SERVER VPN BERBASISKAN LINUX DENGAN *CLIENT WINDOWS XP SP2*

Sarman
Sekolah Menengah Teknologi Industri (SMTI)
Departemen Perindustrian Perdagangan dan Koperasi (Deprindagkop)
Jln. Kusumanegara Yogyakarta, Hp: 08121594511,
email: sarman_id2@yahoo.com, sarman@dprin.go.id

Abstrak

Dunia teknologi informasi telah berkembang pesat. Kebutuhan informasi yang dapat diakses darimana saja perlahan namun pasti berubah menjadi kebutuhan mutlak. Kemudahan untuk mengakses data yang bersifat penting dan rahasia pada sebuah jaringan komputer internal suatu instansi, any time, any where, penting dan diperlukan.Untuk itu diperlukan suatu 'tools" untuk menjembataninya. Server Virtual Private Network (VPN) yang berjalan dengan sistem operasi Linux Fedora Core 3, menggunakan protokol L2TP sebagai sistem koneksi. Protokol IPSec untuk pengamanan terhadap lalulintas data. Server ini dibuat dengan tujuan memberikan kemudahan kepada yang berhak (legal user) untuk men-dial local server, dan mengakses data pribadi, di samping tidak mengabaikan segi keamanan data. Hanya user yang telah terdaftar dan mendapatkan login user, password serta kunci keamanan rahasia, yang diperkenankan masuk jaringan lokal. User akan memperoleh IP jaringan lokal dari server secara otomatis. Client didesain menggunakan sistem operasi Microsoft Windows XP SP2. Program aplikasi ataupun data pribadi yang berada di jaringan lokal, dapat diakses langsung oleh client.

Kata kunci: *VPN, L2TP, IPSec*

1. PENDAHULUAN

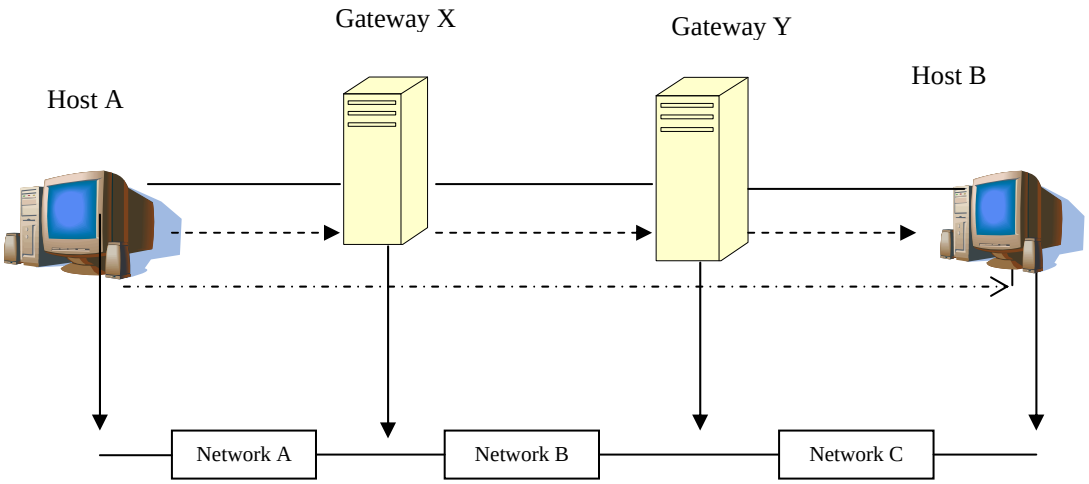
Intranet menjadi sebuah komponen penting dalam sistem informasi perusahaan/instansi saat ini. Sebuah *intranet* adalah sebuah jaringan internal pada perusahaan/instansi yang menggunakan teknologi *internet* untuk komunikasi dan pembagian informasi. Akses *internet* saat ini juga sudah menjadi kebutuhan rutin bagi hampir sebagian besar perusahaan/instansi. *Internet* yang memberikan suatu fenomena tersendiri bagi perusahaan/instansi.

Untuk mengatasi faktor mahalnya pembangunan sebuah jaringan pribadi baru secara fisik, maka dirintislah sebuah teknik baru, yang kemudian dikenal sebagai *VPN* (*Vitual Private Network*). *VPN* merupakan suatu solusi untuk mengembangkan jaringan komputer sehingga seluruh *server* dan *mobile-client* mampu mengakses aplikasi maupun informasi perusahaan setiap saat. *VPN* merupakan suatu metode untuk mengembangkan jaringan sistem informasi yang tidak tergantung dari topologi (lokasi fisik). Tujuan utama penggunaan VPN adalah menyatukan komputer komputer yang tersebar secara geografis agar dapat diatur sebagai satu jaringan lokal, misalnya antara *workstation* dan *server* perusahaan , maupun *remote LAN* dan *main server (server–server)*. Teknologi *VPN* mempunyai keuntungan mampu untuk menggunakan jaringan publik yaitu *internet.* Teknologi *VPN* mengimplementasikan batasan akses jaringan tanpa mengorbankan fitur-fitur dasar keamanan. Dengan metode *tunneling*, paket paket data dikirimkan dengan terselubung atau enkapsulasi, paket ini dikirimkan melalui jaringan *Internet* ke tujuannya.

2. DATAGRAM *ROUTING*

Sebuah *gateway internet* umumnya berupa sebuah *Router IP* sebab perangkat ini memakai *Internet Protokol* untuk melalukan paket data diantara jaringan komputer. Dulu dikenal dua jenis perangkat untuk jaringan komputer yaitu *gateway* dan *host*. *Gateway* meneruskan paket data di antara jaringan komputer dan *host* tidak melakukannya. Namun, jika sebuah *host*

tersambung ke lebih dari satu buah jaringan komputer (disebut *multihomed host*), itu dapat meneruskan paket data diantara jaringan komputer. Pada saat *host* seperti ini mulai meneruskan paket data, *host* itu berperan seperti sebuah *gateway* dan terlihat sebagai sebuah *gateway*. Terminologi komunikasi data saat ini kadang kadang membuat pembatasan antara *gateway* dan *router*, namun dalam uraian ini dipergunakan terminologi *gateway* dan pertukaran *router IP*.



Gambar 1. Contoh diagram routing

3. TEKNOLOGI *VPN*

Pada mulanya sistem jaringan kelas menengah dan luas yaitu MAN dan WAN dikembangkan dengan menggunakan sistem sambungan langsung. Sistem ini menawarkan kecepatan transfer data yang tinggi namun membutuhkan investasi yang mahal. Sistem ini tidak efektif untuk perusahaan kelas menengah ke bawah serta perusahaan yang tersebar di berbagai wilayah yang berjauhan.

Perkembangan *internet* yang sangat cepat menawarkan solusi untuk membangun sebuah *intranet* menggunakan jaringan publik (*internet*). Di lain pihak, kekuatan suatu industri juga berkembang dan menuntut terpenuhinya lima kebutuhan dalam *intranet* yaitu :

a) Kerahasiaan, dengan kemampuan mengacak atau enkripsi pesan sepanjang jaringan yang tidak aman.
b) Kendali akses, menentukan siapa yang diberikan akses ke suatu sistem atau jaringan, sebagaimana informasi apa dan seberapa banyak seseorang dapat menerima.
c) Autentikasi, yaitu menguji identitas dari dua ujung yang sedang melaksanakan transaksi
d) Integritas, menjamin bahwa file atau pesan tidak berubah dalam perjalanan
e) *Non-repudiation*, yaitu mencegah dua ujung saling menyangkal, bahwa mereka telah mengirim atau menerima sebuah file.

Kebutuhan ini sepenuhnya didukung oleh *internet* yang memang dirancang sebagai jaringan terbuka dimana pengguna mendapatkan kemudahana untuk transfer dan berbagi informasi

Solusi untuk tantangan ini adalah Jaringan Maya Pribadi , lebih dikenal sebagai *VPN* (*Virtual Private Network*). *VPN* memanfaatkan jaringan *internet* yang bekerja berdasar *TCP/IP* sebagai media *intranet* sehingga jangkauannya menjadi luas tanpa investasi yang besar. *VPN* menghadirkan teknologi yang mengamankan segala lalu lintas jaringan *virtual* sehingga memberikan rasa aman bagi semua pemakai jaringan.

Berikut adalah kriteria yang harus dipenuhi oleh *VPN* dalam menjawab tantangan industri tersebut:

a. Autentikasi pengguna
b. Manajemen pengalamatan
c. *Enkripsi* data.

d. Manajemen kunci
e. Dukungan untuk *multiprotocol*.

3.1. Penerapan *VPN*

Dalam penerapannya, *VPN* mempunyai banyak fungsi, tergantung dari konfigurasi dari *VPN* tersebut, yaitu :

a. *Remote acces* melalui *Internet*
   Seorang klien cukup berhubungan dengan ISP lokal lalu perangkat lunak *VPN* akan membuat sebuah jaringan khusus secara maya antara pengguna dial-up dengan *server* perusahaan melalui *internet*.
b. Menghubungkan jaringan melewati *internet*
   Seorang klien cukup berhubungan dengan ISP lokal lalu perangkat lunak *VPN* akan membuat sebuah jaringan khusus secara maya antara pengguna dial-up dengan *server* perusahaan melalui *internet*.

3.2. Komponen *VPN*

Sebuah *VPN*, sebenarnya sama seperti jaringan komputer lainnya, yaitu terdiri dari *server* dan klien , hanya saja jalur untuk menghubungkan *server* dan klien ini adalah sebuah jaringan publik *internet*, sehingga perlu dilakukan *tunneling*.

a. *Server* VPN
   Dalam hal ini *server* yang dimaksud adalah sebuah *gateway VPN*. Gerbang/ *gateway* dalam membangun sebuah *VPN* sangat diperlukan karena memiliki fungsi:
   1) Penghubung antara pengakses *mobile* (*road-warior*) atau jaringan lain yang tersambung pada pc *router* dengan jaringan *intranet* lainnya.
   2) Melakukan autentikasi terhadap user yang akan melakukan hubungan ke jaringan *intranet*
   3) Melakukan *tunneling*, enkapsulasi paket pada data yang dikirimkan.
   4) Menerima hubungan secara *tunneling* dan dekapsulasi data yang diterima
   5) Mengalokasikan ip local untuk setiap pengakses roadwarior.
   6) Meneruskan paket data yang dikirim dari sisi klien yang satu ke klien yang lain yang berbeda jaringan.
b. *Klien* VPN
   Klien *VPN* adalah pengguna/pengakses data yang berkomunikasi dengan komputer atau peripheral pada jaringan lain menggunakan jalur yang dibangun dari hubungan *VPN*. Klien *VPN* dapat saling bertukar data dengan klien lain yang berada dalam jaringan *intranet* sesuai kebijakan dari *gateway*. Dalam praktiknya, klien.

3.3. Protokol protokol *VPN*

Protokol adalah bahasa atau standarisasi yang digunakan oleh dua buah media komputer atau lebih untuk agar dapat saling berkomunikasi.Beberapa protokol yang digunakan untuk pengembangan *VPN* adalah sebagai berikut:

a. PPTP (*Point to Point Tunelling Protocol*)
b. L2TP (*Layer Two Tunneling Protocol*)
c. IPSec (*Internet Protocol Security*)
d. PPTP over L2TP
e. IP-in-IP

Dua buah protokol yang paling sering digunakan adalah *PPTP* dan *IPSec*. Pemilihan protokol lebih banyak ditentukan oleh kondisi yang dihadapi pada saat seting *VPN* daripada oleh kebutuhan. Misalnya, jika pada saat setting *VPN server Windows NT* maka protokol yang digunakan adalah *PPTP* karena protokol ini adalah default dari *Windows NT*. Sedangkan setting *VPN* menggunakan *router* dengan tujuan pengguna akhir, maka *VPN* yang digunakan adalah *IPSec* karena protokol ini yang biasanya terinstall secara default pada *router* tersebut.

3.4. *Tunneling*

Tunneling merupakan metode untuk transfer data dari satu jaringan ke jaringan yang lain dengan memanfaatkan jaringan *internet* terselubung. Disebut *tunnel* atau saluran terselubung karena aplikasi yang memanfaatkannya hanya dua ujung akhir, sehingga paket

yang lewat pada *tunnel* hanya akan melakukan satu kali lompatan atau *hop*. Data yang akan ditransfer dapat berupa frame atau paket dari protokol yang lain.

Protokol *tunneling* tidak mengirimkan frame sebagaimana yang dihasilkan oleh node awal begitu saja, melainkan membungkusnya (mengenkapsulasi) dalam header tambahan. *Header* tambahan tersebut berisi informasi routing sehingga data atau frame yang dikirimkan dapat melewati jaringan *internet*. Jalur yang dilewati dalam *internet* disebut *tunnel*. Saat data tiba pada jaringan tujuan, proses yang terjadi selanjutnya adalah dekapsulasi, kemudian data original akan dikirim ke penerima terakhir. *Tunneling* mencakup keseluruhan proses mulai dari enkapsulasi, transmisi dan dekapsulasi.

3.5. Aplikasi *IPSec*

Karena *IPSec* beroperasi pada *layer network*, maka cukup flexible dan dapat digunakan untuk mengamankan trafik *network*. Ada dua aplikasi yang terpisah secara fisik :

a. *Virtual* Private *Network* (*VPN)*, yang mengijinkan banyak *host*/situs untuk berkomunikasi secara aman diatas *Internet* yang 'terbuka' dan kurang aman dengan mengenkripsi data antara *host*/situs.
b. "*Road Warriors*" yaitu *menghubungkan* kantor dari rumah, atau dengan *host* yang *mobile/traveller.*

Cara kerja *IPSec* dapat dibagi dalam lima tahap, yaitu:

a. Memutuskan menggunakan *IPSec* antara dua titik akhir di *internet*
b. Mengkonfigurasi dua buah *gateway* antara titik akhir untuk mendukung *IPSec*
c. Inisialisasi *tunnel IPSec* antara dua *gateway*
d. Negosiasi dari parameter *IPSec*/IKE antara dua *gateway*
e. Mulai melewatkan data

3.6. OPENSWAN

Openswan merupakan pengembangan dari *FreeS/WAN* yang merupakan implementasi protokol *IPSec* (*IP security*) dalam *Linux*. *IPSec* menyediakan layanan enkripsi dan authentifikasi pada *layer IP* (*Internet Protocol*) dari *stack* protokol *network*.

Bekerja pada *layer* ini, *IPSec* dapat melindungi seluruh trafik apapun yang terbawa melalui *IP*, tidak seperti proteksi enkripsi lainnya yang hanya melindungi data-data tertentu pada *layer* yang lebih tinggi (*PGP* untuk *mail*, *SSH* untuk *remote login*, *SSL* untuk *webwork*). Kedua pendekatan ini telah dipertimbangkan keuntungan dan batas-batasan kemampuannya.

IPSec hanya dapat digunakan pada mesin (apapun) yang melakukan *IP network*ing. *Gateway IPSec* yang permanen dapat di pasang dimanapun dibutuhkan perlindungan trafik. *IPSec* juga dapat jalan di *router* maupun mesin *firewall*, beragam aplikasi *server* maupun di titik akhir user : *desktop* atau *laptop*.

Implementasi Openswan pada *Linux* terbagi atas tiga bagian pula :

a. *KLIPS* (*kernel IPSec*) mengimplementasikan AH, ESP, dan *packet handling* didalam kernel
b. *Pluto* (*daemon IKE*) mengimplementasikan IKE, menegosiasikan koneksi dengan sistem-sistem lain.

3.7. L2TP *(Layer 2 Tunneling Protocol*)

L2TP (*Layer* 2 *Tunneling* Protocol) adalah standar IETF yang berbasis pada Microsoft Point to Point Protokol (*PPTP*) dan Cisco *Layer*2 Forward Protocol (L2F) yang menyediakan layanan akses *dialup remote* ke sebuah jaringan korporat dengan banyak protokol dan terenkripsi, melalui *internet*. *PPTP* dan *L2TP* terletak pada lapisan ke2 dari susunan lapisan *TCP* / *IP*.

PPTP sangat rentan terhadap serangan gangguan dari luar, terutama berkaitan dengan integritas data dan pengalamatan asal data, masalah yang terbesar adalah *PPTP* hanya mengunakan autentikasi berbasis password. Jadi bila password ini jatuh ke tangan yang salah, maka bisa disalahgunakan untuk mengakses data dalam jaringan pribadi perusahaan. Karena hal hal diatas maka dikembangkan mekanisme keamanan yang ditambahkan pada *VPN* berbasis *L2TP*. Dua jenis autentikasi yang didukung oleh *L2TP* yaitu *Certificate Authority* dan *Preshared Key*. Sertifikat autentikasi yang didukung oleh *L2TP* termasuk *PAP, CHAP, MS-CHAP versi 1* dan *MS-CHAP versi 2*. *L2TP* juga mendukung algoritma enkripsi *3DES, dan RSA*.

3.8. Road Warrior

Roadwarior adalah istilah bagi klien yang melakukan akses *remote VPN*, klien biasanya berupa *pc* atau *laptop* yang berada secara fisik berada diluar lingkungan perusahaan namun melakukan hubungan *VPN* sehingga klien ini mendapat alamat ip privat dalam jaringan, sehingga seolah olah klien ini adalah bagian dari jaringan privat dibelakang *gateway*. Adakalanya karena bersifat mobile, maka ip yang digunakan oleh roadwarior akan berganti ganti, misal karena dia berganti *ISP*,atau karena berada di lokasi yang berbeda.

3.9. Men-*dial* dari Roadwarrior

Microsoft memberikan kemudahan pada pengguna sistem operasinya untuk menampilkan memilih beberapa item *checklist* untuk otomatisasi dalam mengkonfigurasi komponen dari sistem operasi *Windows* yang dikenal dengan *Wizard.*

a. Koneksi yang berhasil akan menghasilkan komentar "*verifing user name and password*" kemudian jendela koneksi akan mengecil ke *system tray* seperti pada saat mendial modem.

Gambar 2. Menghubungkan dengan *IP Gateway*

b. Sesaat kemudian koneksi *VPN* akan mengecek autentikasi user.

Gambar 3. Proses autentikasi

c. Jika autentikasi berhasil maka *host* akan didaftarkan pada jaringan internal, dan akan memperoleh IP.

Gambar 4. Mendaftarkan diri ke jaringan internal

Dari keterangan di atas, koneksi *VPN* telah berhasil dibuat dari alamat IP komputer 192.168.4.231 ke alamat 192.168.4.230 yang merupakan gateway dari jaringan 192.168.193.0/24 dan mendapatkan alokasi IP lokal 192.168.193.201 pada jaringan internal. Hasil dapat dibuktikan dengan cara mengakses komputer yang berada di jaringan internal.

4. Membuka Aplikasi

4.1. Membuka Web

Hasil dari koneksi akan dipraktekan dengan membuka situs internal *VPN* dengan membuka *Internet Explorer* dan mengisikan alamat situs 192.168.193.2 pada *address bar.*

Gambar 5. Tampilan web dari host 192.168.193.2

4.2. Uji koneksi menggunakan perintah *ICMP*

ICMP kepanjangan dari *Incoming Control Message Protokol*, digunakan untuk mengtest koneksi keberhasilan koneksi dari *peer* ke *peer* yang lain. Cara untuk menguji koneksi antara dilakukan dengan perintah ping, dengan langkah langkah *Start -> Run->* ketik "*command*" diikuti perintah sebagai berikut:

1. Dari sisi klien *roadwarrior* dengan ip 192.168.193.201 melakukan ping ke *Gateway* VPN 192.168.193.1

```
C:> ping 192.168.193.1 -t
PING 192.168.193.1 (192.168.193.1) from 192.168.193.201 : 56(84) bytes of data.
64 bytes from 192.168.193.1: icmp_seq=1 ttl=64 time<1 ms
64 bytes from 192.168.193.1: icmp_seq=2 ttl=64 time=1 ms
64 bytes from 192.168.193.1: icmp_seq=3 ttl=64 time=1 ms
64 bytes from 192.168.193.1: icmp_seq=4 ttl=64 time=1 ms
64 bytes from 192.168.193.1: icmp_seq=5 ttl=64 time=1 ms
64 bytes from 192.168.193.1: icmp_seq=6 ttl=64 time=1 ms
64 bytes from 192.168.193.1: icmp_seq=7 ttl=64 time=1 ms

--- 192.168.193.1 ping statistics ---
9 packets transmitted, 9 received, 0% loss, time 8084ms
rtt min/avg/max/mdev = 1/1/1/1 ms
```

   Uji koneksi diatas menunjukkan bahwa server terhubung dengan server 192.168.193.1 dengan waktu ping 1 ms.

2. Dari sisi *roadwarrior* dengan ip 192.168.193.201 ke *server web* dengan ip 192.168.193.2

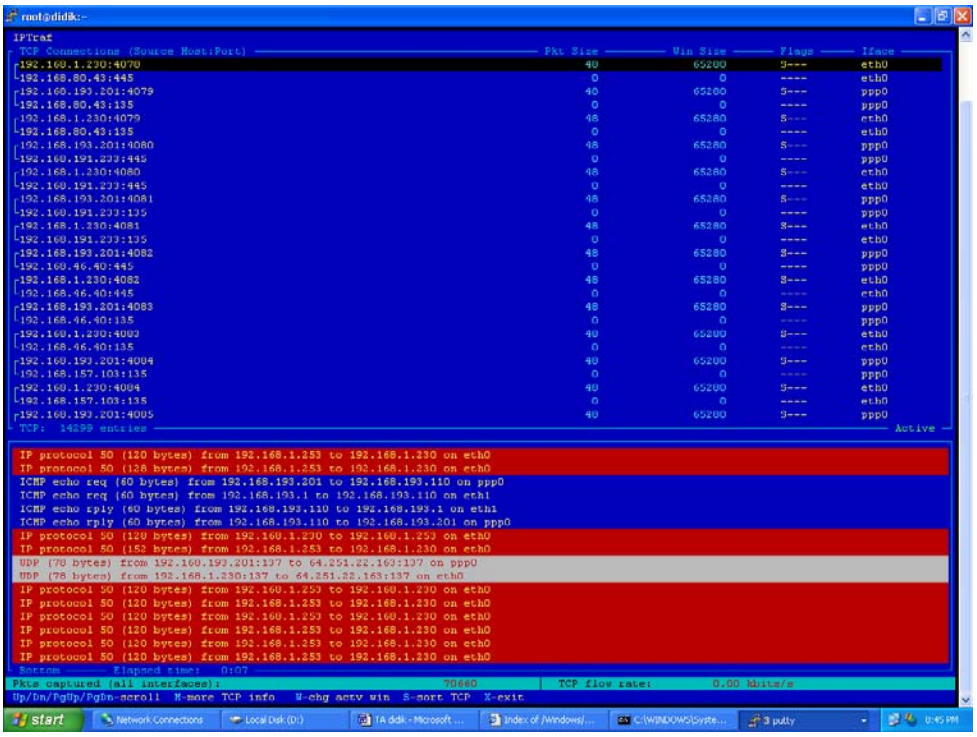
```
C:> ping 192.168.193.2 -t
PING 192.168.193.2 (192.168.193.2) from 192.168.193.201 : 56(84) bytes of data.
64 bytes from 192.168.193.2: icmp_seq=1 ttl=64 time=1 ms
64 bytes from 192.168.193.2: icmp_seq=2 ttl=64 time=1 ms
64 bytes from 192.168.193.2: icmp_seq=3 ttl=64 time=1 ms
64 bytes from 192.168.193.2: icmp_seq=4 ttl=64 time=1 ms
64 bytes from 192.168.193.2: icmp_seq=5 ttl=64 time=1 ms
64 bytes from 192.168.193.2: icmp_seq=6 ttl=64 time=1 ms
64 bytes from 192.168.193.2: icmp_seq=7 ttl=64 time=1 ms

--- 192.168.193.2 ping statistics ---
9 packets transmitted, 9 received, 0% loss, time 8084ms
rtt min/avg/max/mdev = 1/1/1/1 ms
```

Dari hasil tes koneksi dengan server 192.168.193.2 dibuktikan bahwa koneksi dari klien roadwarrior sudah terhubung dengan jaringan lokal, dalam hal ini sebagai contoh adalah koneksi ke 192.168.193.2 waktu 1ms.

4.3. Hasil pengamatan melalui software iptraf

Iptraf adalah software bawaan linux yang dapat digunakan sebagai monitoring lalulintas trafik pada sebuah server. Software ini digunakan oleh penulis untuk menganalisa trafik yang dikirimkan oleh ip lokal. Namun pada hasil yang diperoleh, data ip yang dikenali sudah berupa ip lokal saja, tidak mengenali mode *tunnel* nya, karena mode enkapsulasi dan dekapsulasi dari paket sudah terenkripsi dan tidak dapat dilihat secara software, kecuali tahapan tahapan dari sebuah koneksi seperti di atas dengan menggunakan perintah # tail –f /var/log/secure atau #tail –f var/log/messages.

Dari trafik melalui iptraf hanya mengindikasikan input yang berasal dari port 50 UDP yang berasal dari koneksi VPN. Namun pada layar tidak nampak dari protokol UDP karena hasil dekapsulasi dari protokol diatasnya yaitu L2TP dan IPSec sehingga hanya ditampilkan sebagai protokol IP saja.



Gambar 6. hasil pengamatan menggunakan iptraf.

4.4. Keuntungan program

Keuntungan dari Server *Gateway* VPN yang dibuat dengan model IPSec dan L2TP ini adalah:

1. Mempunyai nilai ekonomis tinggi
   Sebuah klien dan sever cukup menyediakan layanan internet dari provider Internet lokal, tanpa harus membangun jaringan tetap.
2. Karena menggunakan proteksi IPsec dan L2TP maka data dilindungi oleh dua buah lapisan IP, yaitu:
   a. L2TP yang membuat tunnel secara terselubung dengan enkripsi MD5 dan 3DES
   b. IPsec yang mengenkripsi setiap paket dalam proteksi ESP
3. Karena menggunakan protokol IPsec dan L2TP maka semua protokol IP yang berada diatas layer transport dapat dijalankan. Berikut contoh protokol yang dapat di jalankan.
   a. Protokol http untuk akses web.

b. Protokol ftp untuk bertukar file.
c. Protokol snmp untuk berkirim *e-mail.*
d. Protokol mms untuk pengiriman video dengan format Wndows Media.
e. Protokol rstp untuk pengiriman *audio/video* dengan format Real.

5. KESIMPULAN

Dari perancangan dan implementasi yang telah dilakukan dapat diambil beberapa kesimpulan yang dapat dikemukakan sebagai hasil penelitian, antara lain :

1. Pada *Gateway VPN* yang dibuat, *daemon L2TP* memberikan akses *tunneling* dari jaringan lain dengan *interface Point-to-Point-Protocol,* sedangkan untuk keamanan paket digunakan teknologi *IPSec*.
2. *VPN* dengan teknik *Remote Access VPN* memberikan kemudahan pengakses bergerak *(roadwarior)* untuk mengakses jaringan intranet perusahaan.
3. Unjuk kerja dari *ISP* tempat gateway *server VPN* akan sangat menentukan kecepatan akses bagi *Roadwarior.*

DAFTAR PUSTAKA

[1] Purbo, O.W., "**TCP/IP Standar, Desain, dan Implementasi***",* PT. Elex Media Komputindo Jakarta, 2002.
[2] Syahputra, A., "**Jaringan Berbasis Linux*",*** Andi Offset, Yogyakarta, 2002.
[3] Wendy, A, dan Ramadhana, A.S., "**Membangun VPN Linux Secara Cepat**", ANDI OFFSET, Yogyakarta, 2000.
[4] Wijaya, H. , ***"*Microsoft Windows 2000 Server**", PT. Elek Media Komputindo, Jakarta, 2002.
[5] ....., "**Securing L2TP using Ipsec**", *http://www.networksorcery.com/enp/rfc/rfc3193.txt*