

JURNAL

TELEMATIK

VOLUME 6 NOMOR 2 APRIL 2014

Kata Pengantar*Assalamu 'alaikum Warahmatullahi Wabarakatuh*

Puji dan syukur atas kehadiran Allah SWT, karena atas Rahmat dan HidayahNya, Jurnal Ilmiah Volume 6 Nomor 3 Bulan Juli Tahun 2014 ini dapat diterbitkan. Jurnal Ilmiah ini bernama Telematik yang berarti *Teknik ELEktro*, teknik infor*MAT*ika, *s*istem informasi dan *K*omputer akuntansi yang diterbitkan oleh Fakultas Teknik Universitas Muhammadiyah Bengkulu.

Dengan diterbitkannya Jurnal Ilmiah Telematik ini diharapkan dapat bermanfaat dalam perkembangan Ilmu Pengetahuan dan Teknologi. Berkenaan dengan harapan tersebut kepada para peneliti produktif dan staf pengajar yang memiliki hasil-hasil penelitian untuk dapat kiranya mengirimkan naskah ringkasannya untuk dimuat pada Jurnal Ilmiah Telematik ini dengan mengikuti ketentuan sebagaimana yang telah ditetapkan oleh pihak dewan redaksi.

Akhirnya tak lupa kami mengucapkan banyak terima kasih kepada semua pihak yang telah membantu penerbitan Jurnal Ilmiah Telematik ini.

Wasalamu 'alaikum Warahmatullahi Wabarakatuh

Bengkulu, Juli 2014

Dewan Redaksi

JURNAL

TELEMATIK

VOLUME 6 NOMOR 3 JULI 2014

Visi

Sebagai media yang dapat memberikan
Sumbangan terhadap perkembangan Ilmu Pengetahuan dan Teknologi

Misi

Dapat menyumbangkan dan menyebarkan berupa Hasil penelitian (*research*) Maupun hasil kajian,
Pendapat dan pemikiran dalam bidang Ilmu Pengetahuan dan Teknologi

Pelindung / Penasehat

Dr. H. Khairil, M.Pd
(Rektor Universitas Muhammadiyah Bengkulu)

Penanggung Jawab

Ir. Yukiman Armadi, M.Si
(Dekan Fakultas Teknik)

Penyunting Ahli

Dr. Bahrin, M.Si
Ir. Z. Hartawan, MM, DM

Pimpinan Redaksi

Sastia H. Wibowo, S.Kom, M.Kom

Sekretaris Redaksi

Yulia Darmi, S.Kom, M.Kom

Staf Redaksi

Diana, S.Kom

Distribusi dan Pemasaran

Dedy Abdullah, ST

Penerbit

Fakultas Teknik
Universitas Muhammadiyah Bengkulu

Alamat Redaksi

Fakultas Teknik
Universitas Muhammadiyah Bengkulu
Jl. Bali Po. Box 118 Bengkulu
Telp. 0736-22765, Fax. 0736-26161
Email : jurnalilmiahtelematik@gmail.com

Frekuensi Terbit

4(Empat) kali setahun

DAFTAR ISI

1. ANALISIS KONEKTIFITAS AKSES POINT DENGAN JARINGAN KABEL DAN WI-FI ACCESS POINT PADA JENIS GADGET 1381 – 1390
Dedy Abdullah, Yocki Arkino Trianugerah
2. SISTEM KEAMANAN DATA PADA SAMBA SERVER BERBASIS VPN (*VIRTUAL PRIVATE NETWORK*) MENGGUNAKAN PROTOKOL SSL (*SECURE SOCKET LAYER*) DAN *IP TUNNELING* 1391 – 1399
Mustaziri, Maha Dwi Putra
3. ANALISIS DAN PERANCANGAN SISTEM INFORMASI PERPUSTAKAAN POLITEKNIK SEKAYU 1400 – 1408
Ricky Maulana Fajri
4. PERENCANAAN BUNCH SCRAPPER CONVEYOR DENGAN KAPASITAS 5 TON/JAM UNTUK MENGANGKUT JANJANGAN KOSONG DARI MESIN PERONTOK KE PENAMPUNGAN 1409 – 1429
Antonius.FA.Silaen

PENDAHULUAN

Perkembangan teknologi jenis gadget semakin hari semakin mengalami kemajuan yang sangat pesat, bahkan gadget pada zaman sekarang ini sudah menjadi bagian hidup bagi sebagian orang di mukabumi. Hal ini menyebabkan

*Analisis Konektivitas Akses Point Dengan Jaringan Kabel Dan Wi-Fi
Access Point Pada Jenis Gadget
Dedy Abdullah, Yocki Arkino Trianugerah*

SISTEM KEAMANAN DATA PADA SAMBA SERVER BERBASIS VPN (VIRTUAL PRIVATE NETWORK) MENGGUNAKAN PROTOKOL SSL (SECURE SOCKET LAYER) DAN IP TUNNELING

Oleh : Mustaziri, Maha Dwi Putra

ABSTRAK

Sistem keamanan data pada samba server berbasis VPN (Virtual Private Network) menggunakan Protokol SSL (Secure Socket Layer) dan IP Tunneling. Pada penelitian perancangan sistem keamanan data ini menggunakan software opensource OpenVPN dan Open SSL untuk membuat IP Tunnel, juga dibutuhkan sertifikat server dan sertifikat client yang dikeluarkan oleh server, dimana sertifikat client dibutuhkan oleh komputer client untuk mengakses samba server menggunakan aplikasi OpenVPN GUI.

Kata kunci: IP Tunneling, Virtual Private Network, OpenVPN

PENDAHULUAN

Samba bagian dari program *open source* pada sistem operasi *linux* yang berfungsi untuk *sharing file* dan *printer* di jaringan yang terletak pada *server*. Perusahaan yang memiliki kantor pusat dan kantor cabang, dengan menggunakan *samba server* kantor cabang dapat mengakses *file-file* yang ada di kantor pusat dan sebaliknya melalui jaringan komputer. Jaringan dapat menghubungkan kedua kantor tersebut menggunakan teknologi VPN. VPN yaitu jaringan *private*. Teknologi VPN adalah sebuah *software* yang dijalankan oleh kedua pihak yang hendak berkomunikasi melalui *internet*. Dibandingkan dengan teknologi jaringan WAN, teknologi VPN lebih efektif karena infrastruktur yang dibutuhkan oleh VPN murah serta mudahnya dalam instalasi, maka koneksi ini lebih efisien dibandingkan dengan metode WAN.

Bagi pengguna *internet* yang memerlukan *privasi* dalam berkomunikasi untuk menjaga kerahasiaan datanya, misalnya Perusahaan mengirimkan dokumen penting kepada kantor cabang melalui *internet* memerlukan jalur yang aman dari gangguan apapun. Untuk mengatasi permasalahan di atas dapat menggunakan *IP Tunneling*. Dalam penerapannya di VPN, *tunnel* dilengkapi dengan sebuah sistem enkripsi untuk menjaga data yang melewati *tunnel* tersebut. Sistem enkripsi pada *tunnel* dibuat dengan menggunakan protokol SSL (*Secure Socket Layer*). Paket data yang menggunakan SSL (*Secure Sockets Layer*) akan dienkripsi sehingga walaupun nantinya tertangkap oleh *Network Sniffer*, maka orang lain akan sulit untuk membaca informasi.

KAJIAN TEORI

Internet adalah singkatan dari *Interconnected Network*. *Internet* merupakan sebuah sistem komunikasi yang mampu menghubungkan jaringan – jaringan komputer di seluruh dunia (Ramadhan : 2007:1).

Berbagai jenis komputer dan spesifikasi yang berbeda – beda dapat saling berkomunikasi melalui *internet*. Beberapa bentuk jaringan yang berbeda – beda dapat saling bertukar informasi dan data melalui *internet* menggunakan seperangkat aturan yang disebut protokol TCP/IP. Untuk membedakan setiap komputer atau jaringan yang terhubung ke *internet* maka digunakan sebuah identitas tertentu yang disebut alamat *IP* (*IP Address*). *IP Address* dibagi menjadi dua macam berdasarkan pemakaiannya di *internet*, yaitu : *Private IP Address* dan *Public IP Address*.

Samba

Samba adalah aplikasi yang bertujuan agar komputer dapat berkomunikasi dengan sistem operasi *Linux*, dapat berbagi *file* dan *print server* yang berbasis protokol SMB (*Session Message Block*). Samba memungkinkan *Linux* bisa mengakses *resources* yang ada pada jaringan *windows*. Bisa dikatakan, Samba adalah jembatan penghubung antara *Windows* dan *Linux*. Samba terdiri atas dua program yang berjalan di *background*: *SMBD* merupakan *file server* yang akan menghasilkan proses baru untuk setiap *client* yang aktif dan *NMBD* yang bertugas mengonversi nama komputer (*NetBIOS*) menjadi alamat *IP* dan juga memantau *share* yang ada di jaringan. Kerja *SMBD* diatur dengan *file* konfigurasi */etc/samba/smb.conf*. Dengan *file* konfigurasi yang tepat, Samba dapat dijadikan *file server*, *print server*, *domain controller*, dan banyak fungsi lainnya. Dengan Samba *linux* bisa berbagi *resource* di antara mesin yang memakai sistem operasi *Windows/DOS* ataupun *OS/2* untuk berbagi *resource file* dan *printer*, melakukan pencarian berkas yang ada pada sebuah *network neighborhood*, memberikan autentikasi kepada klien yang ingin *login* ke dalam sebuah *domain* (Wahyono : 2007:161).

VPN (*Virtual Private Network*)

VPN merupakan mekanisme menyambungkan titik (*node*) di jaringan komputer dengan titik yang lain. VPN dapat digunakan untuk mengakses LAN yang berada dan berjauhan dengan menggunakan *internet* juga untuk melakukan transmisi data paket secara pribadi dengan enkripsi, tetapi *traffic* antar *remote-site* tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan

traffic yang tidak semestinya ke dalam *remote-site* VPN berupa koneksi *virtual* yang bersifat *private*. VPN menghubungkan komputer dengan jaringan *public* atau *internet* namun sifatnya *private*, karena bersifat *private* maka tidak semua orang bisa terkoneksi ke jaringan. Untuk keamanan data dalam VPN, menggunakan VPN *tunnel* yang menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Disebut *tunnel* karena koneksi *point-to-point* tersebut sebenarnya terbentuk dengan melintasi jaringan umum, namun koneksi tersebut tidak mempedulikan paket-paket data milik orang lain yang sama-sama melintasi jaringan tersebut, (Feilner : 2006:5).

OpenVPN

OpenVPN merupakan aplikasi yang mengimplementasikan teknik *Virtual Private Network* (VPN) untuk membuat koneksi *point-to-point* atau *site-to-site* dan fasilitas *remote access* secara aman. Untuk melakukan *autentifikasi* pada saat membangun suatu koneksi, *OpenVPN* menggunakan *pre-shared key*, *certificate*, dan *username / password*, yang mana untuk proses enkripsinya menggunakan *OpenSSL*. *OpenVPN* menggunakan SSL untuk menangani *tunneling*. *OpenVPN* mendukung berbagai macam produk-produk *open source* terutama untuk aplikasi yang menangani proses enkripsi, SSL/TLS dan otentikasi. Secara *default*, *OpenVPN* menggunakan *library* *OpenSSL* untuk membangun *tunnel*.

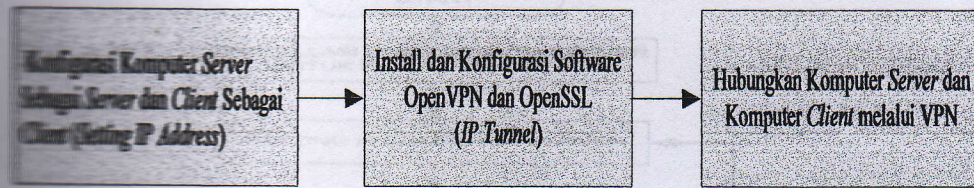
Protokol SSL/TLS

SSL, TLS dan *OpenSSL Secure Socket Layer* (SSL) dan *Transport Layer Security* (TLS) merupakan protokol kembar yang digunakan untuk menangani keamanan paket data yang ditransmisikan melalui jaringan. Ketika SSL digunakan, maka *server* atau penyedia jasa akan memberikan sertifikat publik dan klien untuk melakukan otentikasi keabsahan identitas dari *server*. Ketika sudah terotentikasi, maka koneksi antara *server* dengan klient akan dienkrpsi (Cartealy :2013:19).

METODOLOGI

Perancangan Sistem Pada Komputer Server

Perancangan sistem membahas mengenai proses membangun sistem keamanan data serta VPN pada komputer *server*.

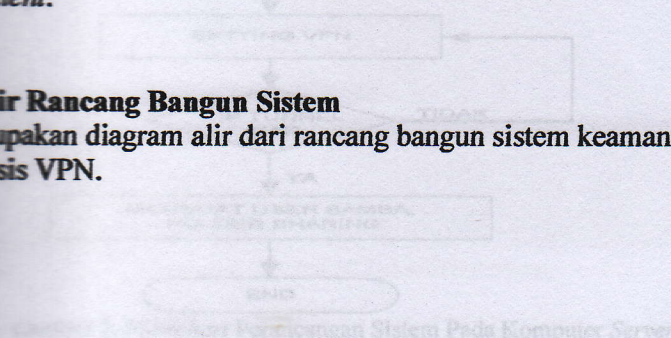


Gambar 1. Blok Diagram Perancangan Sistem

Cara kerja dari blok diagram pada Gambar 1 yaitu, dilakukan konfigurasi komputer server sebagai server yang bersistem operasi linux Ubuntu server, setting IP Address. Setelah terhubung ke internet, lakukan instalasi software Samba, OpenVPN dan OpenSSL sebagai sistem keamanan dan IP Tunnel. Untuk membuat IP Tunnel dibutuhkan sertifikat server dan sertifikat untuk client. Pada komputer client, untuk mengakses komputer server dibutuhkan software OpenVPN client.

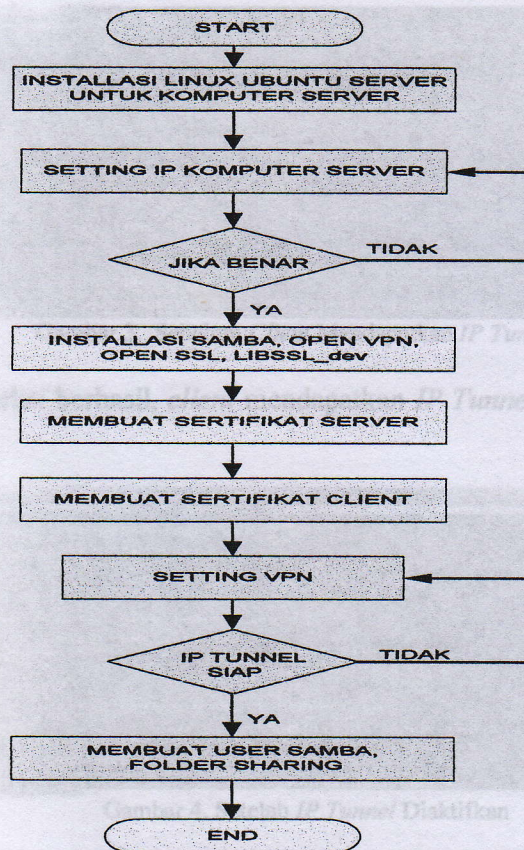
Diagram Alir Rancang Bangun Sistem

Berikut merupakan diagram alir dari rancang bangun sistem keamanan data samba server berbasis VPN.



BASIL DAN PEMBAHASAN

Langkah-langkah IP Tunnel dan Akses Samba Server
 Langkah pertama instalasi dan konfigurasi OpenVPN pada server dan client yang akan digunakan untuk membentuk Virtual Private Network (VPN) yang digunakan untuk melindungi komunikasi data yang bersifat pribadi dan point to point. Lalu langkah kedua yaitu dengan mengetikkan perintah ipconfig pada command prompt komputer client untuk konfigurasi IP address yang akan digunakan untuk akses ke server. Berikut ini



Gambar 2. Flowchart Perancangan Sistem Pada Komputer Server

HASIL DAN PEMBAHASAN

Pengujian Koneksi IP Tunnel dan Akses Samba Server

Setelah proses instalasi dan konfigurasi OpenVPN pada *server* dan *client* telah dilakukan, maka dihasilkan *Virtual Private Network* (VPN) yang digunakan untuk melakukan komunikasi data yang bersifat pribadi dan *point to point*. Lalu Cek IP Tunnel *client*, dengan cara ketikkan perintah `ipconfig` pada *command prompt*. Seperti Gambar 2 berikut ini


```

C:\Windows\system32\cmd.exe
Ethernet adapter Network Bridge:
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::a4e6:20a8:323e:a8a2x32
    IPv4 Address. . . . . : 192.168.137.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Local Area Connection 3:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wireless Network Connection 3:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wireless Network Connection 2:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{13C15FC1-0969-4492-B047-80F26014626E}:

```

Gambar 3. Sebelum Client Mendapatkan IP Tunnel

3. Setelah koneksi berhasil, *client* mendapatkan IP Tunnel, seperti pada Gambar

```

C:\Windows\system32\cmd.exe
Ethernet Bridge:
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::a4e6:20a8:323e:a8a2x32
    IPv4 Address. . . . . : 192.168.137.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Local Area Connection 3:
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::fe82:8604:2f98:aadbx30
    IPv4 Address. . . . . : 10.10.0.0
    Subnet Mask . . . . . : 255.255.255.252
    Default Gateway . . . . . : 

Wireless LAN adapter Wireless Network Connection 3:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wireless Network Connection 2:
    Media State . . . . . : Media disconnected

```

Gambar 4. Setelah IP Tunnel Diaktifkan

Client mendapatkan IP Tunnel yaitu, 10.10.0.6. Lakukan ping ke IP Tunnel server dengan mengetikan perintah pada *command prompt* seperti berikut: Ping 10.8.0.1. Lakukan ping ke IP Tunnel client dari server dengan mengetikan perintah sebagai berikut: Ping 10.10.0.6. Apabila OpenVPN Client telah terkoneksi dengan samba server dan tes ping berhasil, maka langkah selanjutnya yaitu mengakses samba server dari client menggunakan IP Tunnel. Masuk ke Windows explorer masukan IP Tunnel server pada network. Setelah berhasil masuk ke samba, terdapat folder data yang telah dibuat, seperti pada gambar 3.21 dan 3.22. Client yang telah terhubung dengan server bisa memasukan file ke dalam folder tersebut. Untuk masuk ke dalam folder data, masukan username dan password yang telah dibuat. Client bisa memasukan file apa saja yang akan di sharing. Gunakan perintah pada server: chown -R namauser namadirectory. Perintah tersebut digunakan untuk mendapatkan hak akses user untuk folder data yang akan di sharing.

Pengujian Sistem Keamanan Data Menggunakan Wireshark

Setelah dilakukan konfigurasi pada OpenVPN untuk mengamankan proses *transfer data samba server*, maka akan dilakukan pengujian terhadap keamanan sistem dalam proses *transfer data samba server* menggunakan *tools* yaitu wireshark. Berikut hasil *capture* dengan kondisi *client* mengakses *samba server* menggunakan *IP Tunnel* dan juga saat *client* tidak menggunakan *IP Tunnel*. Dimana pada hasil *capture* proses *transfer data*, packet data yang dikirim dapat terlihat dengan mudah dengan aplikasi wireshark jika tanpa menggunakan *Virtual Private Network (VPN) / IP Tunnel*, seperti pada Gambar 4.

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. The filter is set to 'ip.addr == 192.168.137.3'. The packets include various SMB (Server Message Block) and TCP (Transmission Control Protocol) traffic. Below the packet list, the packet details pane shows the structure of a selected packet (No. 26), including Ethernet II, Internet Protocol, Transmission Control Protocol, and Message Session Service (SMB) fields.

No.	Time	Source	Destination	Protocol	Info
5	6.197483	192.168.137.1	192.168.137.3	SMB	Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path:
7	6.199458	192.168.137.1	192.168.137.3	SMB	Trans2 Request, QUERY_PATH_INFO, Query File Standard Info, Path:
9	6.397384	192.168.137.1	192.168.137.3	TCP	pcolp > microsoft-ds [ACK] Seq=161 Ack=193 Win=16425 Len=0
10	6.419621	192.168.137.1	192.168.137.3	SMB	Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path:
12	6.420708	192.168.137.1	192.168.137.3	SMB	Trans2 Request, QUERY_PATH_INFO, Query File Standard Info, Path:
14	6.422768	192.168.137.1	192.168.137.3	SMB	NT Create AndX Request, FID: 0x31cf, Path:
16	6.424489	192.168.137.1	192.168.137.3	SMB	Trans2 Request, QUERY_FILE_INFO, FID: 0x31cf, Query File Internal Info
18	6.425745	192.168.137.1	192.168.137.3	SMB	NT Trans Request, NT NOTIFY, FID: 0x31cf
19	6.436144	192.168.137.1	192.168.137.3	SMB	NT Create AndX Request, Path: \desktop.ini
22	6.437488	192.168.137.1	192.168.137.3	SMB	NT Create AndX Request, FID: 0x31d2, Path:
24	6.438214	192.168.137.1	192.168.137.3	SMB	Trans2 Request, QUERY_FILE_INFO, FID: 0x31d2, Query File Standard Info
26	6.438774	192.168.137.1	192.168.137.3	SMB	Trans2 Request, FIND_FILES2, Pattern: *
28	6.439787	192.168.137.1	192.168.137.3	SMB	Close Request, FID: 0x31d2
30	6.451828	192.168.137.1	192.168.137.3	SMB	Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path:
32	6.452081	192.168.137.1	192.168.137.3	SMB	Trans2 Request, QUERY_PATH_INFO, Query File Standard Info, Path:

Frame 26: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits)
 # Ethernet II, Src: 02:26:6c:46:60:22 (02:26:6c:46:60:22), Dst: 0-1-Inktr_85:7e:fe (1c:bd:h9:85:7e:fe)
 # Internet Protocol, Src: 192.168.137.1 (192.168.137.1), Dst: 192.168.137.3 (192.168.137.3)
 # Transmission Control Protocol, Src Port: pcolp (4172), Dst Port: microsoft-ds (445), Seq: 855, Ack: 862, Len: 90
 # MESSAGE Session Service
 # SMB (Server Message Block Protocol)

Gambar 5. Hasil *Capture* Pada Proses *Transfer Data* Saat *OpenVPN* Dimatikan

Setelah menggunakan *OpenVPN / IP Tunnel* data yang ditransfer tidak dapat dibaca dengan mudah. Semua data terbaca sebagai protokol *UDP (User Datagram Protocol)*.

Capturing from Microsoft MMC - Bridge-Virtual NIC - WinPcap

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: @44=192.168.137.1 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
149	226.004161	192.168.137.1	192.168.137.1	UDP	Source port: 54075 Destination port: openvpn
151	226.005102	192.168.137.1	192.168.137.1	UDP	Source port: 54075 Destination port: openvpn
153	226.006100	192.168.137.1	192.168.137.1	UDP	Source port: 54075 Destination port: openvpn
155	226.008160	192.168.137.1	192.168.137.1	UDP	Source port: 54075 Destination port: openvpn
157	226.009182	192.168.137.1	192.168.137.1	UDP	Source port: 54075 Destination port: openvpn
159	226.218121	192.168.137.1	192.168.137.1	UDP	Source port: 54075 Destination port: openvpn
160	227.309604	192.168.137.1	192.168.137.1	UDP	Source port: 54075 Destination port: openvpn
162	227.598837	192.168.137.1	192.168.137.1	UDP	Source port: 54075 Destination port: openvpn
164	227.739775	192.168.137.1	192.168.137.1	UDP	Source port: 54075 Destination port: openvpn
166	227.749111	192.168.137.1	192.168.137.1	UDP	Source port: 54075 Destination port: openvpn
168	227.748406	192.168.137.1	192.168.137.1	UDP	Source port: 54075 Destination port: openvpn
170	227.747662	192.168.137.1	192.168.137.1	UDP	Source port: 54075 Destination port: openvpn
172	227.749411	192.168.137.1	192.168.137.1	UDP	Source port: 54075 Destination port: openvpn
174	227.750104	192.168.137.1	192.168.137.1	UDP	Source port: 54075 Destination port: openvpn
176	227.752363	192.168.137.1	192.168.137.1	UDP	Source port: 54075 Destination port: openvpn

Frame 26: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits)
 # Ethernet II, Src: 02:26:6c:46:60:22 (02:26:6c:46:60:22), Dst: 0-linkin_85:7e:fe (1c:bd:b9:85:7e:fe)
 # Internet Protocol, Src: 192.168.137.1 (192.168.137.1), Dst: 192.168.137.1 (192.168.137.1)
 # Transmission Control Protocol, Src Port: pcip (4172), Dst Port: microsoft-ds (445), Seq: 855, Ack: 862, Len: 90
 # NetBIOS Session Service
 # SMB (Server Message Block Protocol)

Gambar 6. Hasil Capture Pada Proses Transfer Data Saat OpenVPN Diaktifkan

PENUTUP

Kesimpulan

Berdasarkan dari hasil penelitian maka dapat diambil kesimpulan sebagai berikut:

1. Dengan menggunakan Protokol SSL (*Secure Socket Layer*) dan *IP Tunneling* dapat mengamankan proses transfer data pada samba server melalui internet.
2. *Virtual Private Network* (VPN) dapat membuat suatu jalur komunikasi data pribadi, seolah-olah data yang dikirim secara *point-to-point*, padahal data tersebut dikirim melalui jaringan internet.
3. Untuk mengakses samba server menggunakan VPN, komputer client harus mempunyai sertifikat *client* dikeluarkan oleh komputer server dan juga harus terdaftar pada *server basis data*.
4. Pada saat *IP Tunnel* tidak diaktifkan, proses transfer data dapat dilihat dengan mudah, saat *IP Tunnel* diaktifkan Proses transfer data jadi tidak terlihat, karena data terlihat menjadi *openvpn*.

Saran

1. Rancangan ini dapat ditambahkan keamanan ganda, dengan penambahan *firewall*.
2. Sebaiknya menggunakan OpenVPN GUI versi terbaru, agar *compatible* dengan Sistem Operasi yang terbaru

DAFTAR PUSTAKA

1. Cartealy, Imam. 2013. *Linux Networking*. Jakarta : Jasakom
2. Feilner, Markus. 2006. *OpenVPN: Building and Integrating Virtual Private Networks*. Birmingham : Packt Publishing
3. Jusak. 2012. *Teknologi Komunikasi Data Modern*. Yogyakarta : Penerbit Andi Offset.
4. Kurniawan, Agus. 2012. *Network Forensics Panduan Analisis Dan Investigasi Paket Data Jaringan Menggunakan Wireshark*. Yogyakarta : Penerbit Andi Offset.
5. Ramadhan, Arief. 2007. *Spk Internet & Aplikasinya*. Jakarta : Elex Media Komputindo.
6. Stallings, William. 2011. *Data and Computer Communications 7th Edition*. New Jersey : Pearson Prentice Hall
7. Sukmaji, Anjik dan Rianto. 2008. *Konsep Dasar Pengembangan Jaringan*. Yogyakarta : Penerbit Andi Offset.
8. Stiawan, Deris. 2006. *Sistem Keamanan Komputer*. Jakarta : Elex Media Komputindo
9. Tuxkeren. *Ubuntu Server : Panduan Singkat & Cepat*. Jakarta : Jasakom
10. Wahyono, Teguh. 2007. *Building & Maintenance PC Server*. Jakarta : Elex Media Komputindo