ISSN 1979-8555

JURNAL
TELEMATIK
VOLUME 6 NOMOR 2 APRIL 2014

Kata Pengantar

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji dan syukur atas kehadirat 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 ***T***eknik ***ELE***ktro, teknik infor***MAT***ika, s***I***stem 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

ISSN 197

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

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

ISSN 1979-8555

JURNAL
TELEMATIK
VOLUME 6 NOMOR 3 JULI 2014

DAFTAR ISI

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 mengunakan 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 memungkin *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 identikasi kepada klien yang ingin *login* ke dalam sebuah *domain* (Wahyono : 2007:161).

VPN (*Virtual Privte 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 dienkripsi (Cartealy :2013:19).

METODOLOGI

Perancangan Sistem Pada Komputer *Server*

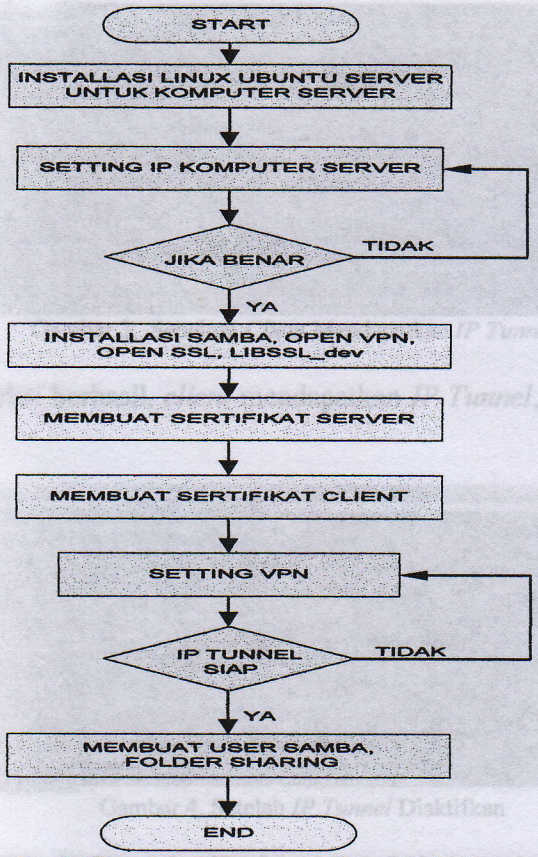
Perancangan sistem membahas mengenai proses membangun sistem keamanan data serta VPN pada komputer *server*.

Gambar 1. Blok Diagram Perancangan Sistem

Cara kerja dari blok diagarm pada Gambar 1 yaitu, dilakukan konfigurasi komputer *server* sebagai *server* yang bersistem operasi linux Ubuntu *server*, setting *IP Address*. Setelah terhubung ke internet, lakukan installasi 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.

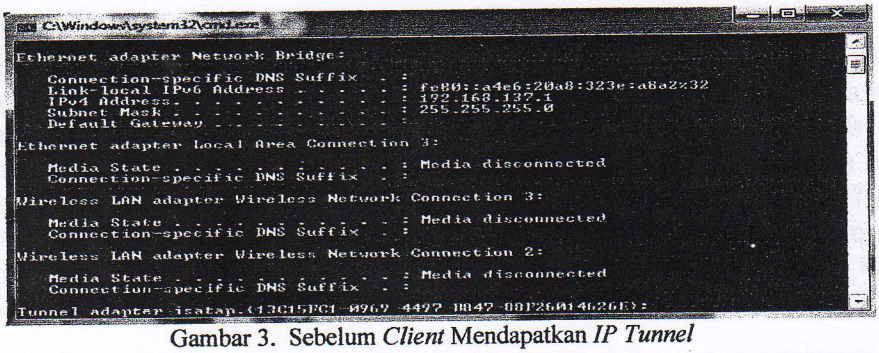


Gambar 2. *Flowchart* Perancangan Sistem Pada Komputer *Server*

HASIL DAN PEMBAHASAN

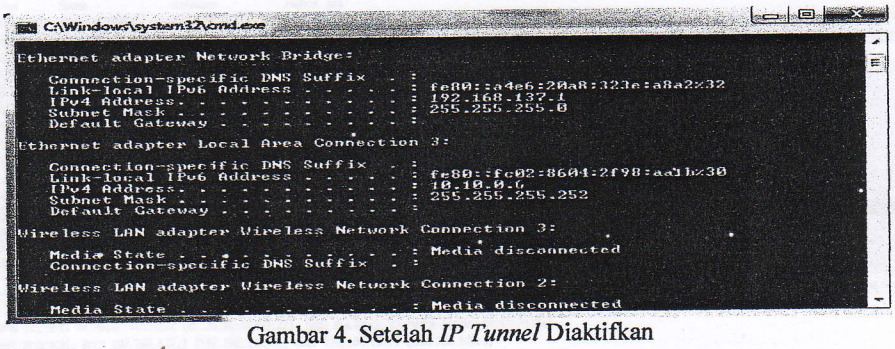
Pengujian Koneksi *IP Tunnel* dan Akses Samba *Server*

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



Gambar 3. Sebelum *Client* Mendapatkan *IP Tunnel*

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

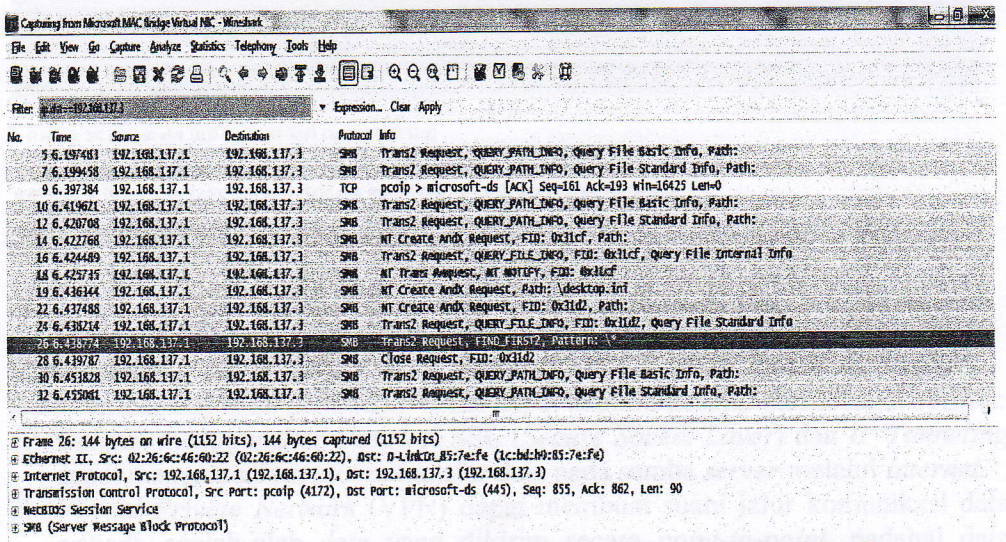


Gambar 4. Setelah *IP Tunnel* Diaktifkan

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*.

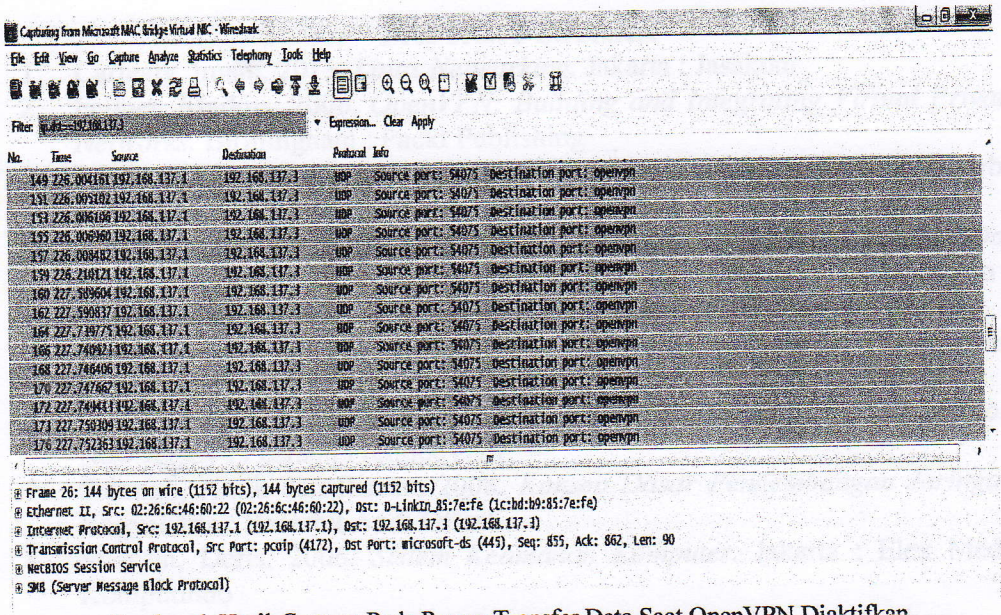
Pengujian Sistem Keamanan Data Menggunakan Wireshark

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.



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*).



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