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

Burhanuddin[1], Mohammad Badrul[2]
Program Studi Teknik Informatika[1], Program Studi Sistem Informasi[2]
Sekolah Tinggi Manajemen Informatika dan Komputer(STMIK) Nusa Mandiri Jakarta
Jl. Damai No. 8 Warung Jati Barat (Margasatwa) Jakarta Selatan
Burhanudin46@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 communication mediation in addition to very useful but still has flaws in its security. PT. Valdo International to build a computer network to facilitate the conduct of operations, such as Rejuvenation application systems and other purposes. we need a way to connect to the intranet access existing LAN network at headquarters and branch offices in order to be able to access data easily and safely. , Data information is not safe to be in the public network because it can be intercepted by unauthorized parties. Therefore PT. Valdo International build VPN (Virtual Private Network) using the PPTP mirkrotik with lines, and can perform other operations in private in the public network, with connections an economical and secure data security.

Keyword: *computer networkings, Virtual Private network, pptp*.

ABSTRAK

Perkembangan teknologi informasi mengalami perkembangan yang pesat dari tahun ketahun. Penggunaan internet sebagai suatu mediasi komunikasi selain sangat bermanfaat namun tetap memiliki kelemahan dalam keamanannya. PT. Valdo International membangun jaringan komputer untuk mempermudah melakukan kegiatan operasional, seperti Peremajaan sistem aplikasi dan keperluan lainnya. dibutuhkan suatu cara untuk menghubungkan akses intranet dengan jaringan LAN yang ada di kantor pusat dan kantor cabang agar bisa melakukan akses data dengan mudah dan aman. Data informasi tidak aman berada di jaringan publik karena dapat disadap oleh pihak yang tidak berkepentingan. Oleh karena itu PT. Valdo International membangun jaringan *VPN (Virtual Private Network)* menggunakan mirkrotik dengan jalur *PPTP*, dan dapat melakukan kegiatan operasional lainnya secara *private* di dalam jaringan publik, dengan koneksi yang ekonomis dan keamanan data yang terjamin.

Kata Kunci : Jaringan, *Virtual Private network,* PPTP

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.

PT. Valdo International adalah perusahaan yang bergerak di bidang *Outsourcing Tele Marketing* bank dan asuransi yang selalu memperhatikan kebutuhan klien akan keamanan data di internet. Ketika klien melakukan pertukaran informasi data, hal ini sangat memungkinkan ada pihak yang melakukan pencurian selama data ditransmisikan di internet.

Salah satu cara untuk membangun keamanan komunikasi data dalam jaringan internet adalah dengan menggunakan jaringan *Virtual Private Network (VPN).* Teknologi *Virtual Private Network (VPN*) memungkinkan user yang berada di lokasi

berbeda dapat mengakses sumber daya yang berada dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama seperti secara fisik berada di tempat dimana jaringan lokal itu berada

Karena Masalah yang sering muncul di PT. Valdo Internasional adalah ketika IT Program ingin mengakses sebuah alamat web yang sifatnya lokal menggunakan aplikasi *teamviewer,* dan membuituhkan *bandwitch* internet yang cukup besar dan terkadang mengalami koneksi akses internet lambat dan tidak seperti yang diharapkan, dengan adanya *Virtual Private Network (VPN)* IT Program yang memakai VPN akan lebih mudah dalam mengakses aplikasi lokal.

PT. Valdo Internasional menggunakan salah satu *provider* internet TACHYON dengan besaran *Bandwidth*-nya 10 Mbps. Dengan paket tersebut diharapkan dapat mencukupi kebutuhan koneksi internet untuk semua user dan membangun jaringan *Virtual Private Network (VPN).*

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). *Local Area Network* (LAN) adalah jaringan komputer yang jaringannya hanya mencakup wilayah kecil, seperti jaringan komputer kampus, gedung, kantor, dalam rumah, sekolahan atau yang lebih kecil. Saat ini, kebanyakan 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 Wi-fi) juga sering digunakan untuk membentuk LAN. Tempat-tempat yang menyediakan koneksi LAN dengan teknologi Wi-fi biasa disebut *hotspot* (aditya,2011).

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). 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). Metropolitan Area Network* (MAN) suatu jaringan dalam suatu kota dengan transfer data berkecepatan tinggi, yang menghubungkan berbagai lokasi seperti kampus, perkantoran, pemerintahan, dan sebagainya(aditya,2011). 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

C. WAN

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. 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[5]. *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. 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 computer dilokasi yang lain(aditya,2011).

D. IP ADDRESS

IP Address merupakan singkatan dari *Internet Protocol Address*, *IP Address* adalah identitas numeric yang diberikan kepada suatu alat seperti komputer, router atau printer yang terdapat dalam suatu jaringan komputer yang menggunakan internet protokol sebagai sarana komunikasi, *IP Address* memiliki dua fungsi yaitu (Winarto, Zaki, & Community, 2013) :

1. Sebagai alat identifikasi host atau antarmuka pada jaringan.
2. Sebagai alamat lokasi jaringan.

IP Address sendiri memakai system bilangin 32 bit, system ini dikenal dengan nama *Internet Protocol* version 4 atau IPv4. Saat ini IPv4 masih ramai digunakan, untuk memudahkan dalam pembagiannya maka *IP Address* dibagi ke dalam kelas-kelas yang berbeda, yaitu sebagai berikut :

1. Kelas A

IP Address kelas *A* terdiri atas 8 bit untuk network ID dan sisanya 24 bit digunakan untuk host ID, sehingga *IP Address* kelas A digunakan untuk jaringan dengan jumlah host sangat besar. Pada bit pertama diberikan angka 0 sampai dengan 127.

2. Kelas B

IP Address kelas *B* terdiri atas 16 bit untuk network ID dan sisanya 16 bit digunakan untuk host ID, sehingga *IP Address* kelas B digunakan untuk jaringan dengan jumlah host tidak terlalu besar. Pada 2 bit pertama, diberikan angka 10.

3. Kelas C

IP Address kelas *C* terdiri atas 24 bit untuk network ID dan sisanya 8 bit digunakan untuk host ID, sehingga *IP Address* kelas C digunakan untuk jaringan berukuran kecil. Kelas C biasanya digunakan untuk jaringan *Local Area Network* atau LAN. Pada 3 bit pertama, diberikan angka 110 .

Kelas *IP Address* lainnya adalah D dan E, namun kelas IP D dan E tersebut tidak digunakan untuk alokasi IP secara normal tetapi digunakan untuk *IP multicasting* dan untuk eksperimental.

Nilai *subnet mask* berfungsi untuk memisahkan *network ID* dengan *host ID.* Subnet mask diperlukan oleh TCP/IP untuk menentukan, apakah jaringan yang dimaksud adalah jaringan lokal atau nonlokal. Untuk jaringan Nonlokal berarti TCP/IP harus mengirimkan paket data melalui sebuah Router. Dengan demikian, diperlukan *address mask* untuk menyaring *IP Address* dan paket data yang keluar masuk jaringan tersebut.

Network ID dan host ID didalam *IP Address* dibedakan oleh penggunaan subnet mask. Masing-masing subnet mask menggunakan pola nomor 32-bit yang merupakan *bit groups* dari semua satu (1) yang menunjukkan *network ID* dan semua nol (0) menunjukkan *host ID* dari porsi *IP Address*(madcom,2010).

E. VPN

(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 (Sofana,2012) 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.

(Sofana,2012) 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)

Dalam memudahkan pembuatan dan pengumpulan data-data yang diperlukan dalam penelitian ini, maka peneliti menggunakan metode penelitian sebagai berikut :

1. Teknik Pengumpulan Data

Teknik yang dilakukan untuk pengumpulan data adalah sebagai berikut :

a. Observasi
   Penulis melakukan pengamatan langsung dalam membangun server yang akan digunakan sebagai VPN dan di perusahaan tempat penulis melakukan penelitian.
b. Wawancara
   Penulis melakukan proses wawancara dalam membangun server VPN dan melakukan tanya jawab terhadap pokok persoalan yang ada dalam penelitian yang penulis ambil.
c. 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.

2. Analisa Penelitian

Analisa penelitian yang dilakukan dengan metode water fall terdiri dari :

a. Analisa Kebutuhan
   Penelitian ini menggunakan pemodelan jaringan untuk mensimulasikan sistem VPN Server sebagai Jaringan pribadi di dalam perusahaan. Kebutuhan untuk dibangunnya server VPN berguna untuk pemakaian koneksi internet agar dapat menggunakan akses internet sesuai kebutuhan yang diperlukan yang dimana dibutuhkan perangkat lunak dan perangkat keras.
b. Desain
   Tahap pertama dalam pembuatan server VPN tersebut adalah melakukan desain rancangan jaringan yang akan dibangun dan menyiapkan perangkat Mikrotik.
c. Testing
   Untuk tahap testing akan dilakukan di PT. Valdo Internasional yang akan menggunakan Server VPN. VPN Server akan bekerja sesuai dengan *User account* yang telah di daftarkan dan *Accesst Control List* berdasarkan IP Address ataupun alamat website yang di daftarkan pada Access Control List (ACL) untuk Proxy Server.
d. Implementasi
   Server VPN ini akan di implementasikan di PT. Valdo Internasional dimana server VPN ini difungsikan sebagai VPN dan Proxy Server yang berfungsi sebagai penghubung jaringan internal dengan menggunakan akses internet dan filter

dalam penggunaan internet yang digunakan oleh user setiap hari.

HASIL DAN PEMBAHASAN

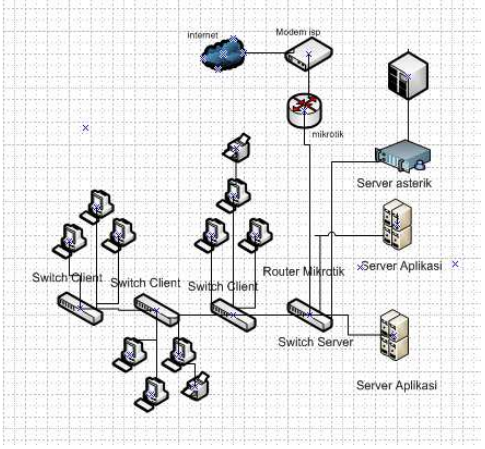
Dalam pembahasan ini penulis membahas tentang jaringan yang sedang diterapkan di perusahaan dan usulan jaringan yang penulis usulkan.

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 PT. Valdo Internasional adalah ketika IT Program ingin mengakses sebuah alamat web yang sifatnya lokal menggunakan aplikasi *teamviewer,* dan membuituhkan *bandwitch* internet yang cukup besar dan terkadang mengalami koneksi akses internet lambat dan tidak seperti yang diharapkan . *Traffic* data mengalir dari *node* ke *central node* dan kembali lagi dan juga jika salah satu kabel *node* terputus yang lainnya tidak terganggu.



Gambar 1 Topologi Jaringan awal

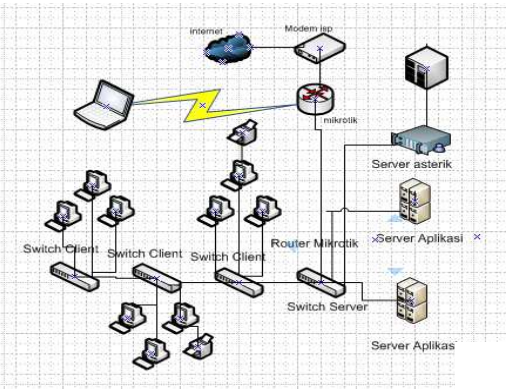
B. Jaringan Usulan dari Penulis

Seperti yang sudah penulis dijelaskan dalam bab sebelumnya yaitu agar para pegawai bisa akses jaringan Lokal melalui jaringan publik maka penulis mengusulkan untuk menambahkan *virtual private network* server pada jaringan. *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

Penulis mengusulkan untuk menambahkan sebuah *VPN server* dengan mikrotik sebagai keamanan jaringan yang berada di dalam PT. Valdo Internasional untuk membatasi dan memonitoring penggunaan akses internet sedangkan untuk *bandwith* internet yang sudah digunakan untuk koneksi internet sebesar 10 Mbps sudah cukup. Dan membutuhkan perangkat keras untuk membangun sebuah *VPN server* yaitu mikrotik sedangkan untuk infrastruktur yang sudah ada didalam PT. Valdo Internasional hanya tinggal dikonfigurasi sedikit untuk melakukan penyesuaian dengan pertumbuhan yang ada..

Topologi jaringan usulan yang digunakan mengalami perubahan dari topologi jaringan yang sedang berjalan, dimana topologi jaringan usulan menggunakan VPN pada configurasi mikrotik



Sumber:hasil penelitian, 2014

Gambar 2. Topologi jaringan usulan

C. Perancangan Aplikasi

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

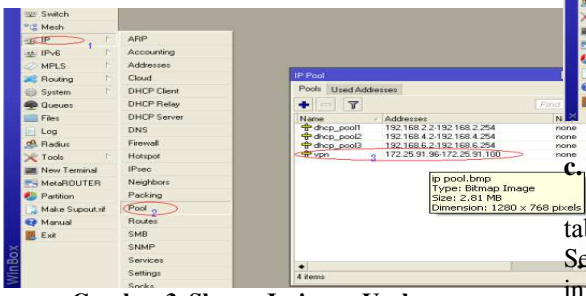
Dalam mengaktifkan Fitur PPTP server ada beberapa tahapan. Parameter -parameter yang di setting :

1. Pebuatan ip pool

Pembuatan ip pool di buat untuk membatasi berapa jumlah ip yang akan kita berikan pada klien yang akan di daftarkan pada pembuatan PPTP Server di dalam mikrotik, berikut langkah-langkah untuk membuat ip pool pada mikrotik .

- Masuk kedalam menu winbox
- Pilih tombol IP, selanjutnya POOL, kemudian kita klik tombol +(plus), untuk

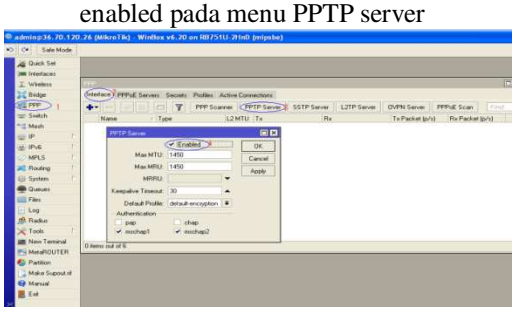
membuat IP POOL, yaitu ip yang akan kita berikan pada klien, dengan contoh ip yang saya buat 172.25.91.96-172.25.91.100, berarti jumlah klien yang bias kita daftarkan hanya 6 (enam) user saja, dengan contoh gambar sebagai berikut



Gambar 3. Skema Jaringan Usulan

a. Membuat VPN dengan PPTP Server dalam hal ini penulis membuat VPN dengan teknologi PPTP, berikut cara pembuatan PPTP Server

- Masuk ke tombol PPTP
- Pilih interface, kemudian PPTP Server, dan akan tampil kolom baru, ceklis enabled pada menu PPTP server

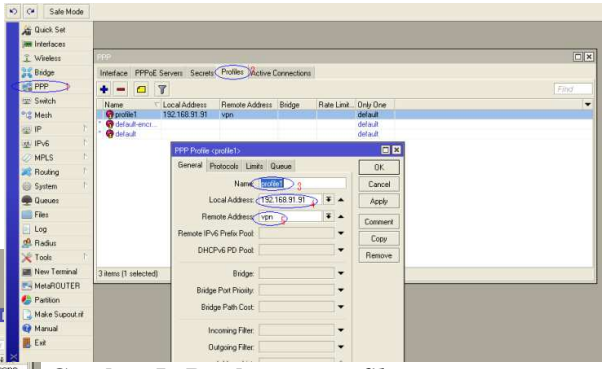


Gambar 4. Pemilihan akses vpn PPTP Server

b. Membuat PPP Profil

PPP profil berfungsi untuk menempatkan ip pool yang sudah kita buat di tahap ke 1 (Pertama), untuk pembuatan PPTP profil sebagai berikut,

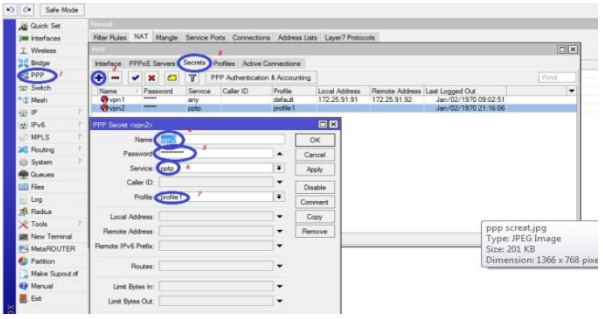
- Pilih tombol PPP
- Kemudian pilih Profil, General, masukan Name dengan contoh PROFIL1, kemudian Local Address denagn contoh 172.25.91.91 dan remote address kita pilih interface VPN yang sudah kita buat di ip pool di tahap ke 1 (pertama), pengertian dari local address yaitu pengalamatan ip address vpn server, sedangkan remote address yaitu ip yang di sediakan untuk klien dengan contoh gambar sebagai berikut



Gambar 5. Pembuatan *profile PPTP*

c. Membuat *Authenticated* user / VPN user

Tahapan membuat User VPN ada dimenu tab "Secret". Setting Username, Password, Service dan Profile seperti gambar dibawah ini :



Gambar 6. Membuat *user vpn client*

2. Konfigurasi *Client*

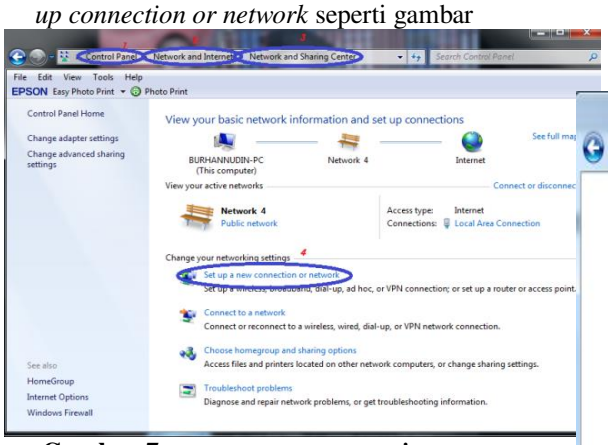
Konfigurasi VPN *client* adalah untuk mempermudah pengaksesan suatu jaringan *intranet* (lokal area) di manapun user berada selama ada koneksi dengan internet melalui koneksi VPN server. Dalam konfigurasi VPN *Client*, ada beberapa tahapan yang harus dilakukan diantaranya :

1. Tahap VPN *Client* Configuration.
2. Tahap *Dialing* VPN / *Connecting* VPN.
3. Tahap *Ping Test* & *Working*.

a. Tahap Konfigurasi *Client*

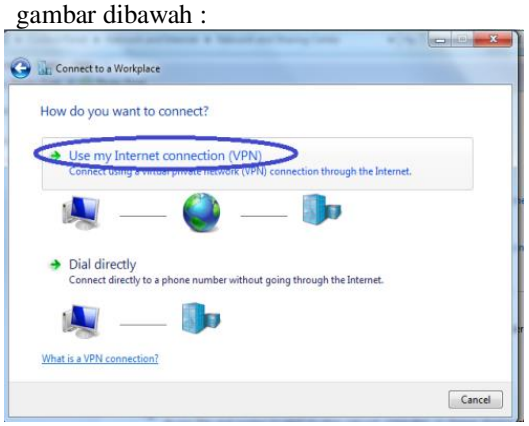
Pengunaan VPN untuk *Client* personal adalah menghubungkan suatu client dengan network VPN Server melalui jalur internet dan pengguna seolah-olah berada dalam satu jaringan lokal. Dalam mengkoneksikan *client* dengan VPN server dibutuhkan beberapa tahapan settingan pada komputer client. Berikut adalah settingan-setingan *client*/user untuk koneksi ke VPN menggunakan Microsoft Windows 7 :

1.) Masuk ke windows Control Panel kemudian klik *network* and internet *connections, network and sharing center, set up connection or network* seperti gambar



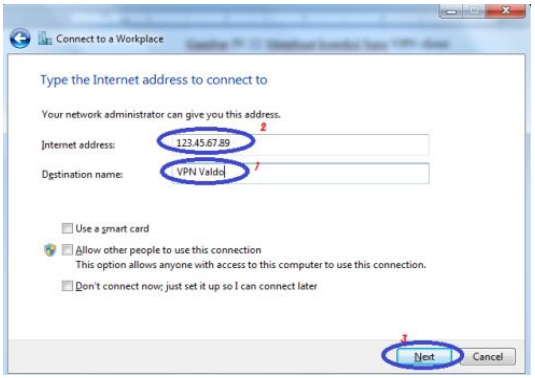
Gambar 7. *set up a new connection or network*

2.) Klik *set up connection or network* kemudian Pilih " Buat koneksi baru denagn memilih, connect a workplace, use my internet connection (VPN) seperti gambar dibawah :



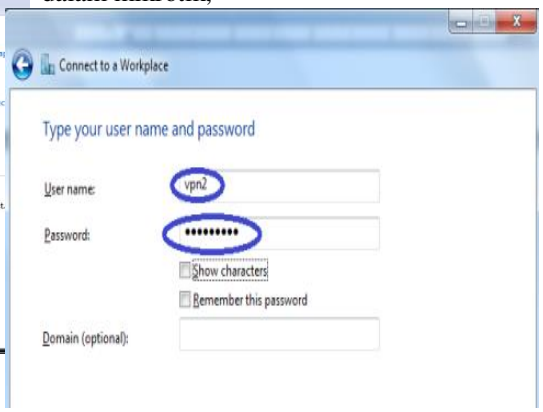
Gambar 8. Membuat koneksi baru VPN client

3.) Masukan nama untuk sambungan VPN dalam penulisan *Destination name* ini saya masukan nama (VPN Valdo), dan internet address kita masukan ip public PT Valdo International dengan contoh 12345678 dan klik next..



Gambar 9. Pemberian *IP Public VPN*

4.) Kemudian pada selanjutnya aka ada tampilan baru untuk pengisian username, dan password VPN yang telah kita buat di dalam mikrotik,

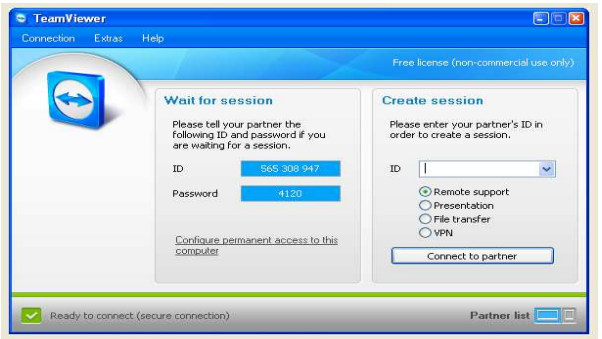


Gambar 10. Login Vpn User

3. Pengujian Jaringan

Pengujian jaringan dilakukan untuk melihat adanya perbedaaan antara jaringan awal dan jaringan akhir yang diusulkan penulis.

1. Pengujian Jaringan Awal

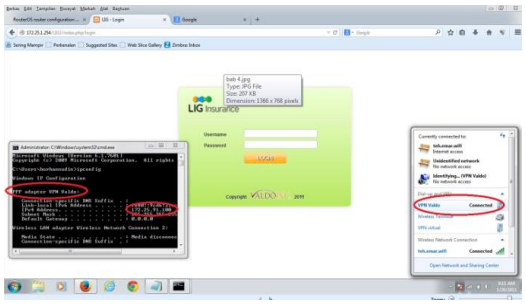


Gambar 11. Pengujian Jaringan Awal

Sebelum dibuat jaringan VPN pada PT. Valdo International, perusahaan masih menggunakan teamViewer untuk meremote kantor yang aplikasi yang sifatnya lokal.

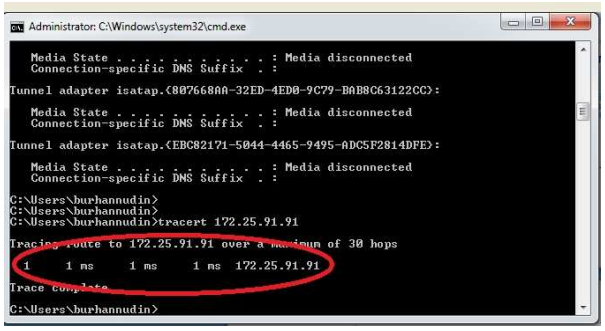
2. Pengujian Jaringan Akhir

Mengkoneksikan PPTP VPN dan membuka aplikasi local Pengujiannya sebagai berikut :



Gambar 12. Hasil Pengujian VPN

Dari percobaan koneksi VPN diatas terlihat bahwa koneksi PPTP VPN ke PT. Valdo International sudah berhasil dilakukan dan sudah berhasil mengakses program aplikasi lokal LIG2 insurance.



Gambar 13. Pengujian Jaringan Akhir

KESIMPULAN

Berdasarkan penelitian jaringan komputer pada PT. Valdo International mengenai penerapan metode open vpn-access server, maka dapat di ambil kesimpulan bahwa membangun jaringan VPN (Virtual Private Network) menggunakan mirkrotik dengan jalur PPTP, dan dapat melakukan kegiatan operasional lainnya secara private di dalam jaringan publik, dengan koneksi yang ekonomis dan keamanan data yang terjamin.

UCAPAN TERIMA KASIH

Terima kasih kami ucapkan kepada Direktur, bagian IT dan seluruh karyawan PT. Valdo International atas ijin dan bantuannya sehingga kami dapat menyelesaikan penelitian ini.

DAFTAR PUSTAKA

Aditya, A. Mahir Membuat Jaringan Komputer. Jakarta: Dunia Komputer, 2011

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

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

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

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