**Dosen : Wenripin Chandra, S.Kom**

Pengantar Jaringan Komputer  
STMIK - STIE MIKROSKIL  
Jurusan Teknik Informatika  
Semester IV  
TA : 2013/2014

**vpn**

**(VIRTUAL PRIVATE NETWORK)**

Pengantar Jaringan Komputer

**Disusun Oleh :**

1. Kelvin (12.111.0031)  
   2. Jeffry Tandiono (12.111.0812)  
   3. Steven (12.111.0235)  
   4.Alwin Mario (12.111.1010)

5. Soewandi Koerniawan Syahputra (12.111.0162)

**VPN**

**(VIRTUAL PRIVATE NETWORK)**

1. **DEFENISI DASAR VPN**

VPN merupakan singkatan dari **Virtual Private Network** yaitu sebuah koneksi private melalui jaringan public (internet). Terdiri dari 2 kata yang dapat dipecahkan yaitu:

* **Virtual,** yang berarti bahwa infrastruktur jaringan harus transparan untuk koneksi VPN. Dalam kebanyakan kasus, itu menunjukkan bahwa jaringan tidak dimiliki oleh pengguna VPN tetapi merupakan jaringan public yang dibagikan pada user lainnya.
* **Private,** yang berarti jaringan yang terbentuk bersifat private dimana tidak semua orang bisa mengaksesnya. Data yang dikirimkan terenkripsi sehingga tetap rahasia meskipun melalui jaringan public.
* **Network,** yang berarti jaringan harus dibuat untuk yang lainnya, yang menunjukkan perangkat dan aplikasi menggunakan topologi seperti routing dan pengalamatan.

Dengan VPN ini kita seolah-olah membuat jaringan di dalam jaringan atau biasa disebut *tunnel* (terowongan). **Tunneling** adalah suatu cara membuat jalur private menggunakan infrastruktur pihak ketiga. VPN merupakan perpaduan antara teknologi tunneling dan enkripsi. VPN menggunakan salah satu dari 3 teknologi tunneling yang ada yaitu:

* PPTP (Point to Point Tunneling Protocol) : sebuah protocol yang mengizinkan hubungan Point-to-Point Protocol (PPP) melewati jaringan IP, dengan membuat Virtual Private Network (VPN).
* L2TP (Layer 2 Tunneling Protocol) dan standar terbaru : sebuah standar Internet Engineering Task Force (IETF) untuk masalah protocol tunneling yang digunakan untuk melakukan enkapsulasi terhadap frame-frame protocol Point-to-Point Protokol (PPP) untuk ditransmisikan melalui jaringan TCP/IP, X.25, frame relay atau jaringan Asynchronous Transfer Mode (ATM).

Sejak orang mulai menggunakan teknologi untuk berkomunikasi selalu ada yang jelas pembagian antara jaringan public dan swasta. Sebuah jaringan public, seperti komunikasi system dan internet merupakan proses yang banyak bertukar informasi bebas kepada satu sama lain.

VPN menggunakan PVC (Permanent Virtual Circuit) yang berjalan pada Internet tapi bagi user akan terlihat sebagai private networks. Packets dikirim melalui PVC, yang disebut tunnel, di-encapsulate denga nmenggunakan protocol khusus yang juga mengenkripsi IP packets yang dikirim. Pertumbuhan VPN yang populer ini adalah berdasarkan biaya yang rendah dan fleksibilitasnya.

Beberapa alasan mengapa orang lain menggunakan VPN ketika melakukan aktivitas di internet :

1. Keamanan Berinternet

Keamanan adalah kondisi yang diinginkan oleh setiap orang, tidak terkecuali ketika seseorang sedang melakukan aktivitas browsing di internet. Anda pasti ingin tetap bebas melakukan aktivitas di internet dan tetap aman. VPN memberikan keamanan pribadi untuk Anda ketika berinternet. VPN menciptakan sebuah jalur pribadi dengan otentikasi yang kuat dan enkripsi yang mengamankan komunikasi Anda di Internet.

1. Privasi Berinternet

Setiap orang memiliki privasi, dan kita harus menghargai privasi orang lain. Demikian pula dalam hal yang berhubungan dengan aktivitas intenet, kita membutuhkan privasi. Namun internet adalah jaringan publik yang berarti bisa terjadi orang lain melihat apa yang kita lakukan di internet. Hal yang perlu di kuatirkan khususnya adalah ketika alamat IP publik Anda bisa mengungkap data Anda seperti posting alamat rumah Anda di situs web publik. Alamat IP publik juga dapat digunakan untuk mengambil alamat fisik Anda, mengambil informasi tentang profil Anda, dan penyusup WiFi / cracker dapat menggunakan alamat IP Anda untuk men-download data-data penting Anda. VPN menyembunyikan alamat IP publik Anda untuk melindungi privasi Anda.

1. Perlindungan saat Berinternet

Keprihatinan utama lainnya adalah ketika mengunjungi sebuah situs web yang memiliki kode berbahaya seperti kode malware yang dapat menyebabkan kerusakan besar pada identitas pribadi dan pencurian informasi credential termasuk informasi login dan password. Hanya karena Anda mengunjungi sebuah situs web yang sah tidak berarti bahwa situs tersebut aman. Karena jalur internet adalah jalur publik, maka bisa saja data-data anda dilihat dan diambil. Ip publik Anda bisa memberikan peluang serangan berbahaya terhadap data-data pribadi Anda. VPN menyembunyikan alamat IP publik dan menjadi perisai Anda terhadap serangan tersebut.

1. Akses tanpa batas Berinternet

Aksesibilitas untuk setiap konten web seharusnya menjadi hak setiap manusia di seluruh dunia di mana pun mereka tinggal. Banyak negara telah memberlakukan kebijakan untuk memblokir warga mereka dari hak-hak dasar untuk mengakses konten web tertentu di internet. China dan beberapa negara di Timur Tengah melakukan pemblokiran Facebook dan Twitter. VPN mendukung metode canggih untuk menghindari pembatasan tersebut untuk memberikan akses ke konten web di mana pun Anda tinggal.

1. **Fungsi VPN**

Teknologi VPN menyediakan 3 fungsi utama untuk penggunanya, yaitu :

1. **Confidentiality (Kerahasiaan)**

Teknologi VPN memiliki sistem kerja mengenkripsi semua data yang lewat melaluinya. Dengan adanya teknologi enkripsi ini, maka kerahasiaan Anda menjadi lebih terjaga. Biarpun ada pihak yang dapat menyadap data Anda yang lalu-lalang, namun belum tentu mereka bisa membacanya dengan mudah karena memang sudah diacak. Dengan menerapkan sistem enkripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data Anda dengan mudah.

1. **Data Integrity (Keutuhan Data)**

Ketika melewati jaringan Internet, data Anda sebenarnya sudah berjalan sangat jauh melintasi berbagai negara. Di tengah perjalanannya, apapun bisa terjadi terhadap isinya. Baik itu hilang, rusak, bahkan dimanipulasi isinya oleh orang-orang iseng. VPN memiliki teknologi yang dapat menjaga keutuhan data yang Anda kirim agar sampai ke tujuannya tanpa cacat, hilang, rusak, ataupun dimanipulasi oleh orang lain.

1. **Origin Authentication (Autentikasi Sumber)**

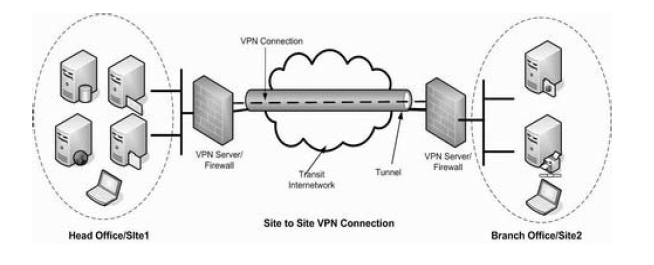
Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi source datanya. Kemudian alamat source data ini akan disetujui jika proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima oleh Anda berasal dari sumber yang semestinya. Tidak ada data yang dipalsukan atau dikirimkan oleh pihak-pihak lain.

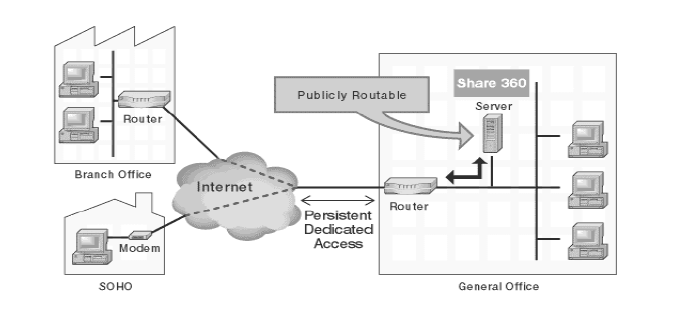
1. **Tipe VPN**

Secara umum VPN dapat dikelompokkan menjadi :

* **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 atau laptop yang sudah dilengkapi perangkat tertentu untuk melakukan koneksi dengan jaringan LAN di kantor.

Sebelum koneksi, maka akan dilakukan proses dial-up terlebih dahulu ke network access server (NAS). Biasanya NAS disebabkan oleh provider yang memberikan layanan VPN. Sedangkan pengguna cukup menyediakan komputer dan aplikasi untuk men-dial NAS. Secara umum VPDN hampir mirip dengan dial-up Internet connection. Namun, secara teknis tentu saja VPN lebih canggih dan lebih secure dibandingkan dial-up internet. Koneksi biasanya hanya dilakukan sewaktu-waktu.



* **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 terus menerus (24 jam) sehari.

Jika ditinjau dari segi kendali atau administrative control. Secara umum site-to-site VPN dapat dibagi menjadi :

1. **Intranet VPN**

Manakala VPN hanya digunakan untuk menghubungkan beberapa lokasi yang masih satu instansi atau satu perusahaan. Seperti kantor pusat dihubungkan dengan kantor cabang. Dengan kata lain, administrative control berada sepenuhnya bawah satu kendali.

1. **Extranet VPN**

Manakala VPN digunakan untuk menghubungkan beberapa instansi atau perusahaan yang berbeda namun di antara mereka memiliki hubungan "dekat". Seperti perusahaan tekstil dengan perusahaan angkutan barang yang digunakan oleh perusahaan tekstil tersebut. Dengan kata lain, administrative control berada di bawah kendali beberapa instansi terkait.

1. **Access VPN**

Manakala VPN digunakan untuk mengizinkan pekerja-pekerja mengakses ke jaringan organisasinya dari lokasi remote.

1. **Arsitektur Dasar VPN**

Setiap lokasi terhubung ke VPN adalah yang pertama terhubung ke ISP yang menyediakan VPN service menggunakan leased circuit, seperti T-1 line yang mana terhubung ke PVC ISP pada access point ISP.

Paket yang keluar dari VPN dikirim melalui routers or switches khusus.

Peralatan pengirim VPN encapsulate paket yang keluar dengan protokol yang digunakan untuk memindahkannya melalui tunnel ke VPN device pada sisi yang lainnya.

Peralatan VPN pada sisi receiver, strips off paket VPN dan mengantarkannya sampai destination network.

VPN adalah transparan bagi user, ISP, dan Internet secara keseluruhannya, dia ada untuk menyederhanakan sebuah stream dari packet yang berpindah di Internet.

1. **Manfaat & Kegunaan VPN**

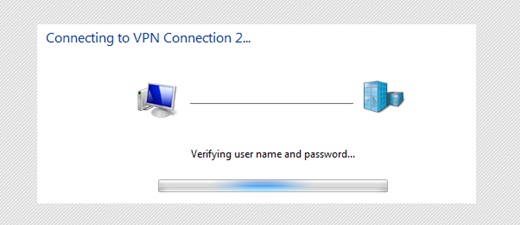
* Kemampuan membentuk jaringan LAN yang tidak di batasi tempat dan waktu, karena koneksitasnya dilakukan via internet. Koneksi internet apapun dapat digunakan seperti Dial-Up, ADSL, Cable Modem, WIFI, 3G, CDMA Net, GPRS,& . sistem PVN ini paling tepat digunakan untuk penggunaan suatu database terpusat untuk mengkomunikasikan antara server dan client via internet seperti Aplikasi Perdagangan, Purchase, P.O.S, Accounting, Cashir, Billing system, General Ledger, DLL
* Tidak ada ketergantungan terhadap keharusan memiliki IP Publik yang berharga mahal. Cukup menggunakan IP dynamic saja dengan kata lain  asal PC anda bisa berinternet .
* Anda bisa ngeprint dari rumah kekantor anda via internet
* Anda bisa melakukan transfer data atau remote view untuk mengendalikan komputer dirumah/kantor anda dimana saja
* Tidak membutuhkan Peralatan/hardware tambahan yang berfungsi sebagai IP forwarder/Port Forwader yang menambah investasi anda.
* Dimanapun anda berada seperti anda sedang berada di warnet ataupun saat anda traveling di luar negeri, dapat melakukan koneksitas dengan PC dikantor anda misalnya dengan memanfaatkan software yang bekerja dijaringan LAN seperti Citrix, Windows Terminal Server 2003, VNC, Radmin, VOIP, DLL
* Dengan menggunakan software yang bekerja dijaringan LAN anda dapat melakukan pertukaran data secara langsung, Printing , Remote View, Mengatur administrasi PC anda, yang kesemua itu dapat dilakukan dimanapun anda berada selama anda bisa terhubung ke internet
* Dapat mengakses akses yang diblok
* Berselancar dengan aman ketika di akses internet publik / hotspot
* Jika perusahaan ingin mengoptimalkan biaya untuk membangun jaringan mereka yang luas. Oleh karena itu VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media jaringan public yang sudah ada.
* Jangkauan jaringan lokal yang dimiliki suatu perusahaan akan menjadi luas, sehingga perusahaan dapat mengembangkan bisnisnya di daerah lain. Waktu yang dibutuhkan untuk menghubungkan jaringan lokal ke tempat lain juga semakin cepat, karena proses instalasi infrastruktur jaringan dilakukan dari perusahaan / kantor cabang yang baru dengan ISP terdekat di daerahnya. penggunaan VPN secara tidak langsung akan meningkatkan efektivitas dan efisiensi kerja.
* Penggunaaan VPN dapat mengurangi biaya operasional bila dibandingkan dengan penggunaan leased line sebagai cara tradisional untuk mengimplementasikan WAN.
* VPN dapat mengurangi biaya pembuatan jaringan karena tidak membutuhkan kabel (leased line) yang panjang. Penggunaan kabel yang panjang akan membutuhkan biaya produksi yang sangat besar. Semakin jauh jarak yang diinginkan, semakin meningkat pula biaya produksinya.
* VPN menggunakan internet sebagai media komunikasinya. Perusahaan hanya membutuhkan biaya dalam jumlah yang relatif kecil untuk menghubungkan perusahaan tersebut dengan pihak ISP (internet service provider) terdekat.
* Penggunaan VPN akan meningkatkan skalabilitas.
* VPN memberi kemudahan untuk diakses dari mana saja, karena VPN terhubung ke internet. Sehingga pegawai yang mobile dapat mengakses jaringan khusus perusahaan di manapun dia berada. Selama dia bisa mendapatkan akses ke internet ke ISP terdekat, pegawai tersebut tetap dapat melakukan koneksi dengan jaringan khusus perusahaan.

1. **Kekurangan & Kelemahan VPN**

* Koneksi internet (jaringan publik) yang tidak bisa kita prediksi. Hal ini dapat kita maklumi karena pada dasarnya kita hanya *“nebeng”* koneksi pada jaringan pihak lain sehingga otomatis kita tidak mempunyai kontrol terhadap jaringan tersebut.
* Perhatian lebih terhadap keamanan. Lagi-lagi karena faktor penggunaan jaringan publik, maka kita perlu memberikan perhatian yang lebih untuk mencegah terjadinya hal-hal yang tidak diinginkan seperti penyadapan, hacking dan tindakan cyber crime pada jaringan VPN.
* Internet-based VPN tidak standar, jadi tidak semua peralatan vendor dan service-nya kompatibel.

1. **Tutorial Cara Setting VPN Server di Windows 7**

Setting **Virtual Private Network** di **Windows 7** menggunakan Point-to-Point Tunnelling Protocol (PPTP) tanpa menggunakan software tambahan. Layanan VPN yang dipilih adalah WebSiteVPN yang memiliki server UK (United Kingdom) dan USA (United States) dengan pertimbangan free services, kecepatan akses serta kemudahan setting konfigurasi untuk computer windows.

Setting PPTP VPN siap terkoneksi dengan server tujuan.  
Berbeda dengan aplikasi virtual private network, cara setting PPTP di windows 7 mengharuskan anda untuk membuat koneksi internet baru di control panel.

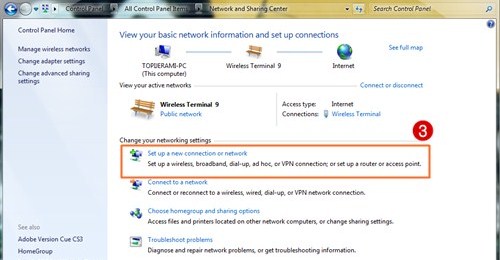
Tidak perlu download software karena computer akan berfungsi sebagai client secara langsung dengan **protokol PPTP**.

* Layanan yang digunakan adalah WebSiteVPN dengan **free VPN account**, tanpa registrasi serta 99,9% up-time guarantee.
* **Perlu diketahui**, pengaturan Virtual Private Network di windows 7 berikut ini dapat diaplikasikan untuk semua layanan/penyedia VPN. Hanya saja disini menggunakan contoh layanan gratis dari WebSiteVPN.
* Beberapa hal yang harus anda siapkan sebelum melakukan koneksi VPN adalah nama server atau alamat server atau IP server (tergantung pihak penyedia VPN menyebutnya), username dan password untuk login ke server VPN.

Membuat Konfigurasi PPTP VPN Baru di Windows 7

1. Buka **control panel** windows 7, lihat pojok kanan atas pilih **View by : Small icon** kemudian pilih menu **Network and Sharing Center**

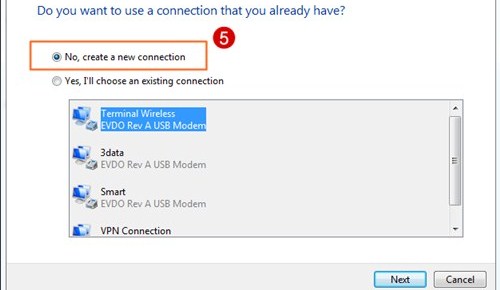
2. Pilih **Set up a new connection or network**



3. Muncul jendela baru, pilih **Connect to a workplace** kemudian NEXT



4. Pada jendela berikutnya, pilih **No, create a new connection** kemudian NEXT



5. Pilih **Use my Internet Connection (VPN)**

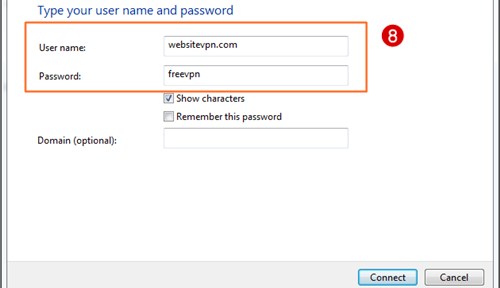


6. Masukkan alamat server VPN atau ip server public atau Internet address yang diberikan oleh penyedia VPN yang anda gunakan. Karena memakai **layanan free VPN** dari WebSiteVPN maka, saya mengisikan us.websitevpn.com.



Untuk kolom Destination Name biarkan saja, atau isi sesuai keinginan anda. Kolom ini digunakan sebagai nama koneksi VPN, klik NEXT untuk melanjutkan.

7. Masukkan username dan password penyedia VPN yang anda gunakan, berikut contoh data login WebSiteVPN yang diisikan.



8. Klik **connect** untuk melakukan koneksi ke server **Virtual Private Network** yang sudah anda masukkan sebelumya.