**VPN**

(VIRTUAL PRIVATE NETWORK)

1. **DEFENISI DASAR VPN**

VPN merupakan singakatan dari **Virtual Private Network** yang akan mengizinkan pengguna untuk melakukan koneksi ke berada didalam satu jaringan (jaringan lokal) yang sama seperti VPN.

Apa itu VPN..? VPN adalah sebuah jaringan virtual yang dapat dihubungkan ke komputer kita melalui internet. ketika anda menghubungkan perangkat anda (bisa komputer, smartphone, tablet dlsb) ke dalam jaringan VPN maka perangkat anda akan bertindak seolah-olah berada didalam satu jaringan yang sama dengan si VPN. semua traffic atau lalu lintas data anda dalam internet di suplai oleh si VPN yang memiliki koneksi yang aman dan bersih. karena komputer anda seolah-olah berada dalam satu jaringan yang sama dengan VPN maka komputer anda bisa memanfaatkan resource jaringan virtual tersebut meskipun anda sedang berada di belahan dunia yang lain. Komputer anda juga bisa mengakses internet seolah-olah berasal dari lokasi atau negara yang sama dengan VPN yang anda gunakan. dengan prinsip kerja ini maka anda bisa mengakses website-website yang diblokir oleh sebuah negara atau lokasi.

ketika anda melakukan browsing menggunakan VPN, maka secara tidak langsung komputer anda melakukan kontak dengan website menggunakan koneksi VPN yang terenkripsi, sehingga data-data anda akan aman dan nggak akan diendus oleh orang-orang yang tidak bertanggung jawab.

ketika anda mengakses sebuah website maka VPN akan melakukan request terhadap website tersebut kemudian meneruskannya ke pada anda secara aman, jadi ibaratnya VPN dapat berfungsi sebagai saringan yang menyaring koneksi kotor yang berbahaya sehingga anda dapat melakukan browsing internet dengan aman dan nyaman.

Fungsi VPN

setelah mengetahui apa itu VPN, selanjutnya apa fungsi VPN? VPN bisa digunakan untuk berbagai macam kebutuhan, diantaranya adalah :

1. Mengakses Home Network saat dalam perjalanan

. saat anda dalam perjalanan anda bisa tetap mengakses jaringan Home anda. anda juga bisa meremote komputer anda yang ada dirumah melalui VPN.

1. Menyembunyikan aktivitas browsing anda.

dengan menggunakan VPN anda bisa menyembunyikan aktivitas browsing anda, sehingga data-data yang anda input saat browsing tidak akan bisa diendus oleh orang-orang yang tidak bertanggung jawab.

1. Mengakses Website yang di blokir

dengan VPN anda bisa mengakses website-website yang diblokir menggunakan sistem geo blocked atau website yang di blokir berdasarkan wilayah atau kebijakan suatu  negara. jadi jika anda melakukan perjalanan di china anda tetap bisa mengakses facebook via VPN. karena Facebook di china itu di blokir dan dilarang akses loh.

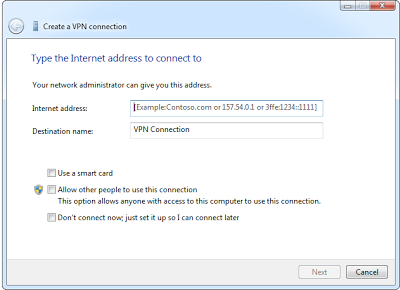
1. membypass internet censorship

dengan VPN anda bisa mengakses situs-situs atau konten-konten yang di sensor.

1. Download files.

banyak orang yang memanfaatkan VPN untuk mendownload files terutama menggunakan Torrent. menggunakan VPN untuk mendownload Torrent akan meningkatkan kecepatan download anda. apalagi jika konten torrent yang anda download adalah konten legal.

**Penggunaan VPN**  
VPN adalah alat yang cukup sederhana, tetapi dapat digunakan untuk melakukan berbagai hal:  
  
Akses Jaringan Bisnis Ketika di Perjalanan : VPN sering digunakan oleh pelancong bisnis untuk mengakses jaringan bisnis mereka, termasuk semua sumber daya jaringan lokal, ketika di perjalanan. Sumber daya lokal tidak harus terhubung langsung ke Internet, sehingga meningkatkan keamanan.  
  
Akses Jaringan Rumah Anda Ketika Bepergian : Anda juga dapat mengatur VPN Anda sendiri untuk mengakses jaringan Anda sendiri saat bepergian. Ini akan memungkinkan Anda untuk mengakses Remote Desktop Windows melalui Internet, berbagi berkas file, dan bermain game melalui internet seolah-olah Anda berada di LAN yang sama (local area network).  
  
Menyembunyikan Aktivitas Browsing Anda Dari Jaringan Lokal Anda dan ISP : Jika Anda menggunakan koneksi Wi-Fi publik, aktivitas browsing Anda di situs web non-HTTPS terlihat untuk semua orang, jika mereka tahu bagaimana mencarinya. Jika Anda ingin menyembunyikan aktivitas browsing Anda untuk sedikit lebih privasi, Anda dapat terhubung ke VPN. Jaringan lokal hanya akan melihat satu sambungan aman VPN. Semua traffic lain akan melakukan perjalanan melalui koneksi VPN. Meskipun hal ini dapat digunakan untuk memotong koneksi-monitoring oleh penyedia layanan Internet Anda, ingatlah bahwa penyedia VPN dapat memilih untuk log lalu lintas di ujungnya.  
  
Akses Website yang di Blokir : Ini adalah cara yang paling ampuh untuk bisa mengakses situs-situs yang diblokir dengan sangat mudah. Anda bisa menggunakan layanan VPN berbayar maupun layanan VPN gratis.  
  
Bypass Sensor Internet : Banyak orang China menggunakan VPN untuk mengakali Great Firewall of China dan memperoleh akses ke seluruh internet. (Namun, Great Firewall tampaknya telah mulai mengganggu VPN)  
  
Download File : Banyak orang menggunakan koneksi VPN untuk men-download file melalui BitTorrent. Ini sebenarnya dapat berguna bahkan jika Anda men-download torrents yang sepenuhnya legal - jika ISP Anda memblokir BitTorrent dan membuatnya sangat lambat, Anda dapat menggunakan BitTorrent pada VPN untuk mendapatkan kecepatan lebih cepat. Hal yang sama berlaku untuk jenis lain dari lalu lintas ISP Anda yang mungkin mengganggu (kecuali mereka mengganggu lalu lintas VPN itu sendiri.)  
  
**Menggunakan VPN**  
Menghubungkan ke VPN cukup sederhana. Pada Windows, tekan tombol Windows, ketik VPN, dan klik pilihan Set up virtual private network (VPN). (Jika Anda menggunakan Windows 8, Anda harus mengklik kategori Settings setelah mencari.) Gunakan wizard untuk memasukkan alamat dan login dari layanan VPN yang ingin Anda gunakan. Anda kemudian dapat menghubungkan dan memutuskan sambungan dari VPN menggunakan ikon jaringan di system tray yang sama di mana Anda mengelola jaringan Wi-Fi Anda.  
  
Beberapa penyedia VPN dapat menawarkan klien yang melakukan konfigurasi ini untuk Anda.



**Layanan VPN gratis**  
Jika Anda baru saja mengenal VPN dan ingin VPN dasar untuk digunakan pada hotspot Wi-Fi atau mengakses situs-wilayah terbatas, ada beberapa layanan gratis yang cukup baik.  
  
[TunnelBear](http://www.tunnelbear.com/) memiliki setup yang mudah dan sederhana. Anda cukup meng-klik tombol dalam aplikasi, Anda bahkan tidak perlu mengkonfigurasi VPN pada Windows. Versi gratis membatasi Anda untuk 500 MB per bulan, tapi itu mungkin baik untuk penggunaan sesekali.  
  
Ada juga [proXPN](http://proxpn.com/) , yang menyediakan klien bebas. Gratis klien terbatas pada 300kbps, tapi lalu lintas sebaliknya terbatas.  
  
Anda juga mungkin tertarik dalam mendirikan VPN di server Anda sendiri, yang dapat Anda lakukan dengan menggunakan beberapa aplikasi seperti Tomat atau OpenWRT. Tentu saja, ini tidak akan memungkinkan Anda untuk mengakses situs web yang diblokir, kecuali jika Anda bepergian ke luar negeri dan mengakses jaringan Anda sendiri dari jarak jauh.

Cara Kerja Virtual Private Network  
  
  
Virtual private network (VPN) : Sebuah koneksi yang aman antara dua bagian dari sebuah jaringan pribadi yang digunakan pada sebuah jaringan publik seperti Internet untuk mengurangi biaya operasional.  
  
Anda harus bekerja walau sedang tidak berada di kantor. Mungkin saat Anda tengah berada di jalan atau bekerja di rumah, atau sedang berada di lapangan di tengah-tengah proyek, Anda memerlukan akses ke file-file, e-mail, dan database di kantor pusat Anda. Mengkoneksikan diri langsung ke server kantor Anda mungkin merupakan salah satu solusi, tetapi hal tersebut bisa menjadi sangat mahal dan memerlukan hardware dan dukungan teknis yang rumit. Mengirim file melalui Internet mungkin menjadi sarana yang paling mudah, tetapi belum tentu file yang Anda kirim aman dari para pengendus (sniffer) yang suka mencuri dan mengintip rahasia orang lain. Jadi, kenapa tidak Anda bawa saja jaringan tersebut kemana-mana?  
  
Anda dapat mengakses secara aman pada jaringan bisnis Anda dengan biaya semurah telepon lokal. Pertanyaannya adalah, bagaimana caranya? Gunakan saja jaringan Internet dan sebuah virtual private network (VPN). Dengan VPN, Anda tidak perlu pusing-pusing mengurus instalasi yang rumit--yang Anda perlukan hanyalah mendapatkan sebuah ISP (internet service provider) untuk mengelola VPN tersebut untuk Anda. Lebih jauh mengenai VPN:  
  
· Menciptakan sebuah koneksi yang aman untuk jaringan bisnis Anda untuk dapat diakses oleh kantor cabang atau pekerja telekomuter yang bekerja di rumah  
· Biaya yang dikeluarkan lebih hemat 70 persen dibanding akses dial-up dan modem biasa.  
· Dapat dijalankan pada berbagai jenis jaringan, termasuk Internet.  
  
Sebuah VPN menyediakan koneksi yang aman antara dua segmen pada sebuah jaringan, dimana satu ujungnya berada pada gateway (sebuah pintu masuk ke dalam jaringan, seperti sebuah router) jaringan di kantor Anda, dan ujung yang satunya lagi berada pada PC di rumah Anda atau pada sebuah gateway jaringan lainnya, misalnya pada kantor cabang di luar kota. Kedua segmen tersebut dikoneksikan melalui sebuah jaringan publik, biasanya adalah Internet. Untuk dapat mengamankan jaringan di dalamnya, VPN memakai dua teknologi utama: tunneling dan enkripsi.  
  
Tunneling memungkinkan dua ujung dari VPN dapat saling berkomunikasi melalui Internet. Karena sistem Internet berbeda dengan sistem jaringan Anda, sebuah lorong (tunnel) khusus dibuat untuk memaketkan data yang Anda kirim sehingga Internet dapat melewatkannya di dalam jaringannya.

**Membuat Sebuah Koneksi**  
  
Saat Anda membuat sebuah koneksi VPN, software pada ujung di bagian Anda mengontak gateway VPN, sebagai contoh mungkin adalah router Ethernet di kantor Anda. Gateway biasanya memverifikasi apakah Anda seorang pemakai yang terotorisasi dengan mengecek password Anda. Kemudian software VPN akan membuatkan sebuah tunnel dan menambahkan sebuah header pada paket data Anda yang dimengerti oleh jaringan Internet. Saat paket mencapai endpoint dari gateway, gateway akan menarik kembali header Internet tersebut, dan mengarahkan paket tersebut ke tujuan akhirnya. VPN menggunakan salah satu dari tiga teknologi tunneling yang ada: PPTP, L2TP, dan standar terbaru, Internet Protocol Security (biasa disingkat menjadi IPSec).  
  
Bila tunnel membuatkan jaringan, enkripsi akan menciptakan privasi/keamanan di dalamnya, dengan mengacak data yang lewat sehingga hanya pihak yang memiliki kunci digital saja yang dapat membacanya. PPTP dan L2TP dapat memverifikasi sebuah identifikasi pengguna dan mengacak data menggunakan kriptografi dasar, yaitu mengacak dan menenkripsikan seluruh file secara bersamaan. Untuk situasi dan kalangan bisnis tertentu, metoda pengamanan tersebut masih mencukupi. Untuk perusahaan yang memerlukan tingkat keamanan super-ketat mungkin lebih baik menggunakan protokol IPSec, yang memiliki proses tingkat lanjut, memverifikasi dan mengenkripsi setiap paket data untuk dapat mencapai privasi tingkat maksimum.

Fungsi, Cara Kerja dan Apakah VPN

VPN adalah singkatan **Virtual Private Network**, yaitu sebuah koneksi private melalui jaringan publik atau [internet](http://softkompi.blogspot.com/search/label/internet), **virtual network** berarti jaringan yang terjadi hanya bersifat virtual.. **Private**yaitu jaringan yang terbentuk *bersifat private* dimana tidak semua orang bisa mengaksesnya. Data yang dikirimkan *terenkripsi* sehingga tetap rahasia meskipun melalui jaringan publik. Jika menggunakan VPN kita seolah-olah membuat jaringan didalam jaringan atau biasa disebut tunnel. VPN menggunakan salah satu dari tiga teknologi tunneling yang ada yaitu: *PPTP, L2TP* dan standar terbaru,*Internet Protocol Security* (biasa disingkat menjadi IPSec). VPN merupakan perpaduan antara teknologi tunneling dan enkripsi.

Cara kerja VPN *(dengan protokol PPTP)* adalah sebagai berikut:

* VPN membutuhkan sebuah server yang berfungsi sebagai penghubung antar [PC](http://softkompi.blogspot.com/), ***Server VPN*** ini bisa berupa [komputer](http://softkompi.blogspot.com/)dengan aplikasi VPN Server atau sebuah Router.
* Untuk memulai sebuah koneksi, komputer dengan aplikasi VPN Client mengontak Server VPN, VPN Server kemudian memverifikasi *username* dan *password* dan apabila berhasil maka VPN Server memberikan IP Address baru pada komputer client dan selanjutnya sebuah koneksi / tunnel akan terbentuk.
* Selanjutnya komputer client bisa digunakan untuk mengakses berbagai resource (komputer atau LAN) yang berada dibelakang VPN Server misalnya melakukan transfer data, ngeprint dokument, browsing dengan gateway yang diberikan dari VPN Server, melakukan remote desktop dan lain sebagainya.

**Apakah Fungsinya VPN?**  
Teknologi VPN menyediakan tiga fungsi utama untuk penggunanya. Fungsi utama tersebut adalah sebagai berikut:

**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.

**2. 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.

**3. 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.

Demikianlah penjelasan singkat tentang VPN atau Virtual Private Network, Jika ingin mencoba VPN silahkan lihat postingan yang berjudul VPN Gratis Tanpa Software dan Registrasi.  
Semoga bermanfaat serta dapat menambah wawasan kita semua.  
Jika ada yang kurang silahkan memberikan komentar di bawah.

**Apa itu VPN?**

VPN merupakan singkatan dari ***Virtual Private Network***, yaitu sebuah koneksi private melalui jaringan publik (dalam hal ini internet). Disini ada 2 kata yang dapat kita garis bawahi yaitu:

* ***virtual network***, yang berarti jaringan yang terjadi hanya bersifat virtual. Tidak ada koneksi jaringan secara riil antara 2 titik yang akan berhubungan.
* ***private***, jaringan yang terbentuk *bersifat private* dimana tidak semua orang bisa mengaksesnya. Data yang dikirimkan *terenkripsi* sehingga tetap rahasia meskipun melalui jaringan publik.

Dengan VPN ini kita seolah-olah membuat jaringan didalam jaringan atau biasa disebut*tunnel* (terowongan). ***Tunneling*** adalah suatu cara membuat jalur privat dengan menggunakan infrastruktur pihak ketiga. VPN menggunakan salah satu dari tiga teknologi tunneling yang ada yaitu: *PPTP, L2TP* dan standar terbaru,*Internet Protocol Security*(biasa disingkat menjadi IPSec). VPN merupakan perpaduan antara teknologi tunneling dan enkripsi.

Dibawah ini adalah gambaran tentang koneksi VPN yang menggunakan protokol PPTP. PPTP *(Pont to Point Tunneling Protocol)* adalah sebuah protokol yang mengizinkan hubungan *Point-to Point Protocol* (PPP) melewati jaringan IP, dengan membuat *Virtual Private Network* (VPN).

**Cara Kerja VPN**

Dari gambar diatas secara sederhana cara kerja VPN *(dengan protokol PPTP)* adalah sebagai berikut:

* VPN membutuhkan sebuah server yang berfungsi sebagai penghubung antar PC,***Server VPN*** ini bisa berupa komputer dengan aplikasi VPN Server atau sebuah Router, misalnya MikroTik RB 750.
* Untuk memulai sebuah koneksi, komputer dengan aplikasi VPN Client mengontak Server VPN, VPN Server kemudian memverifikasi *username* dan *password* dan apabila berhasil maka VPN Server memberikan IP Address baru pada komputer client dan selanjutnya sebuah koneksi / tunnel akan terbentuk.
* Untuk selanjutnya komputer client bisa digunakan untuk mengakses berbagai resource (komputer atu LAN) yang berada dibelakang VPN Server misalnya melakukan transfer data, ngeprint dokument, browsing dengan gateway yang diberikan dari VPN Server, melakukan remote desktop dan lain sebagainya.

**Keuntungan atau Manfaat VPN**

Beberapa keuntungan dari teknologi VPNdiantaranya adalah:

* *Remote Access*, dengan VPN kita dapat mengakses komputer atau jaringan kantor, dari mana saja selama terhubung ke internet
* Keamanan, dengan koneksi VPN kita bisa berselancar dengan aman ketika menggunakan akses internet publik seperti *hotspot* atau*internet cafe*.
* Menghemat biaya setup jaringan, 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 tanpa perlu membangun jaringan pribadi.
* dan lain2 yang saya belum mengerti

**Kekurangan atau Kelemahan VPN**

Setiap ada kelebihan pasti ada kekurangannya, beberapa kekurangan dari VPN diantaranya adalah:

* 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.
* dan lain2 yang saya belum mengerti

Demikianlah catatan sederhana*tentang VPN*, *cara kerja VPN*, *keuntungan dan kelemahan VPN.* Beberapa link dibawah ini mungkin bisa menambah pengetahuan kita tentang VPN.

VPN merupakan paket solusi komunikasi data (baik berupa data suara, video, atau file digital lainnya) yang memberikan layanan berbasis IP ke *end user*. Layanan VPN dapat mengirimkan data antar-dua komputer yang melewati jaringan publik, misal nya Internet, sehingga seolah-olah terhubung secara *pointto-point*.

Perusahaan dengan banyak kantor cabang yang tersebar di berbagai kota. Anda pasti membutuhkan jalur komunikasi private yang terjangkau dan aman, untuk mengontrol dan mengintegrasikan semua proses bisnis di masing-masing kantor.

VPN adalah solusi yang tepat untuk menjawab kebutuhan tersebut. Virtual Private Network (VPN), dari namanya saja Anda pasti sudah dapat membayangkan benda apa ini: sebuah jaringan (network) yang tidak private (public), yang dibuat seolaholah private. VPN sangat dibutuhkan sebagai jembatan komunikasi antar beberapa kantor cabang, menggantikan modus komunikasi tradisional menggunakan sambu ngan telepon private (leased line).

Penggunaan banyak sambungan telepon tentu akan membengkakkan fi xed cost. Solusi untuk permasalahan di atas adalah penggunaan VPN yang memanfaatkan jaringan publik, Internet, sebagai media intranet, sehingga daerah jangkauannya menjadi luas tanpa investasi yang besar. Setiap dibuka kantor baru, Anda cukup menyediakan akses ke Internet, maka tersambunglah kantor tersebut dengan kantor pusat dan kantor-kantor cabang lainnya.

Anda sama sekali tidak perlu memasang jaringan sendiri yang merepotkan pengelolaan, serta membutuhkan biaya yang tidak sedikit.

Data dienkapsulasi (dibungkus atau dikenal dengan istilah tunneling) dengan header yang berisi informasi routing untuk mendapatkan koneksi point-to-point, sehingga dapat melewati jaringan Internet dan dapat mencapai tujuan. Sedangkan untuk mendapatkan koneksi yang bersifat private, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaanya, sehingga paket yang tertangkap ketika mele wati jaringan publik tidak terbaca, karena harus melewati pro ses deskripsi.

Dengan demikian, komunikasi antara beberapa kantor cabang yang semula dilakukan secara interlokal melalui sambungan telepon, kini bi sa dilakukan sebagai hubungan lokal.

Penggunaan VPN tidak hanya menekan biaya komunikasi yang harus dikeluarkan perusahaan, tetapi juga menjamin keamanan data yang ditransmisikan melalui jaringan publik dari penyadapan, penyalinan, atau pengubahan yang dilakukan pihak ketiga.

**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

VPN telah dikembangkan menjadi beberapa jenis. Para ahli berbeda pendapat tentang pembagian jenis **VPN (Virtual Private Network)**tersebut. Ada yang berpendapat bahwa pembagian VPN berdasarkan jenis protokol yang digunakan, jenis proteksi data, dan sebagainya. Secara umum VPN dapat dikelompokkan menjadi:

* **Remota Access VPN**  
  Remota 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-tosite VPN dapat dibagi menjadi:
  1. **Intranet**  
     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.
  2. **Extranet**  
     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.