FIREWALL DAN VPN

A. Definisi Firewall

Firewall didefinisikan sebagai suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk **melindungi**, baik dengan **menyaring**, **membatasi** atau bahkan **menolak** suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya (Muammar W. K, 2004).

Firewall (dari buku Building Internet Firewalls, oleh Chapman dan Zwicky) didefinisikan sebagai sebuah komponen atau kumpulan komponen yang membatasi akses antara sebuah jaringan yang diproteksi dan internet, atau antara kumpulan-kumpulan jaringan lainnya.

Stiawan (2008) mengatakan bahwa, firewall adalah sebuah komputer yang memproteksi jaringan dari jaringan yang tidak dipercaya yang memisahkan antara jaringan lokal dengan jaringan publik, dengan melakukan metode filtering paket data yang masuk dan keluar (Marcus Goncalves, Firewall Completed:227)

Arman (2007) mendefinisikan firewall sebagai sebuah titik diantara dua/lebih jaringan dimana semua lalu lintas (trafik) harus melaluinya (chooke point); trafik dapat dikendalikan oleh dan diautentifikasi melalui sautu perangkat, dan seluruh trafik selalu dalam kondisi tercatat (logged).

Dari beberapa definisi diatas, penulis dapat memberikan definisi dimana firewall adalah sebuah pembatas antara suatu jaringan lokal dengan jaringan lainnya yang sifatnya publik (dapat diakses oleh siapapun) sehingga setiap data yang masuk dapat diidentifikasi untuk dilakukan penyaringan sehingga aliran data dapat dikendalikan untuk mencegah bahaya/ancaman yang datang dari jaringan publik

B. Tujuan Penggunaan

- Firewall biasanya digunakan untuk mencegah atau mengendalikan aliran data tertentu. Artinya, setiap paket yang masuk atau keluar akan diperiksa, apakah cocok atau tidak dengan kriteria yang ada pada standar keamanan yang didefinisikan dalam firewall.
- Untuk melindungi dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN).
- Penggunaan firewall yang dapat mencegah upaya berbagai trojan horses, virus, phishin, spyware untuk memasuki sistem yang dituju dengan cara mencegah hubungan dari luar, kecuali yang diperuntukan bagi komputer dan port tertentu

C. Teknik-Teknik yang Digunakan firewall

1. Service control (kendali terhadap layanan)

Berdasarkan tipe-tipe layanan yang digunakan di Internet dan boleh diakses baik untuk kedalam ataupun keluar firewall. Biasanya firewall akan mencek no IP Address dan juga nomor port yang di gunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi software untuk proxy yang akan menerima dan menterjemahkan setiap permintaan akan suatu layanan sebelum mengijinkannya. Bahkan bisa jadi software pada server itu sendiri , seperti layanan untuk web ataupun untuk mail.

2. Direction Control (kendali terhadap arah)

Berdasarkan arah dari berbagai permintaan (request) terhadap layanan yang akan dikenali dan diijinkan melewati firewall.

3. User control (kendali terhadap pengguna)

Berdasarkan pengguna/user untuk dapat menjalankan suatu layanan, artinya ada user yang dapat dan ada yang tidak dapat menjalankan suatu servis,hal ini di karenakan user tersebut tidak di ijinkan untuk melewati firewall. Biasanya digunakan untuk membatasi user dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.

4. Behavior Control (kendali terhadap perlakuan)

Berdasarkan seberapa banyak layanan itu telah digunakan. Misalnya, firewall dapat memfilter email untuk menanggulangi/mencegah spam.

D. Arsitektur Firewall

1. Singgle Box

Arsitektur firewall sederhana memiliki objek tunggal yang bertindak sebagai firewall. Secara umum, keuntungan keamanan single-box architectures adalah bahwa mereka menyediakan satu tempat untuk dapat berkonsentrasi dan pastikan bahwa firewall telah dikonfigurasi dengan benar, dan kerugiannya adalah bahwa keamanan sepenuhnya tergantung pada satu tempat. Tidak ada pertahanan berlapis, namun konfigurasi tahu persis apa link terlemah, dan titik itu jauh lebih sulit ditembus dengan beberapa lapisan.

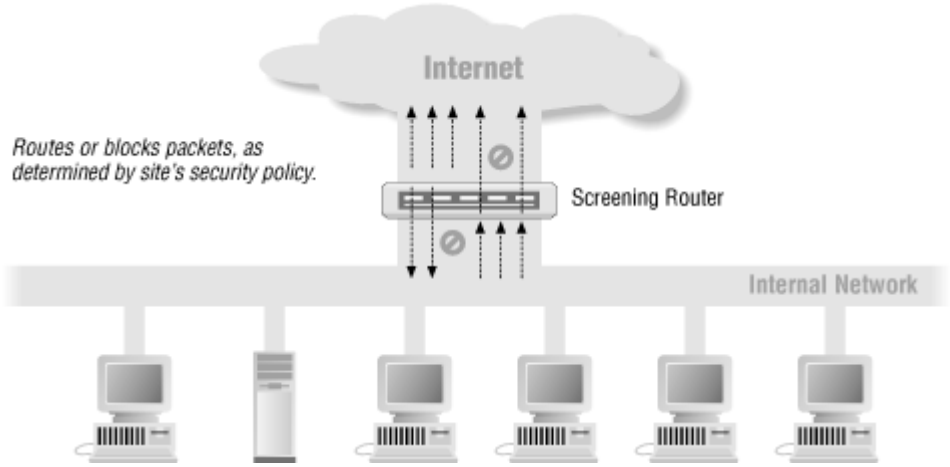
Dalam prakteknya, keuntungan dari single-box architectures bukan keamanan mereka tetapi dalam masalah praktis lainnya. Dibandingkan dengan sistem multi-layer yang telah terintegrasi dengan jaringan, single-box architectures lebih murah, lebih mudah untuk memahami dan menjelaskan kepada manajemen, dan lebih mudah untuk mendapatkan dari vendor eksternal. Hal ini membuat solusi pilihan untuk situs kecil. Hal ini juga membuatnya menjadi solusi menggiurkan bagi orang-orang yang mencari solusi keamanan ajaib yang dapat dimasukkan sekali dan melupakan.

terbagi dua yaitu :

Screening Router dan Dual-homed host architecture

a) Screening Router

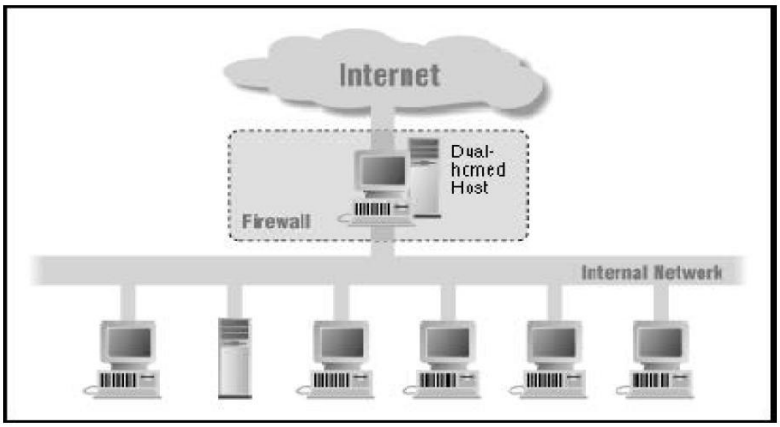
Hal ini dimungkinkan untuk menggunakan sistem packet filtering dengan sendirinya sebagai firewall, dengan hanya menggunakan screening router untuk melindungi seluruh jaringan. Karena sistem ini murah, juga karena hampir selalu perlu router untuk menghubungkan ke Internet, dan hanya dapat mengkonfigurasi packet filtering di router itu. Di sisi lain, itu tidak sangat fleksibel, dapat mengizinkan atau menolak protokol dengan nomor port, tapi sulit untuk memungkinkan beberapa operasi sementara menyangkal jaringan lain dalam protokol yang sama, atau untuk memastikan bahwa apa yang datang pada port tertentu sebenarnya adalah protokol yang ingin dijalankan. Selain itu,tidak memberikan kedalaman pertahanan. Jika router terganggu, maka jaringan tidak memiliki keamanan lebih lanjut.



b) Dual-homed host architecture

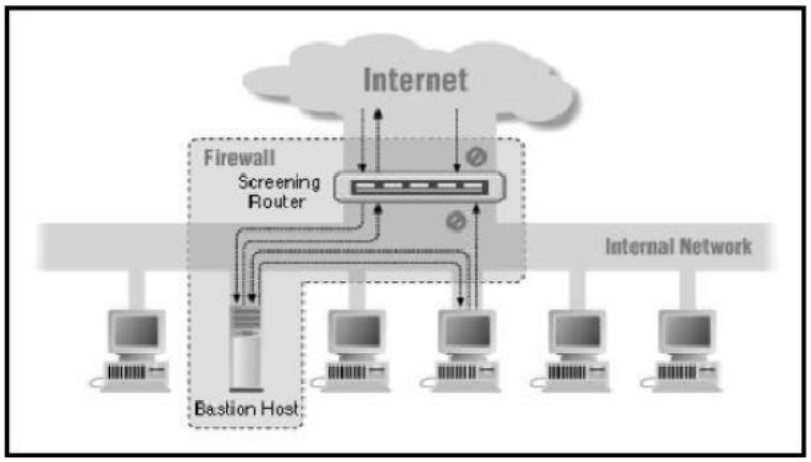
Arsitektur dual-home host yaitu komputer yang memiliki paling sedikit dua interface jaringan. Untuk mengimplementasikan tipe arsitektur dual-homed host, fungsi routing pada host ini di non-aktifkan. Sistem di dalam firewall dapat berkomunikasi dengan dual-homed host dan sistem di luar firewall dapat berkomunikasi dengan dual-homed host, tetapi kedua sistem ini tidak dapat berkomunikasi secara langsung.

Dual-homed host dapat menyediakan service hanya dengan menyediakan proxy pada host tersebut, atau dengan membiarkan user melakukan logging secara langsung pada dual-homed host.



2. Screened host architecture

Arsitektur screened host menyediakan service dari sebuah host pada jaringan internal dengan menggunakan router yang terpisah. Pada arsitektur ini, pengamanan utama dilakukan dengan packet filtering

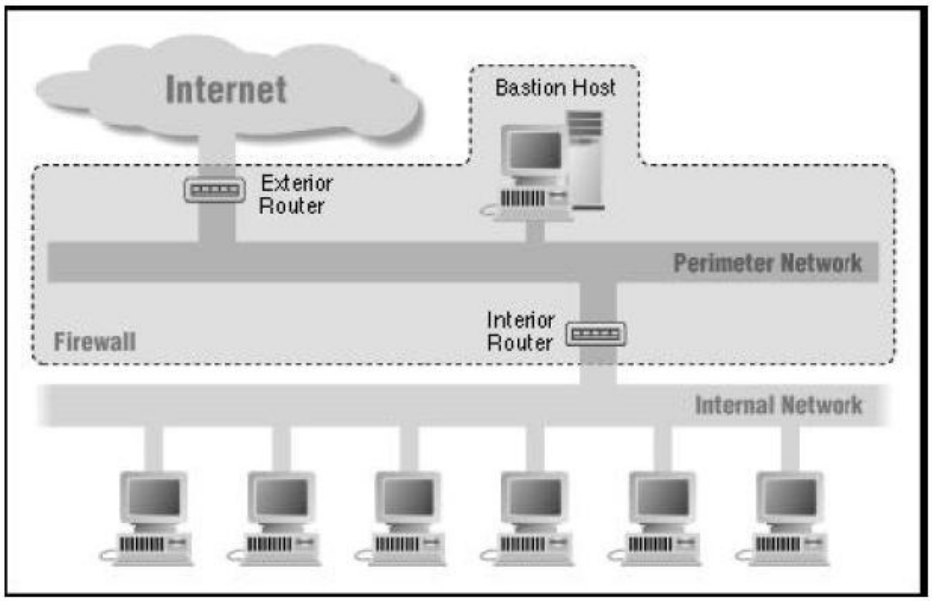


Bastion host berada dalam jaringan internal. Packet filtering pada screening router dikonfigurasi sehingga hanya bastion host yang dapat melakukan koneksi ke Internet (misalnya mengantarkan mail yang datang) dan hanya tipe-tipe koneksi tertentu yang diperbolehkan. Tiap sistem eksternal yang mencoba untuk mengakses sistem internal harus berhubungan dengan host ini terlebih dulu. Bastion host diperlukan untuk tingkat keamanan yang tinggi.

3. Screened subnet architecture

Arsitektur screened subnet menambahkan sebuah layer pengaman tambahan pada arsitekture screened host, yaitu dengan menambahkan sebuah jaringan perimeter yang lebih mengisolasi jaringan internal dari jaringan Internet. Jaringan perimeter mengisolasi bastion host sehingga tidak langsung terhubung ke jaringan internal.

Arsitektur screened subnet yang paling sederhana memiliki dua buah screening router, yang masing-masing terhubung ke jaringan perimeter. Router pertama terletak di antara jaringan perimeter dan jaringan internal, dan router kedua terletak di antara jaringan perimeter dan jaringan eksternal (biasanya Internet).



E. Tipe-Tipe Firewall ada 4

1. Packet Filtering Router

Firewall jenis ini memfilter paket data berdasarkan alamat dan pilihan yang sudah ditentukan terhadap paket tersebut. Ia bekerja dalam level internet protokol (IP) paket data dan membuat keputusan mengenai tindakan selanjutnya (diteruskan atau tidak diteruskan) berdasarkan kondisi dari paket tersebut. Firewall jenis ini terbagi lagi menjadi tiga subtipe:

- **Static Filtering:** Jenis filter yang diiplementasikan pada kebanyakan router, dimana modifikasi terhadap aturan-aturan filter harus dilakukan secara manual.
- **Dynamic Filtering:** Apabila proses-proses tertentu di sisi luar jaringan dapat merubah aturan filer secara dinamis berdasarkan even-even tertentu yang diobservasi oleh router (sebagai contoh, paket FTP dari sisi luar dapat diijinkan apabila seseorang dari sisi dalam me-request sesi FTP).
- **Stateful Inspection:** Dikembangkan berdasarkan teknologi yang sama dengan dynamic filtering dengan tambahan fungsi eksaminasi secara bertingkat berdasarkan muatan data yang terkandung dalam paket IP.

Baik dynamic maupun static filtering menggunakan tabel status (state table) dinamis yang akan membuat aturan-aturan filter sesuai dengan even yang tengah berlangsung. Muammar W. K (2004) menambahkan bahwa kelemahan tipe ini adalah cukup rumitnya untuk menyetting paket yang akan difilter secara tepat, serta lemah dalam hal authentikasi. Adapun serangan yang dapat terjadi pada firewall dengan tipe ini adalah:

- IP address spoofing : Intruder (penyusup) dari luar dapat melakukan ini dengan cara menyertakan/menggunakan ip address jaringan lokal yang telah diijinkan untuk melalui firewall.
- Source routing attacks : Tipe ini tidak menganalisa informasi routing sumber IP, sehingga memungkinkan untuk membypass firewall.
- Tiny Fragment attacks : Intruder membagi IP kedalam bagian-bagian (fragment) yang lebih kecil dan memaksa terbaginya informasi mengenai TCP header. Serangan jenis ini di design untuk menipu aturan penyaringan yang bergantung kepada informasi dari TCP header. Penyerang berharap hanya bagian (fragment) pertama saja yang akan di periksa dan sisanya akan bisa lewat dengan bebas. Hal ini dapat di tanggulangi dengan cara menolak semua packet dengan protokol TCP dan memiliki Offset = 1 pada IP fragment (bagian IP)

2. Circuit Gateways

Firewall jenis ini beroperasi pada layer (lapisan) transpor pada network, dimana koneksi juga diautorisasi berdasarkan alamat. Sebagaimana halnya Packet Filtering, Circuit Gateway (biasanya) tidak dapat memonitor trafik data yang mengalir antara satu network dengan network lainnya, tetapi ia mencegah koneksi langsung antar network.

Cara kerjanya adalah gateway akan mengatur kedua hubungan tcp tersebut, 1 antara dirinya (gw) dengan TCP pada pengguna lokal (inner host) serta 1 lagi antara dirinya (gw) dengan TCP pengguna luar (outside host). Saat dua buah hubungan terlaksana, gateway akan menyalurkan TCP segment dari satu hubungan ke lainnya tanpa memeriksa isinya. Fungsi pengamanannya terletak pada penentuan hubungan mana yang di ijinkan. Penggunaan tipe ini biasanya dikarenakan administrator percaya dengan pengguna internal (internal users).

3. Application Gateways

Firewall tipe ini juga disebut sebagai firewall berbasis proxy. Ia beroperasi di level aplikasi dan dapat mempelajari informasi pada level data aplikasi (yang dimaksudkan disini adalah isi (content) dari paket data karena proxy pada dasarnya tidak beroperasi pada paket data). Filterisasi dilakukan berdasarkan data aplikasi, seperti perintah-perintah FTP atau URL yang diakses lewat HTTP. Dapat dikatakan bahwa firewall jenis ini "memecah model client-server".

Cara kerjanya adalah apabila ada pengguna yang menggunakan salah satu aplikasi semisal FTP untuk mengakses secara remote, maka gateway akan meminta user memasukkan alamat remote host yang akan di akses. Saat pengguna mengirimkan user ID serta informasi lainnya yang sesuai maka gateway akan melakukan hubungan terhadap aplikasi tersebut yang terdapat pada remote host, dan menyalurkan data diantara kedua titik. apabila data tersebut tidak sesuai maka firewall tidak akan meneruskan data tersebut atau menolaknya. Lebih jauh lagi, pada tipe ini Firewall dapat di konfigurasikan untuk hanya mendukung beberapa aplikasi saja dan menolak aplikasi lainnya untuk melewati firewall.

Kelebihannya adalah relatif lebih aman daripada tipe packet filtering router lebih mudah untuk memeriksa (audit) dan mendata (log) semua aliran data yang masuk pada level aplikasi. Kekurangannya adalah pemrosesan tambahan yang berlebih pada setiap hubungan. yang akan mengakibatkan terdapat dua buah sambungan koneksi antara pemakai dan gateway, dimana gateway akan memeriksa dan meneruskan semua arus dari dua arah.

4. Hybrid Firewalls

Firewall jenis ini menggunakan elemen-elemen dari satu atau lebih tipe firewall. Firewall komersial yang pertama, DEC SEAL, adalah firewall berjenis hybrid, dengan menggunakan proxy pada sebuah bastion hosts (mesin yang dilabeli sebagai "gatekeeper") dan packet filtering pada gateway ("gate"). Sistem hybrid seringkali digunakan untuk menambahkan layanan baru secara cepat pada sistem firewall yang sudah tersedia.

Kita bisa saja menambahkan sebuah circuit gateway atau packet filtering pada firewall berjenis application gateway, karena untuk itu hanya diperlukan kode proxy yang baru yang ditulis untuk setiap service baru yang akan disediakan. Kita juga dapat memberikan autentifikasi pengguna yang lebih ketat pada Stateful Packet Filer dengan menambahkan proxy untuk tiap service.

F. Sistem Pengamanan Menggunakan Firewall

1. **Packet Filtering**

Sistem pada paket filtering merupakan sistem yang digunakan untuk mengontrol keluar, masuknya paket dari antara host yang didalam dan host yang yang diluar tetapi sistem ini melakukannya secara selektif. Sistem ini dapat memberikan jalan atau menghalangi paket yang dikirimkan, sistem ini sangat mengkitalkan arsitektur yang disebut dengan 'Screened Router'. Router ini menjadi filter dengan menganalisa bagian kepala dari setiap paket yang dikirimkan. Karena bagian kepala dari paket ini berisikan informasi penting yaitu :

- IP source address.
- IP destination address.
- Protocol (dengan melihat apakah paket tersebut berbentuk TCP, UDP atau ICMP).
- Port sumber dari TCP atau UDP.
- Port tujuan dari TCP atau UDP.
- Tipe pesan dari ICMP.
- Ukuran dari paket.

Cara Kerja Sistem Packet Filtering ini adalah mengawasi secara individual dengan melihat melalui router, sedangkan router yang telah dimaksud adalah sebuah perangkat keras yang dapat berfungsi sebagai sebuah server karena alat ini harus membuat keputusan untuk me-rout seluruh paket yang diterima. Alat ini juga harus menentukan seperti apakah pengiriman paket yang telah didapat itu kepada tujuan yang sebenarnya. Dalam hal ini router tersebut saling berkomunikasi dengan protokol-protokol untuk me-rout. Protokol yang dimaksudkan adalah Routing Information Protocol (RIP) atau Open Shortest Path First (OSPF) yang menghasilkan sebuah table routing.

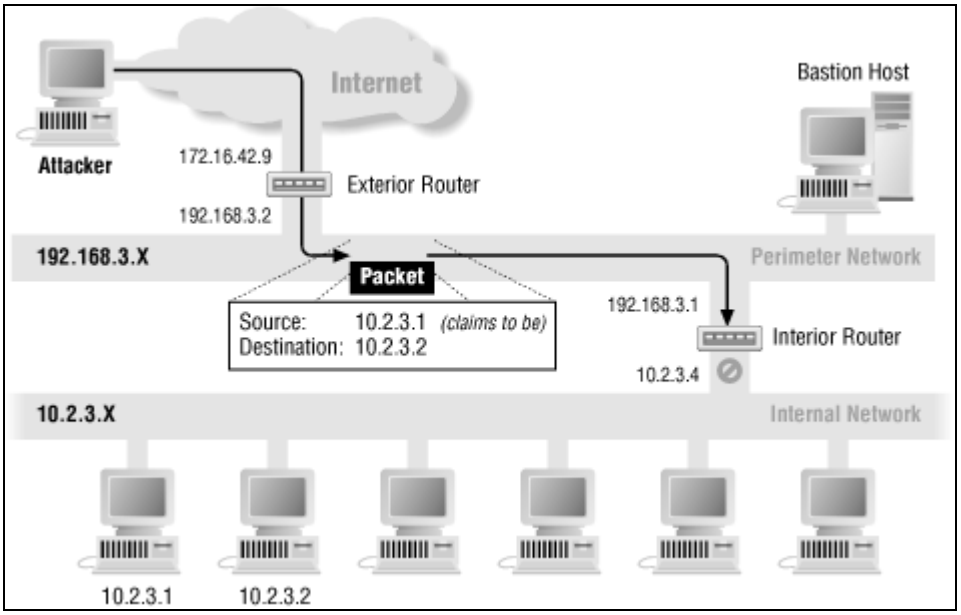
Tabel routing itu menunjukkan kemana tujuan dari paket yang diterima. Router yang menjadi filter pada packet filtering dapat menyediakan sebuah choke point (sebuah channel yang sempit yang sering digunakan untuk dipakai oleh penyerang sistem dan tentu saja dapat dipantau juga dikontrol oleh kita) untuk semua pengguna yang memasuki dan meninggalkan network. Karena sistem ini beroperasi ditingkat Network Layer dan Transport Layer dari tingkatan protokol pada tingkatan pada Transmission Control Protocol (TCP/IP). Bagian kepala dari network dan transport mengawasi informasi-informasi berikut:

Protokol (IP header, pada network layer); didalamnya byte 9 mengidentifikasikan protokol dari paket.

- Source address (IP header, pada network layer); alamat sumber merupakan alamat IP 32 bit dari host yang menciptakan oleh paket.
- Destination address (IP header, pada network layer); alamat tujuan yang berukuran 32 bit dari host yang menjadi tujuan dari paket.
- Source port (TCP atau UDP header, pada transport layer); pada setiap akhir dari koneksi TCP atau UDP tersambung dengan sebuah port, Walaupun port-port TCP terpisah dan cukup jauh dari port-port user datagram protocol (UDP). Port-port yang mempunyai nomor dibawah 1024 diterbalikan karena nomor-nomor ini telah didefinisikan secar khusus, sedangkan untuk port-port yang bernomor diatas 1024 (inklusif) lebih dikenal dengan port ephermal. Konfigurasi dari nomor pengalamatan ini diberikan sesuai dengan pilihan dari vendor.
- Destination port (TCP atau UDP header, transport layer); nomor port dari tujuan mengindikasikan port yang dikirimi paket. Servis yang akan diberikan pada sebuah host dengan mendengarkan port. Adapun port yang difilter adalah 20/TCP dan 21/TCP untuk koneksi ftp atau data, 23/TCP untuk telnet, 80/TCP untuk http dan 53/TCP untuk zona transfer DNS.
- Connection status (TCP atau UDP header, transport layer); status dari koneksi memberitahukan apakah paket yang dikirim merupakan paket pertama dari sesi di network. Jika paket merupakan paket pertama maka pada TCP header diberlakukan ‘false’ atau 0 dan untuk mencegah sebuah host untuk mengadakan

TCP & UDP menggunakan port number ini untuk membedakan pengiriman paket data ke beberapa aplikasi berbeda yang terletak pada komputer yang sama (Stiawan, 2008). Pada saat paket data di alamatkan ke tujuan, komputer tujuan harus mengetahui yang harus dilakukan pada paket tersebut, protocol TCP/IP menggunakan salah satu dari 65,536 pengelamatan penomeran port. Port number inilah yang akan membedakan antara satu aplikasi dengan aplikasi lainnya atau satu protocol dengan protocol lainnya pada saat proses
transmisi data antara sumber dan tujuan.

Untuk dapat melewatkan paket data dari sumber ke tujuan pada router terdapat protocol pengelamatan atau routing protocol yang saling mengupdate antara satu dengan yang lainya agar dapat melewatkan data sesuai dengan tujuannya. Di peralatan router layer 3 diperlukan konfigurasi khusus agar paket data yang masuk dan keluar dapat diatur, Access Control List (ACL) adalah pengelompokan paket berdasarkan kategori yang mengatur lalu lintas network. Dengan menggunakan ACL ini kita bisa melakukan filtering dan blocking paket data yang yang masuk dan keluar dari network atau mengatur akses ke sumber daya di network (Stiawan, 2008).

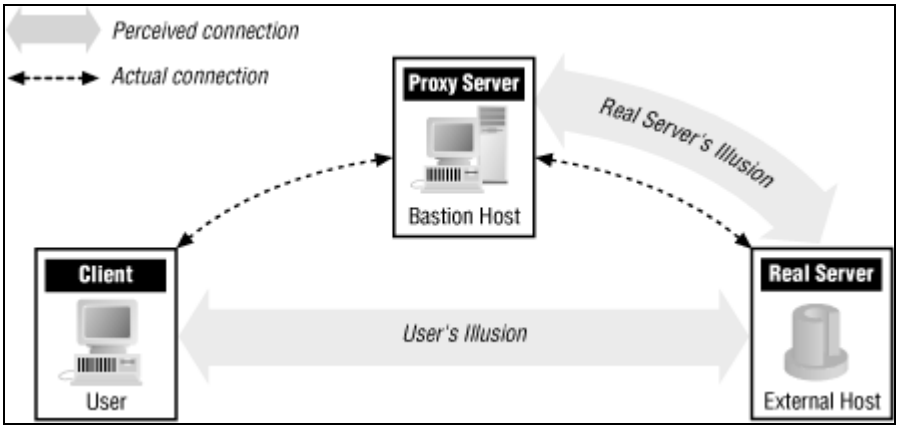


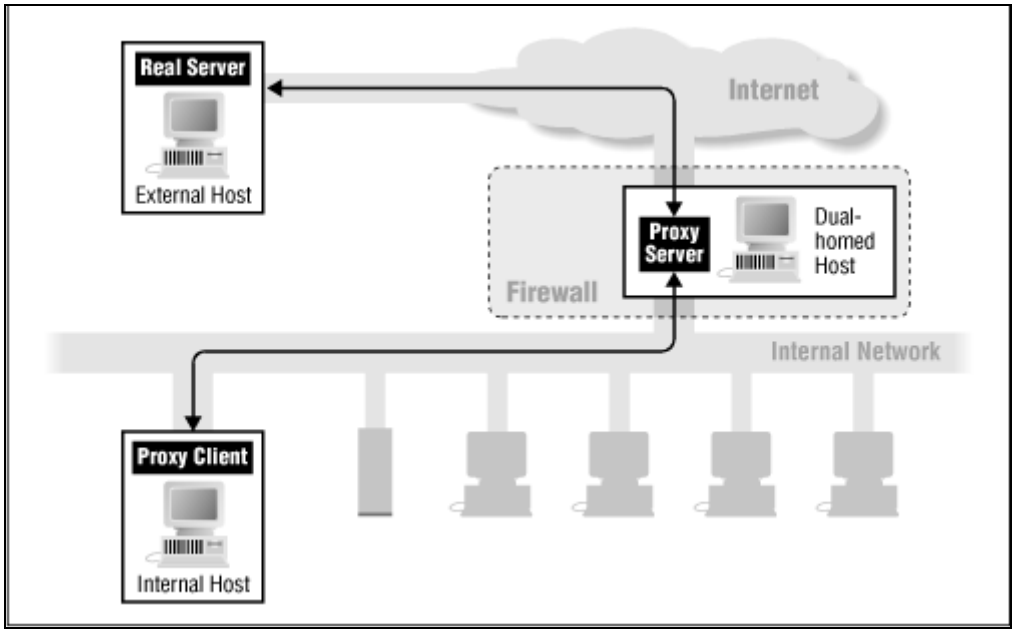
2. Proxy Services

Proxy memberikan akses internet untuk satu buah host atau host yang dalam jumlah kecil dengan terlihat seperti menyediakan akses untuk seluruh host kita. Sebuah proxy server untuk protokol tertentu atau sebuah set dari protokol dapat dijalankan pada sebuah dual-homed host atau pada bastion host. Pada proxy ini sangat mendukung arsitektur dari client/server. Clinet/server ini membentuk sebuah sistem dimana komponen-komponen dari software saling berinteraksi.

Dalam hal ini para klien dapat meminta seluruh kebutuhan dan pelayanan yang dinginkan dan server menyediakannya. Sistem proxy ini harus mendukung seluruh pelayanan yang diminta dan diperlukan oleh klien. Karena hal ini maka server harus mempunyai file server yang sangat besar dan selalu aktif dimana file-file yang terdapat pada server akan digunakan oleh setiap komputer yang terhubung baik dalam Lokal Area Network (LAN) ataupun Wide Area Network (WAN).

Pada file server selain dari list yang cukup panjang sebagai database yang dapat digunakan oleh setiap klien yang akan menggunakan alamat IP yang legal, terdapat juga file-file untuk aplikasi yang bekerja pada server utama. Proxy merupakan sistem pengamanan yang memerlukan alamat IP yang jelas dan valid, karena server yang utama terdapat di internet. Pada proxy terdapat empat pendekatan yang akan dilakukan pada sisi klien yang sangat berperan penting.





Pendekatanpendekatan tersebut yaitu :

- **Proxy-aware application software**

  Dengan pendekatan ini software harus mengetahui bagaimana untuk membuat kontak dengan proxy server daripada dengan server yang sebenarnya ketika user membuat suatu permintaan; dan bagaimana memberitahukan proxy server, server asli yang mana yang harus dibuatkan koneksi.

- **Proxy-aware operating system software**

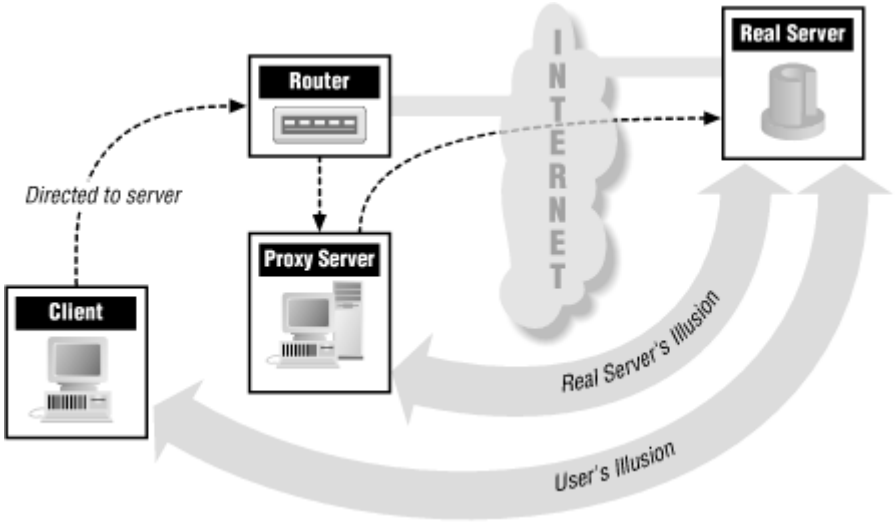
  Dengan pendekatan ini, sistem operasi yang dijalankan oleh user sudah harus dimodifikasikan sehingga koneksi IP yang sudah diperiksa untuk apakah paket tersebut harus dikirimkan kepada proxy server. Mekanisasi dari ini sangat bergantung sekali pada runtime linking yang dinamis (kemampuannya untuk memberikan library ketika program dijalankan).mekanisme ini tidak selalu berjalan dengan mulus dan dapat gagal yang tidak wajar untuk user.

- **Proxy-aware user procedures**

  Pendekatan ini pengguna menggunakan software client yang tidak mengerti bagaimana me-proxy, dimana untuk berbicara (berkomunikasi) ke server proxy dan memberitahukan proxy server untuk melakukan hubungan kepada server yang sebenarnya daripada memberitahukan software klien untuk berkomunikasi secara langsung ke server yang sebenarnya.

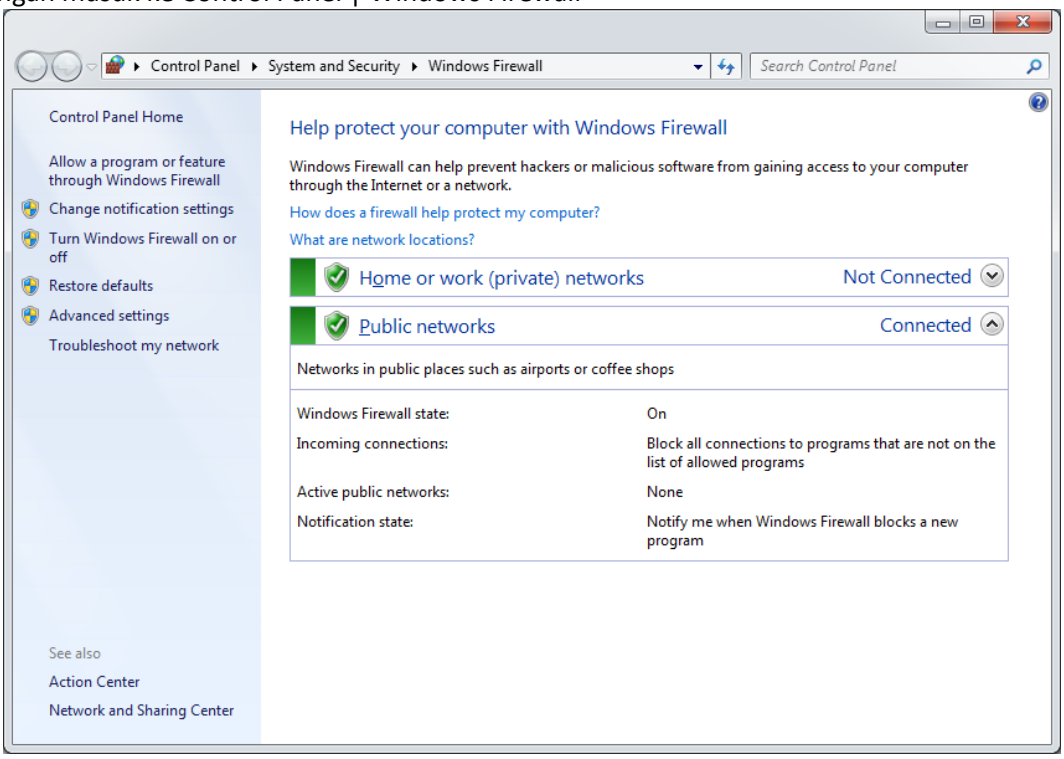
- **Proxy-aware router**

  Pendekatan yang terakhir ini software yang klien gunakan tidak dimodifikasikan tetapi sebuah router akan mengantisipasi koneksi dan melangsungkan ke proxy server atau proxy yang diminta. Mekanisme ini membutuhkan sebuah router yang pintar disamping software proxy (meskipun me-proxy dan me-rout tidak bisa tampil pada mesin yang sama)



Setting Firewall pada Windows 7

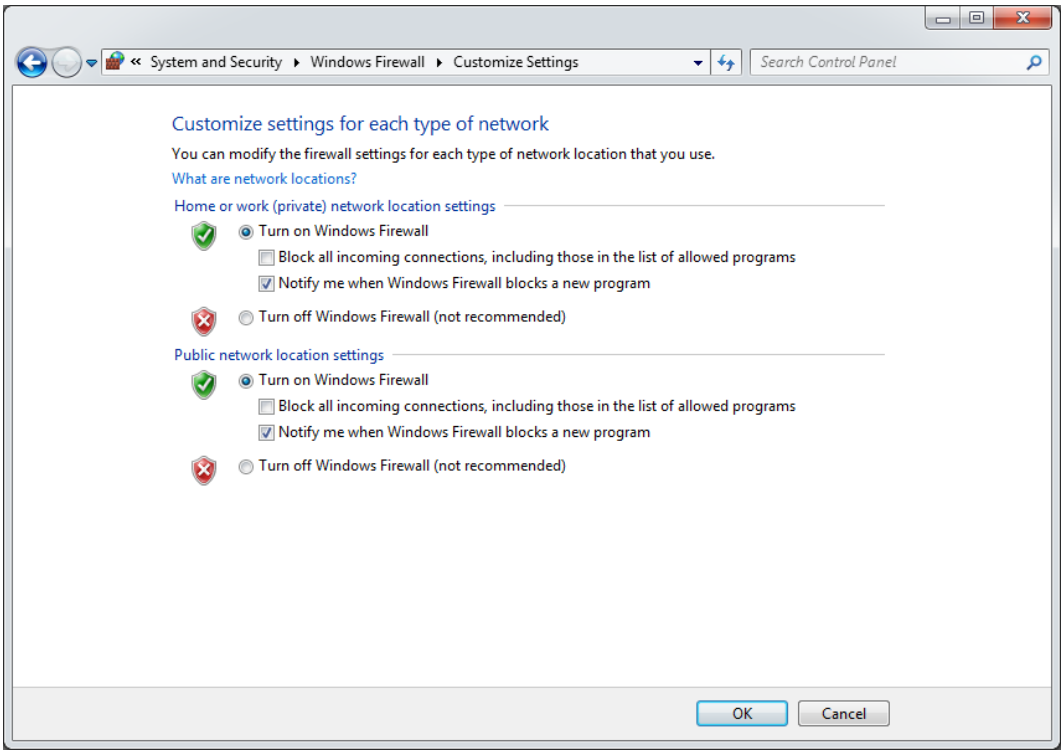
Windows 7 Firewall dapat diatur untuk menfilter semua koneksi baik itu yang masuk (inbound) maupun keluar (outbound). Firewall yang disertakan pada Windows 7 memiliki banyak fungsi, powerful, dan penggunaannya juga sangat mudah. Untuk melakukan setting firewall di Windows 7 dilakukan dengan masuk ke Control Panel | Windows Firewall



Windows Firewall memberikan 3 pilihan profil yaitu Home Network, Work Network dan Public Network. Home dan Work Network diklasifikasikan sebagai private network dimana kondisi jaringan dinilai relatif aman. Dengan memilih opsi “Home Network“, kita bisa membuat Homegroup dimana network discovery akan dihidupkan dan membuat kita bisa melihat komputer lain yang terhubung dengan Network yang sama dengan kita. Bergabung dengan Homegroup akan membuat komputer yang terkoneksi dapat me-share gambar, musik, video dan dokumen maupun sharing Printer. Bila ada folder yang ada di libraries kita yang tidak ingin dishare dapat dipilih untuk tidak dishare. Jika memilih “Work network“, network discovery akan hidup secara default tapi kita tidak akan bisa membuat atau bergabung ke dalam Homegroup.

Bila kita bergabung ke Domain Windows(Control Panel | System | Advanced System Settings | Computer Name tab) dan telah berhasil diautentifikasi, secara otomatis Windows Firewall akan mengenalinya dan mengklasifikasikan sebagai domain network. “Public Network“ merupakan pilihan yang tepat bila kita sedang mengakses internet di area publik seperti restoran, kafe, ataupun saat memakai koneksi dengan internet melalui handphone.

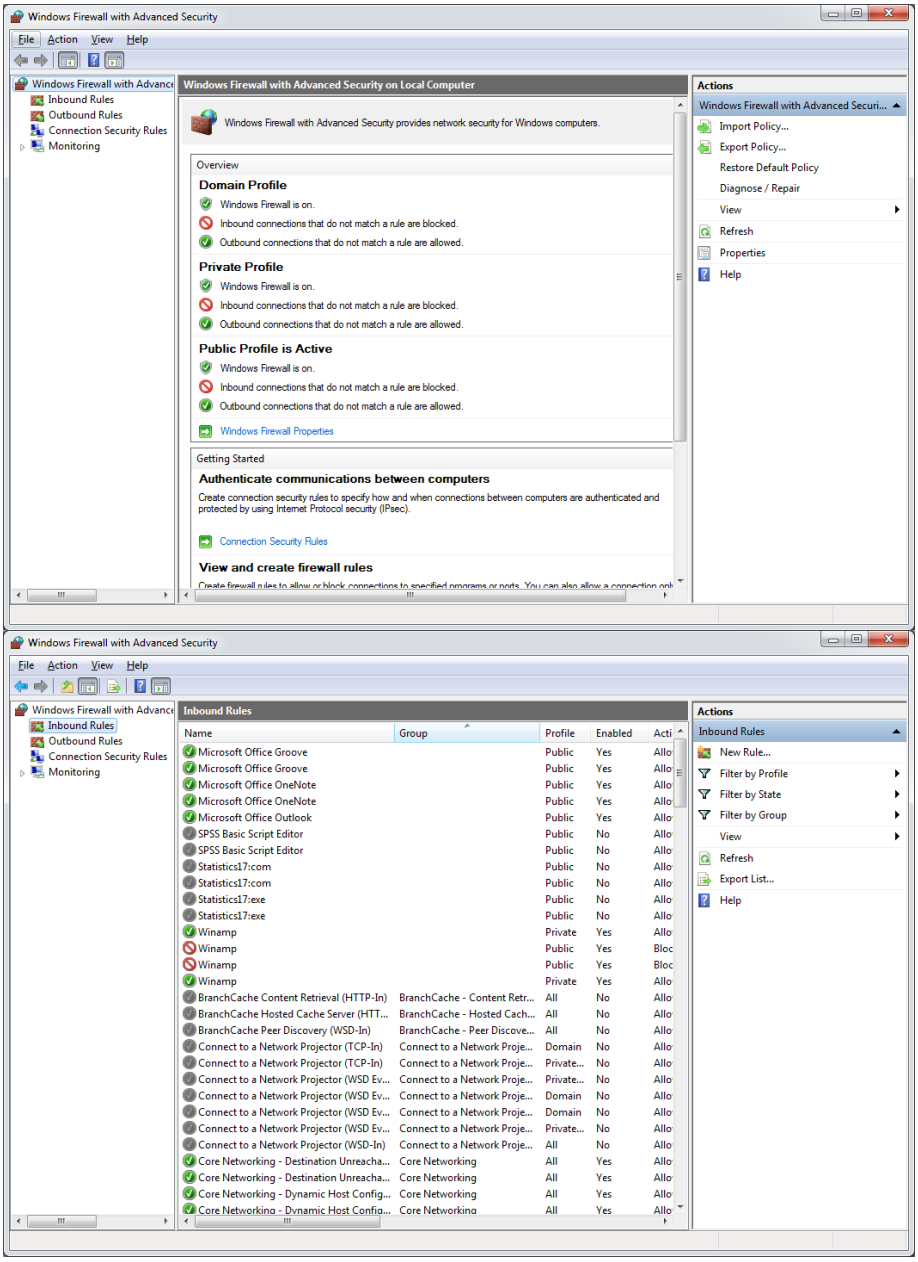
Memilih Public Network akan membuat setting Network Discovery off secara default sehingga komputer lain di jaringan tidak bisa melihat keberadaan anda dan pilihan profil ini akan membuat anda tidak bisa membuat atau bergabung kedalam homegroup.ntuk setiap profil network, secara default Windows Firewall akan memblokir koneksi dari program yang tidak ada didalam daftar whitelist. Namun Windows 7 memperbolehkan anda melakukan setting berbeda untuk setiap profil, beserta juga pengaturan notifikasi saat Firewall memblokir applikasi.



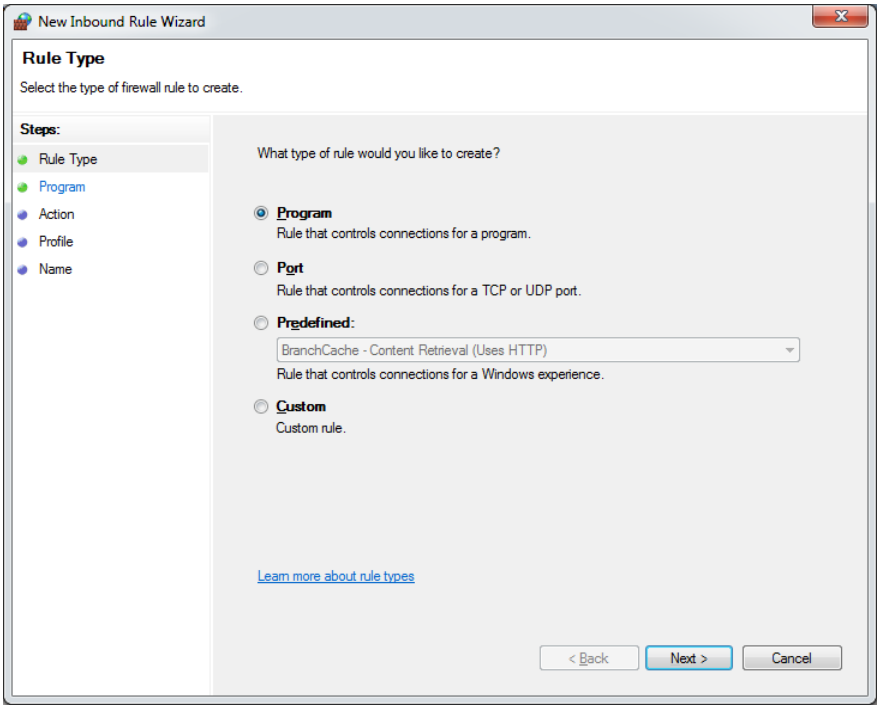
Kita bisa mengkonfigurasikan pilihan akses program untuk setiap profile dengan memilihAdvanced Setting di bagian kiri layar utama. Beberapa setting yg dapat kita rubah antara lain:

- On/off status of the Windows firewall
- Koneksi yang masuk ke komputer kita “Inbound connections” (block, block all connections, atau allow)
- Koneksi yang keluar dari komputer kita “Outbound connections” (allow atau block)
- Notifikasi bila ada program yang diblokir oleh Windows Firewall (Display notifications)
- Perbolehkan unicast response ataupun broadcast traffic
- Pilihan untuk mempergunakan pengaturan Firewall dan keamananan yang dibuat oleh administrator lokal ditambah dengan pengaturan yang ada di setting Group Policy

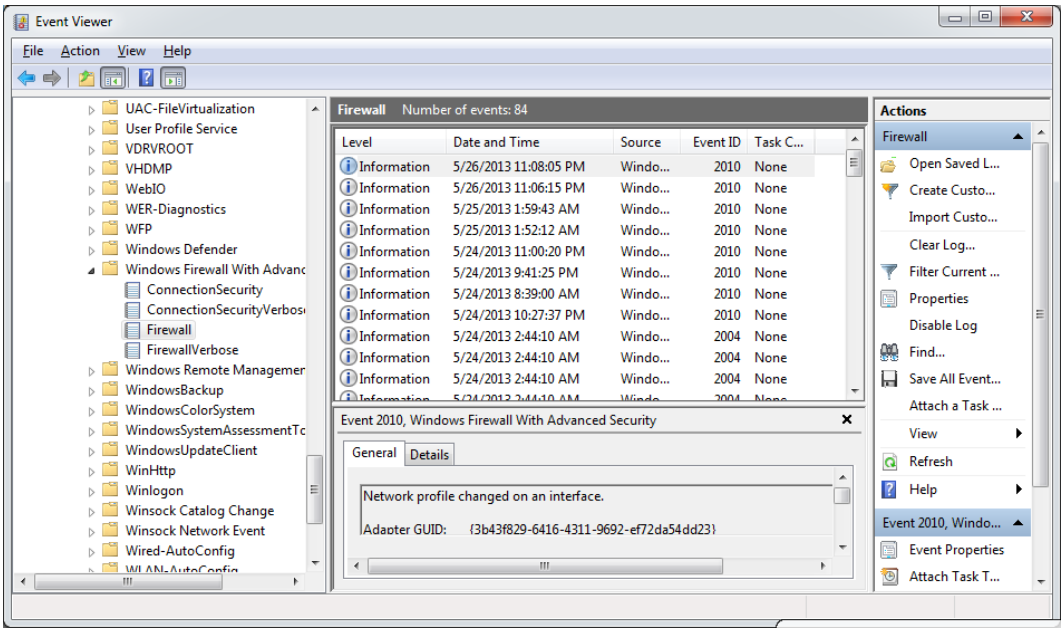
Untuk melakukan setting program, range IP address, ataupun port mana saja yang diperbolehkan untuk mengakses jaringan, baik untuk akses masuk (inbound) ataupun akses keluar (outbound), bisa melakukan pengaturan di Control Panel > Advanced Setting, setelah itu dibagian kiri pilih opsi Inbound Rules atau Outbound Rules.



Untuk menambahkan pengaturan rules baru klik menu New Rule, lalu pilih tipe rule yang ingin dibuat (program, port, predifined setting, dan custom rule) lalu ubah nilainya sesuai dengan kebutuhan dan tentukan aksi yang akan dilakukan apakah akan memblokir atau mengijinkan koneksi ke jaringan.

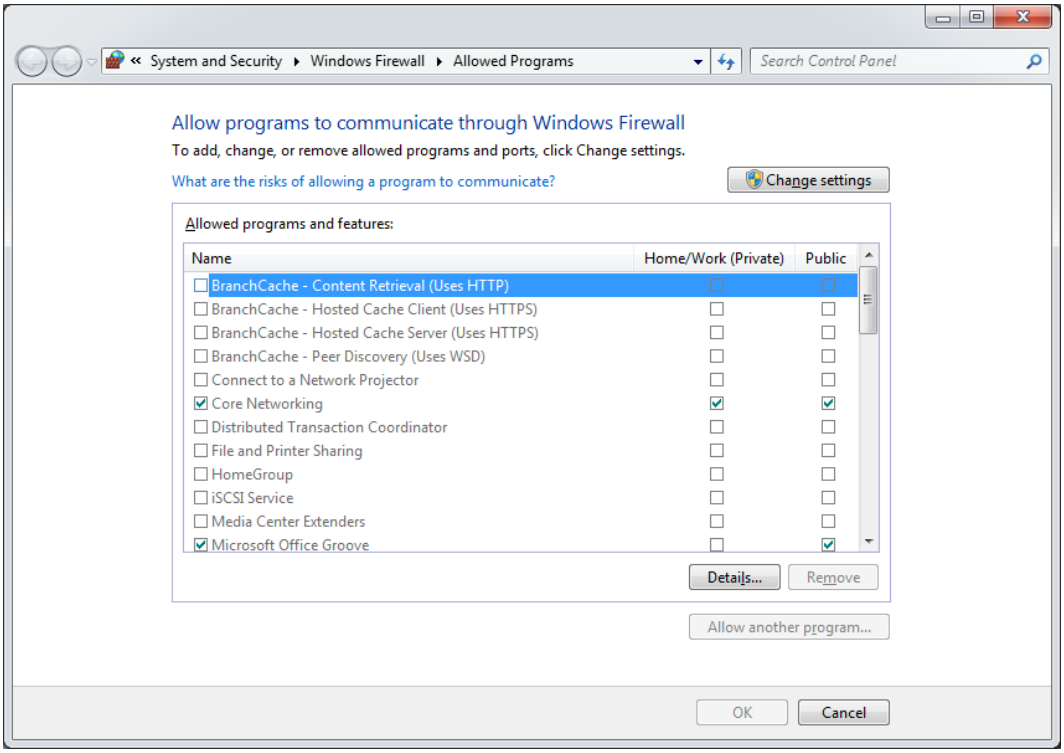


Kita juga bisa melihat log / catatan aktifitas dari Windows Firewall untuk koneksi yang diijinkan ataupun diblokir dengan membuka Event Viewer di menu All Programs | Administrative Tools | Event Viewer Di Event Viewer bagian panel kiri pilih Applications and Services Log | Microsoft | Windows | Windows Firewall with Advanced Security untuk melihat log lengkapnya.



Membuka Port Tertentu pada Firewall

Setelah kita bisa menentukan program atau fitur Windows mana saja yang dapat melalui Windows firewall, adakalanya kita membutuhkan port tertentu untuk bisa melewati firewall. Port tersebut bisa jadi dibutuhkan oleh aplikasi tertentu seperti game atau aplikasi lain yang berhubungan dengan jaringan. Untuk melakukannya, buka Advanced Setting pada window utama Windows Firewall. Allow a programs to communicate through Windows Firewall



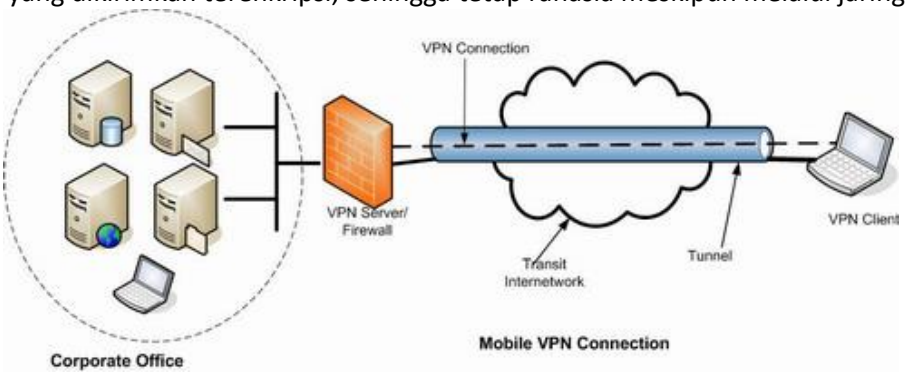
PENGERTIAN VPN

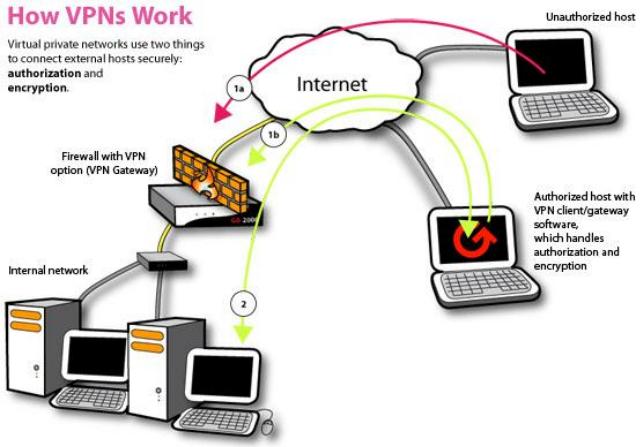
Jika dibahas dari masing-masing kata dari VPN, yaitu : Virtual, Private dan Network, maka akan diperoleh arti sebagai berikut :

1. Maya (Virtual)
   - Bukan suatu hubungan physical dedicated pada struktur jaringan.
2. Privat (Private)
   - Kebebasan dalam addressing dan routing – topological isolation
   - Keamanan data (authentication, encryption, integrity)
3. Jaringan (Network)
   - Sekumpulan alat-alat jaringan yang saling berkomunikasi satu dengan yang lain melalui beberapa metode arbitrary (berubah-ubah).

Sedangkan pengertian dari Virtual Networking dan Private Networking, yaitu :

1. Virtual Networking
   Menciptakan sebuah 'terowongan' melalui jaringan publik seperti Internet. Jadi seolah-olah ada hubungan point-to-point dengan data yang dienkapsulasi.
2. Private Networking
   Data yang dikirimkan terenkripsi, sehingga tetap rahasia meskipun melalui jaringan publik.





VPN adalah singkatan dari virtual private network, yaitu jaringan pribadi (bukan untuk akses umum) yang menggunakan medium nonpribadi (misalnya internet) untuk menghubungkan antar remote-site secara aman. Perlu penerapan teknologi tertentu agar walaupun menggunakan medium yang umum, tetapi traffic (lalu lintas) antar remote-site tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan traffic yang tidak semestinya ke dalam remote-site.

VPN adalah suatu jaringan privat (biasanya untuk instansi atau kelompok tertentu) di dalam jaringan internet (publik), dimana jaringan privat ini seolah-olah sedang mengakses jaringan lokalnya tapi menggunakan jaringan public

VPN adalah sebuah koneksi Virtual yang bersifat private mengapa disebut demikian karena pada dasarnya jaringan ini tidak ada secara fisik hanya berupa jaringan virtual dan mengapa disebut private karena jaringan ini merupakan jaringan yang sifatnya private yang tidak semua orang bisa mengaksesnya. VPN Menghubungkan PC dengan jaringan public atau internet namun sifatnya private, karena bersifat private maka tidak semua orang bisa terkoneksi ke jaringan ini dan mengaksesnya. Oleh karena itu diperlukan keamanandata.

Konsep kerja VPN pada dasarnya VPN

Pada dasarnya VPN membutuhkan sebuah server yang berfungsing sebagai penghubung antar PC. Jika digambarkan kira-kira seperti ini:

internet <—> VPN Server <—-> VPN Client <—-> Client

Bila digunakan untuk menghubungkan 2 komputer secara private dengan jaringan internet maka seperti ini:

Komputer A <—> VPN Clinet <—> Internet <—> VPN Server <—> VPN Client <—> Komputer B

Jadi semua koneksi diatur oleh VPN Server sehingga dibutuhkan kemampuan VPN Server yang memadai agar koneksinya bisa lancar.

Cara Kerja VPN

- 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.

Teknologi VPN memiliki tiga fungsi utama, di antaranya adalah :

Confidentially (Kerahasiaan)

Teknologi VPN merupakan teknologi yang memanfaatkan jaringan publik yang tentunya sangat rawan terhadap pencurian data. Untuk itu, VPN menggunakan metode enkripsi untuk mengacak data yang lewat. Dengan adanya teknologi enkripsi itu, keamanan data menjadi lebih terjamin. Walaupun ada pihak yang dapat menyadap data yang melewati internet bahkan jalur VPN itu sendiri, namun belum tentu dapat membaca data tersebut, karena

data tersebut telah teracak. Jadi, confidentially ini dimaksudkan agar informasi yang ditransmisikan hanya boleh diakses oleh sekelompok pengguna yang berhak.

Data Integrity (Keutuhan Data)

Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada VPN terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.

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 dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain.

YANG DILAKUKAN OLEH VPN

Pertama-tama VPN Server harus dikonfigurasi terlebih dahulu kemudian di client harus diinstall program VPN baru setelah itu bisa dikoneksikan. VPN di sisi client nanti akan membuat semacam koneksi virtual jadi nanti akan muncul VPN adapter network semacam network adapter (Lan card) tetapi virtual. Tugas dari VPN Client ini adalah melakukan authentifikasi dan enkripsi/dekripsi.
Nah setelah terhubung maka nanti ketika Client mengakses data katakan client ingin membuka situs http://www.google.com. Request ini sebelum dikirimkan ke VPN server terlebih dahulu dienkripsi oleh VPN Client misal dienkripsi dengan rumus A sehingga request datanya akan berisi kode-kode. Setelah sampai ke server VPN oleh server data ini di dekrip dengan rumus A, karena sebelumnya sudah dikonfigurasi antara server dengan client maka server akan memiliki algorith yang sama untuk membaca sebuah enkripsi. Begitu juga sebaliknya dari server ke Client

Keamanan Dengan konsep demikian maka jaringan VPN ini menawarkan keamanan dan untraceable, tidak dapat terdeteksi sehingga IP kita tidak diketahui karena yang digunakan adalah IP Public milik VPN server. Dengan ada enkripsi dan dekripsi maka data yang lewat jaringan internet ini tidak dapat diakses oleh orang lain bahkan oleh client lain yang terhubung ke server VPN yang sama sekalipun. Karena kunci untuk membuka enkripsinya hanya diketahui oleh server VPN dan Client yang terhubung. Enkripsi dan dekripsi menyebabkan data tidak dapat dimodifikasi dan dibaca sehingga keamananya terjamin.

Untuk menjebol data si pembajak data harus melalukan proses dekripsi tentunya untuk mencari rumus yang tepat dibutuhkan waktu yang sangat lama sehingga biasa menggunakan super computing untuk menjebol dan tentunya tidak semua orang memiliki PC dengan kemampuan super ini dan prosesnya rumit dan memakan waktu lama, agen-agen FBI atau CIA biasanya punya komputer semacam ini untuk membaca data-data rahasia yang dikirim melaui VPN.

Apakah Koneksi menggunakan VPN itu lebih cepat?

Hal ini tergantung dari koneksi antara client dengan VPN server karena proses data dilakukan dari VPN otomatis semua data yang masuk ke komputer kita dari jaringan internet akan masuk terlebih dahulu ke VPN server sehingga bila koneksi client ke VPN server bagus maka koneksi juga akan jadi lebih cepat. Biasanya yang terjadi adalah penurunan kecepatan menjadi sedikit lebih lambat karena harus melewati 2 jalur terlebih dahulu temasuk proses enkripsi. VPN ini bisa digunakan untuk mempercepat koneksi luar (internasional) bagaimana caranya??? misal kita punya koneksi lokal (IIX) sebesar 1mbps dan koneksi luar 384kbps kita bisa menggunakan VPN agar koneksi internasional menjadi sama dengan koneksi lokal 1mbps. Cara dengan menggunakan VPN Lokal yang diroute ke VPN Luar

internet <—->VPN Luar<—>VPN lokal <—>Client

mengapa model jaringan ini bisa lebih cepat sebab akses ke jaringan luar dilakukan oleh VPN luar lalu kemudian diteruskan oleh VPN lokal nah kita mengakses ke jaringan lokal yang berarti kecepatan aksesnya sebesar 1mbps. Tentunya diperlukan VPN dengan bandwith besar agar koneksinya bisa lancar.

Nah kenapa dengan koneksi HSDPA macem telkomsel dan indosat bisa lebih cepat???operator membatasi bandwith dari internet kita katakan IM2 dengan paket 256kbps bila kita memakai jaringan 3G dan HSDPA maka kita sebenarny memiliki bandwith sebesar 384kbps dan 3,6mbps untuk HSDPA tetapi hanya digunakan 256kbps karena dibatasi operator dengan VPN server batasan tersebut bisa ditembus cara akan dibahas lebih lanjut.

Kebutuhan-kebutuhan Keamanan

Dalam tantangan kepercayaan dalam sebuah lingkungan terbuka, berubah, kita akan menyelidiki kebutuhan-kebutuhan keamanan terlebih dahulu. Keamanan untuk sebuah intranet berdasarkan pada beberapa komponen hardware dan software. Teknologi dan mekanisme khusus akan bervariasi, tetapi apa yang disebut keamanan "kekuatan industri" harus selalu memenuhi lima kebutuhan dasar :

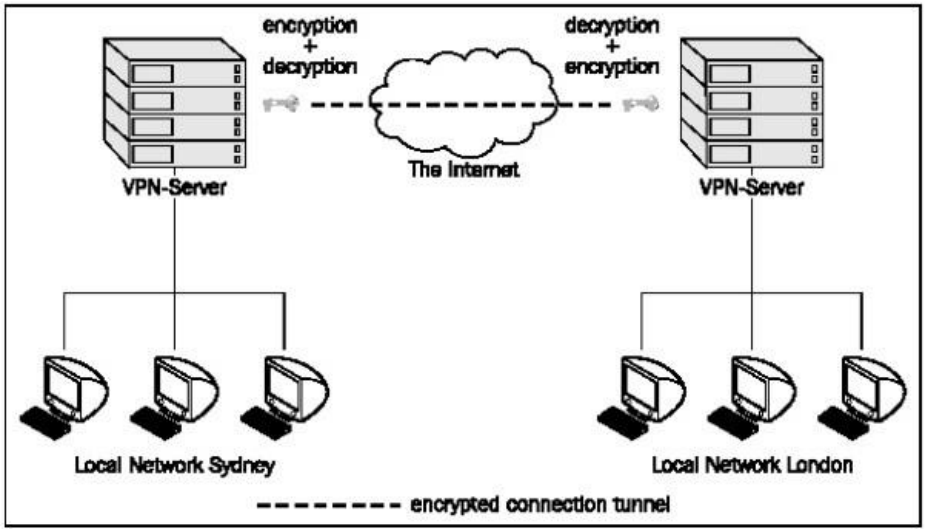
- Kerahasiaan, dengan kemampuan scramble atau encrypt pesan sepanjang jaringan yang tidak aman
- Kendali akses, menentukan siapa yang diberikan akses ke sebuah sistem atau jaringan, sebagaimana informasi apa dan seberapa banyak seseorang dapat menerima
- Authentication, yaitu menguji identitas dari dua perusahaan yang mengadakan transaksi
- Integritas, menjamin bahwa file atau pesan tidak berubah dalam perjalanan
- Non-repudiation, yaitu mencegah dua perusahaan dari menyangkal bahwa mereka telah mengirim atau menerima sebuah file

CONTOH KASUS MEMANFAATKAN CELAH VPN

Apakah bisa bikin internet gratisan dan non-quota??? jawabanya bisa selama celah yang digunakan belum diketahui operator . Cara melakukannya adalah dengan menggunakan akses port tertentu ke VPN server. Operator biasanya menggunakan port tertentu untuk perhitungan billing dan total data yang terpakai celah inilah yang dapat dimanfaatkan. Misal terdapat port tertentu yang bisa digunakan untuk terhubung ke server VPN maka internet bisa digunakan secara gratis dan bebas qouta. Kenapa bisa begitu???port tersebut tidak digunakan untuk perhitungan billing sehingga kita tidak melewati billing server nah dengan port ini maka kita bisa terhubung ke VPN server melalui jaringan internet.kita konek ke internet tetapi tidak melewati billing server otomatis kita tidak dikenakan charge dan count data tidak dihitung kalaupun dihitung hanya sedikit sekali untuk proses ping ke server. Dengan terhubung ke VPN server maka semua akses akan dilakukan oleh VPN server dan dikirimkan melalui port yang terbuka tadi sehingga kita bisa bebas mengakses intenet. kurang lebih tekniknya seperti itu mungkin ada teknik-teknik lain karena VPN memiliki banyak kelebihan

CONTOH PENGGUNAAN VPN

Mari kita menggunakan suatu contoh untuk menjelaskan bagaimana VPN bekerja. Virtual Entity Networks Inc. (VEN Inc.) mempunyai dua cabang, London dan Sydney. Jika cabang Australian di Sydney memutuskan untuk mengontrak penyalur, kemudian kantor London harus mengetahui langsung. Bagian utama dari infrastruktur IT disediakan di London. Di Sydney ada duapuluh orang yang pekerjaannya tergantung pada ketersediaan data menjadi tuan rumah pada Server London.

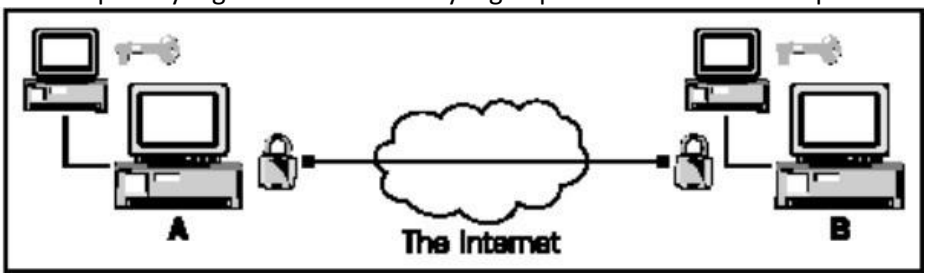


Kedua lokasi dilengkapi dengan suatu jalur internet permanen. Suatu Internet router gateway adalah di-set sampai menyediakan Internet mengakses untuk staff itu. Penerus ini diatur untuk melindungi jaringan yang lokal lokasi dari akses tidak syah dari sebelah, yang mana adalah itu “kejahatan” internet. Penerus seperti itu menyediakan untuk menghalangi lalu lintas khusus dapat disebut suatu firewall dan harus ditemukan didalam tiap-tiap cabang yang dikira untuk ambil bagian dalam VPN itu.

Perangkat lunak VPN harus diinstall pada firewall ini atau suatu server atau alat yang dilindungi oleh itu. Banyak firewall peralatan modern dari pabrikan seperti Cisco atau Bintec meliputi corak ini, dan ada VPN Perangkat lunak untuk semua perangkat keras dan lunak platform.

Pada langkah berikutnya, VPN Perangkat lunak harus diatur untuk menetapkan koneksi pada sisi lainnyasebagai contoh VPN server London harus menerima koneksi dari Sydney server, dan Sydney server harus menghubungkan ke London atau sebaliknya. Jika langkah ini berhasil diselesaikan, perusahaan mempunyai suatu Virtual Network. Kedua cabang dihubungkan dengan internet dan dapat bekerja sama seperti di dalam suatu jaringan riil.

Di sini, kita mempunyai suatu VPN tanpa keleluasaan pribadi, sebab banyak roter internet antar London dan Sydney dapat membaca pertukaran data. Suatu pesaing yang memperoleh kendali pada suatu roter internet bisa membaca semua relevan data bisnis jaringan yang sebetulnya itu. Maka bagaimana cara kita membuat Virtual Network Private? Solusinya adalah enkripsi. Jalur VPN antar dua cabang dikunci dengan kunci khusus, dan hanya para orang atau komputer yang memiliki kunci ini yang dapat membuka dan nampak di data pengirim.



Semua data dikirim dari Sydney ke London atau dari London ke Sydney harus terenkripsi sebelum dan didekripsi setelah transmisi. Encryption melindungi data di dalam koneksi seperti dinding dari suatu terowongan melindungi kereta dari gunung di sekitar itu. Ini menjelaskan mengapa VPN sering dikenal sebagai terowongan (tunnel) atau VPN tunneling, dan teknologinya sering disebut tunneling—even jika tidak ada mekanika kwantum lain yang melibatkan.

Metoda encryption yang tepat dan menyediakan kunci bagi semua partisi melibatkan salah satu dari faktor pembeda utama antar VPN solusi yang berbeda. Suatu koneksi VPN yang secara normal dibangun antara dua akses router internet yang dilengkapi dengan suatu firewall dan perangkat lunak VPN. Perangkat lunak harus di-set sampai menghubungkan pada VPN partner, firewall harus di-set sampai bisa mengakses, dan menukar data antara VPN partner dengan encryption. Encryption kunci harus disajikan untuk semua VPN partner, sedemikian sehingga data yang ditukar hanya dapat dibaca oleh VPN partner yang diberi hak.

Kelemahan & Kelebihan VPN

Di artikel berikut, disajikan kelebihan dan kelemahan VPN yang telah dirasakan hingga kini. Antara lain :

- **Kelebihan VPN**

VPN sering dianalogikan dengan istilah kapal selam dalam mengarungi samudera yang luas. Ini berkaitan dengan sifatnya yang pribadi dan tingkat keamanan yang dia tawarkan. Seperti halnya kapal selam yang hampir tak dapat diketahui posisinya saat ia mengarungi samudera luas sekalipun.

Selain keamanan, beberapa hal yang ditawarkan sebagai bentuk kelebihan VPN adalah :

1. Sangat cepat
   Berkaitan dengan koneksi. Karena VPN memiliki saluran sendiri, maka komunikasi yang dilakukan hanya sebatas pengguna pribadi, tidak terjadi banyak antrian sehingga komunikasi data berlangsung sangat cepat,
2. Tidak mudah dilihat
   Erat kaitannya dengan kelebihan poin pertama, yaitu saluran pribadi. Karena memiliki saluran pribadi meskipun dalam jaringan publik, maka VPN tidak mudah terlihat oleh pengguna lain, ini berdampak pengguna lain yang tidak bisa berkomunikasi dengan pengguna yang ada dalam saluran pribadi tersebut.
3. Biaya relatif terjangkau
   Biaya terjangkau yang dimaksud disini adalah pada sisi pengembangan teknologi. Karena memanfaatkan wireless jadi tidak memerlukan banyak piranti penghubung, misal kabel, dalam pengembangannya
4. Melindungi saat melakukan komunikasi
   Saat melakukan komunikasi dijaringan publik, tentu sangat rawan akan adanya pencurian data karena kita terlihat oleh pengguna yang lain. Dengan VPN karena layanan yang diberikannya

berupa saluran pribadi, maka ini bisa menjadi pelindung untuk tidak terlihat pengguna lain dan terhindar dari pencurian data.

5. Teknologi VPN semakin berkembang
   Salah satunya adalah adanya Cisco VoIP Softphone yang rupanya berjalan sangat bagus di jaringan VPN. Teknologi tersebut menawarkan pada kita utuk menjadikan PC kita sebagai telephone yang aman.

KELEBIHAN TAMBAHAN:

6. Menyediakan keamanan "industrial-strength"
7. Mengakomodasi komunitas pengguna yang berubah secara dinamis
8. Menyediakan kemampuan pertukaran informasi dalam berbagai bentuk form (web, file, dll)
9. Mengakomodasi pengguna yang berbeda dengan berbagai macam browser, aplikasi, sistemoperasi, dll
10. Memungkinkan pengguna masuk ke dalam grup atau administrator memasukkan identitas dalamsebuah cara yang dikendalikan tetapi mudah
11. Memelihara integritas sepanjang waktu, tanpa memperhatikan pergantian administrasi, perubahanteknologi, atau peningkatan kompleksitas sistem informasi perusahaan

❖ **Kelemahan VPN**

Selain beberapa kelebihan yang diutarakan diatas, VPN memiliki beberapa kelemahan, terutama dalam sifatnya sebagai jaringan nirkabel. Beberapa kelemahan VPN yang disajikan secara empiris adalah sebagai berikut :

1. **Rawan Penyadapan**
   Meskipun sebagai saluran pribadi, VPN tetap berjalan di saluran publik. Untuk menghindari adanya penyadapan data, hacking atau bahkan cyber crime maka diperlukan kajian lebih mendalam atau bahkan pemanfaatan teknologi terbaru untuk pelindungan data terutama data-data yang bersifat pribadi.
2. **Tidak ada Kendali Utama Pengguna**
   Pengguna tidak memiliki kendali atas pengguna dan kecepatan aliran data, performa hingga pada kendali lain, misalkan jaringan yang tidak bekerja sama sekali karena mati lampu. Praktis, pengguna tidak memiliki kendali apapun atas kendala yang berhubungan dengan layanan dan pengguna hanya sebatas sebagai pengguna.
3. **Perangkat Tidak Sesuai**
   Dikarenakan perangkat-perangkat pada VPN biasanya bersifat ekslusif. Dalam artian ini adalah bisa dimungkinkan satu perangkat tidak bisa digantikan perangkat dengan merk berbeda. Sehingga dalam pembangunannya perlu memperhatikan jenis dan bahkan merk perangkat yang digunakan.
4. **Tidak Adanya Standar Yang Memenuhi**
   Sebagai jaringan nirkabel, VPN dan banyak jenis yang lain, mengalami masalah ini, yaitu tidak adanya standar yang memenuhi. Antara satu pabrikan dengan pabrikan yang lain memiliki ketentuan masing-masing. Akibatnya seperti yang dijelaskan dalam poin ketiga, termasuk akibat lain yang antara jaringan satu dengan yang lain tidak mampu berkomunikasi hanya karena perbedaan pada sisi perangkat.

HUBUNGAN FIREWALL DAN VPN

Sebuah VPN dapat berbasis pada router dan firewall. Router adalah komputer yang mengendalikan lalu lintas pada sebuah jaringan. Sebuah firewall adalah sebuah metoda yang memproteksi satu jaringan terhadap jaringan yang lain. Keduanya terletak antara jaringan internal dengan jaringan luar untukmemblok lalu lintas yang tak diinginkan. Jika pengguna mengirimka sebuah pesan, pesan tersebut mengalir melewati firewall meunju internet. Firewall akan memblok lalu lintas dari user ini jika ia tidak mempunyai izin ke internet, atau ia menggunakan protokol yang tak diizinkan. Sebuah VPN berbasis router dan firewall dapat dibuat dalam jaringan dan lalu lintas antar jaringan.

Walaupun demikian, router tak membedakan antara komunitas dan user, sehingga user pada dua jaringan harus menggunakan nama user dan password. Prosedur ini membuat sebuah logon single sangat sulit. Sebagai tambahan, nama user dan password dapat dibaca oleh orang luar, sehingga transmisi membutuhkan enkripsi. Dengan router yang terenkripsi, komunikasi dapat dilakukan antar jaringan dengan tingkat keamanan yang cukup.

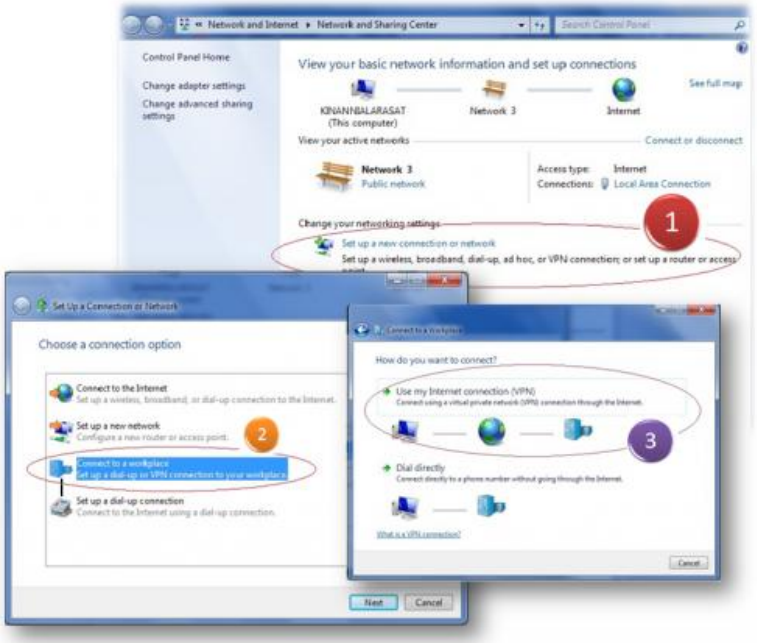
Sebuah sistem yang menggunakan router dan firewall tidak termasuk authentication mutual atau unilateral : seorang user tidak perlu membuktikan identitasnya di luar nama user dan password. Router juga secara khusus membagikan symmetric-key yang sama. Ini berarti keamanan dapat dikompromikan oleh seseorang dengan menggunakan key yang dicuri.

Lebih penting lagi, sebuah sistem router sangat rapuh untuk mengakomodasi grup user yang dinamis dan banyak. Tiap perubahan pada sistem sangat sulit untuk membuat dan / atau keamanan terhadap compromise.

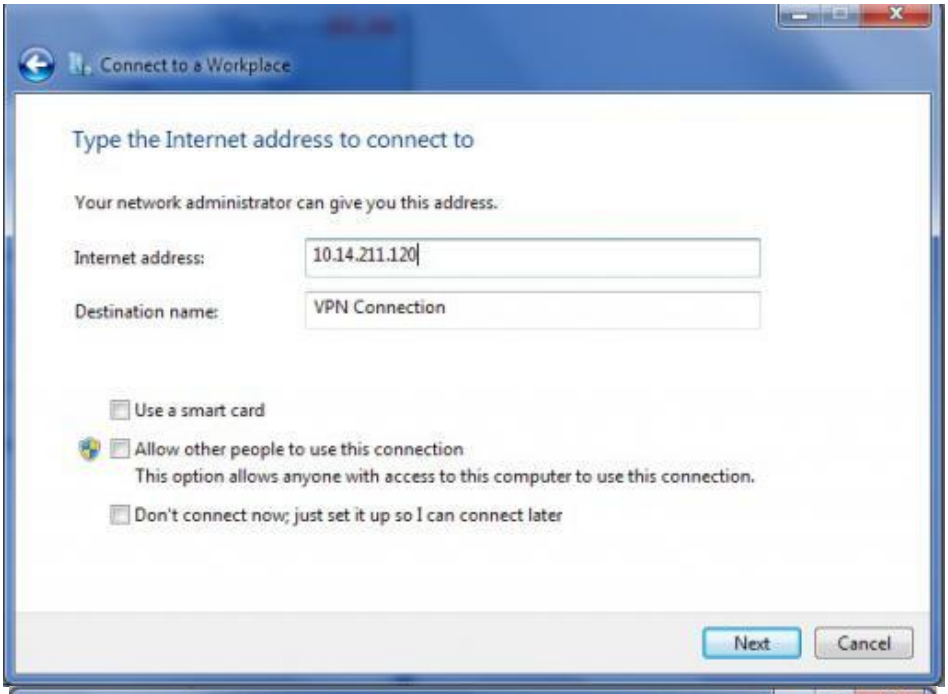
Cara Setting VPN (Virtual Private Network) PADA WINDOWS 7

Berikut adalah langkah membuat koneksi VPN pada windows 7 :
Pertama, *Membuat interface PPTP terlebih dahulu*

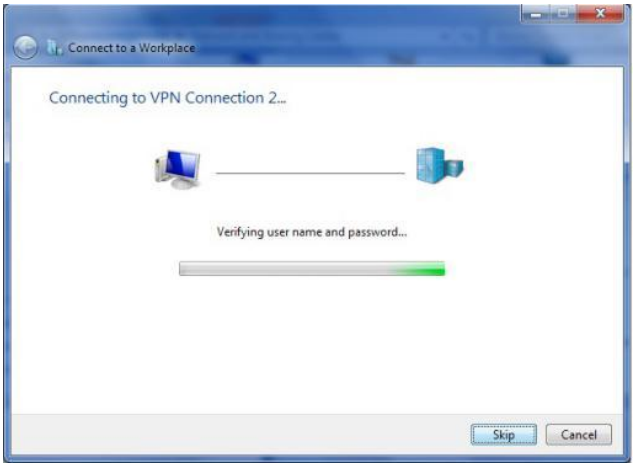
1. Buka **Network and Sharing Center** yang berada di Control Panel, pilih **Set up a new connection or network**
2. Pilih **Connect to a workplace**, pada window yang muncul, kemudian Next
3. Pilih **Use my Internet Connection (VPN)** pada window berikutnya.



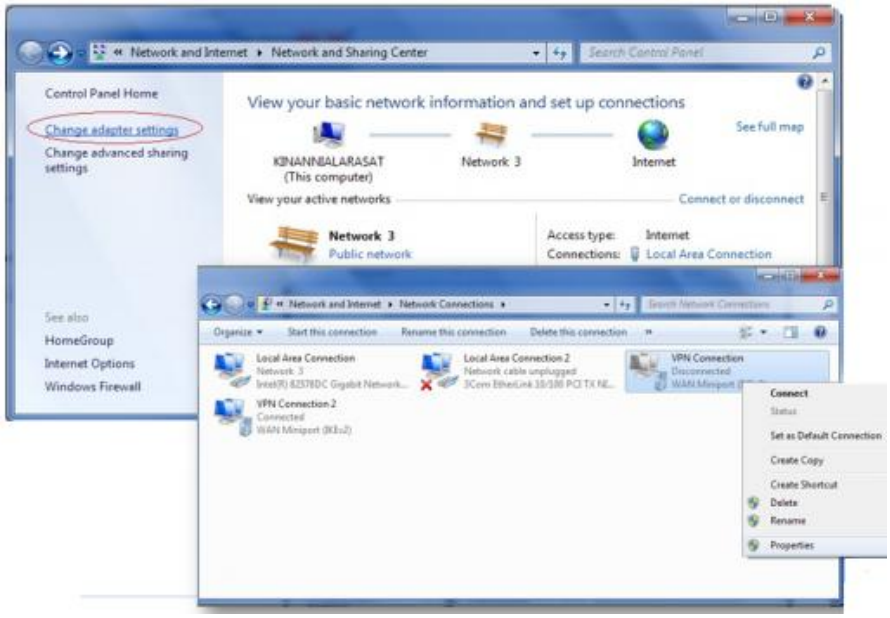
Kedua, *lakukan konfigurasi PPTP* yaitu isi **Internet address** dengan 10.14.211.120 atau 10.14.211.121 (untuk mahasiswa silakan pilih salah satu dari dua IP address tersebut) dan **Destination Name** bebas. Kemudian masukkan **username** dan **password** vpn yang telah didapat (Tidak perlu mengisi Field Domain).



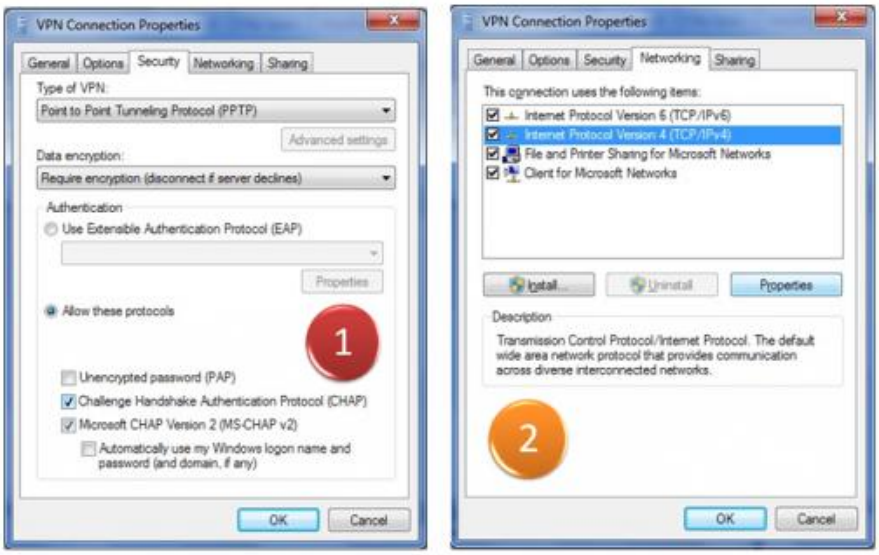
Selanjutnya Klik connect. Jika ada tampilan berikut, pilih *Skip*.



Interface PPTP sudah terbentuk. Namun ada beberapa hal lagi yang harus diatur. Masih berada pada **Network and Sharing Center** yang berada di Control Panel, klik **Change adapter settings**.

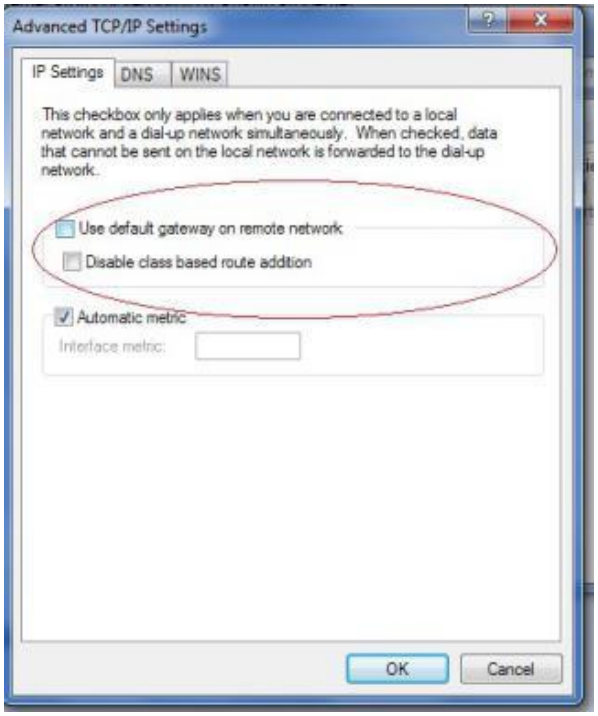


Kemudian Klik kanan interface VPN Connection yang tadi telah dibuati, kemudian pilih **Properties**.
Pada tab **Security**, pilih *Point to Point Tunneling Protocol (PPTP)* sedangkan pada tab **Networking**, beri tanda check pada *Internet Protocol Version 4 (TCP/IP V4)*

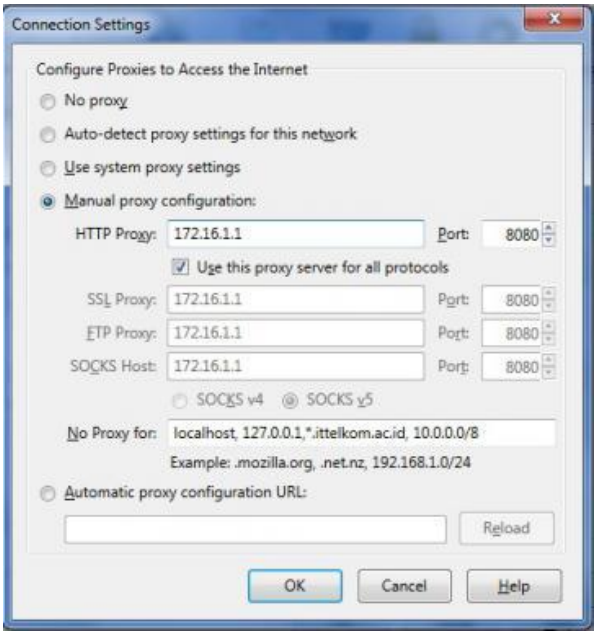


kemudian klik **Properties**

Lalu klik **advance** hingga muncul tampilan berikut, kemudian Uncheck **Use default gateway on remote network** seperti pada gambar. Kemudian tekan ok.



Langkah akhir, lakukan **Setting proxy** pada web browser seperti di bawah ini (Setting Mozilla Firefox):



Internet siap diakses menggunakan VPN. Semoga tutorial ini bisa membantu.

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.
- 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.

Protokol Tunneling Utama VPN

- **Point-to-Point Tunneling Protocol (PPTP)**

PPTP dikembangkan oleh Microsoft dan Cisco merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP (Snader, 2005). 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.

PPTP terdapat sejak dalam sistem operasi Windows NT server dan Windows NT Workstation versi 4.0. Komputer yang berjalan dengan sistem operasi tersebut dapat menggunakan protokol PPTP dengan aman untuk terhubung dengan private network sebagai klien dengan remote access melalui internet. PPTP juga dapat digunakan oleh komputer yang terhubung dengan LAN untuk membuat VPN melalui LAN.

Fasilitas utama dari penggunaan PPTP adalah dapat digunakannya public-switched telephone network (PSTNs) untuk membangun VPN. Pembangunan PPTP yang mudah dan berbiaya murah untuk digunakan secara luas, menjadi solusi untuk remote users dan mobile users karena PPTP memberikan keamanan dan enkripsi komunikasi melalui PSTN ataupun internet.

- **Layer 2 Tunneling Protocol (L2TP)**

L2TP adalah tunneling protocol yang memadukan dua buah tunneling protokol yaitu L2F (Layer 2 Forwarding) milik cisco dan PPTP milik Microsoft (Gupta, 2003). L2TP biasa digunakan dalam membuat Virtual Private Dial Network (VPDN) yang dapat bekerja membawa semua jenis protokol komunikasi didalamnya. Umunnya L2TP menggunakan port 1702 dengan protocol UDP untuk mengirimkan L2TP encapsulated PPP frames sebagai data yang di tunnel.Terdapat dua model tunnel yang dikenal (Lewis, 2006), yaitu compulsorydan voluntary. Perbedaan

utama keduanya terletak pada endpoint tunnel-nya. Pada compulsory tunnel, ujung tunnel berada pada ISP, sedangkan pada voluntaryujung tunnel berada pada client remote.

- **IPsec**

IPSec merupakan suatu pengembangan dari protokol IP yang bertujuan untuk menyediakan keamanan pada suatu IP danlayer yang berada diatasnya (Carmouche, 2006). IPSec (Internet Protocol Security) merupakan salah satu mekanisme yang diimplementasikan pada Virtual Private Network. Paket IP tidak memiliki aspek security, maka hal ini akan memudahkan untuk mengetahui isi dari paket dan alamat IP itu sendiri. Sehingga tidak ada garansi bahwa menerima paket IP merupakan dari pengirim yang benar, kebenaran data ketika ditransmisikan. IPSecmerupakan metode yang memproteksi IP datagram ketika paket ditransmisikan pada traffic. IPSec berkerja padalayer tiga OSI yaitu network layer sehingga dapat mengamankan data dari layer yang berada atasnya.

IPSec terdiri dari dua buah security protokol (Carmouche, 2006) :

- AH (Authentication Header) melakukan autentikasi datagram untuk mengidentifikasi pengirim data tersebut

- ESP (Encapsulating Security Header) melakukan enkripsi dan layanan autentifikasi.

IPSec menggunakan dua buah protokol berbeda untuk menyediakan pengamanan data yaitu AH dan ESP keduanya dapat dikombinasikan ataupun berdiri sendiri. IPSec memberikan layanan security pada level IP dengan memungkinkan suatu system memilih protokol security yang dibutuhkan, algoritma yang digunakan untuk layanan, dan menempatkan kunci kirptografi yang dibutuhkan unutk menyediakan layanan. Dua buah protokol yang digunakan untuk memberikan layanan kemanan yaitu autentikasi protokol yang ditunjuk pada header protokol yaitu AH (Authentication Header) dan sebuah protokol yang mengkombinasikan enkripsi dan autentikasi yang ditunjuk oleh header paket untuk format tersebut yaitu ESP (Encapsulating Security Payload).

Perbedaan Antara PPTP, L2TP, dan IPSec

Adanya perbedaan sistem dari masing-masing protocol menimbulkan pertanyaan bagaimana QoS (Quality of Services) dari masing-masing protocol pada jaringan VPN. Menurut Arora, 2001 menyebutkan IPsec adalah protocol yang memberikan keamanan paling kuat diantara protocol lainnnya, sementara L2TP protocol yang mempunyai basic keamanan seperti protocol PPTP, tetapi protocol L2TP ini dapat di gabungkan dengan IPsec apabila ingin mendapatkan interoperabilitas yang lengkap dan keamanan yang kuat. Penelitian yang dilakukan oleh Arora ini menggunakan beberapa vendor yang berbeda dengan menggunakan indikator seperti keamanan, performansi dengan meliputi throughput dan latency, skalabilitas, flesibelitas, interoperabilitas dan aplikasi.

Penelitian lain menyebutkan bahwa perbedaan kinerja protocol VPN ini berada pada sistem security dari masing-masing protocol. Menurut Berger, 2006 menyebutkan bahwa perbedaan terdapat pada komplesitas dari metode autentikasi dari masing-masing protocol. Semakin aman sebuah protocol mengirimkan sebuah data maka semakin rumit proses enkasulasi dan enkripsi pada data tersebut, sehingga menyebabkan penambahan ukuran file yang akan di transferkan. Penelelitian yang dilakukan Berger untuk membandingkan performansi dari protocol tunneling vpn ini menggunakan vendor yang berbeda. Perbandingan dilakukan dengan menggunakan indikator seperti fungsional dasar VPN establishment time, link quality, dan tunnel re-initiation time,Performansi menggunakan parameter throughput, dan keamanan.

Dari ke dua penelitian di atas dilakukan dengan membandingkan performansi dealam berbagai aspek seperti fusgionalitas, keamanan, sakalabilitas, dan aplikasi. Hasil dari kedua percobaan di atas menunjukan masing-pasing protokol memiliki kelebihan dan kelemahan dalam performansi di dalam jaringan VPN. Oleh karena itu penelitian terbaru harus dilakukan karena dengan perkembangan teknologi dan metode yang berkembang pada tunneling VPN. Penellitian ini dimaksudkan untuk melihat perkembangan metode tunneling VPN, dalam hal ini yang akan di bandingkan adalah Tunneling VPN L2TP pada Layer 2 dan IPsec pada Layer 3. pada peneleitian ini PPTP tidak dikutsertakan karena Implementasinya saat ini sudah tidak banyak yang memamkai. QoS (Quality of Services) menjadi sorotoan utama dari penelitian ini, parameter yang akan digunakan adalah delay, jitter, dan throughput sebagai indikator performansi metode tunneling pada jaringan VPN.

VPN pada dasarnya legal yang saat ini banyak digunakan pada jaringan extranet ataupun intranet perusahaan-perusahaan besar. VPN harus dapat mendukung paling tidak 3 mode pemakaian :

* Koneksi client untuk akses jarak jauh
* LAN-to-LAN internetworking
* Pengontrolan akses dalam suatu intranet

Akses internet melalui VPN tersebut sebetulnya dapat juga dilakukan dengan memanfaatkan celah keamanan server ISP pada port tertentu untuk diakses secara illegal, karena tanpa sepengetahuan ISP yang akan dibobol. Dengan melakukan metode bypass maka server billing dari ISP tidak mendeteksi kehadiran kita, sehingga otomatis tidak ada billing yang ditagihkan alias gratis.

Akhir-akhir ini banyak iklan menawarkan akses internet melalui VPN hanya dengan transfer Rp.30 ribu s.d. Rp. 50 ribu dapat mengunakan internet unlimited. Tentu saja hal ini sangat menarik digunakan namun layak untuk berhati-hati, karena akses VPN ilegal dapat dilakukan pemblokiran tiba-tiba dari ISP yang mengetahui terdapat celah port yang terbuka, sehingga segera ditutup oleh team teknisi ISP tersebut. Dengan adanya pemblokiran tadi otomatis akses internet VPN ilegal tersebut terhenti atau tidak bisa mengakses internet lagi dan kita tidak dapat meminta ganti rugi kepada penjual VPN ilegal, jadi istilah lain uang kita hilang atau tidak dapat dikembalikan.

Namun selain yang bayar tetapi legal atau illegal juga ada yang gratis, bagi yang tertarik untuk mencoba akses VPN gratis ini bisa juga dilakukan tanpa software maupun regristrasi yaitu melalui:

Freecanadavpn
Server Hostname: freecanadavpn.com
Encryption Mode: Auto
Username: free
Password: UfreeVPN
Server Canada:
PPTP Server: cavpn.ufreevpn.com
Username: ufreevpn.com
Password: free
Server USA:
PPTP Server: usvpn.ufreevpn.com
Username: ufreevpn.com
Password: free
Server UK:
PPTP Server: ukvpn.ufreevpn.com
Username: ufreevpn.com
Password: free

Daftar Pustaka :

- http://docstore.mik.ua/orelly/networking_2ndEd/fire/index.htm

by Elizabeth D. Zwicky, Simon Cooper and D. Brent Chapman
ISBN: 1-56592-871-7
Second edition, published June 2000.

- http://ilmukomputer.org