Jurnal Techno Nusa Mandiri | **Vol. XII No. 1, Maret 2015**

PENERAPAN METODE OPEN VPN-ACCESS SERVER SEBAGAI RANCANGAN JARINGAN WIDE AREA NETWORK

Fikri Firmansyah[1], Mohammad Badrul[2]
Program Study Teknik Informatika[1], Program Study Sistem Informasi[2]
Sekolah Tinggi Manajemen Informatika dan Komputer(STMIK) Nusa Mandiri Jakarta
Jl. Damai No. 8 Warung Jati Barat (Margasatwa) Jakarta Selatan
Fikri.bip@gmail.com[1], Mohammad.mbl@nusamandiri.ac.id[2]

ABSTRACT

The development of information technology has developed rapidly from year to year. The use of the Internet as a very useful addition to mediation communications but still has weaknesses in its security.Ecosystem service assurance is one unit of work on solution division convergance PT. Telekomunikasi Indonesia, Tbk. can not be separated from the use of networks and the Internet for Operational work Units. kendal faced by the few employees Units Ecosystem Service Assurance often get assignments meetings and training outside of town. Sometimes employees get into trouble when had to send the data documentation of meetings and training to upload a file in a web application portal Unit Ecosystem Service Assurance by using email, copy and save the file first before uploading, this method is not very safe and effective. needed a way to connect the mobile intranet access with the existing LAN network at the central office in order to perform data access easily and safely. Solutions that can be used for this problem is to build a network Wide Area Network (WAN) technology with a Virtual Private network applications that can use OpenVPN Access Server. OpenVPN Access Server delivers ease and security in forming a network of virtual private network

Keyword: *computer networkings, Virtual Private network,* OpenVPN-Access Server.

PENDAHULUAN

Jaringan komputer memberikan kemampuan sebagai media komunikasi yang dapat mempercepat proses kerja baik dari segi waktu maupun ruang. 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 terbataskan oleh ruang 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. untuk itu dalam pemanfaatan internet sebagai media transmisi data perlu dilakukan peningkatan keamanannya.

Unit *Ecosystem Service Assurance* PT. Telekomunikasi Indonesia, merupakan salah satu Unit yang menguji coba, menangani beberapa gangguan dan layanan baru di Telkom untuk di kembangkan dan di jual, dimana semua aktifitas pengelolaan dan penanganan gangguan aplikasi harus menggunan jaringan intranet lokal kantor pusat, untuk menjaga keamana data. Beberapa tim dari Unit *Ecosystem Service Assurance* PT. Telekomunikasi Indonesia sering mendapatkan tugas rapat dan pelatihan diluar kota. Terkadang karyawan mendapatkan kesulitan saat harus mengirimkan data dokumentasi hasil rapat dan pelatihan untuk meng*upload file* di aplikasi web portal Unit *Ecosystem Service Assurance* PT. Telekomunikasi Indonesia, maka untuk bisa tetap menjalankan aktifitasnya, para karyawan membutuhkan suatu cara untuk menghubungkan akses intranet yang bersifat *mobile* dengan jaringan LAN yang ada di kantor pusat agar bisa melakukan akses data dengan mudah dan aman. Untuk menjawab masalah tersebut penulis mengusulkan untuk membangun sebuah jaringan WAN dengan teknologi *Virtual* yang lebih dikenal dengan VPN (*virtual Private network*)

Banyak teknologi *software* dan *hardware* yang bisa dipakai untuk mengembangkan VPN ini. Dari teknologi yang *opensource* 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. dalam implementasi dan penggunaanya relatif mudah karena sudah menggunakan *Grapical User Interface(GUI)* berbasis WEB.

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 media 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 dan Atmaja(2009:58))

BAHAN DAN METODE

Jaringan komputer adalah "suatu sistem yang menghubungkan komputer menggunakan suatu teknologi transmisi data", wagito,2005. 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.

A. LAN

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 (wagito,2005).

B. MAN

Menurut MAN adalah sebuah jaringan komputer besar yang mencangkup sebuah kota atau sebuah kampus besar. MAN biasanya merupakan gabungan dari LAN yang menggunakan teknologi *backbone* berkecepatan tinggi dan menyediakan layanan ke jaringan yang lebih besar seperti WAN dan *Internet*(wagito,2005)..

C. WAN

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.

D. VPN

Menurut Iwan Sofana (2012) VPN boleh jadi termasuk ke dalam salah satu kandidat WAN. Namun, VPN menggunakan WAN sebagai media transportasi data. VPN atau *Virtual Private Network* adalah teknologi jaringan komputer yang memanfaatkan media komunikasi publik (*open connection* atau *virtual circuits*), seperti *internet*, untuk menghubungkan beberapa jaringan lokal. Informasi yang berasal dari *node-node* VPN akan "dibungkus" (*tunneled*) dan kemudian mengalir melalui jaringan publik. Sehingga informasi menjadi aman dan tidak mudah dibaca oleh yang lain.

Umumnya VPN diimplementasikan oleh lembaga/perusahaan besar. Biasanya perusahaan semacam ini memiliki kantor cabang yang lokasinya cukup jauh dari kantor pusat. Sehingga diperlukan solusi yang tepat untuk mengatasi keterbatasan LAN. VPN dapat menjadi sebuah pilihan yang cukup tepat. Tentu saja VPN boleh diimplementasikan oleh pengguna rumah atau oleh siapa pun yang membutuhkannya.

Menurut Iwan Sofana (2012:229) VPN sendiri memiliki beberapa jenis, VPN yang

biasa dikenal adalah *Remote-Access VPN* dan *Site-to-Site VPN*.

1. *Remote Access* VPN

Remote access VPN disebut juga *Virtual Private Dial-up Network* (VPDN). VPDN adalah jenis *user-to*-LAN *connection*. Artinya, user dapat melakukan koneksi ke *private network* dari manapun, apabila diperlukan. Biasanya VPDN dimanfaatkan oleh karyawan yang bekerja di luar kantor. Mereka dapat memanfaatkan komputer laptop yang sudah dilengkapi perangkat tertentu untuk melakukan koneksi dengan jaringan LAN dikantor.

2. *Site-to-Site* VPN

Site-to-site VPN diimplementasikan dengan memanfaatkan perangkat *dedicated* yang dihubungkan *via internet. Site-to-site* VPN digunakan untuk menghubungkan berbagai *area* yang sudah *fixed* atau tetap, misal kantor cabang dengan kantor pusat. Koneksi antara lokasi-lokasi tersebut berlangsung secara menerus (24jam) sehari.

Menurut Iwan Sofana (2012:31) untuk mengamankan informasi yang berasal dari jaringan internal, VPN menggunakan beberapa metode *security*, seperti *Firewall yang* menyediakan "penghalang" antara jaringan lokal dengan *internet*. Pada *firewall* dapat ditentukan *port – port* mana saja yang boleh dibuka, paket apa saja yang boleh melalui *firewall*, dan protokol apa saja yang dibolehkan.

a. Enkripsi

Enkripsi merupaka metode yang umum untuk mengamankan data. Informasi akan "acak" sedemikian rupa sehingga sukar dibaca oleh orang lain. Secara umum ada dua buah metode enkripsi yaitu : *Symmetric-key encryption* dimana metode ini masing-masing komputer pengirim dan penerima harus memiliki "*key*" yang sama, *Public-key encryption* yang mana metode ini Komputer pengirim menggunakan *publik-key* milik komputer penerima untuk melakukan enkripsi.

b. IPSec

Internet Protocol Security Protocol (IPSec) menyediakan fitur *security* yang lebih baik. Seperti algoritma enkripsi yang lebih bagus dan *comprehensive authentication*. IPSec menggunakan dua buah mode enkripsi, yaitu *Tunnel* yang melakukan enkripsi pada *header* dan *payload* masing – masing paket.dan *Transport yang* hanya melakukan enkripsi pada *payload* masing – masing paket.

Secara umum ada dua buah asumsi yang digunakan untuk menentukan *security* pada VPN. Yang pertama yaitu dengan mempercayai bahwa *network* yang digunakan aman atau dapat dipercaya. Ini yang disebut sebagai *trusted* model. Yang kedua adalah sebaliknya, diasumsikan *network* tidak aman sehingga diperlukan mekanisme *security* tertentu. Ini yang disebut *secure* model.

Autentikasi merupakan proses untuk memastikan data dikirim kepada penerima yang diinginkan. Sebagai tambahan, autentikasi juga memastikan integritas penerima dari pesan dan sumbernya. Dalam bentuk yang paling sederhana, autentikasi memerlukan paling sedikit *username* dan *password* untuk menerima akses ke sumber spesifik. Dalam bentuk yang kompleks, autentikasi dapat didasari dari *secret-key encryption* atau *public-key encryption*. Autorisasi merupakan proses memberikan atau menolak akses ke sumber yang berlokasi dalam jaringan setelah pengguna telah berhasil diidentifikasi dan diautentiksi.

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.

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 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)

E. 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.

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.

F. *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)

G. 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.

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.

Certificate Revocation List (CRL) dapat digunakan untuk melakukan pencabutan sertifikat yang dipunyai *client* yang tidak diperbolehkan untuk melakukan koneksi dengan VPN. Koneksi akan ditolak apabila tidak ada sertifikat yang dimaksud, sertifikat yang berbeda dan memiliki CA yang salah, sertifikat yang telah dicabut haknya sebelumnya. Sertifikat-sertifikat ini dapat digunakan untuk berbagai macam tujuan. HTTPS dan OpenVPN adalah hanya dua aplikasi yang menggunakan ini dari berbagai macam aplikasi lainnya. Markus Feilner (2006)

H. 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.

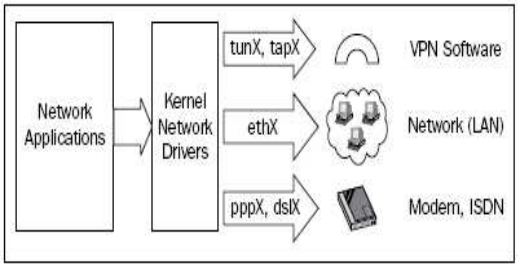
Struktur modular dari OpenVPN tidak hanya bisa ditemukan dalam model keamanannya sendiri, tetapi juga bisa ditemukan di dalam kerangka jaringan. **James Yonan** memilih *driver Universal* TUN/TAP untuk lapisan jaringan dari OpenVPN.

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 dibandingankan 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 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).

Analisa penelitian yang dilakukan terdiri dari :

a. Analisa Kebutuhan

Dalam analisa kebutuhan ini penulis mencoba menyiapkan analisa kebutuhan seperti:

1. Jurnal
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.

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.

HASIL DAN PEMBAHASAN

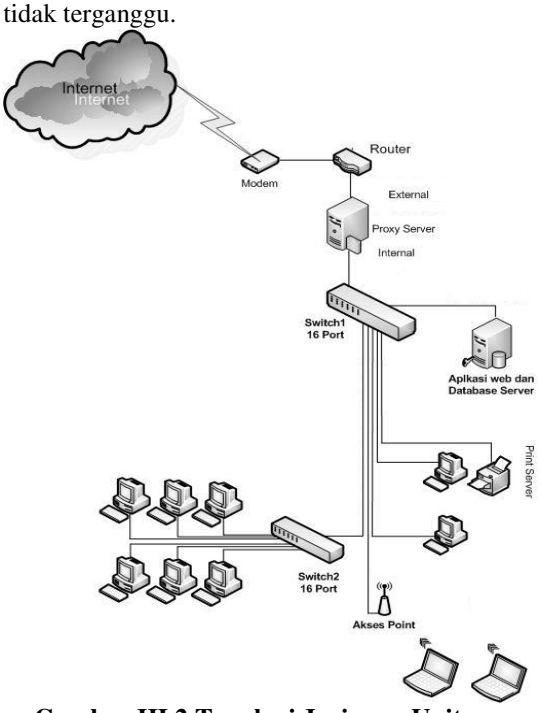
Dalam pembahasan ini penulis membahas tentang jaringan yang sedang diterapkan di perusahaan dan usulan jaringan yang penulis usulkan.

A. 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 Unit *Ecosystem Service Assurance* 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.



Gambar III.2 Topologi Jaringan Unit *Ecosystem Service Assurance*

2. Arsitektur Jaringan

Arsitektur jaringan yang digunakan pada Unit *Ecosystem Service Assurance* 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. Misalnya, 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 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 Unit *Ecosystem Service Assurance* 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 Unit *Ecosystem Service Assurance*

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 Unit *Ecosystem Service Assurance*. Unit *Ecosystem Service Assurance* juga menggunakan akses *point* untuk menghubungkan perangkat jaringan melalui media *wireless* seperti laptop dan perlangkat wireless lainnya.

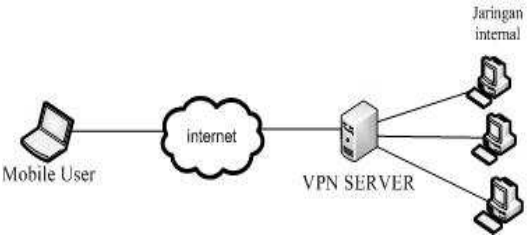
Untuk aksses internet Unit *Ecosystem Service Assurance* menggunakan jasa ISP Speedy dari PT. Telkom dengan bandwidth sebesar 2Mbps yang dishare ke semua *client* di jaringan internal Unit *Ecosystem Service Assurance* melalui *Proxy server*. Akses *internet* ini sangat vital peranannya karena digunakan untuk komunikasi terutama dalam penggunakan *e-mail* dan *messenger. E-mail* digunakan untuk komunikasi dengan *client* yang bekerjasama dengan Unit *Ecosystem Service Assurance* untuk transaksi bisnis. *E-mail* juga digunakan untuk mengirim laporan kepada para mitra kerja Telkom dan *Project Owner*.

B. Jaringan Usulan dari Penulis

Seperti yang sudah penulis dijelaskan dalam bab sebelumnya yaitu agar para pegawai Unit *Ecosystem Service Assurance* bisa akses jaringan Lokal melalui jaringan publik maka penulis mengusulkan untuk menambahkan *virtual private network* server pada jaringan Unit *Ecosystem Service Assurance*. *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. Pembahasan jaringan 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 Unit *Ecosystem Service Assurance* 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 Unit *Ecosystem Service Assurance* dari jaringan publik. Berikut penulis sajikan gambar topologi jaringan



Sumber:hasil penelitian, 2014

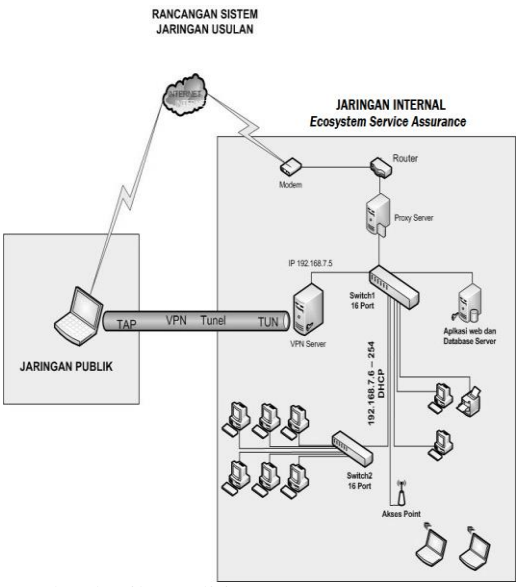
Gambar 3. Topologi jaringan usulan

2. 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 Unit *Ecosystem Service Assurance*. 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*.

.



Sumber:hasil penelitian, 2014

Gambar IV.2 Skema Jaringan Usulan

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.*

1. 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). Yang pertama dilakukanya yaitu mengunduh file instalasi OpenVPN-Access Server pada website openvpn.net dengan mengetikan perintah:

wget http://swupdate.openvpn.org/as/openvpn- as-1.8.5 Ubuntu12.amd_64.deb

Setelah proses unduh selesai diteruskan dengan proses instalasi dengan mengetikan:

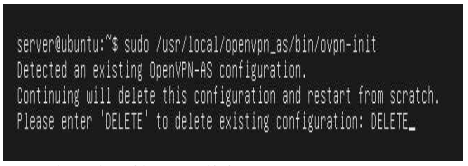
dpkg –i openvpn-as-1.8.5 Ubuntu12.amd_64.deb

Setelah instalasi selesai maka masuk ke tahap konfigurasi.

2. Konfigurasi VPN Server

Setelah tahap instalasi selesai maka masuk ke tahap konfigurasi, berikut ini langkah-langkahnya:

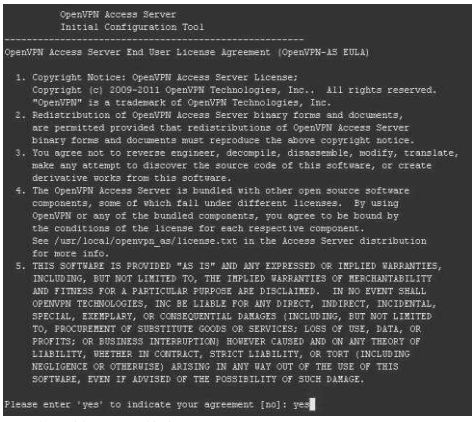
Ketik **sudo /usr/local/openvpn_as/bin/ovpn-init** kemudian akan tampil pertanyaan apakan akan menghapus konfigurasi sebelumnya, ketik DELETE untuk menghapus konfigurasi dan memulai konfigurasi ulang OpenVPN-Access Server.



Sumber:hasil penelitian, 2014

Gambar 5. Konfigurasi Awal

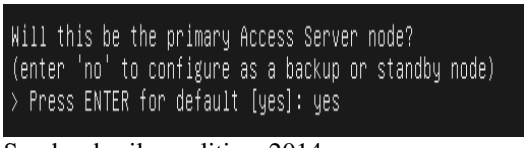
Dilanjutkan dengan pertanyaan persetujuan *License Agreement,* ketik *yes* yang menyatakan bahwa kita menyetujui dengan syarat dan ketentuaan dari OpenVPN-access server.



Sumber:hasil penelitian, 2014

Gambar 6. *License Agreement* OpenVPNAccess Server

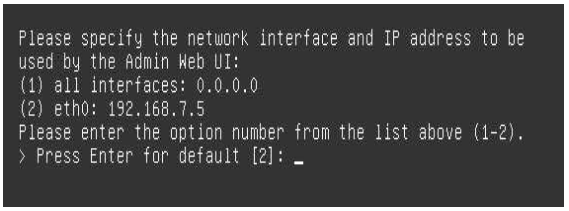
Dilanjutkan dengan pertanyaan apakan server ini digunakan untuk server utama, jawab yes karena penulis akan memfungsikan sebagai server utama bukan server backup.



Sumber:hasil penelitian, 2014

Gambar 7. Pemilihan Fungsi Server

Dilanjutkan dengan pemilihan *interface* dan *ip address* yang digunakan untuk mengakses Admin UI:

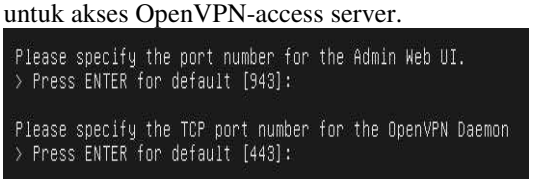


Sumber:hasil penelitian, 2014

Gambar 7 Pemilihan Interface dan IP Address

Pilih yang ke dua (2) eth0 dengan ip address 192.168.7.5.

Setelah pemilihan *interface* dan *ip address* maka pertanyaan selanjutnnya pemilihan port untuk akses OpenVPN-access server.

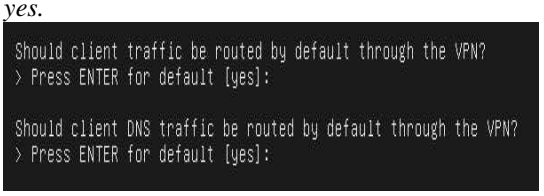


Sumber:hasil penelitian, 2014

Gambar 8. Pemilihan Port VPN

Default-nya *port* 943 digunakan untuk mengakses admin web UI dan *port* 443 untuk OpenVPN Daemon, *port* ini bisa diubah sesuai kebutuhan, untuk percoban kali ini penulis menggunakan *port default.*

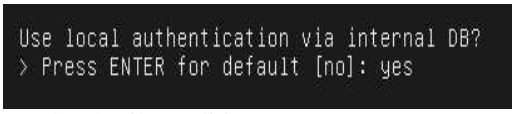
Selanjutnya untuk konfigurasi routing dan DNS, konfigurasi ini menentukan apakah *traffic* bisa masuk ke jaringan lokal yang ada di belakang VPN server, karena tujuan awal penulis yaitu agar para pekerja yang berada diluar Kantor Mediatron bisa mengakses jaringan lokal maka dalam tahap ini jawab *yes.*



Sumber:hasil penelitian, 2014

Gambar 9. Routing dan DNS

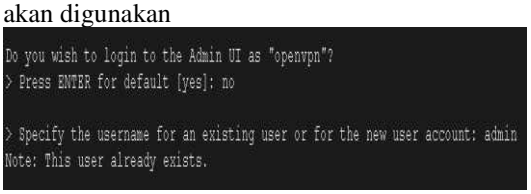
Selanjutnya pertanyaan apa akan menggunakan user internal dari database OpenVPN-Access Server, jika jawabannya NO authentikasi user akan menggunakan usermane dan password yang sudah ada di sistem operasi ubuntu untuk bisa login ke OpenVPN-access server sedangakan jika dijawab YES maka harus membuar user baru di database OpenVPN.



Sumber:hasil penelitian, 2014

Gambar 10. Pemilihan User untuk Akses OpenVPN-Access Server

Pada tahap selanjutnya membuat user untuk akses Admin web UI user ini gunakan untuk masuk ke halaman konfigurasi Web UI dan melakukan konfigurasi VPN server. pada tahap ini isikan username dan password yang akan digunakan



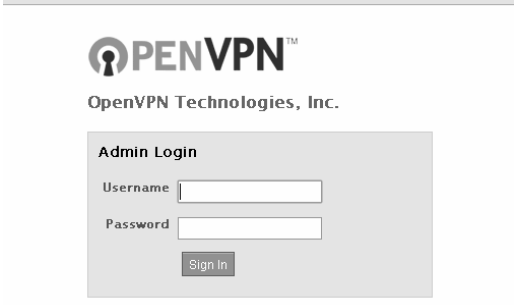
Sumber:hasil penelitian, 2014

Gambar 11 Pemilihan User Untuk Akses Admin Web UI

Setelah pengaturan selesai maka kita dapat lanjutkan konfigurasi melalui Admin Web UI dengan mengetikan alamat IP VPN server di aplikasi browser seperti firefox atau chrome.

3. Konfigurasi OpenVPN Server di Web UI

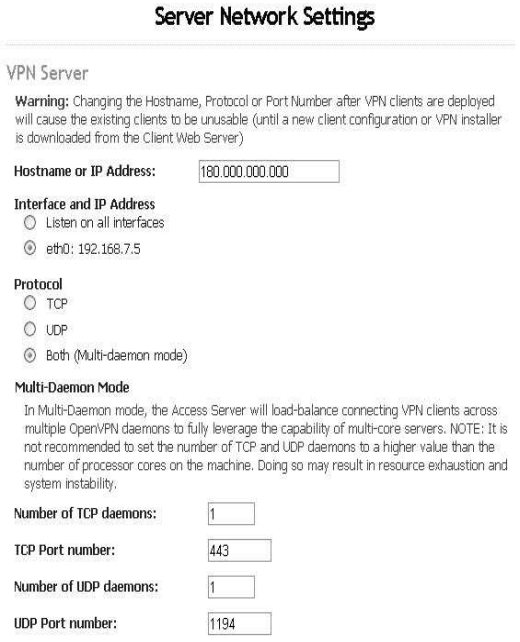
Untuk masuk ke konfigurasi Web UI bisa menggunakan komputer lain yang satu jaringan dengan server VPN, gunakan aplikasi browser mozila firefox, chrome atau browser lainnnya dalam hal ini penulis menggunakan browser chrome. Ketik alamat: https://192.168.100.1/admin di *address* browser maka akan muncul halaman login seperti pada gambar IV.11



Sumber:hasil penelitian, 2014

Gambar 12. Halaman Login Admin Web UI

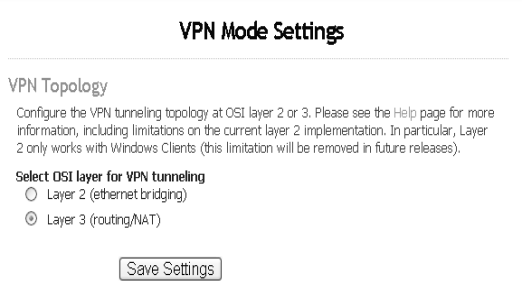
Langkah selanjutnya melakukan pengaturan VPN Server, meliputi setting IP publik, pemilihaan *port* dan *interface* yang digunakann untuk akses VPN. Untuk pengaturan *host name* dan *ip address* masukan *ip publik* dari ISP Speedy 180.xxx.xxx.xxx. Atas permintaan pihak Mediatron maka IP publik perusahaan 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.`



Sumber:hasil penelitian, 2014

Gambar 13. Setting IP dan Port VPN

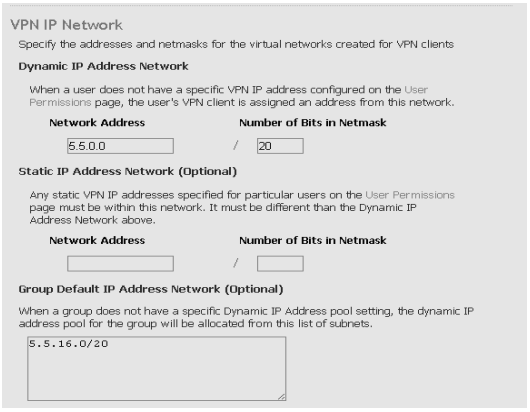
Langkah selanjutnya konfigurasi pemilihan mode VPN disini ada 2 pilhan yang pertama Layer 2 *(Ethernet Bridging)* dan Layer 3(*routing* NAT), Layer 2 *(Ethernet Bridging)* digunakan untuk koneksi VPN site to site sedangkan Layer 3(*routing* NAT) digunakan untuk membuat *remote access* VPN, penulis memilih Layer 3(*routing* NAT) karena VPN akan digunakaan sebagai *remote acccess.*



Sumber:hasil penelitian, 2014

Gambar 14. Pemilihan Mode VPN

Berikutnya menentukan alamat IP untuk diberikan ke *virtual netwok interface* Tun dan Tap pada sisi server dan pada sisi klien. Ada 2 (dua) pilihan untuk pemberian IP address ke ke *virtual netwok interface* Tun dan Tap yaitu Ip dinamik dan ip statik, jika dipilih ip statik setiap user melakukan koneksi maka IP yang didapat klien akan tetap tidak berubah, tapi jika menggunakan ip dinamik maka setiap klien melakukan koneksi akan mendapat ip baru. Secara default Ip yang diberikan adalah 5.5.0.0/20, ip ini bisa dirubah sesuai kebutuhan.



Sumber:hasil penelitian, 2014

Gambar 15. Setting IP Addres untuk Virtual Network Interface Tun/Tap

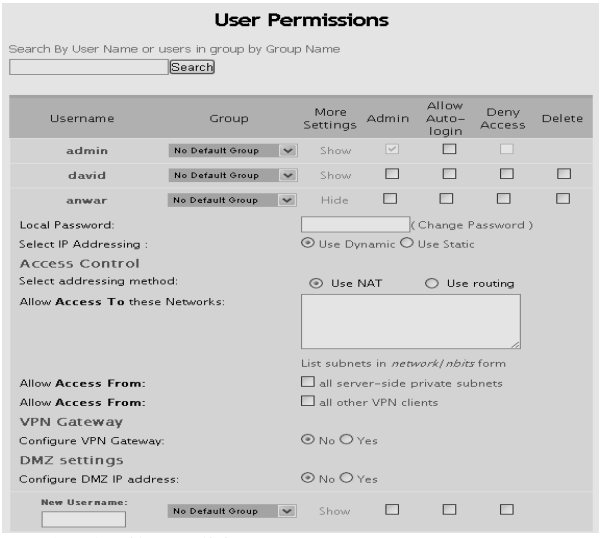
Langkah selanjutnya yaitu membuat user yang akan diberikan ijin untuk bisa koneksi dengan VPN server ada beberapa point yang perlu diisikan yaitu:

User Name: isikan mana pengguna yang akan terhubung ke VPN server

Local Password: isi password yang akan digunakan untuk authentikasi

Allow auto login: diceklist agar VPN klien bisa login secara automatis

Access Control: pilih USE NAT, dengan memilih NAT VPN Klien dapat mengakses subnet pribadi, dan alamat virtual setiap VPN Klien ditransformasikan melalui NAT sehingga alamat IP Access Server host digunakan sebagai alamat sumber pada paket klient yang ditujukan untuk subnet pribadi.

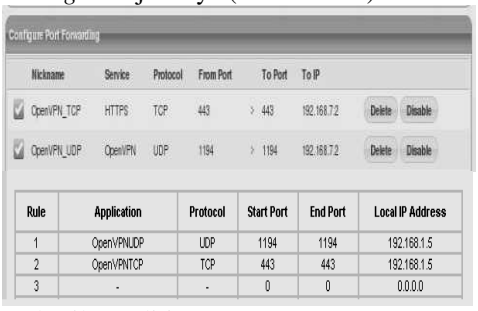


Sumber:hasil penelitian, 2014

Gambar 16 Membuat User VPN

4. 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*).



Sumber:hasil penelitian, 2014

Gambar 17. Port Forward pada Proxy server dan Modem

Berikut penulis jelaskan langka-langkanya untuk port forward pada modem dan proxy server.

a. *Port Forward* Pada Modem Tp-Link

Pertama login untuk masuk ke konfigurasi modem menggunakan browser ketik IP modem dalam kali ini Ip modem yang penulis gunakan 192.168.1.1, setelah

masuk ke konfigurasi modem lalu pilih advance setup kemudan pilh NAT kemudan pilh virtual server, pertama port forward untuk port UDP, pilih rule index 1, pada kotak *aplication* isikan nama service OpenVPNUDP yang akan digunakan. pada kolom protokol pilih UDP, start port number dan end port number isikan dengan 1194 pada kolom To IP isikan alamat dari *proxy server* dan pilih save. Langkan untuk port forward untuk port TCP pilih rule index 2 isikan nama service OpenVPNTCP yang akan digunakan. pada kolom protokol pilih TCP, start port number dan end port number isikan dengan 443, pada kolom To IP isikan alamat ip dari *proxy server* dan pilih save untuk menyimpan konfigurasi

b. *Port Forward* Pada *Proxy Server*

Masuk ke porxy server melalui browser kemudan ketik alamat ip proxy server 192.168.7.1, setelah masuk ke menu konfigurasi pilih network > firewall, yang pertama setting port forward untuk port UDP. Pada kolom nick name isikan dengan mana OpenVPNUDP kemudan pilih protokol UDP, isikan kolom *from port* dan *to port* dengan angka 1194. Pada kolom *local address* isikan dengan IP VPN server kemudan klik add, untuk *port forward* port TCP pada kolom nick name isikan dengan mana OpenVPNTCP kemudan pilih protokol TCP, isikan kolom *from port* dan *to port* dengan angka 443 pada kolom local address isikan dengan IP VPN server kemudan klik add.

DAFTAR PUSTAKA

Astawa, I Nyoman Gede Arya, I Made Ari Dwi Suta Atmaja. 2012. Implementasi Vpn Pada Jaringan Komputer Kampus Puliteknis Negri Bali. Bali.

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

Sofana, Iwan. 2009. Cisco CCNA dan Jaringan Komputer Edisi Revisi. Bandung: Informatika.

Syafrizal, Melwin. 2005. Pengantar Jaringan Komputer. Yogyakarta: Andi Offset

Wagito. 2005. Jaringan Komputer, Teori dan Implementasi Berbasis Linux. Yogyakarta: GAVA MEDIA