

Firewall & VPN

Kelompok:

MUHAMMAD NUR HELMI / 115610083

UNGGUL CAHYONO / 115610085

ARDI SANTOSO / 125610091

ROSARDI VIDIASTAMA / 125610159

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.

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
- Firewall akan mem-filter serta meng-audit traffic yang melintasi perbatasan antara jaringan luar maupun dalam.

Teknik-Teknik yang Digunakan firewall

- Service control (kendali terhadap layanan)
- Direction Control (kendali terhadap arah)
- User control (kendali terhadap pengguna)
- Behavior Control (kendali terhadap perlakuan)

Service control (kendali terhadap layanan)

Berdasarkan tipe-tipe layanan yang digunakan di Internet dan boleh diakses baik untuk ke dalam ataupun keluar firewall. Biasanya firewall akan mengecek no IP Address dan juga nomor port yang digunakan 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.

Direction Control (kendali terhadap arah)

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

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 dikarenakan user tersebut tidak di ijin untuk melewati firewall. Biasanya digunakan untuk membatasi user dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.

Behavior Control (kendali terhadap perlakuan)

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

Arsitektur Firewall

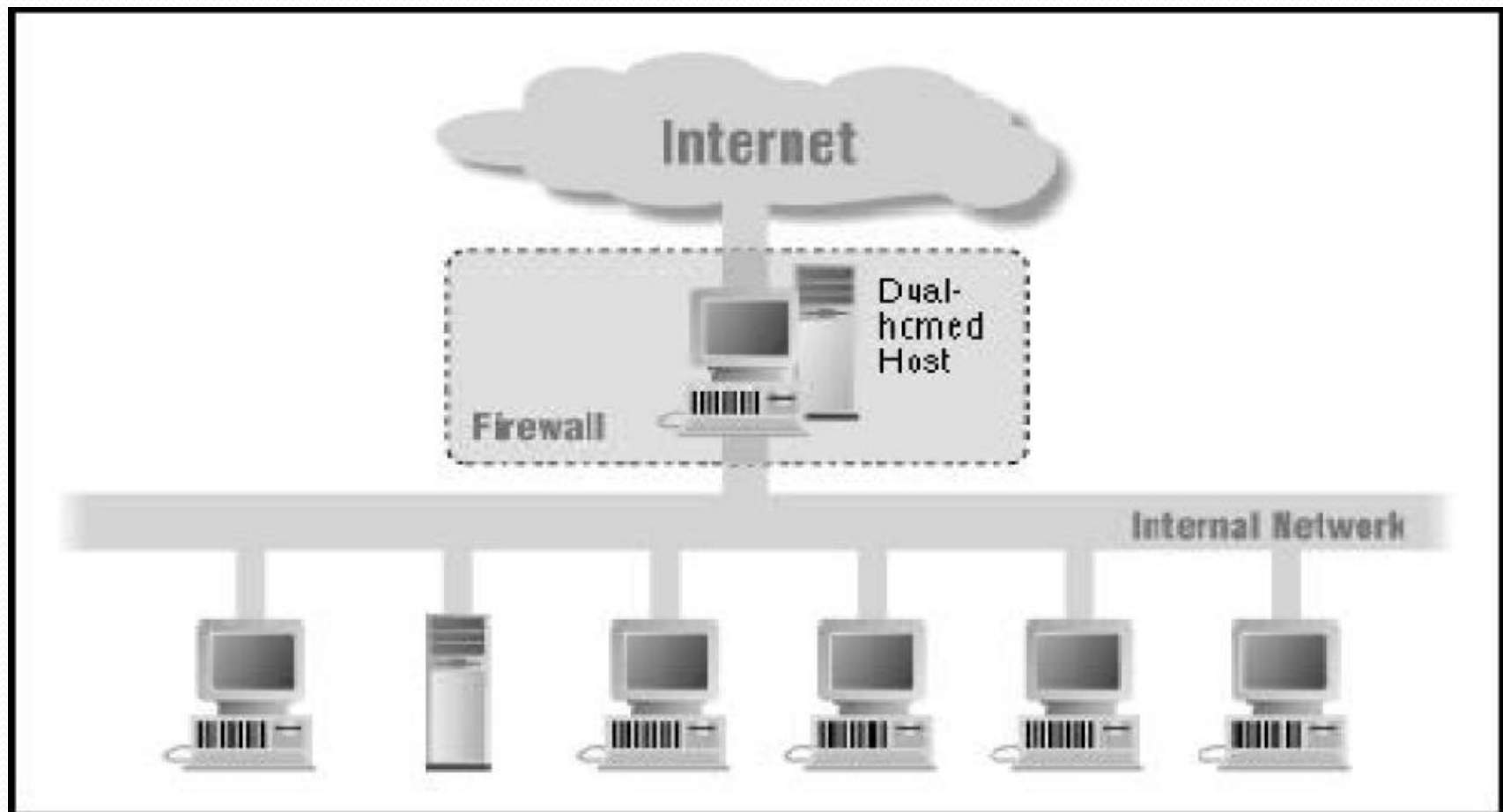
- SingleBox architecture
 - Screening Router
 - Dual-homed host architecture
- Screened host architecture
- Screened subnet architecture

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.

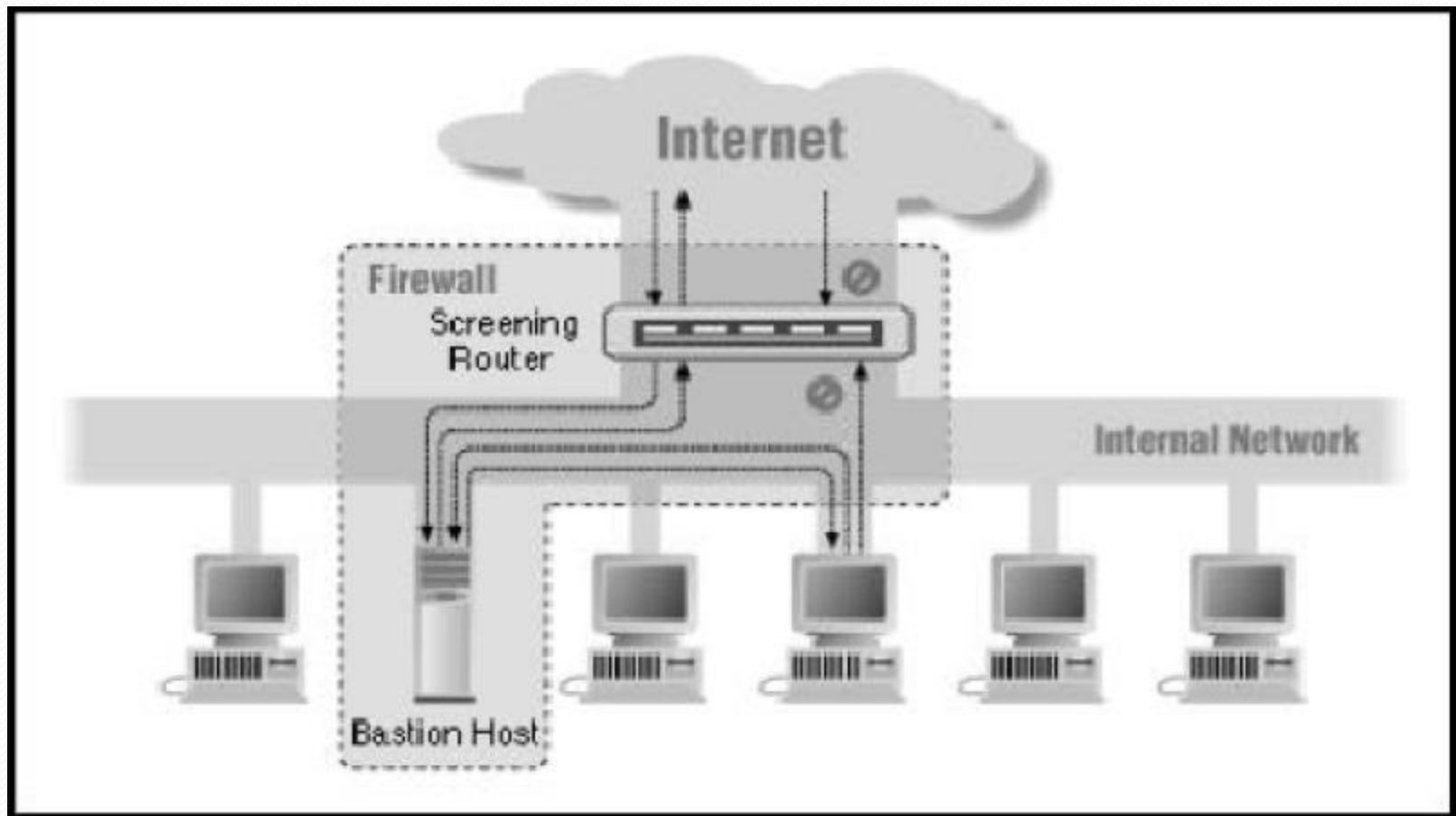
Dual-homed host dapat menyediakan service hanya dengan menyediakan proxy pada host tersebut, atau dengan membiarkan user melakukan logging secara langsung pada dual-homed host.



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

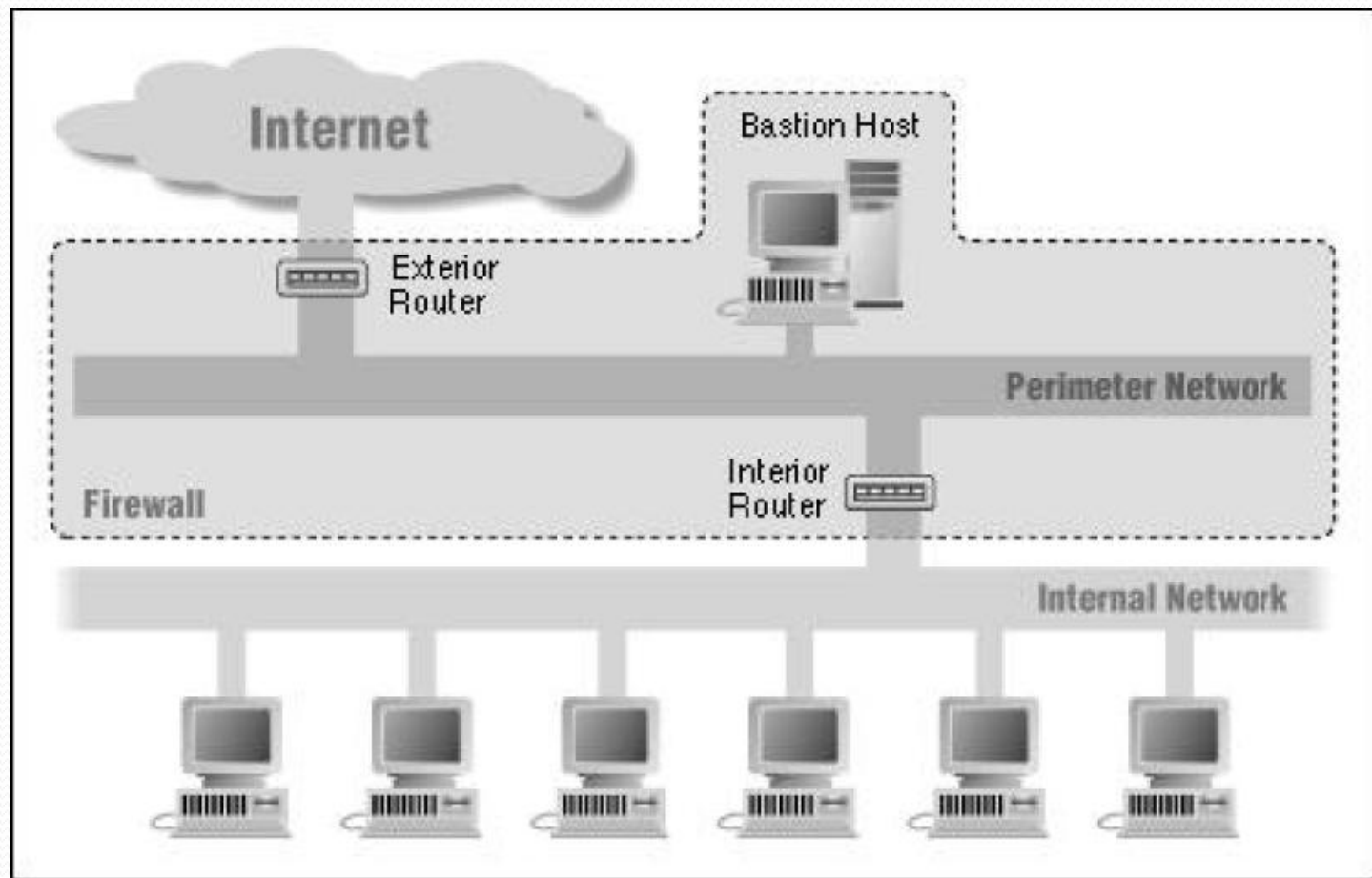
Bastion host berada dalam jaringan internal. Packet filtering pada screening router dikonfigurasi sehingga hanya bastion host yang dapat melakukan koneksi ke Internet (misalnya mengantarkan mail yang datang) dan hanya tipe-tipe koneksi tertentu yang diperbolehkan. Tiap sistem eksternal yang mencoba untuk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



Screened subnet architecture

Arsitektur screened subnet menambahkan sebuah layer pengaman tambahan pada arsitektur 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).



Type-Type Firewall

- Packet Filtering Router
- Circuit Gateways
- Application Gateways
- Hybrid Firewalls

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 subtype: Static Filtering, Dynamic Filtering, Stateful Inspection

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 ijin. Penggunaan tipe ini biasanya dikarenakan administrator percaya dengan pengguna internal (internal users).

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.

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.
- Bisa 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. Dapat memberikan autentifikasi pengguna yang lebih ketat pada Stateful Packet Filer dengan menambahkan proxy untuk tiap service.

Sistem Pengamanan Menggunakan Firewall

Packet Filtering

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

Proxy Services

Proxy merupakan sistem pengamanan yang memerlukan alamat IP yang jelas dan valid, karena server yang utama terdapat di internet.

Sistem proxy ini 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.

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)

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.

3. Jaringan (Network)

- Sekumpulan alat-alat jaringan yang saling berkomunikasi satu dengan yang lain melalui beberapa metode arbitrary (berubah-ubah).

VPN adalah

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 media 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.

Protokol Tunneling Utama VPN

1. 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. PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP datagrams agar dapat ditransmisikan melalui internet. PPTP juga dapat digunakan pada jaringan private LAN-to-LAN.

2. 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. L2TP biasa digunakan dalam membuat Virtual Private Dial Network (VPDN) yang dapat bekerja membawa semua jenis protokol komunikasi didalamnya.

3. Internet Protocol Security (IPsec)

IPSec merupakan suatu pengembangan dari protokol IP yang bertujuan untuk menyediakan keamanan pada suatu IP dan layer yang berada di atasnya (Carmouche, 2006). IPSec 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. IPSec merupakan metode yang memproteksi IP datagram ketika paket ditransmisikan pada traffic.

Fungsi Utama VPN

- Confidentially (Kerahasiaan)

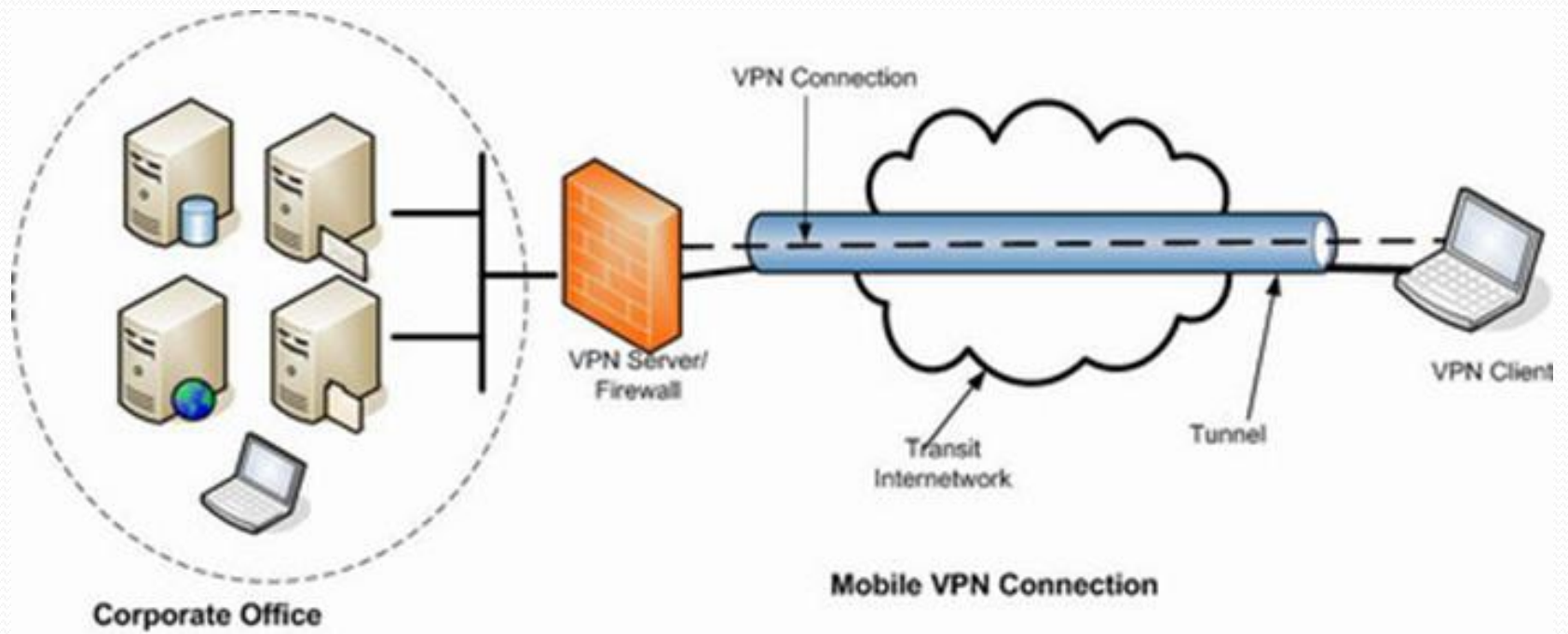
Teknologi VPN merupakan teknologi yang memanfaatkan jaringan publik yang tentunya sangat rawan terhadap pencurian data. Untuk itu, VPN menggunakan metode enkripsi untuk mengacak data yang lewat. Dengan adanya teknologi enkripsi itu, keamanan data menjadi lebih terjamin. Walaupun ada pihak yang dapat 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.



Cara kerja VPN *(dengan protokol PPTP)*

- 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, printing dokument, browsing dengan gateway yang diberikan dari VPN Server, melakukan remote desktop dan lain sebagainya.

Kelebihan VPN

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. Aman

Virtual Networking, menciptakan 'tunnel' dalam jaringan yang tidak harus direct. Sebuah 'terowongan' diciptakan melalui public network seperti internet. Sehingga seolah-olah terdapat hubungan point-to-point dengan data yang dienkapsulasi. Tunnel dalam Virtual Networking sebenarnya hanya logical point-to-point connection dengan otentikasi dan enkripsi. Teknologi ini dapat dibuat di atas jaringan dengan pengaturan IP Addressing dan IP Routing yang sudah matang. Maksudnya, antara sumber tunnel dengan tujuan tunnel telah 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.

4. 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

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 untuk menjadikan PC kita sebagai telephone yang aman.

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 perlindungan 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 eksklusif. 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.


Contoh Kasus Celah VPN

Membuat internet gratisan dan non-quota

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 quota. Karena, port tersebut tidak digunakan untuk perhitungan billing sehingga kita tidak melewati billing server dengan port ini maka kita bisa terhubung ke VPN server melalui jaringan internet. Kita terkoneksi ke internet tetapi tidak melewati billing server, otomatis kita tidak dikenakan charge dan count data tidak dihitung walaupun 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 internet.

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 untuk memblokir lalu lintas yang tak diinginkan. Jika pengguna mengirimkan sebuah pesan, pesan tersebut mengalir melewati firewall menuju internet. Firewall akan memblokir 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.

SEKIAN DAN TERIMA KASIH