UNIVERSITAS GUNADARMA

MENGENAL SISTEM FIREWALL

Oktaviani, Skom., MMSI

2007

MENGENAL SISTEM FIREWALL

Oktaviani, Skom., MMSI
Universitas Gunadarma
oktaviani@staff.gunadarma.ac.id

Abstraksi

Dalam sebuah jaringan, istilah "firewall" tentunya terdengar sudah tidak asing lagi. Karena saat ini firewall sudah banyak digunakan, terutama dalam sebuah jaringan komputer yang terkoneksi langsung ke jaringan publik atau yang dikenal dengan internet. Dengan pesatnya perkembangan internet, dapat memberikan dampak positif bagi kita sebagai penyedia layanan informasi dan komunikasi, selain itu internet juga dapat memberikan dampak negatif sekaligus ancaman bagi penggunanya. Sehingga akses jaringan kita dengan internet harus dibatasi oleh sebuah pembatas yang dikenal dengan firewall.

Kata Kunci: *firewall, jaringan komputer*.

Pendahuluan

Saat ini internet sudah semakin banyak diakses oleh banyak orang. Penggunaan internet nampaknya sudah semakin tidak dapat dipisahkan di berbagai bidang dalam kehidupan manusia di dunia ini. Dengan adanya internet, seseorang dapat dengan mudah mengetahui dan mendapatkan informasi, mudah berkomunikasi dengan rekan tanpa memandang jarak dan waktu, mudah melakukan transaksi dimanapun dan kapanpun, mudah melakukukan aktivitas belajar mengajar jarak jauh dan masih banyak lagi kemudahan yang diberikan oleh internet. Seolah olah dengan adanya internet kita merasakan bahwa dunia itu seperti tanpa batas. Dibelahan dunia manapun saat ini sudah dapat dihubungkan dengan internet, yang menyediakan beragam informasi yang dapat diakses oleh siapapun.

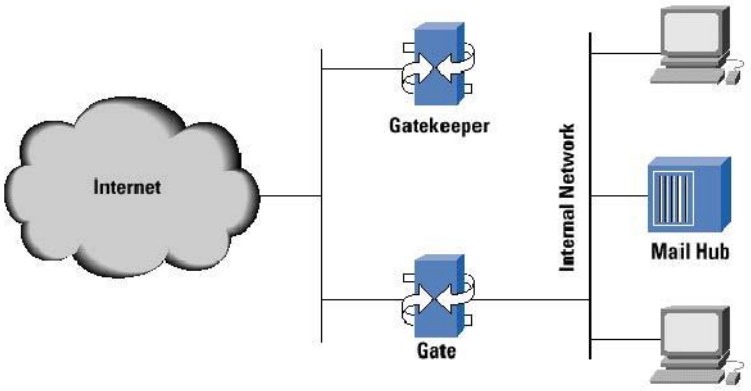
Sejalan dengan pesatnya perkembangan internet, selain memberikan dampak positif sebagai penyedia layanan informasi dan komunikasi, internet juga dapat memberikan dampak negatif sekaligus ancaman bagi penggunanya. Ancaman itu bentuknya berbagai macam dari virus, trojan, cacker, dan yang lainnya. Dengan akses yang tak terbatas, diibaratkan rumah yang tidak memiliki tembok yang dapat dimasuki oleh siapa saja yang berkepentingan tanpa dapat diketahui niatnya baik ataupun buruk. Dengan keadaan seperti itu, sudah seharusnya kita memberikan perlindungan terhadap rumah kita dengan mendirikan tembok baik dari beton atau kayu, sehingga akses kerumah lebih mudah dikontrol. Sama halnya dengan komputer yang terhubung dengan internet, juga harus diberikan tembok pelindung yang sering disebut dengan "firewall' untuk melindungi komputer dari ancaman yang datang dari internet.

Pembahasan

Mengenal Sejarah Firewall

Network firewall yang pertama muncul pada akhir era 1980 an yaitu berupa perangkat router yang dipakai untuk memisahkan suatu network menjadi jaringan lokal (LAN) yang lebih kecil, dimana kondisi ini penggunaan firewall hanya dimaksudkan untuk mengurangi masalah peluberan (spillover) data dari LAN keseluruh jaringan untuk mencegah masalah masalah semacam error pada manajemen jaringan, atau aplikasi yang terlalu banyak menggunakan sumberdaya meluber ke seluruh jaringan. Penggunaan firewall untuk keperluan sekuriti (security firewall) pertama kali digunakan pada awal dekade 1990 an, berupa router IP dengan aturan filter tertentu. Aturan sekuriti saat itu berupa sesuatu seperti: ijinkan setiap orang "disini" untuk mengakses "keluar sana" , juga cegahlah setiap orang (atau apa saja yang tidak disukai) "diluar sana" untuk masuk "kesini". Firewall semacam ini cukup efektif, tetapi memiliki kemampuan yang terbatas. Seringkali sangat sulit untuk menggunakan aturan filter secara benar. Sebagai contoh, dalam beberapa kasus terjadi kesulitan dalam mengenali seluruh bagian dari suatu aplikasi yang dikenakan restriksi. Dalam kasus lainnya, aturan filter harus dirubah apabila ada perubahan "diluar sana".

Firewall generasi selanjutnya lebih fleksibel, yaitu berupa sebuah firewall yang dibangun pada apa yang disebut "Bastion Host". Firewall komersial yang pertama dari tipe ini, yang menggunakan filter dan gateway aplikasi (proxies), kemungkinan adalah produk dari Digital Equipment Corp (DEC). DEC yang dibangun berdasarkan firewall korporat DEC. Brian Reidd anti mengineering di laboratorium sistem jaringan DEC di Pallo Alto adalah pencipta firewall DEC. Firewall komersial pertama di konfigurasi untuk, dan dikirimkan kepada pelanggan pertamanya, sebuah perusahaan kimia besar yang berbasis di pantai timur AS pada 13 Juni 1991. Dalam beberapa bulan kemudian, Marcus Ranum dari Digital Corp. Menciptakan security proxies dan menulis ulang sebagian besar kode program firewall. Produk firewall tersebut kemudian diproduksi massal dengan nama dagang DECSEAL (singkatan dari Security External Access Link). DECSEAL tersusun atas sebuah sistem eksternal yang disebut gatekeeper sebagai satu satunya sistem yang dapat berhubungan dengan internet, sebuah filtering gateway yang disebut gate, dan sebuah mailhub internal (gambar1).



Gambar 1. DECSEAL Firewall komersial pertama

"Bastion Host" adalah sistem / bagian yang dianggap tempatter kuat dalam sistem keamanan jaringan oleh administrator. Atau dapat disebut bagian terdepan yang dianggap paling kuat dalam menahan serangan, sehingga menjadi bagian terpenting dalam pengamanan jaringan, biasanya merupakan komponen firewall atau bagian terluar sistem publik. Umumnya Bastionhost akan menggunakan Sistem operasi yang dapat menangani semua kebutuhan misal: Unix, linux, NT. Firewall untuk pertama kalinya dilakukan dengan menggunakan prinsip "non routing" pada sebuah Unix host yang menggunakan 2 buah network interface card, network interface card yang pertama dihubungkan ke internet (jaringan lain) sedangkan yang lainnya dihubungkan ke PC (jaringan lokal) (dengan catatan tidak terjadi "route" antara kedua network interface card di PC ini).

Definisi Firewall

Istilah "firewall" sendiri sebenarnya juga dikenal dalam disiplin lain,dan dalam kenyataannya, istilah ini tidak hanya bersangkutan dengan terminology jaringan. Kita juga menggunakan firewall, misalnya untuk memisahkan garasi dari rumah, atau memisahkan satu apartemen dengan apartemen lainnya. Dalam hal ini, firewall adalah penahan (barrier) terhadap api yang dimaksudkan untuk memperlambat penyebaran api seandainya terjadi kebakaran sebelum petugas pemadam kebakaran dating untuk memadamkan api. Contoh lain dari firewall juga bisa ditemui pada kendaran bermotor, dimana firewall memisahkan antara ruang penumpang dan kompartemen mesin.

Untuk firewall didalam terminology jaringan, memiliki beberapa pengertian antara lain adalah sebagai berikut:

Firewall didefinisikan sebagai suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun system 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.

Firewall didefinisikan sebagai sebuah komponen atau kumpulan komponen yang membatasi akses antara sebuah jaringan yang diproteksi dan internet, atau antara kumpulan kumpulan jaringan lainnya.

Definisi lain mengatakan bahwa, firewall adalah sebuah computer yang memproteksi jaringan dari jaringan yang tidak dipercaya yang memisahkan antara jaringan local dengan jaringan publik, dengan melakukan metode filtering paket data yang masuk dan keluar

Ilmuwan lain mendefinisikan firewall sebagai sebuah titik diantara dua/lebih jaringan dimana semua lalulintas (trafik) harus melaluinya (choke point); trafik dapat dikendalikan oleh dan diautentifikasi melalui sautu perangkat, dan seluruh trafik selalu dalam kondisi tercatat (logged).

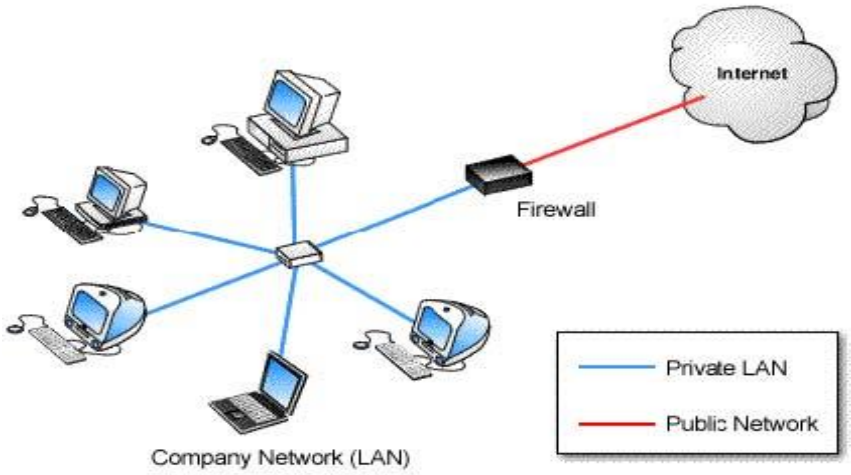
Dari beberapa definisi diatas, penulis dapat memberikan definisi dimana firewall adalah sebuah pembatas antara suatu jaringan local dengan jaringan lainnya yang sifatnya public (dapat diakses oleh siapapun) sehingga setiap data yang masuk dapat diidentifikasi untuk dilakukan penyaringan sehingga aliran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

Tujuan Penggunaan

Terdapat beberapa tujuan penggunaan firewall, antara lain:

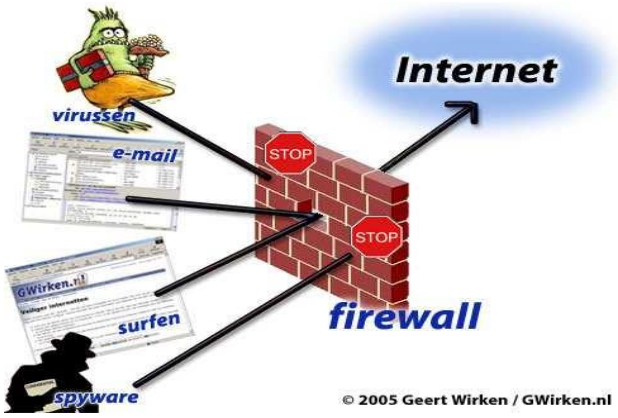
a) Firewall biasanya digunakan untuk mencegah atau mengendalikan aliran data tertentu. Artinya, setiap paket yang masuk atau keluarakan diperiksa, apakah cocok atau tidak dengan criteria yang ada pada standar keamanan yang didefinisikan dalam firewall.

b) 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,



Gambar 2. Firewall sebagai pembatas LAN dengan internet

c) Penggunaan firewall yang dapat mencegah upaya berbagai Trojan horses, virus, phishin, spyware untuk memasuki system yang dituju dengan cara mencegah hubungan dari luar, kecuali yang diperuntukan bagi computer dan port tertentu seperti gambar 3.



Gambar 3. Firewall mencegah virus dan ancaman lain masuk ke jaringan

d) Firewall akan memfilter serta mengaudit traffic yang melintasi perbatasan antara jaringan luar maupun dalam.

Teknik Teknik yang Digunakan firewall

Adapun beberapa teknik yang digunakan dalam firewall adalah sebagai berikut:

- Service control (kendali terhadap layanan) Berdasarkan tipetipe 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 digunakan baik pada protocol 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.

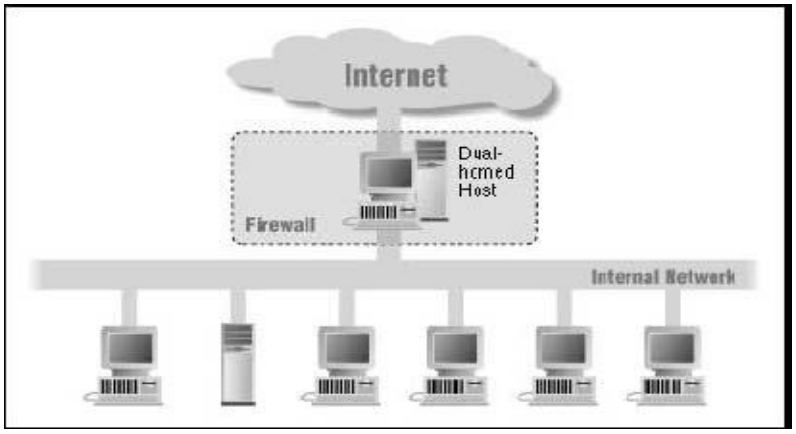
- Direction Conrol (kendali terhadap arah) Berdasarkan arah dari berbagai permintaan (request) terhadap layanan yang akan dikenali dan diijinkan melewati firewall.
- User control (kendali terhadap pengguna) Berdasarkan pengguna/user untuk dapat menjalankan suatu layanan, artinya ada user yang dapat dan ada yang tidak dapat menjalankan suatu servis, hal ini dikarenakan user tersebut tidak diijinkan untuk melewati firewall. Biasanya digunakan untuk membatasi user dari jaringan local 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

Ada beberapa arsitektur atau konfigurasi dari firewall. Pada makalah ini hanya akan dijelaskan beberapa diantaranya, yaitu: dualhomed host architecture, screened host architecture, dan screened sub net architecture. Adapun penjelasannya dapat dijelaskan sebagai berikut.

Dual homed host architecture

Arsitektur dual home host dibuat disekitar computer dualhomed host, yaitu computer yang memiliki paling sedikit dua interface jaringan. Untuk mengimplementasikan tipe arsitektur dualhomed host, fungsi routing pada host ini dinonaktifkan. Sistem di dalam firewall dapat berkomunikasi dengan dualhomed host dan system diluar firewall dapat berkomunikasi dengan dualhomed host, tetapi kedua system ini tidak dapat berkomunikasi secara langsung. Gambaran arsitektur ini seperti gambar 4.

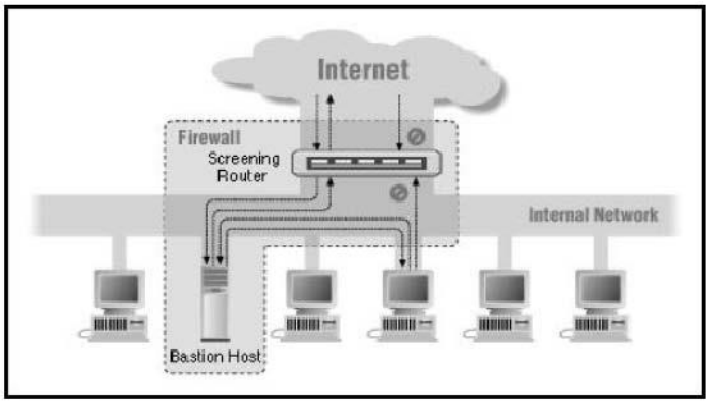


Gambar 4. Dual homed host architecture

Dualhomed 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 seperti gambar 5.

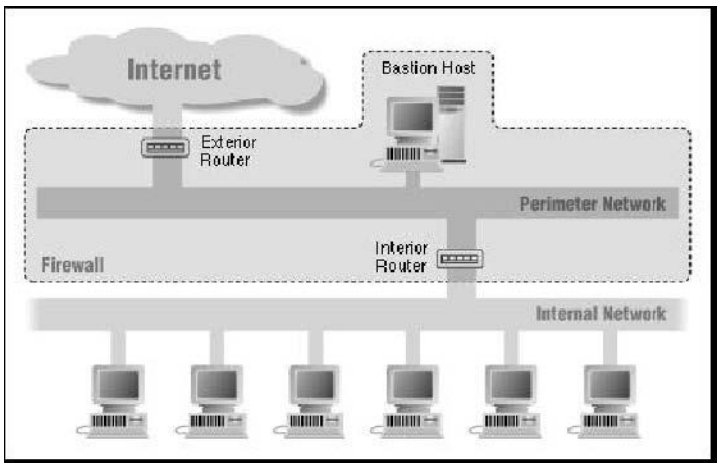


Gambar 5. Screened host architecture

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 tipetipe koneksi tertentu yang diperbolehkan. Tiap system eksternal yang mencoba untuk mengakses system 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 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 masingmasing terhubung ke jaringan perimeter. Router pertama terletak di antara jaringan perimeter dan jaringan internal, dan router kedua terletak diantara jaringan perimeter dan jaringan eksternal (biasanya Internet).



Gambar 6. Screened subnet architecture

Untuk menembus jaringan internal dengan tipe arsitektur screened subnet, seorang intruder harus melewati dua buah router tersebut sehingga jaringan internal akan relative lebih aman. Gambar 6 menunjukan gambar arsitektur screened subnet.

Tipe Tipe Firewall

Ada beberapa tipe dari firewall yang ada. Selanjutnya akan dijelaskan secara lebih rinci seperti berikut. Ada empat jenis firewall, atau lebih tepatnya tiga jenis ditambah dengan satu tipe hybrid (campuran). Disini kita tidak akan membahas setiap jenis secara rinci Karena itu membutuhkan pembahasan tersendiri yang lebih teknis dan umumnya sudah tersedia dalam dokumentasi-dokumentasi tentang firewall. Keempat jenis tersebut masing masing adalah:

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 protocol (IP) paket data dan membuat keputusan mengenai tindakan selanjutnya

(diteruskan atau tidak diteruskan) berdasarkan kondisi dari paket tersebut. Firewall ini dapat digambarkan seperti gambar 7. Firewall jenis ini terbagi lagi menjadi tiga subtipe:

O Static Filtering : Jenis filter yang diiplementasikan pada kebanyakan router, dimana modifikasi terhadap aturan aturan filter harus dilakukan secara manual.

O Dynamic Filtering : Apabila prosesproses tertentu disisi luar jaringan dapat merubah aturan filer secara dinamis berdasarkan eveneven tertentu yang diobservasi oleh router (sebagai contoh, paket FTP dari sisi luar dapat diijinkan apabila seseorang dari sisi dalam merequest sesi FTP).

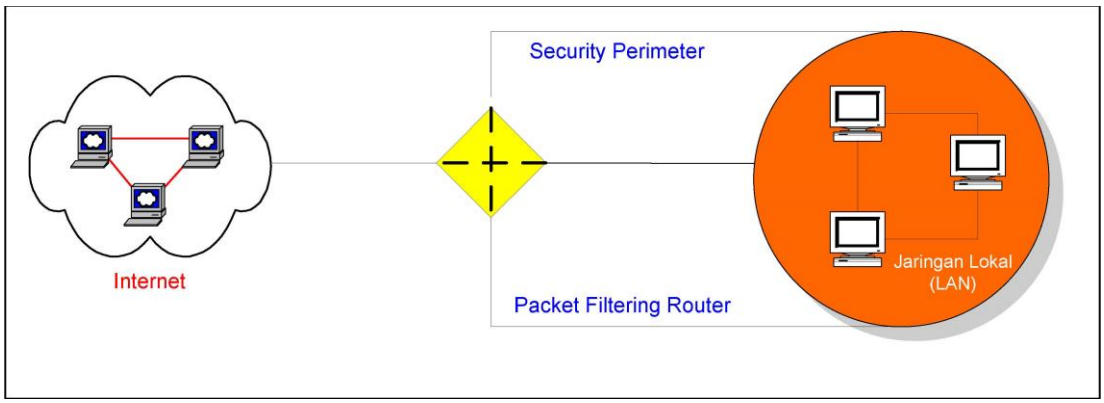
O Stateful Inspection : Dikembangkan berdasarkan teknologi yang sama dengan dynamic filtering dengan tambahan fungsi eksaminasi secara bertingkat berdasarkan muatan data yang terkandung dalam paket IP.

Baik dynamic maupun static filtering menggunakan table status (statetable) dinamis yang akan membuat aturanaturan filter sesuai dengan even yang tengah berlangsung. Ditambahkan 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 local yang telah diijinkan untuk melalui firewall.

- Source routing attacks : Tipe ini tidak menganalisa informasi routing sumber IP, sehingga memungkinkan untuk membypass firewall.

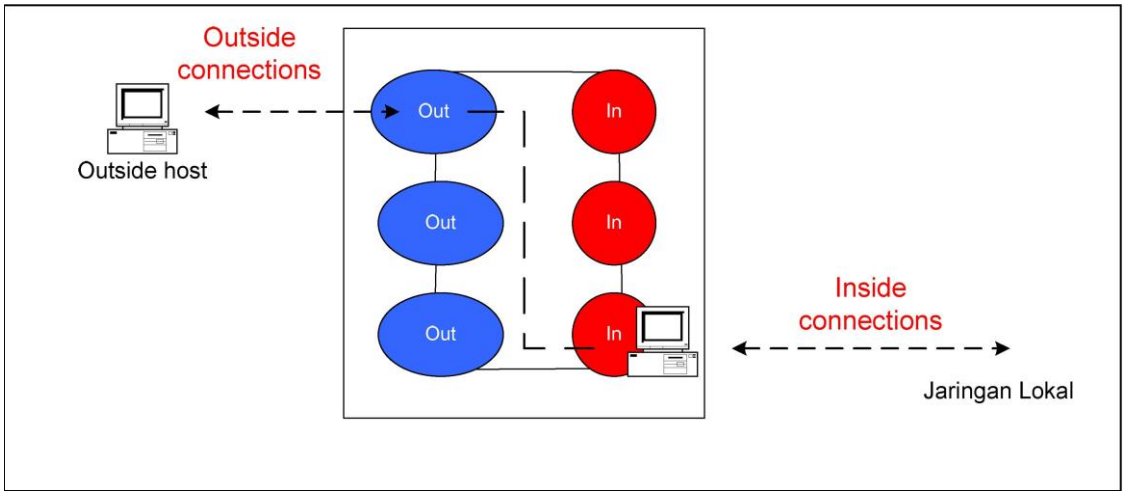
- Tiny Fragment attacks : Intruder membagi IP kedalam bagianbagian (fragment) yang lebih kecil dan memaksa terbaginya informasi mengenai TCP header. Serangan jenis ini didesign untuk menipu aturan penyaringan yang bergantung kepada informasi dari TCP header. Penyerang berharap hanya bagian (fragment) pertama saja yang akan diperiksa dan sisanya akan bisa lewat dengan bebas. Hal ini dapat ditanggulangi dengan cara menolak semua packet dengan protocol TCP dan memiliki Offset = 1 pada IP fragment (bagian IP)



Gambar 7. Packet filtering

2. Circuit Gateways

Firewall jenis ini beroperasi pada layer (lapisan) transport 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 local (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 kelainnya tanpa memeriksa isinya. Fungsi pengamanannya terletak pada penentuan hubungan mana yang diijinkan. Penggunaan tipe ini biasanya dikarenakan administrator percaya dengan pengguna internal (internal users). Dapat digambarkan seperti gambar 8.

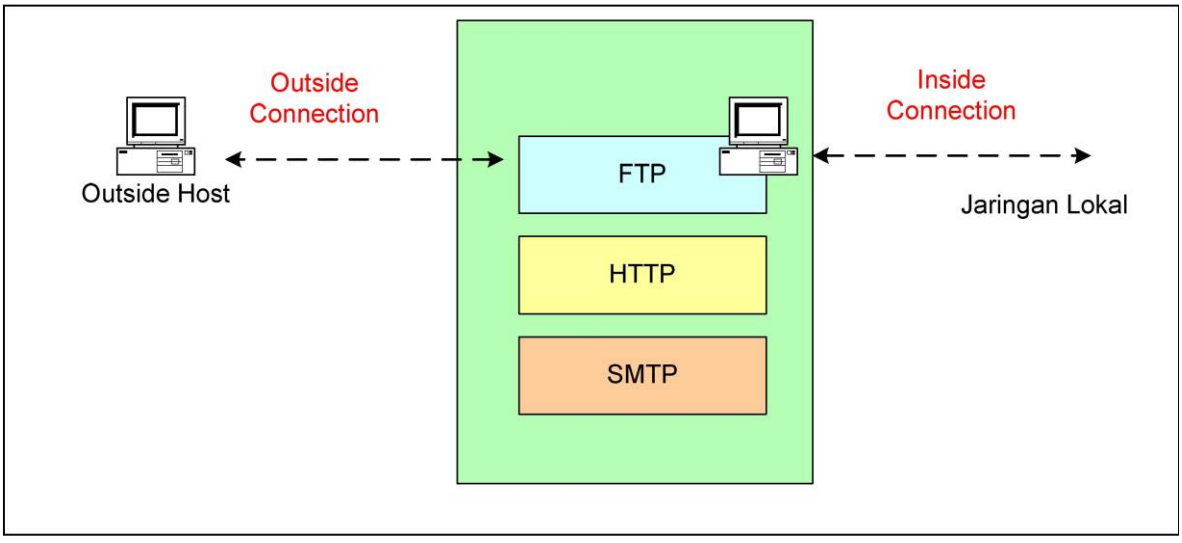


Gambar 8. Circuit Gateways

3. Application Gateways

Firewall tipe ini juga disebut sebagai firewall berbasis proxy. Ia beroperasi dilevel 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 perintahperintah FTP atau URL yang diakses lewat HTTP. Dapat dikatakan bahwa firewall jenis ini "memecah model clientserver". 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 diakses. 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 dikonfigurasikan untuk hanya mendukung beberapa aplikasi saja dan menolak aplikasi lainnya untuk melewati firewall.

Kelebihannya adalah relative 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. Agar lebih jelas, dapat digambarkan seperti gambar 9.



Gambar 9. Application Gateways

4. Hybrid Firewalls

Firewall jenis ini menggunakan elemen elemen dari satu atau lebih tipe firewall. Hybrid firewall sebenarnya bukan sesuatu yang baru. Firewall komersial

yang pertama, DECSEAL, adalah firewall berjenis hybrid, dengan menggunakan proxy pada sebuah bastion hosts (mesin yang dilabeli sebagai "gate keeper") dan packet filtering pada gateway ("gate"). Sistem hybrid seringkali digunakan untuk menambahkan layanan baru secara cepat pada system 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.

Kesimpulan

Berdasarkan penjelasan yang sudah disampaikan, dapat diambil beberapa kesimpulan yaitu keberadaan suatu firewall sangat penting digunakan dalam suatu jaringan yang terkoneksi langsung ke internet atau yang lebih dikenal dengan jaringan public yang dapat diakses oleh siapapun dan dimanapun. Sehingga peran firewall disana sangat berguna karena sebagai pembatas yang mengatur dan mengendalikan akses yang dilakukan untuk mengurangi dan mencegah ancaman-ancaman dari internet yang masuk ke jaringan lokal.

Daftar Pustaka

[1] Arman, *Firewall dari Masa ke Masa*, 2007, http://unms.unimal.ac.id/

[2] Muammar W.K, *Firewall*, 2004, http://ilmukomputer.com