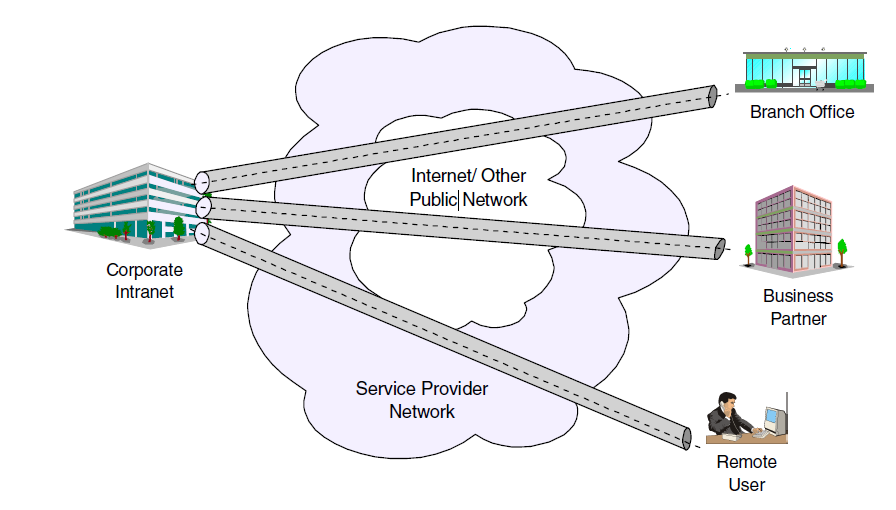
Virtual private network (VPN) merupakan perluasan dari intranet pribadi suatu perusahaan  
di seluruh jaringan publik seperti Internet, menciptakan pribadi koneksi yang aman, yang pada dasarnya melalui terowongan (*tunnel*) pribadi. VPN dapat menyampaikan  
informasi secara aman di Internet yang menghubungkan pengguna remote / remote users, kantor cabang, dan mitra bisnis ke jaringan perusahaan secara luas.

virtual:  
Ini berarti bahwa infrastruktur fisik jaringan harus transparan untuk koneksi VPN. Dalam kebanyakan kasus itu juga berarti bahwa jaringan fisik (physical network) tidak dimiliki oleh pengguna VPN tetapi merupakan jaringan publik bersama untuk para pengguna lain. Untuk memfasilitasi transparansi yang diperlukan untuk lapisan atas, digunakan teknik protokol tunneling. \*Untuk mengatasi implikasi yang tidak memiliki perjanjian jaringan fisik, tingkat layanan denganpenyedia jaringan harus dibentuk untuk memberikan, dalam cara terbaik mungkin,kinerja dan ketersediaan persyaratan yang dibutuhkan oleh VPN.

pribadi:  
Istilah "pribadi" dalam konteks VPN mengacu pada privasi lalu lintas yang mengalir melalui VPN. \*Seperti disebutkan sebelumnya, lalu lintas VPN sering mengalir di atas publik  
jaringan (maka kebingungan dengan kata "pribadi") dan oleh karena itu, tindakan pencegahan harus dilakukan untuk memberikan keamanan yang diperlukan yang diperlukan untuk  
setiap profil lalu lintas tertentu yang mengalir melalui koneksi VPN. Persyaratan keamanan itu meliputi:  
• Enkripsi data  
• otentikasi data asal  
• generasi Aman dan menyegarkan tepat waktu kunci kriptografi yang diperlukan untuk  
enkripsi dan otentikasi (Secure generation and timely refresh of cryptographic keys needed for encryption and authentication).  
• Perlindungan terhadap replay paket dan alamat spoofing  
Jaringan:  
Meskipun tidak ada secara fisik, VPN harus efektif dirasakan dan diperlakukan sebagai perluasan infrastruktur jaringan perusahaan. Ini berarti bahwa VPN harus dibuat tersedia ke seluruh jaringan, untuk semua atau tertentu subset dari perangkat dan aplikasi, dengan cara teratur topologi (regular means of topology) seperti Routing dan addressing.  
Keuntungan VPN

Dengan ledakan pertumbuhan internet, perusahaan mulai bertanya: "Bagaimana kita dapat memanfaatkan internet untuk bisnis kita secara maksimal? "Awalnya, perusahaan menggunakan Internet untuk mempromosikan citra mereka, produk, dan jasa dengan menyediakan akses World Wide Web (WWW) untuk mengelola (corporate) Website. Hari ini, bagaimanapun, potensi dari Internet tak terbatas, dan telah berfokus ke e-bisnis, menggunakan jangkauan global dari internet untuk memudahkan akses ke aplikasi bisnis penting dan data yang berada dalam sistem I/T tradisional. Perusahaan mencari solusi terbaik untuk memperluas jangkauan aplikasi dan data mereka di seluruh dunia secara aman dan hemat biaya. Sedangkan aplikasi Web-enabled dapat digunakan untuk mencapai hal ini, virtual private network menawarkan solusi yang lebih komprehensif dan aman.

  
Gambar 1. Virtual private network (VPN)  
VPN menyampaikan informasi di Internet yang menghubungkan pengguna remote,  
kantor cabang, dan mitra bisnis ke jaringan perusahaan diperpanjang secara aman, seperti  
ditunjukkan pada Gambar 1. Penyedia layanan Internet (ISP) menawarkan akses yang hemat biaya untuk Internet (melalui saluran langsung atau nomor telepon lokal), \*memungkinkan perusahaan untuk menghilangkan mereka saat ini, mahal, leased line, panggilan jarak jauh, dan bebas pulsanomor telepon.

enabling companies to

eliminate their current, expensive, leased lines, long-distance calls, and toll-free

telephone numbers.  
Sebuah laporan penelitian VPN tahun 1997, oleh Infonetics Research, Inc, memperkirakan penghematan dari 20% menjadi 47% dari biaya wide area network (WAN) dengan mengganti leased line menjadi remote site dengan VPN. Dan, untuk remote access VPN, penghematan bisa 60% hingga 80% \*dari akses remote corporate dial-up biaya . Selain itu, akses Internet  
tersedia di seluruh dunia di mana alternatif konektivitas lainnya mungkin tidak tersedia.  
Meskipun teknologi untuk mengimplementasikan virtual private network ini hanya  
menjadi standar, tidak semua produk dapat mendukung semua metode VPN. Sementara beberapa metode VPN dapat digunakan dalam hubungannya dengan satu sama lain,  
beberapa solusi alternatif untuk satu sama lain. Sebuah solusi VPN yang tepat harus  
ditentukan sesuai dengan kebutuhan Anda dengan mengambil isu-isu berikut untuk  
dipertimbangan:  
• Kebutuhan Bisnis  
• Keamanan  
• Perfoma  
• Interoperabilitas dari solusi dengan sistem Anda saat ini  
Kunci untuk memaksimalkan nilai VPN adalah kemampuan bagi perusahaan untuk mengembangkan VPN mereka sebagai perubahan kebutuhan bisnis mereka dan dengan mudah meng-upgrade ke teknologi yang lebih maju. Vendor yang mendukung berbagai perangkat keras dan perangkat lunak produk VPN menyediakan fleksibilitas untuk memenuhi persyaratan ini. \*IPSec VPN berbasis solusi hari ini berjalan terutama di lingkungan IPv4,

tetapi penting bahwa mereka memiliki kemampuan sedang upgrade ke IPv6 untuk tetap interoperable dengan mitra bisnis dan / atau solusi pemasok VPN anda. Mungkin sama pentingnya adalah kemampuan untuk bekerja dengan vendor yang memahami isu-isu menyebarkan VPN. Implementasi VPN yang sukses melibatkan lebih dari teknologi. Pengalaman networking vendor memiliki peran yang tidak kalah pentingnya.

Ada tiga macam tipe interkoneksi VPN, yaitu *Acces* VPN, *Intranet* VPN dan *Extranet* VPN.

1. **Access VPN** : membuat koneksi jarak jauh untuk mengakses ke jaringan intranet atau

ekstranet pelanggan dan pengguna bergerak dengan menggunakan infrastruktur PSTN dial-up, ISDN, DSL, atau Mobile IP untuk membuat koneksi yang aman bagi mobile user, telecommuters dan kantor cabang.

****

Gambar 8. Solusi Access VPN

2. **Intranet VPN** : menghubungkan kantor pusat, kantor cabang, dan remote user ke dalam jaringan internal dengan menggunakan infrastruktur koneksi Dedicated.



Gambar 9. Solusi Intranet VPN

3. **Extranet VPN** : menghubungkan dengan pihak luar seperti pelanggan, supplier, rekan

bisnis, atau suatu komunitas ke dalam jaringan internal dengan menggunakan koneksi *dedicated*. Koneksi ini menghubungkan jaringan internal dengan jaringan di luar perusahaan.



Gambar 10. Solusi Extranet VPN

Sistem keamanan di VPN menggunakan beberapa metode lapisan sistem keamanan, diantaranya ;

1. **Metode tunneling** (terowongan), membuat terowongan virtual diatas jaringan publik

menggunakan protocol seperti *Point to Point Protocol* (PPTP), *Layer 2 Tunneling Protocol* (L2TP), *Generic Routing Encapsulation* (GRE) atau *IP Sec*. PPTP danL2TP adalah layer 2 tunneling protocol.keduanya melakukan pembungkusanpayload pada frame *Point to Point Protocol* (PPP) untuk di lewatkan pada jaringan. IPSec berada di layer 3 yang menggunakan

packet, yang akan melakukan pembungkusan IP header sebelum dikirim ke jaringan.

2. **Metode Enkrpsi** untuk *Encapsulations* (membungkus) paket data yang lewat di

dalam tunneling, data yang dilewatkan pada pembungkusan tersebut, data disini akan

dirubah dengan metode algoritma kripthography tertentu seperti DES, 3DES,

atau AES

3. **Metode Otentikasi User**, karena banyak user yang akan mengakses biasanya

digunakan beberapa metode otentikasi user seperti *Remote Access Dial In User Services*

(RADIUS) dan *Digital Certificates*.

4. **Integritas Data,** paket data yang dilewatkan di jaringan publik perlu penjaminan

integritas data / kepercayaan data apakah terjadi perubahan atau tidak. Metode VPN

menggunakan HMA C-MD5 atau HMA CSHA1 untuk menjadi paket tidak dirubah

pada saat pengiriman.

Beberapa keunggulan menggunakan VPN sebagai pembanding jaringan skala luas

(WAN) yang membuat banyak telco provider menawarkan solusi ini dan banyak perusahaan

mulai beralih ke teknologi tersebut, beberapa keunggulannya adalah ;

1. Standarisasi, kompatibel dengan standarstandar protocol *Internet Engineering Task*

*Force* (IETF) dan vendor dunia lainnya

2. Lebih ekonomis, lebih murah dibandingkan dengan solusi lain karena interkoneksi

dilewatkan di jaringan Internet dan tidak memerlukan perangkat khusus jika infrastruktur yang telah ada mendukung jaringan VPN.

3. Biaya sewa link yang murah dari penyedia jasa backbone dikarenakan menggunakan

layanan jaringan baru yang lebih ekonomis seperti *MultiProtocol Labeling Switching*

(MPLS).

4. Fleksibel Arsitektur, dapat dikoneksikan dengan infrastruktur yang sudah ada seperti

peralatan router/swtich yang mendukung VPN.

5. Integrasi Konektifitas Multimedia yang tinggi, akses dimana saja ke global interkoneksi untuk koneksi data, suara, dan video

6. Skalability, memungkinkan penyedia jasa untuk tetap bisa melayani permintaan pasar tanpa harus kehilangan kesempatan.

7. Security, memungkinkan traffic kritikal bisnis dengan aman dengan digunakannya metode tunneling dan enkripsi.

8. Managable, sangat cocok untuk efektifitas biaya karena kemudahan dalam manajemen vendor untuk multiple service berbasis IP

9. Traffic engineering, mudah dalam pengaturan *traffic bandwidth*, mekanisme *restorasi fault* dan mekanisme proteksi

10. Fast deployment, cocok untuk perusahaan yang memerlukan aplikasi-aplikasi berbasis IP yang cepat perubahannya

11. Jaminan *Service Level Aggreament* (SLA) dan Jaminan Kualitas Layanan atau *Quality* *of Services* (QoS), jaminan layanan *uptime* bagi kebutuhan akan kestabilan interkoneksi dan jaminan yang tinggi atas koneksi dapat dipenuhi dan memungkinkan prioritas berdasarkan kritikan atau traffic yang sensitifitas atas delay.