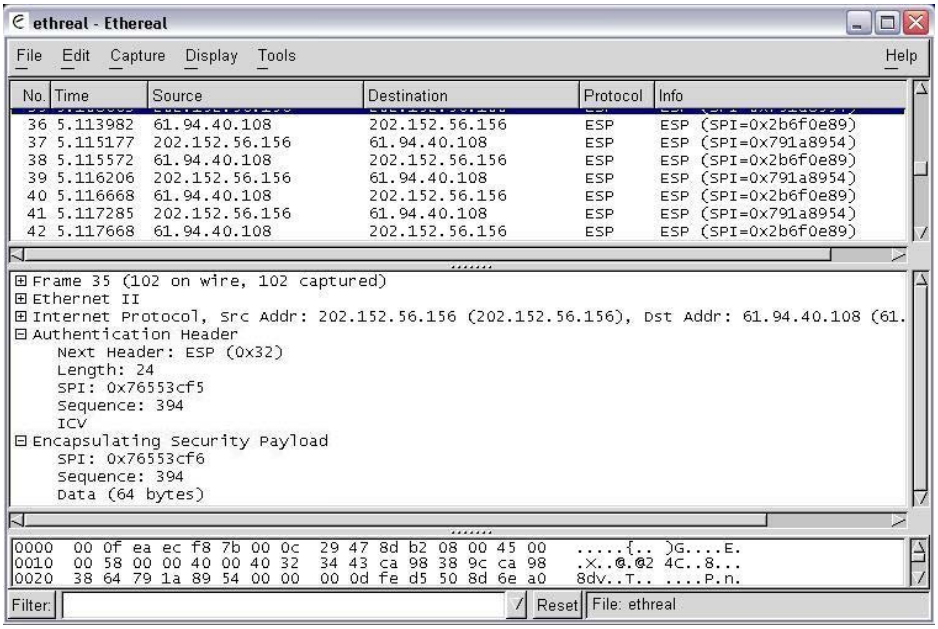
Gambar 8 *Login* Accurate dengan *UserID* BUDI dan *Password* budi2402

Gambar 9 menunjukkan hasil *sniffing* paket-paket data dengan Ethereal sebelum menjalankan VPN.



Gambar 9 *Sniff* Paket Data Tanpa VPN

Sedangkan Gambar 10 menunjukkan hasil *sniffing* paket-paket data setelah menjalankan VPN.



Gambar 10 *Sniff* Paket Data Dengan VPN

Manfaat VPN pada PT Dharma Guna Sakti

Setelah ujicoba implementasi VPN pada perusahaan, maka diharapkan teknologi VPN ini dapat memberikan manfaat pada perusahaan sebagai berikut. Pertama, dengan teknologi VPN yang dirancang pada perusahaan, kantor cabang dapat terhubung dengan kantor pusat, sehingga pada kantor cabang dapat menggunakan *software* Accurate untuk mengirimkan data-data dokumen transaksi secara langsung dari kantor cabang ke kantor pusat. Oleh karena itu, dapat tercipta sentralisasi data antara kantor cabang dan kantor pusat. Kedua, waktu pengiriman dokumen transaksi menjadi lebih cepat dan kantor pusat tidak perlu menunggu data yang dikirim dari kantor cabang yang biasanya dikirim melalui jalan darat. Ketiga, direktur, para manajer, dan pemegang saham yang biasanya berada di luar kantor dapat terhubung dengan kantor pusat untuk memeriksa laporan keuangan pada perusahaan dengan menggunakan *software* Accurate.

PENUTUP

Kesimpulan

Setelah mengadakan analisis dan perancangan VPN (*Virtual Private Network*) pada PT Dharma Guna Sakti, maka didapatkan kesimpulan sebagai berikut. Pertama, *Virtual Private Network* dapat menghubungkan jaringan lokal perusahaan dengan jaringan yang terdapat di luar perusahaan, yaitu antara jaringan kantor pusat dengan kantor cabang. Kedua, dengan VPN, maka kantor cabang dan *mobile user* dapat melakukan koneksi atau hubungan langsung menggunakan *Accurate* pada kantor pusat, sehingga tercipta suatu sentralisasi data pada perusahaan. Ketiga, VPN telah berjalan dengan baik dengan melakukan enkapsulasi pada paket-paket data yang dikirim. Hal ini dapat dilihat pada percobaan yang dilakukan dengan *software sniffing Ethereal* yang dilakukan pada saat *user* login *software Accurate*.

Saran

Adapun saran yang diberikan kepada PT Dharma Guna Sakti, untuk meningkatkan efektifitas dan efisiensi kerja pada masa yang akan datang adalah sebagai berikut. Pertama, menempatkan *Administrator* Jaringan untuk memantau jaringan yang ada, sehingga bila ada masalah maka akan dapat diperbaiki dengan cepat tanpa harus menunggu tenaga ahli dari luar. Kedua, menggunakan tipe VPN *site-to-site* untuk menghubungkan jaringan antara kantor pusat dengan cabang, apabila kebutuhan untuk mengakses informasi data semakin intensif dan terus menerus. Ketiga, menambahkan FTP *server* untuk menampung data-data yang di-*share* pada jaringan. Keempat, memberikan fasilitas VoIP dan FaxIP dengan memanfaatkan infastruktur VPN yang sudah dirancang pada perusahaan.

DAFTAR PUSTAKA

Tanenbaum, Andrew S. (2003). *Computer Networks*, 4th edition. Prentice Hall

Lukas, Jonathan. (2006). *Jaringan Komputer*. Jakarta: Graha Ilmu.

Gupta, Meeta. (2003). *Building a Virtual Private Network*. Premier Press

Thomas. (2004). *Network Security*. Yogyakarta: Andi.

Stallings, William. (2001). *Komunikasi Data dan Komputer*. Thamir Abdul Hafedh Al-hamdany (Penerjemah). Salemba Teknika.

Wendy, Aris. (2005). *Membangun VPN Linux Secara Cepat*. Yogyakarta: Andi.

Leeuw, Jacco dee. (2007). *Using a Linux L2TP/IPsec VPN server*. http://www.jacco2.dds.nl/networking/freeswan-l2tp.html.

Hutapea, Tommy P. M. (2003). *Virtual Private Network (VPN) Dynamic: Jawaban Keamanan untuk Intranet pada Suatu Perusahaan*. Komunitas Elearning Gratis Ilmu Komputer Indonesia. http://ikc.vip.net.id/populer/tommy-vpn.php.

The Internet Society. (2001). *Securing L2TP using IPsec*. http://www.ietf.org/rfc/rfc3193.txt.

Microsoft Technet. (2002). *Administrator's Guide to Microsoft L2TP/IPSec VPN Client*. http://www.microsoft.com/technet/prodtechnol/windows2000serv/support/vpnclientag.mspx.