PEMANFAATAN VIRTUAL PRIVATE NETWORK MENGGUNAKAN PROTOKOL L2TP SEBAGAI PENGHUBUNG ANTAR CABANG CV. KARTA WIDJAYA GROUP

Naskah Publikasi

diajukan oleh

Deni Dwi Kisworo

07.11.1350

kepada

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2011

NASKAH PUBLIKASI

PEMANFAATAN VIRTUAL PRIVATE NETWORK MENGGUNAKAN PROTOKOL L2TP SEBAGAI PENGHUBUNG ANTAR CABANG CV. KARTA WIDJAYA GROUP

disusun oleh

Deni Dwi Kisworo
07.11.1350

Dosen Pembimbing

Sudarmawan, MT

NIK. 190302035

Tanggal, 6 Agustus 2011

Ketua Jurusan
Teknik Informatika

Ir. Abas Ali Pangera, M. Kom.

NIK. 190302010

UTILIZATION OF VIRTUAL PRIVATE NETWORK USING THE L2TP PROTOCOL FOR INTER-BRANCH LIAISON CV. KARTA WIDJAYA GROUP

PEMANFAATAN VIRTUAL PRIVATE NETWORK MENGGUNAKAN PROTOKOL L2TP SEBAGAI PENGHUBUNG ANTAR CABANG CV. KARTA WIDJAYA GROUP

Deni Dwi Kisworo
Jurusan Teknik Informatika
STMIK AMIKOM YOGYAKARTA

ABSTRACT

*CV. Karta Widjaya Group is the parent company of Dokter Komputer. Dokter Komputer is obliged to submit daily report form *. xlsx files in accordance with the daily activities performed. Problems arise because between the central office of CV. Karta Widjaya Group is not located in one area. How that is done so far using the Internet as a medium for data transfer. But this does not guarantee its security because in the internet a lot of fraud.*

As per the above problems is to use a technology that is Virtual Private Network (VPN). VPNs are able to make a hole (tunnel) that seems to be a private network. Data packets through the VPN path can not be easily read by a sniffer on the public network. Many existing VPN protocols such as PPTP, L2F, L2TP, OVPN, in this case use the L2TP protocol because of the ease and security guarantees. L2TP also supports the security system of IP Security (IPsec), which guarantees encryption and data integrity during transfer.

By using a Virtual Private Network technology issues that have been the threat can be resolved. In fact not only in terms of security, CV. Karta Widjaya Group can utilize this network as a local network.

Keywords : *Virtual Private Network, L2TP, IPsec, Security*

1. Pendahuluan

Internet merupakan jaringan terbuka yang bisa diakses semua orang untuk komunikasi dan bertukar informasi. Makin banyaknya penyedia layanan internet maka semakin memudahkan orang untuk mendapatkan akses internet. Melihat kondisi ini CV. Karta Widjaya Group memanfaatkan internet sebagai penghubung jaringan lokal antara kantor pusat dengan jaringan toko cabang untuk menghemat biaya. Namun faktor keamanan masih menjadi permasalahan.

Untuk mengatasi permasalahan keamanan data di jaringan internet ada suatu metode yaitu *Virtual Private Network* (VPN). VPN merupakan jaringan lokal yang terhubung melalui jaringan publik (Internet). Di dalam VPN terdapat metode *tuneling* dan enkripsi yang menjamin keamanan data walaupun data melewati jaringan publik. Hal ini yang membuat VPN handal dalam mengatasi permasalahan ini.

Dalam implementasinya VPN dibagi menjadi dua jenis yaitu *remote access* dan *site-to-site* VPN. *Remote access* VPN merupakan suatu cara meremote *server* atau *host private* melalui jaringan publik dengan aman. Sedangkan *site-to-site* digunakan untuk menghubungkan dua tempat yang berjauhan, misal antara kantor pusat dengan kantor cabang. Dalam kasus ini CV. Karta Widjaya Group ingin menghubungkan antara kantor pusat dengan toko cabang yang letaknya kurang lebih 10 KM. Maka *site-to-site* VPN menjadi pilihan.

VPN mempunyai banyak protokol dalam implementasinya diantaranya *Point to Point Tuneling Protocol* (PPTP), *Layer 2 Tuneling Protocol* (L2TP), dengan teknologi *Internet Protocol Security* (IPSec) dan *Secure Sockets Layer* (SSL). Masing-masing protokol memiliki aturan dan karakteristik berbeda-beda.

Penggunaan L2TP dengan keamanan IPSec sangat tepat digunakan untuk kasus ini. Dimana IPSec menawarkan keamanan data, keutuhan, dan otentikasi antar *peer*. Dengan Metode ini sudah memenuhi standar keamanan pertukaran data melalui jaringan publik.

2. Landasan Teori

2.1 Virtual Private Network

VPN merupakan suatu jaringan komunikasi lokal yang terhubung melalui media jaringan publik.[1] Infrastruktur publik yang paling banyak digunakan adalah internet. Untuk memperoleh komunikasi yang aman (*private*) melalui internet, diperlukan protokol khusus untuk mengatur pengamanan datanya.

Perusahaan yang ingin membuat *wide area network* (WAN) dapat menggunakan VPN sebagai alternatif dalam implementasinya. Penggunaan leased line sebagai implementasi WAN membutuhkan investasi yang sangat besar. Dibutuhkan pengeluaran ribuan dolar (USD) setiap bulannya untuk memperoleh hak istimewa menggunakan kabel yang tak dapat digunakan oleh perusahaan.

Cara kerja Virtual Private Network dapat dianalogikan sebagai berikut:

1. Digging the Tunnel

Tunnel dalam VPN sebenarnya hanya logical point-to-point connection dengan otentikasi dan enkripsi. Analoginya adalah kalau sebuah organisasi/perusahaan punya kantor di dua gedung yang berbeda. Untuk orang/informasi bergerak dari satu kantor ke kantor lainnya, bisa melalui kaki lima atau jalan umum pilihan kedua dengan menggali lubang di bawah tanah (analogi dengan VPN).

2. Proses Enkapsulasi

[1] http://www.essaycoursework.com/essay/definisi-vpn-vpn-merupakan/42460

Paket lama dibungkus dalam paket baru. Alamat ujung tujuan terowongan (tunnel endpoints) diletakkan di destination address paket baru, yang disebut dengan encapsulation header. Tujuan akhir tetap ada pada header paket lama yang dibungkus (encapsulated). Saat sampai di endpoint, kapsul dibuka, dan paket lama dikirimkan ke tujuan akhirnya.

2.1.1 Layer 2 Tunneling Protocol

Layer 2 Tunneling protocol merupakan gabungan dari dua protokol VPN sebelumnya yaitu PPTP dan L2F. L2TP biasa digunakan dalam membuat *Virtual Private Dial Network* (VPDN) yang dapat bekerja membawa semua jenis protokol komunikasi didalamnya. Umunnya L2TP menggunakan port 1702 dengan protokol UDP untuk mengirimkan L2TP encapsulated PPP frames sebagai data yang di tunnel. Terdapat dua model tunnel yang dikenal (Lewis, 2006), yaitu *compulsory* dan *voluntary*. Perbedaan utama keduanya terletak pada *endpoint* tunnel-nya. Pada *compulsory tunnel*, ujung tunnel berada pada ISP, sedangkan pada *voluntary* ujung *tunnel* berada pada *client remote*.

2.2 IP Security

IPSec (singkatan dari IP *Security*) adalah sebuah protokol yang digunakan untuk mengamankan transmisi datagram dalam sebuah *internetwork* berbasis TCP/IP. IPSec mendefiniskan beberapa standar untuk melakukan enkripsi data dan juga integritas data pada lapisan kedua dalam DARPA Reference Model (inter*network* layer). IPSec melakukan enkripsi terhadap data pada lapisan yang sama dengan protokol IP dan menggunakan teknik *tunneling* untuk mengirimkan informasi melalui jaringan Internet atau dalam jaringan Intranet secara aman. IPSec didefinisikan oleh badan *Internet Engineering Task Force* (IETF) dan diimplementasikan di dalam banyak sistem operasi. Windows 2000 adalah sistem operasi pertama dari Microsoft yang mendukung IPSec.

IPSec diimplementasikan pada lapisan transport dalam OSI *Reference Model* untuk melindungi protokol IP dan protokol-protokol yang lebih tinggi dengan menggunakan beberapa kebijakan keamanan yang dapat dikonfigurasikan untuk memenuhi kebutuhan keamanan pengguna, atau jaringan. IPSec umumnya diletakkan sebagai sebuah lapsian tambahan di dalam *stack* protokol TCP/IP dan diatur oleh setiap kebijakan keamanan yang diinstalasikan dalam setiap mesin komputer dan dengan sebuah skema enkripsi yang dapat dinegosiasikan antara pengirim dan penerima. Kebijakan-kebijakan keamanan tersebut berisi kumpulan *filter* yang diasosiasikan dengan kelakuan tertentu. Ketika sebuah alamat IP, nomor *port* TCP dan UDP atau protokol dari sebuah paket datagram IP cocok dengan *filter* tertentu, maka kelakukan yang dikaitkan dengannya akan diaplikasikan terhadap paket IP tersebut.

Untuk membuat sebuah sesi komunikasi yang aman antara dua komputer dengan menggunakan IPSec, maka dibutuhkan sebuah *framework* protokol yang disebut dengan ISAKMP/Oakley. *Framework* tersebut mencakup beberapa algoritma kriptografi yang telah ditentukan sebelumnya, dan juga dapat diperluas dengan menambahkan beberapa sistem kriptografi tambahan yang dibuat oleh pihak ketiga. Selama proses negosiasi dilakukan, persetujuan akan tercapai dengan metode autentikasi dan kemanan yang akan digunakan, dan protokol pun akan membuat sebuah kunci yang dapat digunakan bersama (shared key) yang nantinya digunakan sebagai kunci enkripsi data.

IPSec menggunakan 2 protokol

1. *Authentication Header* (AH): memungkinkan verifikasi identitas pengirim. AH juga memungkinkan pemeriksaan integritas dari pesan/informasi.
2. *Encapsulating Security Payload* (ESP): memungkinkan enkripsi informasi sehingga tetap rahasia. IP original dibungkus, dan outer IP header biasanya berisi *gateway* tujuan. Tetapi ESP tidak menjamin *integrity* dari *router* IP *header*, oleh karena itu dipergunakan bersamaan dengan AH.

2.3 Wireshark

Wireshark adalah salah satu dari sekian banyak *tool Network* Analyzer yang banyak digunakan oleh *Network administrator* untuk menganalisa kinerja jaringannya. Wireshark banyak disukai karena interfacenya yang menggunakan *Graphical User Interface* (GUI) atau tampilan grafis. Wireshark dapat didownload di http://www.wireshark.org secara gratis.

3. Metode Penelitian

3.1 Identifikasi Masalah Perusahaan

CV. Karta Widjaya Group mempunyai beberapa masalah yang perlu dipertimbangkan, yaitu:

1. Jarak yang menghubungkan CV. Karta Widjaya Group dengan Dokter Komputer yang jauhnya kurang lebih 10 kilo meter mempersulit komunikasi secara pribadi.
2. Komunikasi melalui jaringan publik dapat mengatasi jarak tetapi kurangnya keamanan masih menjadi kekhawatiran utama walaupun selama ini belum terjadi pencurian data.
3. Dokter Komputer mempunyai kewajiban mengirimkan laporan harian dan laporan bulanan kepada CV. Karta Widjaya Group sebagai pertanggungjawaban usaha yang dijalankan. Dalam Kasus ini sedang dibangun sistem informasi berbasis web dengan format laporan xml. Tetapi aplikasi tersebut belum selesai, jadi untuk sementara laporan menggunakan format xls (Ms. Excell) yang dikirimkan perhari dan perbulan.
4. Pihak CV. Karta Widjaya Group sebagai penyuplay barang ke Dokter Komputer memberikan Harga Pokok Pembelian (HPP) dan Daftar Harga Jual yang tidak boleh diketahui oleh toko lain bahkan karyawannya sendiri kecuali admin keuangan yang telah dipercaya.
   Data-data yang perlu diamankan dalam proses pertukarannya antara lain: Harga Pokok Pembelian, Harga Jual, Penawaran Tender, Laporan Harian, Laporan Bulanan.

3.1.1 Penyebab Masalah

Dari banyak masalah yang didapat salah satu penyebab utama adalah jarak antara CV. Karta Widjaya Group dengan Dokter Komputer yang cukup jauh. Dari Jarak inilah yang menyebabkan masalah-masalah baru seperti keamanan data.

3.1.2 Solusi Penyelesaian Masalah

Dari uraian di atas CV. Karta Widjaya Group membutuhkan keamanan *transfer* data antara kantor pusat dengan toko cabang. Beberapa alternatif cara yang ditawarkan adalah:

1. Pengiriman data menggunakan *public email* (yahoo, google, dll.)
2. *File Server* menggunakan *Server* dengan *IP Public*
3. *Site-to-Site Virtual Private Network*

Dari tiga alternatif tersebut dibandingkan kekurangan dan kelebihan masing-masing teknologi.

Tabel 3.1 Perbandingan Teknologi yang Ditawarkan

Teknologi	Kelebihan	Kekurangan
Public Email (yahoo, google, dll.)	Mudah dalam penggunaan, Didukung keamanan SSL, Tidak memerlukan infrastruktur khusus.	*Server* berada di luar perusahaan, Tidak ada jaminan keamanan data dari pihak penyedia layanan email, Banyak *spam* yang mengganggu.
Server dengan *IP Public*	Mudah diakses dari mana saja layaknya *Cloud Computing*.	Memerlukan *IP Public* secara permanen, *Server* mudah diserang *attacker* karena jaringan *public* sangat bebas, Jaminan keamanan data sesuai SDM yang ada.
Site-to-Site Virtual Private Network	Mudah diimplementasikan, Jaminan keamanan jalur data, *Server* tidak bisa diserang dari jalur *public* karena *server* berada di belakang *firewall* nat, Dukungan fasilitas *Local Area Network* seperti: *Printer sharing, File Sharing, Remote Desktop* yang sangat mudah diakses layaknya jaringan lokal.	*Delay* bertambah 1 sampai 2 milisecond

Dari Tabel 3.1 dapat disimpulkan bahwa dari ketiga alternatif cara untuk mentransfer data penggunaan site-to-site VPN mempunyai resiko keamanan yang paling kecil dengan kelebihan layaknya jaringan lokal.

3.2 Alat dan Bahan Penelitian

3.2.1 Hardware

Router (dua unit)

1. RB750 MikroTik

PC *Server* di kantor pusat

1. Processor Intel Core 2 Duo
2. Harddisk 160 GB
3. Memori DDR2 2GB

PC Admin 1, Admin 2, Admin 3

1. Processor Intel Core 2 Duo
2. Harddisk 320 GB
3. Memori DDR2 2GB
4. VGA Intregated
5. Sound Intregated

6. Monitor samsung 15”
7. Keyboard + mouse

Switch

1. D-Link 4 Port

3.2.2 Software

Router
1. MikroTik Router OS Lisensi 4

PC *Server*
1. Ubuntu Server 10.04.1 i386
2. Samba File Server

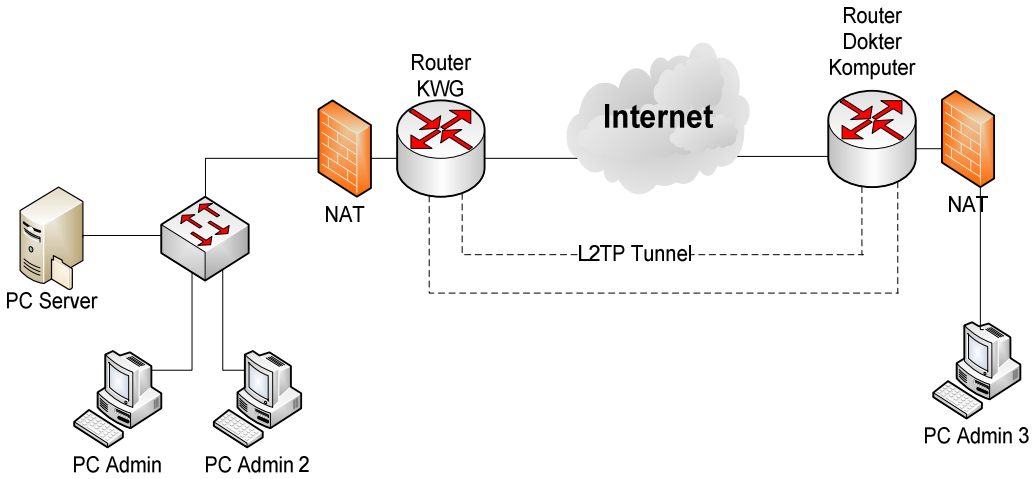
PC Admin 1, Admin 2, Admin 3

1. Microsoft Windows 7
2. Bitvise Tunnelier SSH + SFTP Client

PC Perancangan dan Pengujian

1. Microsoft Windows 7
2. WinBox
3. Bitvise Tunnelier SSH *Client* + SFTP *Client*
4. WireShark
5. Microsoft Office Visio

3.3 Merancang Topologi



Gambar 3.1 Topologi VPN CV. Karta Widjaya Group

3.4 Merancang Alokasi IP Address

Tabel 3.2 Alokasi IP Address

Device	Interface	IP Address	Netmask	Gateway
PC Server	Local Area	192.168.100.200	255.255.255.0	192.168.100.1

Kantor Pusat	Connection (eth0)			
PC Admin 1 Kantor Pusat	Local Area Connection (eth0)	192.168.100.101	255.255.255.0	192.168.100.1
PC Admin 2 Kantor Pusat	Local Area Connection (eth0)	192.168.100.102	255.255.255.0	192.168.100.1
PC Admin 3 Dokter Kom.	Local Area Connection (eth0)	172.16.29.20	255.255.255.240	172.16.29.30
Router Kantor Pusat	ether1	IP Public	/25	Gateway ISP
	ether2	192.168.100.1	255.255.255.0	
	l2tp	10.10.10.1	255.255.255.252	
Router Dokter Kom.	ether1	IP Public		Gateway ISP
	Ether2	172.16.29.30	255.255.255.240	
	l2tp	10.10.10.2	255.255.255.252	

3.5 Konfigurasi Jaringan

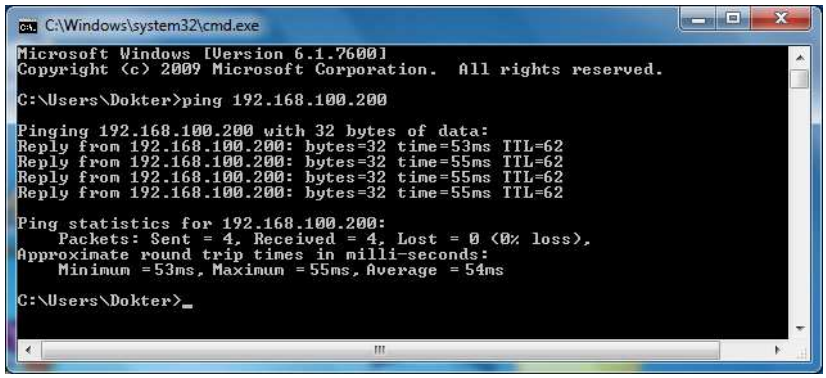
Konfigurasi Jaringan Meliputi:

1. Konfigurasi PC Server, PC Admin, PC Admin 2, PC Admin 3
2. Konfigurasi Router kantor pusat dan Router Dokter Kompuer
3. Konfigurasi L2TP Tunnel
4. Konfigurasi IPsec Tunnel

4. Hasil dan Pembahasan

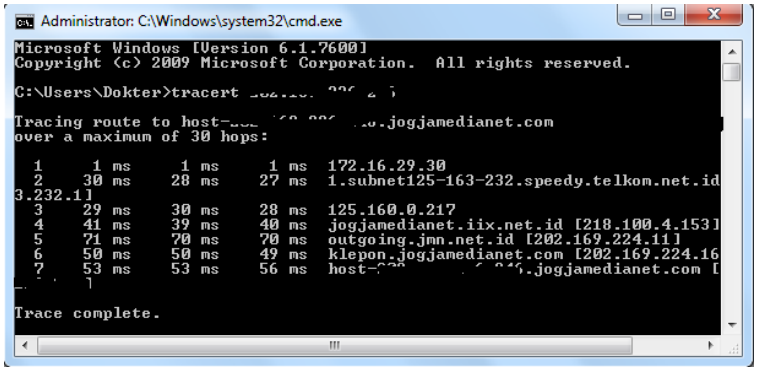
4.1 Uji Koneksi

Ping dari PC Admin 3 ke PC Server

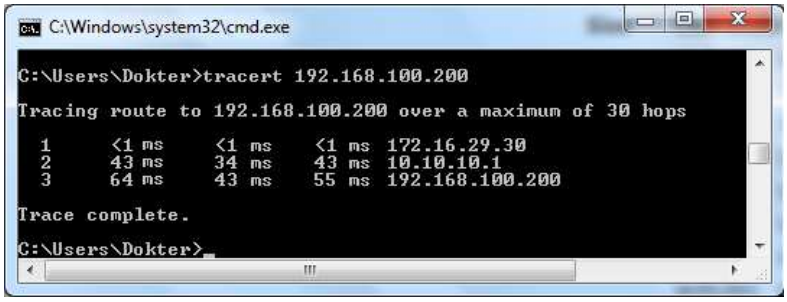


Gambar 4.1 Ping ke PC Server

4.2 Tracert



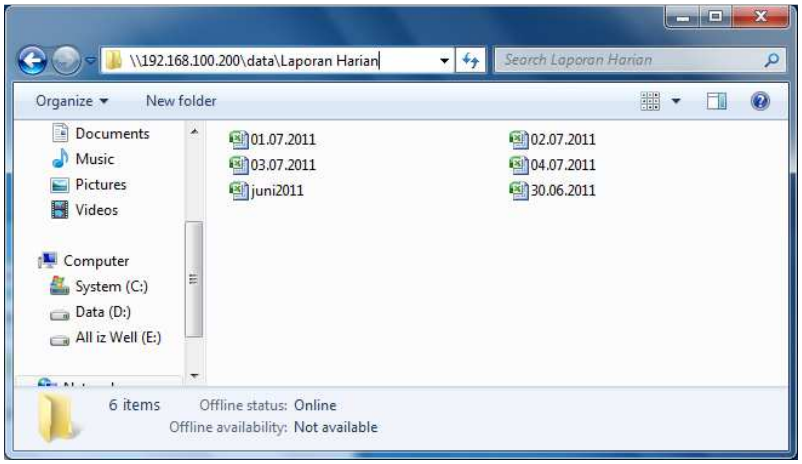
Gambar 4.2 Tracert Tanpa VPN



Gambar 4.3 Tracert Dengan VPN

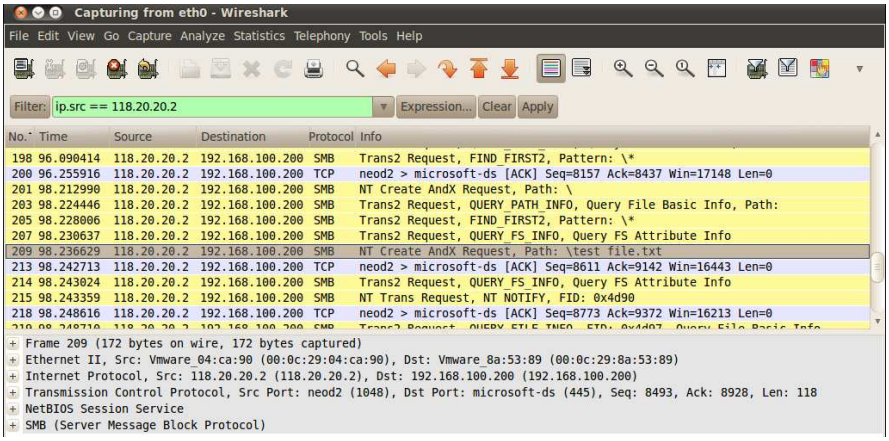
Menggunakan VPN mengurangi jumlah hop yang dilewati paket data.

4.3 File Sharing



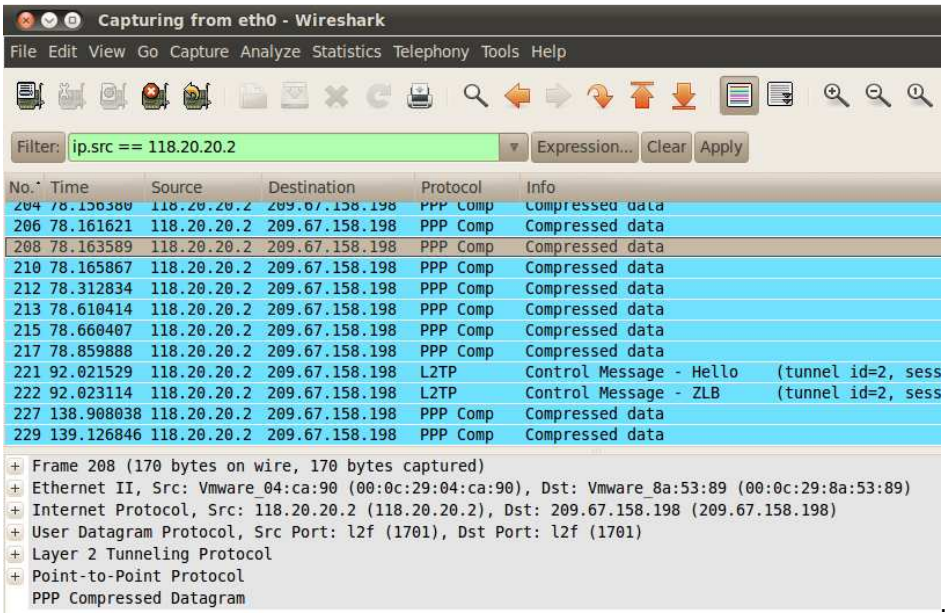
Gambar 4.3 File Sharing PC Server

4.4 Keamanan Jalur Data



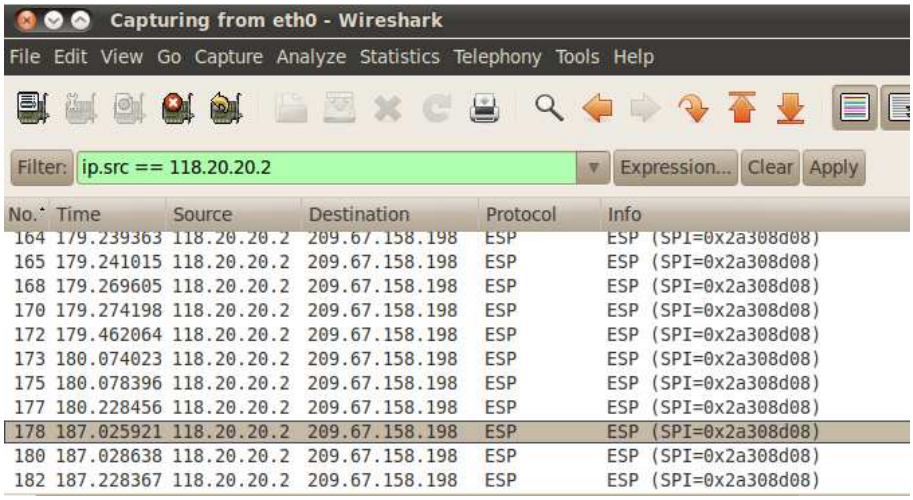
Gambar 4.4 Transfer File Tanpa VPN

Data yang dikirim dapat terbaca dengan mudah menggunakan Wireshark ketika transfer file tanpa menggunakan Virtual Private Network.



Gambar 4.5 Transfer File Menggunakan VPN

Setelah menggunakan VPN semua data yang ditransfer tidak dapat dibaca dengan mudah. Semua data dienkapsulasi oleh l2tp menjadi Compressed Datagram.



Gambar 4.5 Transfer File Menggunakan L2TP+IPsec

Data semakin tidak terlihat ketika ditambahkan IPsec yang membungkus paket setelah dibungkus l2tp menjadi protokol ESP (*Encapsulating Security Payload).*

5. Kesimpulan

Menggunakan Virtual Private Network merupakan cara paling efektif untuk menghubungkan kantor pusat CV. Karta Widjaya Group dengan toko cabang Dokter Komputer. VPN dengan tipe site-to-site membutuhkan router sebagai ujung point-to-point, sedang PC Server dan PC Client berada di belakang firewall nat. Dari segi keamanan penggunaan VPN menjadikan jalur data tidak diketahui pihak-pihak yang berusaha mengintip data yang ditransfer, jika dikombinasikan dengan IPsec maka akan mendapatkan keamanan tunnel ganda. Monitoring menggunakan wireshark tidak mampu membaca data dengan baik.

Daftar Pustaka

Karfianto (2010). Point-to-Point Tunneling Protocol (PPTP), Layer Two Forwarding (L2F), and Layer Two Tunneling Protocol (L2TP). http://karfianto.wordpress.com/2010/05/20/point-to-point-tunneling-protocol-pptp-layer-two-forwarding-l2f-and-layer-two-tunneling-protocol-l2tp/, 13 juli 2011

Networking Server (2011). *IPsec Protokol (AH dan ESP) Header.* *http://blog.code-security.com/2011/02/ipsec-protocol-ah-dan-esp-header.html*, 12 Juni 2011.

Shea, Richard (2000). *L2TP Implementation And Operation.* Adisson Wesley Longman, inc.

Snader, Jon C.. 2006. *VPNs Illustrated : Tunnels, VPN, and IPsec*. USA : Addison Wesley.

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

Wiki MikroTik (2009). *IPSec VPN with Dynamic Routing / Mikrotik and Cisco.* *http://wiki.mikrotik.com/wiki/IPSec_VPN_with_Dynamic_Routing_/_Mikrotik_and_Cisco*, 13 Juni 2011.

Wireshark (2009). *Introduction to Wireshark.* http://wiresharkdownloads.riverbed.com/video/wireshark/introduction-to-wireshark/. 7 Juli 2011

Wiwid (2011). *IPsec VPN site-to-site MikroTik.* *http://wi2d.wordpress.com/2011/04/13/ipsec-vpn-site-to-site-mikrotik/,* 12 Juni 2011.