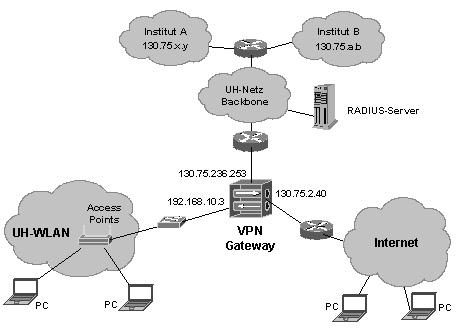
**VPN**

**(VIRTUAL PRIVATE NETWORK)**

1. **Pengertian *Virtual Private Network* (VPN)**

Menurut **K. V. Kale (2008, p69)**, *Virtual Private Network* (VPN) adalah jaringan *private* yang menggunakan jaringan publik seperti internet untuk menghubungkan *remote access* dan *user* secara bersama- sama dengan memberikan tingkat level privasi, *security*, *Quality of Service* (QoS), dan pengelolaan dimana jaringan tersebut dibangun seluruhnya dalam fasilitas yang dimiliki secara pribadi dan *dedicated*.



**Gambar 1. *Virtual Private Network***

# Fungsi VPN

Teknologi VPN menyediakan tiga fungsi utama dalam penggunaannya. Fungsi utama tersebut adalah sebagai berikut :

# Kerahasiaan

Teknologi VPN memiliki sistem kerja mengenkripsi semua data yang melewatinya. Dengan adanya teknologi enkripsi ini, maka kerahasiaan data menjadi lebih terjaga. Meskipun masih ada pihak yang dapat menyadap data, namun belum tentu pihak tersebut dapat membaca data itu dengan mudah karena data tersebut telah dienkripsi. Dengan menerapkan sistem enkripsi ini, maka tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data dengan mudah.

# Integritas data

Ketika melewati jaringan internet, data sebenarnya sudah berjalan sangat jauh melintasi berbagai negara. Di tengah perjalanannya, apapun bisa terjadi terhadap isi data tersebut, baik itu hilang, rusak, atau bahkan dimanipulasi isinya oleh orang lain. VPN memiliki teknologi yang dapat menjaga keutuhan data yang dikirim agar sampai ke tujuan tanpa cacat, hilang rusak, ataupun dimanipulasi oleh orang lain.

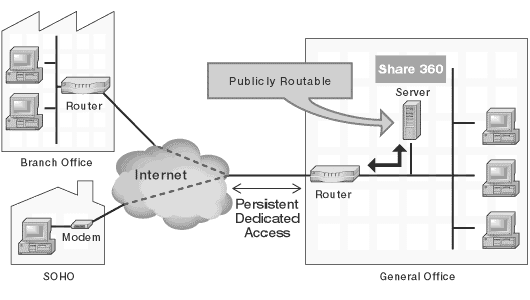
# Autentikasi Sumber

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data. 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 berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirimkan oleh pihak-pihak lain.

# Jenis-jenis VPN

* **Remote Access VPN**

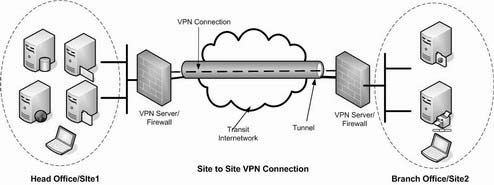
Tipe VPN ini memungkinkan koneksi jarak jauh (remote access) bagi pegawai yang sedang bertugas di luar kantor, luar kota ataupun sedang di luar negeri untuk dapat akses ke LAN di kantor pusat menggunakan jaringan internet. Hal ini terutama sangat berguna untuk dapat menerima email yang tersedia di LAN kantor pusat. Selain itu, hal tersebut juga berlaku bagi kantor cabang yang tidak memiliki koneksi secara terus-menerus ke kantor pusat. Kantor cabang tersebut dapat melakukan koneksi *dial-up* lokal ke suatu ISP dan setelah itu melakukan koneksi ke kantor pusat.



**Gambar 2.1 Remote Access VPN**

# Site-to-Site VPN

Site-to-Site VPN memungkinkan suatu *private network* diperluas melintasi jaringan internet atau layanan *public network* lainnya dengan cara yang aman. Site-to-Site VPN kadang disebut juga sebagai LAN-to-LAN VPN. Site-to-Site VPN merupakan suatu alternatif dari infrastruktur WAN yang biasa menghubungkan kantor-kantor cabang, kantor pusat, atau partner bisnis ke seluruh jaringan yang terdapat di perusahaan.



**Gambar 2.2 Site-to-Site VPN**

Site-to-Site VPN dibedakan menjadi dua jenis, yaitu :

# Intranet VPN

Intranet VPN digunakan untuk menghubungkan antara kantor pusat dengan kantor cabang atau kantor yang letaknya berjauhan melalui suatu *public infrastructure*.

# Extranet VPN

Extranet VPN merupakan intranet dari suatu perusahaan yang diperluas untuk menggabungkan para pemakai dari luar perusahaan, seperti : pemasok, penjual, pelanggan dan relasi bisnis. Sehingga antara kedua perusahaan dapat saling bertukar dan berbagi informasi dengan cepat dan mudah dengan penambahan *firewall* untuk keamanan *internal network* .

# Keamanan VPN

Seperti yang telah dijelaskan bahwa VPN menggunakan internet sebagai media perantaranya, maka keamanan pada jaringan VPN sangatlah diperlukan agar data yang dikirim dan diterima dapat terjamin keamanannya. Beberapa tipe keamanan yang dapat diterapkan pada teknologi VPN adalah enkripsi, autentikasi, autorisasi, dan firewall.

# Enkripsi

Enkripsi merupakan salah satu cara yang digunakan untuk mengubah data asli (sebenarnya) menjadi bentuk sandi (*chipper text*) yang mana sandi-sandi tersebut hanya dapat dimengerti oleh pihak pengirim dan penerima data sehingga data tersebut tidak dapat dibaca oleh orang luar yang tidak mempunyai hak akses untuk melihat data tersebut. Untuk mengubah sandi (*chipper text*) tersebut ke bentuk semula maka digunakan teknik yang dinamakan *dekripsi*. Terdapat dua cara untuk melakukan proses enkripsi, yaitu enkripsi kunci simetrik dan enkripsi kunci asimetrik.

# Enkripsi Kunci Simetrik

Pada enkripsi menggunakan kunci simetrik, setiap komputer memiliki kunci rahasia (kode) yang dapat digunakan untuk mengenkripsi informasi sebelum informasi tersebut dikirim ke komputer lain melalui jaringan. Kunci yang digunakan untuk mengenkripsi data sama dengan kunci yang digunakan untuk mendekripsi data. Oleh karena itu, kunci tersebut harus dimiliki oleh kedua komputer sehingga harus tercapai kesepakatan antara penerima dengan pengirim, misal dengan media telepon, email, atau bertemu langsung.

M etode enkripsi ini harus dijaga ketat agar tidak ada pihak luar yang mengetahuinya dan dengan mudah membaca data tersebut.

# Enkripsi Kunci Asimetrik

Pada enkripsi kunci asimetrik, proses enkripsi dan dekripsi masing-masing menggunakan dua buah kunci yang berbeda, yaitu *private key* dan *public key* yang saling berhubungan secara sistematis. Private key dibuat oleh penerima pesan dan hanya penerima pesan tersebut yang dapat mengetahui isinya, dari private key inilah, sebuah public key terbentuk. Setelah public key terbentuk, public key tersebut dikirimkan kepada pihak yang ingin mengirimkan pesan. Oleh pengirim pesan, public key tersebut digunakan untuk mengenkripsi pesan yang akan dikirim. Setelah pesan tersebut di terima, maka penerima pesan tersebut harus menggunakan private key untuk mendekripsi pesan tersebut. Dikarenakan mempunyai cara kerja yang rumit dan tingkat keamanan yang lebih baik, maka banyak orang yang lebih menggunakan sistem pengenkripsian data seperti ini.

# Autentikasi

Autentikasi merupakan salah satu proses untuk mengindetifikasi pengguna sehingga data yang dikirim akan menjadi jelas isi dan siapa pengirimnya. Biasanya dalam proses autentikasi, diperlukan *username* dan *password* sebagai alat verifikasinya. *Username* dan *password* ini dimaksudkan agar tidak sembarang orang dapat mengakses, mengirim ataupun mengambil data yang bersifat *private*.

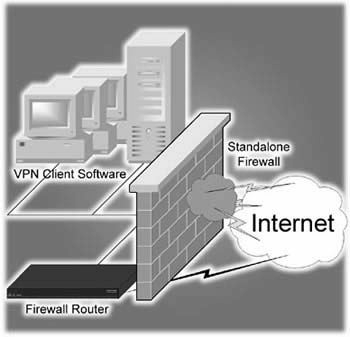
# Autorisasi

Autorisasi adalah pencarian apakah orang yang sudah diidentifikasi (diautentikasi), diizinkan untuk memanipulasi sumber daya atau data tertentu di jaringan VPN tersebut. Proses autorisasi inilah yang menentukan apakah pengguna tersebut dapat melakukan perintah atau tugas yang dikehendakinya pada jaringan VPN tersebut.

# Firewall

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software maupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring.

mambatasi, atau bahkan menolak suatu atau semua hubungan / kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, dan *local area network* (LAN). Firewall merupakan sebuah perangkat yang diletakkan antara *internet* dengan jaringan internal. Informasi yang keluar atau masuk harus melalui firewall ini. Tujuan utama dari firewall adalah untuk menjaga agar orang yang tidak berwenang tidak dapat melakukan akses, baik ke dalam maupun keluar.



**Gambar 4. *Firewall***

Firewall memiliki prinsip kerja dalam menjalankan kendalinya, prinsip kerja yang digunakan adalah sebagai berikut :

1. *Service Control* (Kendali Terhadap Layanan)

Prinsip kerja berdasarkan tipe-tipe layanan yang digunakan di internet dan boleh diakses baik untuk ke dalam ataupun keluar firewall. Firewall akan mengecek nomor IP address dan nomor port yang digunakan, baik pada protokol TCP dan UDP. Firewall bisa dilengkapi software proxy untuk menerima dan menterjemahkan setiap permintaan atas suatu layanan sebelum mengizinkannya. Selain itu, server juga bisa menggunakan software, misalnya untuk layanan web atau mail.

1. *Direction Control* (Kendali Terhadap Arah)

Prinsip kerja berdasarkan arah dari berbagai permintaan (request) terhadap layanan. Layanan akan dikenali dan diizinkan melewati firewall.

1. *User Control* (Kendali Terhadap Pengguna)

Prinsip kerja berdasarkan pengguna / *user* untuk dapat menjalankan suatu layanan. Dengan demikian, ada user yang dapat menjalankan suatu *service* dan ada yang tidak. User tidak dapat menjalankan *service* karena tidak diizinkan untuk melewati *firewall*. Prinsip ini biasa digunakan untuk membatasi akses keluar user jaringan lokal, namun bisa juga diterapkan untuk membatasi akses terhadap pengguna dari luar.

1. *Behavior Control* (Kendali Terhadap Perlakuan)

Prinsip kerja berdasarkan seberapa banyak layanan itu telah digunakan. Misalnya, firewall dapat memfilter email untuk menanggulangi atau mencegah spam.

# Tunneling

Teknologi *tunneling* merupakan teknologi yang bertugas untuk manangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Disebut *tunnel* karena koneksi *point-to-point* tersebut sebenarnya terbentuk dengan melintasi jaringan umum, namun koneksi tersebut tidak mempedulikan paket-paket data milik orang lain yang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari pembuatnya.

Teknologi ini dapat dibuat di atas jaringan dengan pengaturan IP *Addressing* dan IP *Routing* yang sudah baik atau telah terhubung sehingga antara sumber *tunnel* dengan tujuan *tunnel* dapat saling berkomunikasi melalui jaringan dengan pengalamatan IP. Apabila komunikasi antara sumber dan tujuan dari *tunnel* tidak dapat berjalan dengan baik, maka *tunnel* tersebut tidak akan terbentuk dan VPN pun tidak dapat dibangun. Setelah *tunnel* tersebut terbentuk, maka koneksi *point-to-point* tersebut dapat langsung digunakan untuk mengirim dan menerima data. Dalam penerapannya di VPN, t*unnel* dilengkapi dengan sebuah sistem enkripsi untuk menjaga data-data yang melewati *tunnel* tersebut. Proses enkripsi inilah yang menjadikan teknologi VPN menjadi aman dan bersifat pribadi.

## Point to Point Tunneling Protocol (PPTP)

PPTP merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari *remote client* ke *server* pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP.

Teknologi jaringan PPTP merupakan pengembangan dari *remote access* Point-*to*-Point protocol yang dikeluarkan oleh *Internet Engineering Task Force* (IETF). PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP datagrams agar dapat ditransmisikan melalui intenet. PPTP juga dapat digunakan pada jaringan *private* LAN-*to*-LAN.

Umumnya terdapat tiga komputer yang diperlukan untuk membangun PPTP, yaitu sebagai berikut :

* + - * 1. Klien PPTP
        2. Network access server (NAS)
        3. Server PPTP

Akan tetapi tidak diperlukan network access server dalam membuat PPTP tunnel saat menggunakan klien PPTP yang terhubung dengan LAN untuk dapat terhubung dengan server PPTP yang terhubung pada LAN yang sama.

## Layer 2 Tunneling Protocol (L2TP)

L2TP adalah tunneling protokol yang memadukan dua buah tunneling protokol yaitu L2F (Layer 2 Forwarding) milik cisco dan PPTP milik Microsoft. L2TP biasa digunakan dalam membuat *Virtual Private Dial Network* (VPDN) yang dapat bekerja membawa semua jenis protokol komunikasi di dalamnya. Paket data L2TP dikirim melalui protokol UDP. Terdapat dua model tipe L2TP yaitu :

* *Voluntary Tunnel*

*Voluntary Tunnel* merupakan *tunnel* yang dibuat berdasarkan permintaan klien. Pada awalnya klien akan melakukan koneksi kepada ISP yang menyediakan jasa VPN. Setelah menerima permintaan klien, ISP tersebut membuatkan jalur khusus yang menghubungkan klien tersebut dengan VPN servernya.

* *Compulsory Tunnel*

Berbeda halnya dengan *voluntary tunnel*, *compulsory tunnel* dibuat oleh perangkat *intermediate*. Perangkat *intermediate* ini bisa berupa dial-up server ataupun alat lainnya. Ketika klien dan *remote client* yang terhubung dengan LAN ingin membangun koneksi, mereka harus terhubung terlebih dahulu dengan perangkat *intermediate* yang biasanya terletak di ISP. Setelah koneksi sudah terbuat maka perangkat inilah yang membuat tunnel.

* + - 1. **IP *Secu rity* (IPSec)**

Ipsec merupakan *tunneling protocol* yang bekerja pada layer 3. IPSec menyediakan layanan sekuritas pada IP layer dengan mengizinkan sistem untuk memilih protokol keamanan yang diperlukan, memperkirakan algoritma apa yang akan digunakan pada layanan, dan menempatkan kunci kriptografi yang diperlukan untuk menyediakan layanan yang diminta. Protokol yang berjalan dibelakang IPSec adalah:

1. AH (Authentication Header), menyediakan layanan *authentication* (menyatakan bahwa data yang dikirim berasal dari pengirim yang benar), *intregrity* (keaslian data), dan *replay protection* (transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengizinkan), juga melakukan pengamanan terhadap IP header (*header compression*).
2. ESP (*Encapsulated Security Payload*), menyediakan layanan *authentication*, *intregity*, *replay protection*, dan *confidentiality* (keamanan terjaga) terhadap data. ESP melakukan pengamanan data terhadap segala sesuatu dalam paket data setelah header.

# Zentyal

Zentyal atau dengan nama sebelumnya *eBox* merupakan aplikasi *open source* untuk server jaringan terpadu yang menawarkan administrasi jaringan komputer mudah dan efisien untuk usaha kecil dan menengah. Zentyal dapat berfungsi sebagai gateway, *manager* infrastruktur, *unified threat manager*, *server* kantor, *server* komunikasi terpadu atau kombinasi dari fungsi di atas. *Source code* Zentyal dimiliki di bawah ketentuan GNU General Public License, serta dibawah ketentuan hak milik yaitu eBox Technology S.L. Keunggulan salah satunya adalah tampilannya yang *user friendly* karena memiliki *graphic user interface* (GUI) sehingga mudah digunakan dan dipelajari oleh user yang baru pertama kali menggunakan.

# OpenVPN

OpenVPN adalah aplikasi open source yang mengimplementasikan teknik *Virtual Private Network* (VPN) untuk membuat koneksi *point-to-point* atau *site-to-site* dan fasilitas *remote access* secara aman. Untuk melakukan *autentifikasi* pada saat membangun suatu koneksi, OpenVPN menggunakan *pre-shared key*, *certificate*, dan *username / password*, yang mana untuk proses enkripsinya menggunakan OpenSSL

# Kelebihan dan Kekurangan OpenVPN

OpenVPN menawarkan berbagai kelebihan diantaranya adalah :

* Layer 2 dan layer 3 VPN : OpenVPN menawarkan 2 mode dasar yang bekerja baik pada layer 2 maupun layer 3 VPN. Tunnel OpenVPN juga dapat mengirim ethernet frames, paket IPX, dan paket Windows Networking Browsing (NETBIOS).
* Konfigurasi proxy dan pendukungnya: OpenVPN mempunyai proxy pendukung dan dapat di konfigurasikan untuk bekerja sebagai TCP atau UDP, dan sebagai server atau client. Sebagai server, OpenVPN menunggu hingga client meminta koneksi. Dan sebagai client, OpenVPN mencoba untuk membangun sebuah koneksi berikut konfigurasinya.
* Fleksibilitas yang tinggi memungkinkan untuk melakukan *scripting* : OpenVPN menawarkan *scripting* individual. Script ini dapat digunakan untuk berbagai macam tujuan seperti *autentifikasi* untuk failover dan lainnya.
* Instalasi yang mudah pada setiap platform : Langkah instalasi serta penggunaan yang sangat mudah untuk dipelajari.
* OpenVPN menyediakan manajemen interface yang dapat digunakan untuk mengkontrol secara remote atau mengatur openVPN daemon secara terpusat.
* Kelebihan openVPN adalah *cross-platform portability*, stabilitas yang sangat baik, skalabilitas yang sangat tinggi, mencapai ratusan sampai ribuan client, instalasi yang relatif mudah, dan men-*support dynamic IP address* dan *NAT*.

Selain mempunyai banyak kelebihan, OpenVPN juga memiliki kelemahan yaitu :

* Tidak kompatibel dengan IPsec, yang mana IPsec merupakan solusi dari VPN pada umumnya.
* Hanya sedikit orang yang mengetahui cara menggunakan OpenVPN, terutama dalam skenario/masalah jaringan yang sulit.
* Pada saat ini, OpenVPN hanya dapat menghubungkan komputer satu dengan komputer lain, namun ke depannya akan ada perusahaan yang mengintegrasikan *client* OpenVPN pada alat-alatnya.