Open VPN-Access Server Dengan Enskripsi SSL/TI Open SSL

Mohammad Badrul [1,*]

[1] Sistem Informasi; Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK Nusa Mandiri Jakarta); Jl.Damai No. 8 Warung Jati Barat (Margasatwa) Jakarta Selatan, Telp, (021) 78839513 Fax. (021) 78839421; e-mail: mohammad.mbl@nusamandiri.ac.id.

* Korespondensi : e-mail : mohammad.mbl@nusamandiri.ac.id

Diterima: 26 September 2016; Review: 12 Oktober 2016; Disetujui: 20 Oktober 2016

Cara sitasi: Badrul M. 2016. Open VPN-Access Server Dengan Enskripsi SSL/Tl Open SSL. Informatics for Educators and Professionals.1(1): 1 – 12.

Abstrak: Jaringan komputer merupakan salah satu teknologi yang banyak digunakan oleh beberapa perusahaan saat ini. salah satu fungsi dari jaringan komputer adalah menghubungkan satu lokasi dengan lokasi yang lainnya. Penggunaan internet sebagai suatu media komunikasi selain sangat bermanfaat untuk perusahaan, namun tetap memiliki kelemahan dalam hal keamanannya. PT.Indra Jalayatra juga tidak terlepas dari penggunaan jaringan dan internet untuk operasional perusahaan. kendala yang dihadapi yaitu bagaimana mengakses data untuk mendapatkan data-data dari luar kantor yang diperlukan sebagai bahan laporan tanpa harus datang langsung ke kantor, tentunya dengan tingkat keamanan yang sangat memadai. Solusi yang bisa digunakan untuk masalah tersebut yaitu membangun jaringan dengan teknologi *Virtual Private network.* Salah satu aplikasi yang bisa digunakan yaitu OpenVPN-Access Server dengan menerapkan enskripsi menggunakan Open SSL. OpenVPN-Access Server memberikan kemudahan dan keamanan dalam membentuk sebuah jaringan *Virtual Private network.*

Kata kunci: Keamanan, OpenVPN-Access Server,Virtual Private network

Abstract : *Computer network is one technology that is widely used by some companies today. one of the functions of a computer network is to connect one location to another. Use of the Internet as a communication medium other than very beneficial for the company, but still have drawbacks in terms of safety. PT.Indra Jalayatra not be separated from the use of the network and the Internet to the company's operations. constraints faced is how to access the data to obtain data from outside the office are required as a reports without having to come directly to the office, of course, with a very adequate level of security. Solutions that can be used for the issue of building a network with a Virtual Private Network technology. One of the applications that can be used is OpenVPN-Access Server by applying encryption using Open SSL. OpenVPN-Access Server provides convenience and security in forming a network of Virtual Private Network.*

Keywords*: OpenVPN-Access Server, Security, Virtual Private network*

1. Pendahuluan

Pemanfaaatan jaringan komputer untuk perusahaan sudah tidak dapat dipungkiri lagi untuk saat ini. Jaringan komputer memberikan kemampuan sebagai media komunikasi yang dapat mempercepat proses kerja baik dari segi waktu maupun kehandalan. Selain itu teknologi informasi dapat mempermudah dalam mengakses sebuah informasi. Sehingga perkembangan teknologi informasi sangat berpengaruh dalam segala kehidupan manusia. Kehandalan internet memungkinkan komunikasi yang tidak lagi terbatas oleh jarak dan waktu, menjadikan internet kian diminati. Internet sebagai suatu mediasi komunikasi selain sangat bermanfaat namun tetap memiliki kelemahan dalam keamanannya, terlebih sebagai media trasmisi data yang penting.

E-ISSN: 2548-3412 ; 1 – 12

konsekuensi yang harus di tanggung adalah bagaimana jaminan sebuah keamanan bagi jaringan yang terhubung dengan Internet. untuk itu dalam pemanfaatan internet sebagai media transmisi data perlu dilakukan peningkatan keamanannya. Salah satu upaya yang dilakukan adalah dengan membangun jaringan privat pada layanaan jaringan publik atau sering disebut dengan Virtual Private Network. Virtual Private Network (VPN) memberikan suatu mediasi jalur komunikasi melalui jaringan publik dengan proses tunneling dan enkripsi pada data, sehingga data yang akan ditransmisikan hanya dapat diakses oleh client dan terjaga kerahasiaannya (Astawa dkk, 2009). PT.Indra Jalayatra merupakan salah satu perusahaan yang bergerak dalam jasa export import juga tidak terlepas dari penggunaan jaringan dan internet untuk Operasional perusahaan. Aktifitas kerja yang dilakukan oleh karyawan tidak hanya di bagian office saja melainkan ada beberapa karyawan yang melaksanakan pekerjaan diluar kantor seperti lapangan, bahkan di beberapa kantor cabang. Untuk kelancaran komunikasi dan aktifitas layanan di kantor dan di luar kantor, maka perlu suatu cara yang bisa menghubungkan para karyawan yang bersifat mobile dengan jaringan LAN yang ada di kantor agar bisa melakukan akses data dengan mudah dan aman. Untuk menjawab masalah tersebut penulis mengusulkan untuk membangun sebuah jaringan Wide Area Network dengan teknologi Virtual yang lebih dikenal dengan VPN (*Virtual Private Network*). disamping itu karena jaringan sudah terkoneksi ke internet butuh keamanan data supaya data yang keluar masuk bisa dengan aman bisa sampai ke tujuan pengguna baik yang di dalam atau luar kantor.

Banyak teknologi software dan hardware yang bisa dipakai untuk mengembangkan VPN ini. Dari teknologi yang open source sampai yang berbayar dengan masing-masing kelebihannya dan kekurangnya dapat dengan mudah kita temukan. Pada penulisan skripsi ini penulis memilih tertarik untuk menggunakan aplikasi penunjang dalam pembuatan VPN yang bersifat opensource. Aplikasi penunjang tersebut yaitu OpenVPN Access Server. Penulis memilih OpenVPN Access Server karena memiliki semua fitur keamanan OpenVPN, OpenVPN menggunakan private keys, certificate, atau username-password untuk melakukan autentikasi dalam membangun koneksi, dimana untuk enkripsi OpenVPN sendiri menggunakan SSL/TLS yang dimana pembuatan certificate SSL-nya dilakukan oleh OpenSSL yang telah disediakan oleh Linux.dan juga dalam implementasi dan penggunaanya relatif mudah karena sudah menggunakan Grapical User Interface(GUI) berbasis WEB.

a. Jaringan Komputer

Jaringan komputer merupakan suatu sistem yang menghubungkan komputer menggunakan suatu teknologi transmisi data. Secara lebih sederhana, jaringan komputer dapat diartikan sebagai sekumpulan komputer beserta mekanisme dan prosedurnya yang saling terhubung dan berkomunikasi. Komunikasi yang dilakukan oleh komputer tersebut dapat berupa transfer berbagai data, instruksi, dan informasi dari satu komputer ke komputer lain. Ada beberapa pengelompokan jaringan menurut Jaraknya yaitu Jaringan LAN(*Local Area Network*), MAN(*Metropolitan Area Network*) dan WAN (*Wide Area Network*). LAN merupakan sebuah jaringan yang menghubungkan banyak komputer disebuah wilayah yang relatif kecil seperti rumah, kantor, atau kampus. Semua komputer yanng terhubung ke server pada jaringan disebut dengan workstation, workstation merupakan komputer standar yang dikonfigurasi menggunakan kartu jaringan, perangkat lunak jaringan dan kaabel-kabel yang diperlukan untuk menghubungkannya ke server (Aditya,2011). Saat ini, kebanyakaan LAN berbasis pada teknologi IEEE 802.3 *Ethernet* menggunakan perangkat *switch*, yang mempunyai kecepatan transfer data 10, 100, atau 1000 Mbit/s**.** selain teknologi *Ethernet*, saat ini teknologi 802.11b (atau biasa disebut *Wifi*) juga sering digunakan untuk membentuk LAN dengan teknologi *Wifi* biasa disebut *hotspot.* MAN adalah sebuah jaringan komputer besar yang mencangkup sebuah kota atau sebuah kampus besar(Aditya, 2011). MAN biasanya merupakan gabungan dari LAN yang menggunakan teknologi *backbone* berkecepatan tinggi dan menyediakan layanan ke jaringan yang lebih besar seperti WAN dan *Internet*(Madcom, 2010). *Metropolitan Area Network* (MAN) suatu jaringan dalam suatu kota dengan transfer data berkecepatan tinggi, yang menghubungkan berbagai lokasi seperti kampus, perkantoran, pemerintahan, dan sebagainya. Jaringan MAN adalah gabungan dari beberapa LAN. Jangkauan dari MAN ini antara 10 hingga 50 km, MAN ini merupakan jaringan yang tepat untuk membangun jaringan antara kantor-kantor dalam suatu kota antara pabrik/instansi dan kantor pusat yang berada dalam jangkauannya, prinsip sama dengan LAN, hanya saja jarak lebih luas, yaitu 10-50 km(Aditya, 2011). Suatu WAN meliputi area geografi yang lebih luas lagi, yang

meliput suatu negara atau dunia. Umumnya jaringan ditempatkan pada banyak lokasi yang berbeda. WAN digunakan untuk menghubungkan banyak LAN yang secara gografis terpisah. WAN dibuat dengan cara menghubungkan LAN menggunakan layannan seperti Leased Line, dial-up, satelit atau layanaan paket carrier. Dengan WAN, sekolah yang ada di Yogyakarta dapat berkomunikasi dengan sekolah yang ada di Munchen Jerman dalam beberapa menit saja tanpa mengeluarkan biaya yang banyak(Winarto, 2013). *Wide Area Network* (WAN) merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota, atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan router dan saluran komunikasi publik(Aditya, 2011). WAN digunakan untuk menghubungkan jaringan lokal yang satu dengan jaringan lokal yang lain, sehingga pengguna atau komputer di lokasi yang satu dapat berkomunikasi dengan pengguna dan komputer dilokasi yang lain.

b. VPN

Menurut Markus dan Feilner (2006) VPN adalah Virtual, karena tidak ada koneksi jaringan langsung nyata antara dua (atau lebih) mitra komunikasi, tetapi hanya koneksi virtual yang disediakan oleh VPN Software, biasanya melalui koneksi Internet publik. Pribadi, karena hanya anggota perusahaan terhubung oleh Software VPN yang diizinkan untuk membaca data yang ditransfer. Pada VPN terdapat 3 (tiga) mekanisme penting, yaitu enkripsi, autentikasi dan autorisasi.Enkripsi merupakan proses mengubah data ke dalam bentuk yang hanya bisa dibaca oleh penerima yang diinginkan. Untuk membaca pesan yang telah dienkripsi tersebut, penerima data harus mempunyai kunci dekripsi yang benar. *Public-key encryption* menggunakan dua kunci. Satu kunci dikenal sebagai *public key*, yang oleh setiap orang boleh gunakan selama enkripsi dan dekripsi. Walaupun nama kuncinya adalah *public key*, kunci ini dipunyai oleh sebuah entiti. Jika entiti kedua perlu untuk berkomunikasi dengan pemilik kunci, entiti kedua menggunakan *public key* untuk melakukan komunikasi itu. *Public key* mempunyai *corresponding private key. Private key* adalah key yang bersifat pribadi kepada entiti. Sebagai hasilnya, dengan enkripsi *public key* setiap orang dapat menggunakan pemilik *public key* unyuk mengenkripsi dan mengirim pesan. Tetapi, hanya pemilik yang mempunyai *private key* untuk mendekripsi pesan. Dalam berkomunikasi, pengirim menggunakan *public key*-nya untuk mengenkripsi pesan. Penerima menerima pesan dan mendekripsi pesan yang telah didecode menggunakan *private key*. *Pretty Good Privacy* (PGP) dan *Data Encryption Standard* (DES) adalah dua dari *public key* enkripsi yang paling populer.

Pada VPN juga terdapat protokol yang disebut dengan *VPN Tunneling Protocols*, protokol-protokol ini berguna untuk memastikan aspek keamanan dari transaksi melalui VPN. Protokol yang biasa digunakan, yaitu *IP Security* (IPSec), *Point-to-Point Tunneling Protoco*l (PPTP), *Layer 2 Tunneling Protocol* (L2TP), dan protokol-protokol lainnya seperti SSL/TLS. *IP Security* (IPSec). Dikembangkan oleh IETF, IPSec adalah standar terbuka yang memastikan keamanan trasmisi dan autentikasi pengguna melalui jaringan publik. Tidak seperti teknik enkripsi lainnya, IPSec beroperasi pada *Network Layer* dari model tujuh layer OSI. Oleh karena itu, dapat diimplementasikan secara bebas ke aplikasi yang berjalan melalui jaringan. Sebagai hasilnya jaringan dapat diamankan tanpa perlu mengimplementasikan dan mengkoordinasi keamanan untuk setiap aplikasi(Hendra, 2006).

IP Security (IPSec). Dikembangkan oleh IETF, IPSec adalah standar terbuka yang memastikan keamanan trasmisi dan autentikasi pengguna melalui jaringan publik. Tidak seperti teknik enkripsi lainnya, IPSec beroperasi pada *Network Layer* dari model tujuh layer OSI. Oleh karena itu, dapat diimplementasikan secara bebas ke aplikasi yang berjalan melalui jaringan. Sebagai hasilnya jaringan dapat diamankan tanpa perlu mengimplementasikan dan mengkoordinasi keamanan untuk setiap aplikasi.

Point-to-Point Tunneling Protocol (PPTP). Dikembangkan oleh Microsoft, 3COM, dan Ascenf Communicarions, PPTP dimaksudkan sebagai alternatif untuk IPSsec. Tetapi, IPSec masih menjadi favorit tunneling protokol. PPTP beroperasi pada layer kedua (*Data Link Layer*) dari model OSI dan digunakan untuk mengamankan transmisi dari trafik Windows.

Layer 2 Tunneling Protocol (L2TP). Dikembangkan oleh Cisco System, L2TP juga dimaksudkan untuk mengganti IPSec sebagai tunneling protocol. Tetapi IPSec masih terus-menerus menjadi protokol yang dominan untuk komunikasi yang aman melalui *internet.* L2TP adalah kombinasi dari *layer 2forwarding* (L2F) dan PPTP dan digunakan untuk

E-ISSN: 2548-3412 ; 1 – 12

mengenkapsulasi *frame Pointto- Point Protocol* (PPP) yang dikirim melalui X.25, FR, dan jaringan ATM.

Faktor lain yang membedakan antara sistem dan protokol yang dijelaskan di atas adalah:

1. Ketersediaan dari mekanisme autentikasi
2. Mendukung untuk fitur *advanced networking* seperti *Network Address Translation* (NAT)
3. Alokasi dinamis dari IP address untuk partner tunnel dalam mode dial-up
4. Mendukung untuk *Public Key Infrastructures* (PKI)

VPN sendiri memiliki beberapa tipe, VPN yang biasa dikenal adalah *Remote-Access VPN* dan *Site-to-Site VPN*(Hendra, 2006)..

1. Remote-Access VPN

Seperti namanya, *Remote Access* VPN menyediakan akses dengan *remot*e, *mobile*, dan komunikasi karyawan dari sebuah organisasi ke jaringan sumber korporasi. Secara khusus, permintaan *remote* akses dibuat oleh pengguna yang selalu berkembang yang ingin mengakses jaringan LAN perusahaan. Dengan mengimplementasikan *Remote Access* VPN, pengguna remote dan cabang kantor hanya perlu melakukan setting koneksi lokal *dialup* ke ISP dan mengkoneksikan ke jaringan perusahaan melalui *internet*.

2. Site-to-Site VPN

Tipe VPN ini membuat jalur aman dan tetap antar-site dengan site, misalnya antar kantor pusat dan kantor-kantor cabang lewat internet. masing-masing site mempunyai server VPN untuk membuat jalur VPN yang dibutuhkan. Setelah jalur VPN terbina antara kantor cabang dengan kantor pusat, maka pemakai komputer yang berada pada LAN di kantor cabang dapat akses data yang berada pada LAN di kantor pusat. hanya tentu kecepatan akses terbatas dengan bandwidth jalur VPN yang digunakan.

c. OPEN VPN

OpenVPN merupakan aplikasi *open-source* untuk membuat Virtual Private Network (VPN), dimana aplikasi tersebut dapat membuat koneksi *point-to-point tunnel* yang telah terenkripsi. OpenVPN menggunakan *private keys, certificate,* atau *username-password* untuk melakukan autentikasi dalam membangun koneksi, dimana untuk enkripsi OpenVPN sendiri menggunakan SSL/TLS yang dimana pembuatan *certificate* SSL-nya dilakukan oleh *OpenSSL* yang telah disediakan oleh Linux. Cara kerja OpenVPN adalah sebelumnya pada kedua sisi (*server – client*) harus memiliki jalur internet yang permanen. Apabila perusahaan memiliki router maka router tersebut harus dikonfigurasi *firewall*-nya agar dapat mencegah akses terhadap jaringan didalamnya dan juga harus dikonfigurasi agar OpenVPN dapat melewati router tersebut(Markus dan Feilner,2006).

Aplikasi OpenVPN harus terinstall didalamnya, dan harus terkonfigurasi agar koneksi dapat terbuat. Apabila hal ini telah dilakukan maka dua sisi (*server client*) akan dapat terhubung melalui jaringan virtual. Setiap data yang dilewatkan pada OpenVPN dienkripsi terlebih dahulu dan didekripsi sesudah transmisi. Enkripsi menjamin keamanan data seperti sebuah terowongan kereta api di gunung yang menjaga agar kereta api aman melewati gunung tersebut. Terowongan inilah yang lebih dikenal dengan nama *tunnel*. Sebuah koneksi OpenVPN biasanya dibuat diantara dua buah akses *internet* dengan *firewall* dan aplikasi OpenVPN. Aplikasi tersebut harus disetting agar koneksi antara partner VPN dapat dilakukan. *Firewall* juga harus disetting agar membolehkan akses dan pertukaran data antara partner VPN yang telah aman sebelumnya karena telah dilakukan enkripsi. Key enkripsi harus disediakan untuk semua partner VPN sehingga pertukaran data hanya bisa dilakukan oleh partner VPN yang telah terotorisasi.

OpenVPN ini memiliki banyak sekali keunggulan, diantaranya :

1. OpenVPN bersifat *open-source* dan merupakan salah satu *software* yang dapat dipakai diberbagai macam jenis sistem operasi (*multi platform)*.
2. Instalasi OpenVPN sangat mudah dilakukan di sistem operasi apapun (*easy to install)*.
3. OpenVPN menyediakan *interface* yang mudah digunakan.
4. OpenVPN menawakan tingkat *mobility* yang tinggi kepada penggunanya.
5. OpenVPN menawarkan dua mode VPN, yaitu VPN pada Layer 2 ataupun VPN pada Layer 3.

OpenVPN juga menawarkan *tunnel* VPN sebagai tempat lewatnya data sehingga keamanan data menjadi terjamin.

d. *Asymmetric Encryption* dengan SSL/TLS

SSL/TLS menggunakan satu yang terbaik dari teknologi enkripsi yang disebut dengan *asymmetric encryption* untuk memastikan identitas dari partner VPN. Kedua partner enkripsi memiliki dua key, yang satu adalah key public dan satu lagi adalah key pribadi. Key public menangani komunikasi antara partner yang mengenkripsi data dengan SSL/TLS. Karena pemilihan algoritma matematika yang digunakan untuk membuat pasangan key pribadi/publik, dan hanya key pribadi dari penerimalah yang bisa melakukan dekripsi terhadap data yang telah dienkripsi oleh key publiknya(Markus Feilner, 2006)

e. Keamanan SSL/TLS

Library SSL/TLS dapat digunakan untuk melakukan autentikasi dan enkripsi. Library ini adalah bagian dari OpenSSL yang terpasang pada hampir semua sistem operasi modern. SSL, yang juga terkenal sebagai TLS adalah sebuah protokol yang didisain oleh *Netscape Communications Corporation* untuk meyakinkan kemudahan dari integritas dan autentikasi data untuk mengimbangi perkembangan internet pada tahun 1990an. SSL/TLS adalah sebuah teknologi yang sangat baik yang digunakan hampir disemua website milik bank, *e-commerce* ataupun aplikasi yang membutuhkan keamanan dan kerahasiaan(Paulus, 2012).

Pada SSL/TLS terdapat sertifikat yang bernama *Trusted Certificates.* Sertifikat ini merupakan sertifikat yang sebelumnya telah dibuat oleh organisasi tertentu (Bank, *E-Commerce,* dll.) yang digunakan untuk menjamin keaslian identitas dari pemilik sertifikat tersebut. Pada SSL/TLS juga terdapat sertifikat yang disebut dengan *Self-Signed Certificates* yang merupakan sertifikat yang tidak membutuhkan autentikasi seperti pada *Trusted Certificates*, tetapi dengan menggunakan sertifikat yang disebut dengan *Certificate Authority* (CA). Pada OpenVPN, sertifikat SSL/TLS ini dibuat dan didefinisikan dan semua sertifikat yang valid yang dikeluarkan oleh otorisasi merupakan sertifikat yang akan diterima oleh VPN. Setiap *client* harus mempunyai sertifikat yang valid berdasarkan CA dan yang akan diijinkan untuk membuat koneksi ke VPN. Sertifikat-sertifikat ini dapat digunakan untuk berbagai macam tujuan. HTTPS dan OpenVPN adalah hanya dua aplikasi yang menggunakan ini dari berbagai macam aplikasi lainnya(Paulus, 2012).

f. OpenVPN–Access Server

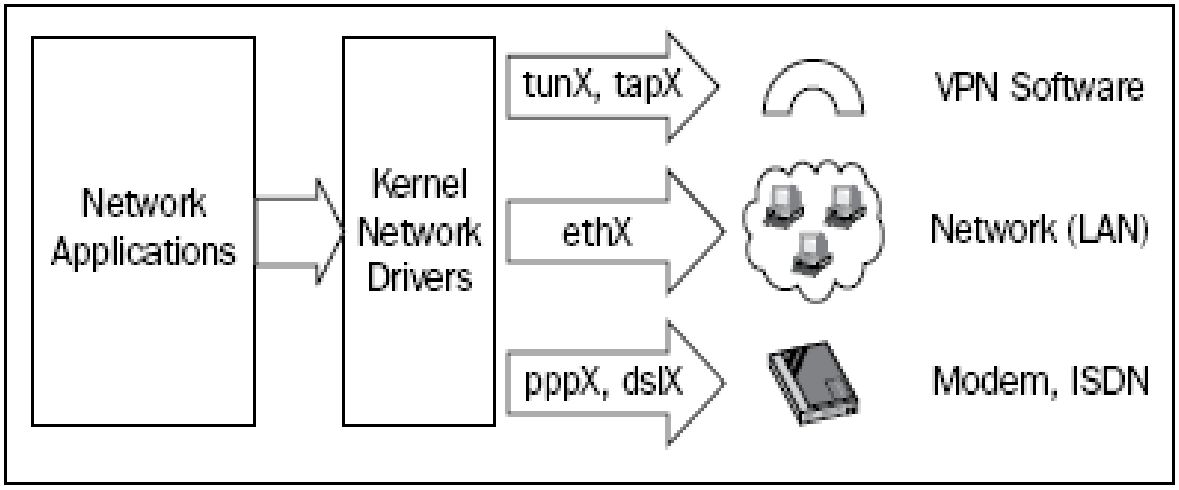
OpenVPN –Access Server adalah sebuah solusi sofware yang mendukung penuh fitur SSL yang mengintegrasikan kemampuan server OpenVPN, kemampuan manajemen perusahaan dan paket software OpenVPN Client yang mengakomodasi Windows, MAC, dan OS Linux. OpenVPN Access Server mendukung berbagai konfigurasi, termasuk akses remote yang aman ke jaringan internal dan atau sumber daya jaringan pribadi serta aplikasi dengan kontrol akses.(OpenVPN.net)**.** OpenVPN–Access Server mempunyai kelebihan dalam penggunaanya karena menggunakan antarmuka sistem berbasis web, karena itu OpenVPN –Access Server relatif mudah di konfigurasi dan gunakan. Dan juga disisi Client jika dengan OpenVPN-Access Server ini Client tidak perlu repot meng-*copy* file *key* dan *certificate* karena client hanya cukup menggunakan browser memasukan alamat VPN Server kemudan Login, setelah login client hanya perlu download file berbentuk *exe* yang di dalamnya sudah disertakan file *key* dan *certificate* kemudain menjalankan file *exe* tersebut untuk menginstal dan mengkonfigurasi OpenVPN client secara otomatis.(Markus dan Feilner,2006).

Struktur modular dari OpenVPN tidak hanya bisa ditemukan dalam model keamanannya sendiri, tetapi juga bisa ditemukan di dalam kerangka jaringan. **James Yonan** memilih *driver Universal* TUN/TAP untuk lapisan jaringan dari OpenVPN. TUN/TAP *driver* adalah sebuah proyek *open-source* yang terdapat di dalam semua distribusi Linux/UNIX yang modern seperti juga Windows dan MacOS X. seperti SSL/TLS, TUN/TAP juga dipakai dalam banyak proyek, oleh karena itu TUN/TAP dengan rutin ditingkatkan dan ditambahkan banyak fitur. Penggunaan TUN/TAP mengebelakangakan banyak kompleksitas dari struktur OpenVPN itu sendiri sehingga dengan strukturnya yang sederhana tersebut dapat meningkatkan keamanan VPN dibandinganken dengan VPN lainnya. Contohnya, IPSec yang memiliki struktur kompleks dengan modifikasi kompleksnya pada *kernel* dan *IP Stack,* yang dapat menyebabkan terciptanya celah-celah kecil pada keamanannya sendiri.

Driver Universal TUN/TAP dikembangkan untuk dapat menyediakan dukungan pada Linux *kernel* untuk keperluan proses *tunneling*. *Driver* ini merupakan sebua *virtual network interface* yang muncul sebagai otentik untuk semua aplikasi dan pengguna; yang mencirikannya dari

E-ISSN: 2548-3412 ; 1 – 12

peralatan lainnya adalah dari penamaannya dengan tunX atau tapX. Setiap aplikasi yang memungkinkan penggunaan *network interface* dapat menggunakan *tunnel* ini. *Driver* ini merupakan salah satu faktor utama yang membuat OpenVPN mudah untuk dimengerti, mudah untuk dikonfigurasi dan tidak lupa keamanannya. Gambar berikut ini menunjukan *interface* sederhana yang digunakan oleh OpenVPN :



Sumber: Markus Feilner (2006)

Gambar 1. OpenVPN *Standard Interface*

Sebuah TUN dapat digunakan seperti sebuah *virtual interface* untuk melakukan koneksi *point-to-point*, seperti sebuah modem atau DSL *link*. Ini disebut dengan mode *routed*, karena rute antara pasangan VPN telah dikonfigurasi sebelumnya. Sebuah TAP dapat digunakan seperti sebuah *virtual Ethernet adapter*. Hal ini memungkinkan *daemon* membaca *interface* untuk menangkap *Ethernet frames* yang tidak mungkin dilakukan oleh TUN. Mode ini disebut dengan *bridging mode* karena jaringan-jaringan yang terhubung seolah-olah berada dalam satu *hardware* yang sama. Aplikasi-aplikasi dapat dibaca/ditulis pada *interface* ini; perangkat lunak (*tunnel driver)* akan mengambil semua data dan menggunakan *cryptographic libraries* dari SSL/TLS untuk mengenkripsi mereka. Data tersebut dibungkus dan dikirim kepada ujung lain dari *tunnel*. Pengemasan ini terselesaikan atas standarisasi UDP atau TCP (opsional). UDP merupakan pilihan pertama, tetapi TCP dapat sangat membantu dalam beberapa hal. Pemilihan protocol ini diserahkan kepada penggunanya.

OpenVPN mendengarkan TUN/TAP, mengatur *traffic*, melakukan enkripsi, dan mengirimkan data kepada pasangan VPN yang lain, dimana proses OpenVPN yang lain akan menerima data, melakukan dekripsi, dan menyampaikannya kepada alat jaringan, dimana aplikasi lainnya sedang menunggu data(Markus Feilner, 2006)

2. Metode Penelitian

Analisa penelitian yang dilakukan terdiri dari :

a. Analisa Kebutuhan
   Dalam analisa kebutuhan ini penulis mencoba menyiapkan analisa kebutuhan seperti:
   1) Perangkat yang dibutuhkan untuk membangun jaringan
   2) Software yang dibutuhkan yaitu VMWare
b. Desain
   Dalam metode ini penulis membuat analisa desain jaringan yang digunakan untuk penerapan *VPN-Access Server*
c. Testing
   Melakukan testing, meliputi tes koneksi dan juga test keamanan untuk memastikan semuanya agar jaringan VPN sesuai yang diharapkan sebelum diimplementasikan.
d. Implementasi
   Dalam tahap implementasi ini, penulis melakukan percobaan tentang VPN-Access Server menggunaan jaringan virtual dengan menggunaakan software VMWare versi 7.0.0 build-203739.

Sedangkan metode pengumpulan data yang penulis lakukan antara lain:

1. Observasi
   Yaitu melakukan pengamatan langsung dilapangan untuk mendapatkan data-data yang dibutuhkan untuk penulisan penelitian ini.
2. Wawancara
   Metode ini dilakukan dengan cara tanya jawab secara langsung dengan administrator jaringan untuk mendapat data-data yang lebih rinci lagi mengenai jaringan yang ada di PT.Indra Jalayatra.
3. Studi Pustaka
   Metode ini merupakan cara untuk mendapatkan data-data secara teoritis sebagai bahan penunjang dalam penyusunan penelitian dengan cara mempelajari, meneliti dan menelaah berbagai literatur-literatur dari perpustakaan maupun dari buku-buku referensinya lainnya, juga dari situs-situs internet yang berkaitan dengan topik penelitian.

3. Hasil dan Pembahasan

Dalam pembahasan ini penulis membahas tentang jaringan yang sedang diterapkan di perusahaan dan usulan jaringan yang penulis usulkan.

3.1. Jaringan yang sedang diterapkan

Pembahasan ini penulis akan membahas tentang topologi jaringan, arsitektur jaringan, skema jaringan dan keamanan jaringan

1. Topologi jaringan
   Topologi jaringan merupakan hal yang paling mendasar dalam membentuk sebuah jaringan, untuk topologi jaringan yang digunakan pada PT. Indra Jalayatra yaitu Topologi *Tree,* dimana semua peralatan jaringan seperti PC, Server, Printer dan lainnya dihubungkan dalam satu konsentrator dalam hal ini Switch kemudian switch tersebut dihubungkan ke switch lainnya untuk membentuk jaringan yang lainnya. *Traffic* data mengalir dari node ke central node dan kembali lagi dan juga jika salah satu kabel node terputus yang lainnya tidak terganggu.
2. Arsitektur Jaringan
   Arsitektur jaringan yang digunakan pada PT. Indra Jalayatra yaitu model OSI (Open Systems Interconnection) yang diciptakan oleh International Organization for Standardization (ISO). OSI menyediakan kerangka logika terstruktur bagaimana proses komunikasi data berinteraksi melalui jaringan. Standard ini dikembangkan untuk industri komputer agar komputer dapat berkomunikasi pada jaringan yang berbeda secara efisien. Terdapat 7 layer pada model OSI. Setiap layer bertanggungjawwab secara khusus pada proses komunikasi data. Misal, satu layer bertanggungjawab untuk membentuk koneksi antar perangkat, sementara layer lainnya bertanggungjawab untuk mengoreksi terjadinya “error” selama proses transfer data berlangsung. Model Layer OSI dibagi dalam dua group: “upper layer” dan “lower layer”. “Upper layer” fokus pada applikasi pengguna dan bagaimana file direpresentasikan di komputer. Untuk Network Engineer, bagian utama yang menjadi perhatiannya adalah pada “lower layer”. Lower layer adalah intisari komunikasi data melalui jaringan aktual. “Open” dalam OSI adalah untuk menyatakan model jaringan yang melakukan interkoneksi tanpa memandang perangkat keras/ “hardware” yang digunakan, sepanjang software komunikasi sesuai dengan standard. Hal ini secara tidak langsung menimbulkan “modularity” (dapat dibongkar pasang). Disamping OSI Layer, di perusahaan ini juga telah menerapkan DNS Server yaitu menggunakan DNS agar tidak perlu menghapal alamat IP pada saat browsing di internet. DNS adalah sebuah sistem yang menyimpan informasi tentang nama host ataupun nama domain dalam bentuk basis data tersebar (*distributed database*) di dalam jaringan komputer, misalkan: Internet. DNS menyediakan alamat IP untuk setiap nama host dan mendata setiap server transmisi surat (mail exchange server) yang menerima surel (email) untuk setiap domain. Menurut browser Google Chrome, DNS adalah layanan jaringan yang menerjemahkan nama situs web menjadi alamat internet.
   DNS menyediakan pelayanan yang cukup penting untuk Internet, ketika perangkat keras komputer dan jaringan bekerja dengan alamat IP untuk mengerjakan tugas seperti pengalamatan dan penjaluran (routing), manusia pada umumnya lebih memilih untuk menggunakan nama host dan nama domain, contohnya adalah penunjukan sumber universal (URL) dan alamat surel. Analogi yang umum digunakan untuk menjelaskan

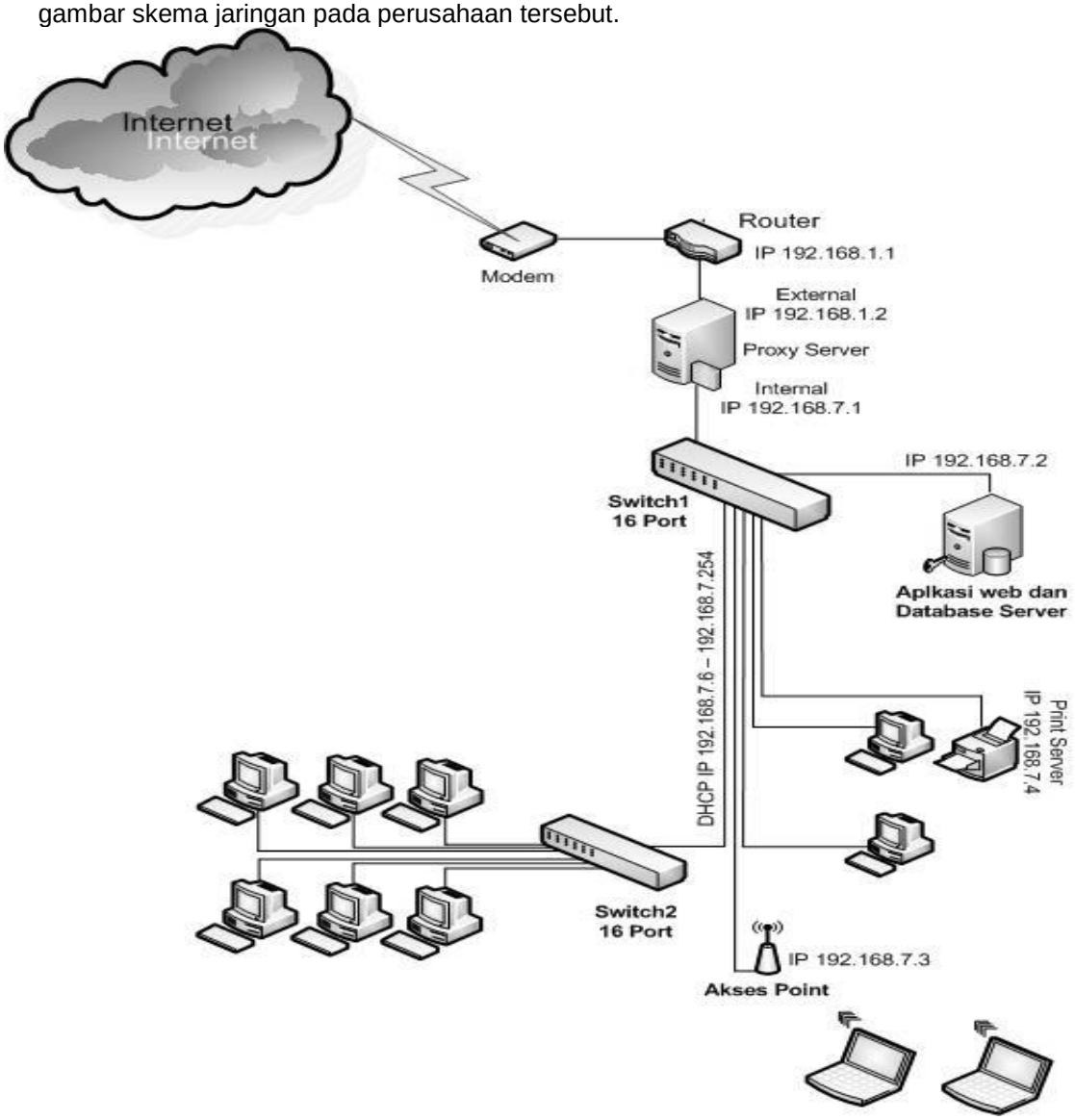
E-ISSN: 2548-3412 ; 1 – 12

fungsinya adalah DNS bisa dianggap seperti buku telepon internet dimana saat pengguna mengetikkan www.indosat.net.id di peramban web maka pengguna akan diarahkan ke alamat IP 124.81.92.144 (IPv4) dan 2001:e00:d:10:3:140::83.

Sedangkan fasilitas lain adalah E-mail yang merupakan fasilitas pada internet yang paling banyak digunakan untuk pengiriman pesan. Pada saat pertama kali berkembang, *e-mail* hanya bisa mengirimkan berupa pesan *text* saja, namun seiring perkembangaannya *e-mail* sudah bisa mengirimkan pesan *text,* HTML, gambar, file dan sebagainya. Perusahaan ini juga menggunakan *e-mail* untuk komunikasi dengan rekan bisnisnya.

3. Skema Jaringan

Jaringan Komputer pada PT.Indra Jalayatra terdiri dari Modem, Router, Proxy server, Web dan database server, dua buah switch, akses point dan client (PC dan Laptop). Berikut gambar skema jaringan pada perusahaan tersebut.



Gambar 2. Skema Jaringan PT.Indra Jalayatra

Switch digunakan untuk menghubungkan seluruh perangkat (PC, Server, Printer dan perangkat jaringan lainnnya). Switch1 digunakan untuk menghubungkan modem, server aplikasi web, proxy server dan juga sebagai link ke akses point dan link ke switch2, sedangkan switch2 digunakan untuk menghubungkan PC-PC yang menjadi klien di jaringan PT.Indra Jalayatra. PT.Indra Jalayatra juga menggunakan akses point untuk menghubungkan perangkat jaringan melalui media wireless seperti laptop dan perlangkat wireless lainnya.

Untuk aksses internet PT. Indra Jalayatra menggunakan jasa ISP Speedy dari PT. Telkom dengan bandwidth sebesar 2 Mbps yang dishare ke semua client di jaringan internal melalui Proxy server. Akses internet ini sangat vital peranannya karena digunakan untuk komunikasi terutama dalam penggunakan *e-mail* dan *messenger. E-mail* gunakan untuk komunikasi dengan client yang bekerjasama dengan Pihak Perusahaan untuk transaksi bisnis.

4. Keamanan Jaringan

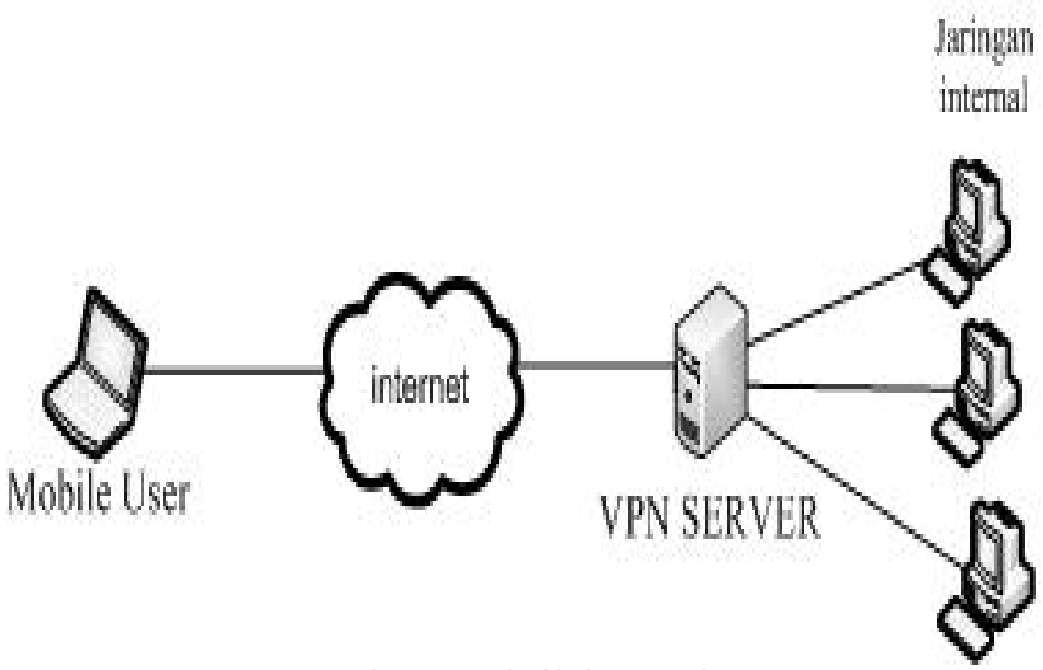
Proxy Server pada PT.Indra Jalayatra memegang peranan penting dalam pengelolaan jaringan karena seluruh pengaturan jaringan seperti management bandwidth dan juga sebagai Internet gateway dipercayakan pada proxy server. Proxy server adalah server yang diletakan antara suatu aplikasi klient dan aplikasi server yang dihubungi. keamanan jaringan dan juga pengaturan akses internet diatur semua di proxy server. Proxy server yang digunakan menggunakan ClearOS versi 5.2. Di *proxy server* juga terdapat *firewall* untuk keamanan jaringan. Menurut Wagito (2005:P143) "*Firewall* adalah alat untuk melindungi jarigan *private* dari jaringan publik(internet)". Firewall melindungi jaringan private dengan cara mengendalikan aliran paket berdasarkan pada asal tujuan, port, dan informasi tipe paket yang terdapat pada masing-masing paket. *Firewall* berisi sederet daftar aturan yang digunakan untuk menentukan nasib pada paket yang datang atau pergi dari *firewall* menurut kriteria dan parameter tertentu. Untuk keamaan disisi klient masing-masing klient diinstall juga program antivirus.

3.2. Jaringan Usulan dari Penulis

Seperti yang sudah penulis dijelaskan dalam bab sebelumnya yaitu agar para pegawai PT. Indra Jalayatra bisa akses jaringan Lokal melalui jaringan publik maka penulis mengusulkan untuk menambahkan *virtual private network* server pada jaringan PT. Indra Jalayatra. *Virtual private network* bekerja membentuk suatu pipa(*tunnel*) yang berada di dalam jaringan publik sehingga aliran data yang lewat didalamnya tidak bisa diakses oleh orang yang tidak memiliki hak akses ke dalam *tunnel* tersebut. Pembahasanjaringan usulan ini penulis akan membahas tentang topologi jaringan, skema jaringan, keamanan jaringan dan perancangan aplikasi.

1. Topologi Jaringan usulan

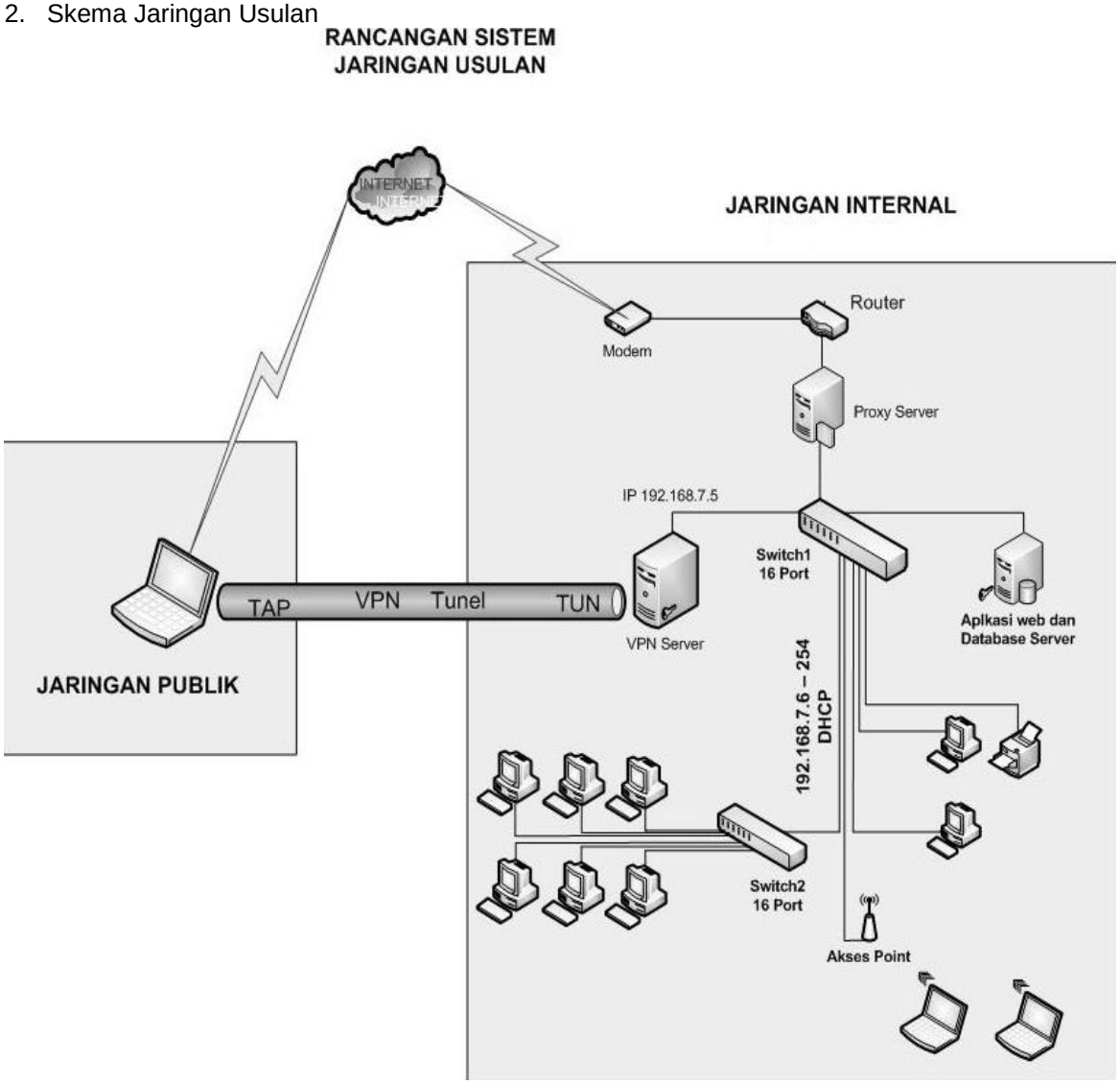
   Untuk topologi jaringan penulis tidak akan merubah topologi jaringan yang sudah ada pada PT. Indra Jalayatra karena topologi yang sekarang digunakan sudah sangat baik dan berjalan sesuai apa yang diharapkan. Jaringan usulan yang penulis usulkan hanya menambahkan server VPN di belakang Proxy Server untuk bisa mengakses jaringan LAN PT. Indra Jalayatra dari jaringan publik. Berikut penulis sajikan gambar topologi jaringan.



Gambar 3. Topologi jaringan usulan

E-ISSN: 2548-3412 ; 1 – 12

2. Skema Jaringan Usulan



Gambar 4. Skema jaringan usulan

Pada Skema jaringan usulan dapat dilihat bahwa ada penambahan satu buah server VPN yang nantinya akan digunakan untuk bisa menghubungkan para pekerja yang berada di luar kantor ke jaringan LAN PT.Indra Jalayatra. Dikarenakan VPN Server ini dipasang di belakang modem/router dan proxy server, maka perlu dilakukan konfigurasi port forward disisi modem/router dan juga proxy server.

3. Keamanan Jaringan

Dengan menerapkan Jaringan VPN dengan OpenVPN maka pertukaran data melalui jaringan publik seperti internet akan terjamin keamannnya ini dikarenakan ada sistem enkripsi data dan juga menggunakan teknologi tunneling antara VPN client dengan VPN server. Dan dalam penerapannya tunnel dilengkapi dengan sistem enkripsi untuk menjaga keamanan tersebut. Dimana data yang telah dienkripsi hanya dapat dibaca setelah didekripsi oleh VPN server atau client itu sendiri. OpenVPN standarnya menggunakan BF-CBC(*Blowfish-Cipher Block Chaining*) untuk Simetrik cipher menggunakan kunci 128-bit. Blowfish merupakan algoritma yang sangat kuat dan belum diketahui kelemahannya. kunci 128-bit memberikan kunci ruang yang cukup besar yang mustahil untuk melakukan serangan *brute force*. Blowfish tidak hanya sangat aman, tapi juga salah satu algoritma yang tercepat. Untuk memastikan integritas data OpenVPN menggunakan apa yang disebut hash, hash berfungsi menerima masukan string yang panjangnya sembarang lalu mentransformasikannya menjadi string keluaran yang panjangnya tetap (fixed). Fungsi *hash*

sangat peka terhadap perubahan 1 bit pada pesan, Pesan berubah 1 bit, nilai *hash* berubah sangat signifikan. OpenVPN secara default menggunakan algoritma hashing SHA-1. untuk menghentikan penyerang yang ingin menghapus hash string, OpenVPN menggunakan HMAC. Pada saat pesan dikirim sebelumnya HMAC memasang kunci rahasia. Kunci ini dilampirkan pada hash bersama dengan pesan yang dikirim. Ketika pesan telah diterima di ujung terowongan, peneriam akan membukan pesan dan memastikan kunci rahasia terbawa bersama dengan pesan yang diterima. jadi jika ada penyerang mengubah pesan dan membuat hash baru maka mereka(penyerang) tidak bisa membuat kunci rahasia dan penerima bisa mengetahui bahwa pesan tersebut sudah berubah.

OpenVPN menggunakan *driver universal* TUN/TAP. *Driver* ini merupakan sebuah *virtual network interface* yang membentuk sebuah *tunnel*, bisa dilihat pada gambar IV.1, *virtual network interface* TUN dibentuk disisi Server VPN dan *virtual network interface* TAP dibentuk disisi VPN klient.

4. Perancangan Aplikasi

Pada perancangan aplikasi penulis akan menjelaskan langka-langkah instalasi dan konfigurasi untuk membangun jaringan *virutal private tenwork.*

a. Instalasi VPN Server

Dalam tahap ini penulis akan menjelasan mengenai langkah-langkah yang dilakukan dalam menginstall software OpenVPN**-**Access Server pada *server* (Ubuntu Server 12.04 LTS).

b. Konfigurasi VPN Server

Setelah tahap instalasi selesai maka masuk ke tahap konfigurasi,

c. Konfigurasi OpenVPN Server di Web UI

Untuk masuk ke konfigurasi Web UI bisa menggunakan komputer lain yang satu jaringan dengan server VPN, gunakan aplikasi browser mozila firefox, chrome atau browser lainnnya dalam hal ini penulis menggunakan browser chrome. Langkah selanjutnya melakukan pengaturan VPN Server, meliputi setting IP publik, pemilihaan *port* dan *interface* yang digunakann untuk akses VPN. Untuk pengaturan *host name* dan *ip address* masukan *ip publik* dari ISP Speedy 180.xxx.xxx.xxx. Atas permintaan pihak PT.Indra Jalayatra maka IP publik perusahaan yang sebenarnya tidak bisa penulis cantumkan. Selanjutnya pemilihan interface dan *ip address* untuk mengkases VPN server yaitu 192.168.7.5 protokol yang digunakan yaitu UDP dan TCP dengan port 1194 untuk UDP dan 443 untuk port TCP. Lebih jelasnya bisa dilihat di gambar IV.12 Setting IP dan Port VPN.Langkah selanjutnya konfigurasi pemilihan mode VPN disini ada 2 pilhan yang pertama Layer 2 *(Ethernet Bridging)* dan Layer 3(*routing* NAT), Layer 2 *(Ethernet Bridging)* digunakan untuk koneksi VPN site to site sedangkan Layer 3(*routing* NAT) digunakan untuk membuat *remote access* VPN, penulis memilih Layer 3(*routing* NAT) karena VPN akan digunakaan sebagai *remote acccess.*

d. Kofigurasi Port Forward

Karena VPN *Server* berada dibelakang router dan juga dibelakang proxy yang juga bertindak sebagai gateway maka konfigurasi pada router dan proxy server juga diperlukan, konfigurasi ini bertujuan agar router dan proxy server mengijinkan paket yang berasal dari luar untuk masuk kedalamnya dan kemudian langsung diarahkan ke VPN *Server*. Konfigurasi tersebut adalah konfigurasi *port forwarding* yang berguna untuk member tahu router apabila ada paket yang ditujukan ke *port* tertentu maka router akan melakukan *forwarding* ke tujuannya (VPN *Server*).

4. Kesimpulan

VPN (*Virtual Private Network)* ini memiliki keamanan yang mumpuni karena menggunakan metode *tunneling* (terowong) serta penerapan autentikasi dan untuk penggunaan pada *client* juga mudah dilakukan dengan menggunakan software atau fasilitas bawaan dari operating sistem seperti windows XP atau windows 7. Setelah melakukan analisis serta uji coba dan simulasi *Virtual Private Network* (VPN), maka dapat disimpulkan sebagai berikut:

1. Dari hasil percobaan yang dilakukan menggunakan software *sniffing* wireshark, terbukti OpenVPN Akses Server memberikan keamanan akses data yang baik.
2. Fitur *Graphical User Interface(GUI)* berbasis WEB terbukti memberikan kemudahan dalam impelemntasi baik disisi server maupun disisi klient.

E-ISSN: 2548-3412 ; 1 – 12

Ucapan Terima Kasih
Ucapan terima kasih kami sampaikan untuk Tim redaksi Jurnal ICT Bina Insani yang sudah memberikan kesempatan kepada kami dan sudah melakukan koreksi, masukan dan saran yang sangat berharga terhadap penulisan yang sudah kami lakukan.

Referensi

Astawa dkk. Implementasi Vpn Pada Jaringan Komputer Kampus Puliteknis Negri Bali. 2012 Bali. [http://p3m.pnb.ac.id/dokument/jurnal/1336100823_Arya%20Arik.pdf]

Hendra. 2006. Belajar Sendiri Cisco ADSL Router, PIX Firewall, dan VPN. Jakarta: PT. Elex Media Komputindo

Madcom. 2010. Sistem Jaringan Komputer untuk Pemula. Madiun: Andi

Markus F. 2006. OpenVPN, Building and Integrating Virtual Private Networks. Birmingham: Packt Publishing Ltd

Melwin S. 2005. Pengantar Jaringan Komputer. Yogyakarta: Andi Offset

Paulus YJ. 2012, Computer Networking, Pengaturan Jaringan, Keamanan Jaringan, Koneksi] dan sharing, Troubleshooting Jaringan. Yogyakarta: Andi

Winarto E, Zaki A, & Community. 2013. Membuat Sendiri Jaringan Komputer. Semarang: PT. Elex Media Komputindo.