FireWall

Ahmad Muammar. W. K

y3dips@echo.or.id
http://echo.or.id

PENGANTAR

Ibarat sebuah rumah yang memiliki pagar sebagai pelindungnya, baik dari kayu, tembok beton, kawat berduri ataupun kombinasi beberapa jenis pagar, maka tak pula mengherankan apabila sebuah komputer yang merupakan sebuah tempat vital dalam komunikasi data yang menyimpan semua harta dan benda yang kita miliki juga patut kita lindungi. Tetapi, apa pula jenis pagar yang akan kita pakai untuk membentengi komputer/jaringan pribadi kita terhadap semua ancaman khususnya dari luar terhadap semua properti pribadi kita yang terdapat didalamnya? Pernah dengar istilah *Tembok Api* ? sedikit terdengar lucu apabila diartikan per suku kata dari kata "*firewall*". Tetapi apa dan bagaimanakah firewall itulah yang akan kita coba kupas dalam tulisan ini.

Pengertian

Firewall merupakan 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. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN) anda.

konfigurasi sederhananya:

pc (jaringan local) ←==→ ***firewall*** ←==→ **internet** (jaringan lain)

Firewall untuk komputer, pertama kali dilakukan dengan menggunakan prinsip “non-routing” pada sebuah Unix host yang menggunakan 2 buah network interface card, network interface card yang pertama di hubungkan 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). Untuk dapat terkoneksi dengan Internet(jaringan lain) maka harus memasuki server firewall (bisa secara remote, atau langsung), kemudian

menggunakan resource yang ada pada komputer ini untuk berhubungan dengan Internet(jaringan lain), apabila perlu untuk menyimpan file/data maka dapat menaruhnya sementara di pc firewall anda, kemudian mengkopikannya ke pc(jaringan lokal). Sehingga internet(jaringan luar) tidak dapat berhubungan langsung dengan pc(jaringan lokal) .

Dikarenakan masih terlalu banyak kekurangan dari metoda ini, sehingga dikembangkan berbagai bentuk, konfigurasi dan jenis firewall dengan berbagai policy(aturan) didalamnya.

Firewall secara umum di peruntukkan untuk melayani :

1. Mesin/Komputer

   Setiap mesin/komputer yang terhubung langsung ke jaringan luar atau internet dan menginginkan semua yang terdapat pada komputernya terlindungi.

2. Jaringan

   Jaringan komputer yang terdiri lebih dari satu buah komputer dan berbagai jenis topologi jaringan yang digunakan, baik yang di miliki oleh perusahaan, organisasi dsb.

Karakteristik sebuah firewall

1. Seluruh hubungan/kegiatan dari dalam ke luar , harus melewati firewall. Hal ini dapat dilakukan dengan cara memblok/membatasi baik secara fisik semua akses terhadap jaringan Lokal, kecuali melewati firewall. Banyak sekali bentuk jaringan yang memungkinkan agar konfigurasi ini terwujud.

2. Hanya Kegiatan yang terdaftar/dikenal yang dapat melewati/melakukan hubungan, hal ini dapat dilakukan dengan mengatur policy pada konfigurasi keamanan lokal. Banyak sekali jenis firewall yang dapat dipilih sekaligus berbagai jenis policy yang ditawarkan.

3. Firewall itu sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan system yang relatif aman.

Teknik yang digunakan oleh sebuah 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 Conrol (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. Misal, firewall dapat memfilter email untuk menanggulangi/mencegah spam.

Tipe-Tipe Firewall

1 .Packet Filtering Router

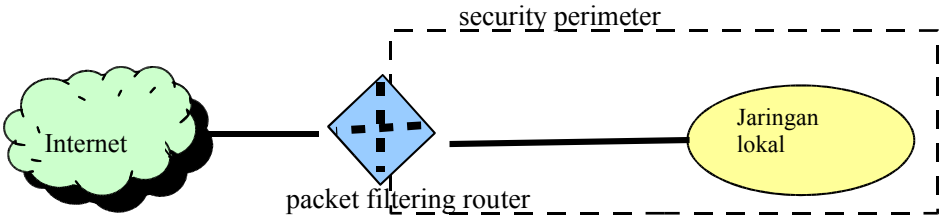
Packet Filtering diaplikasikan dengan cara mengatur semua packet IP baik yang menuju, melewati atau akan dituju oleh packet tersebut. Pada tipe ini packet tersebut akan diatur apakah akan di terima dan diteruskan atau di tolak. Penyaringan packet ini di konfigurasikan untuk menyaring packet yang akan di transfer secara dua arah (baik dari dan ke jaringan lokal). Aturan penyaringan didasarkan pada header IP dan transport header, termasuk juga alamat awal(IP) dan alamat tujuan (IP), protokol transport yang di gunakan(UDP,TCP), serta nomor port yang digunakan. Kelebihan dari tipe ini adalah mudah untuk di implementasikan, transparan untuk pemakai, relatif lebih cepat.

Adapun kelemahannya 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)



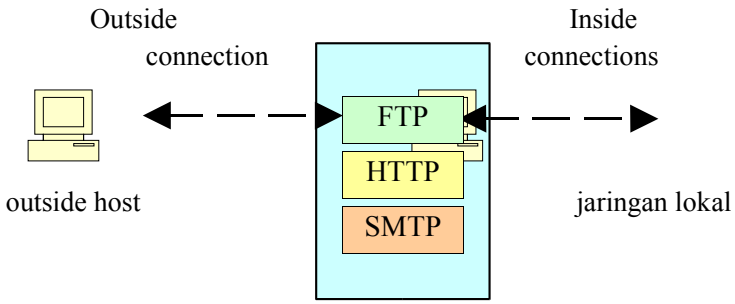
2. Application-Level Gateway

Application-level Gateway yang biasa juga di kenal sebagai proxy server yang berfungsi untuk memperkuat/menyalurkan arus aplikasi. Tipe ini akan mengatur semua hubungan yang menggunakan layer aplikasi ,baik itu FTP, HTTP, GOPHER dll.

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 useer 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.



3. Circuit-level Gateway

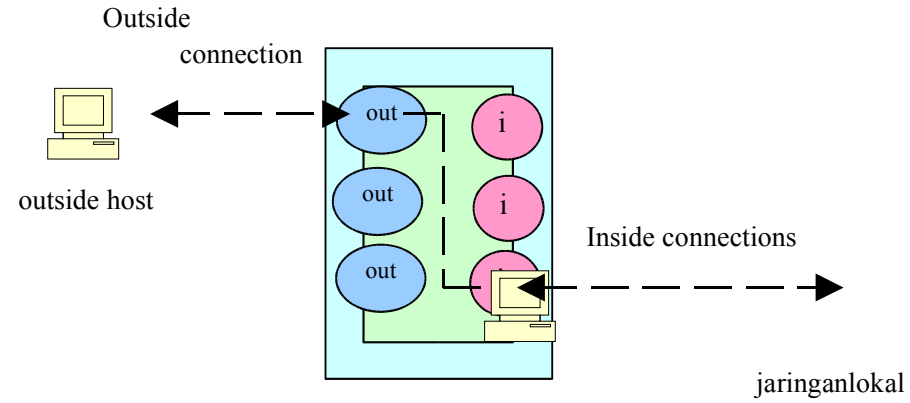
Tipe ketiga ini dapat merupakan sistem yang berdiri sendiri , atau juga dapat merupakan fungsi khusus yang terbentuk dari tipe application-level gateway.tipe ini tidak mengijinkan koneksi TCP end to end (langsung)

Cara kerjanya : 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).

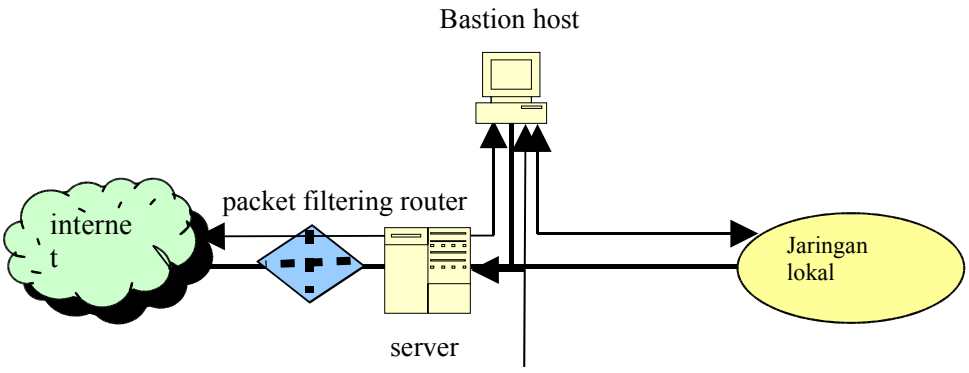
Gambar



Konfigurasi Firewall

1 .Screened Host FIrewall system (single-homed bastion)

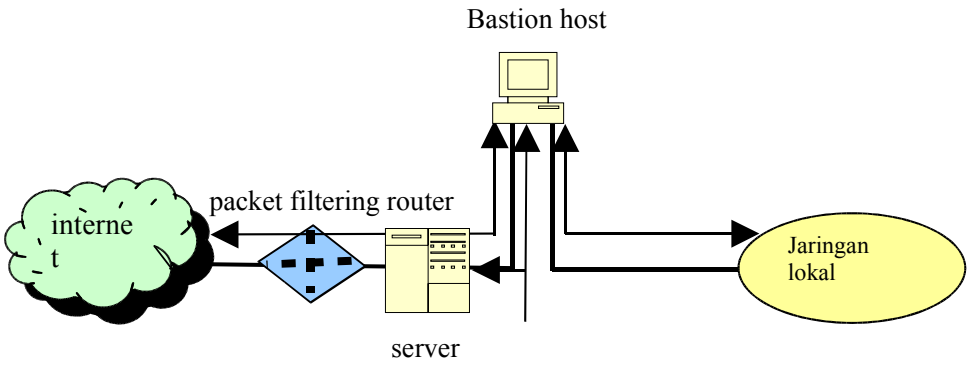
Pada konfigurasi ini, fungsi firewall akan dilakukan oleh packet filtering router dan bastion host*.Router ini dikonfigurasikan sedemikian sehingga untuk semua arus data dari Internet, hanya paket IP yang menuju bastion host yang di ijinkan. Sedangkan untuk arus data (traffic) dari jaringan internal, hanya paket IP dari bastion host yang di ijinkan untuk keluar.
Konfigurasi ini mendukung fleksibilitasdalam Akses internet secara langsung, sebagai contoh apabila terdapat web server pada jaringan ini maka dapat di konfigurasikan agar web server dapat diakses langsung dari internet.
Bastion Host melakukan fungsi Authentikasi dan fungsi sebagai proxy. Konfigurasi ini memberikan tingkat keamanan yang lebih baik daripada packet-filtering router atau application-level gateway secara terpisah.



2. Screened Host Firewall system (Dual-homed bastion)

Pada konfigurasi ini, secara fisik akan terdapat patahan/celah dalam jaringan. Kelebihannya adalah

dengan adanya dua jalur yang meisahkan secara fisik maka akan lebih meningkatkan keamanan dibanding konfigurasi pertama,adapun untuk server-server yang memerlukan direct akses (akses langsung) maka dapat di letakkan ditempat/segmenrt yang langsung berhubungan dengan internet. Hal ini dapat dilakukan dengan cara menggunakan 2 buah NIC (network interface Card) pada bastion Host.

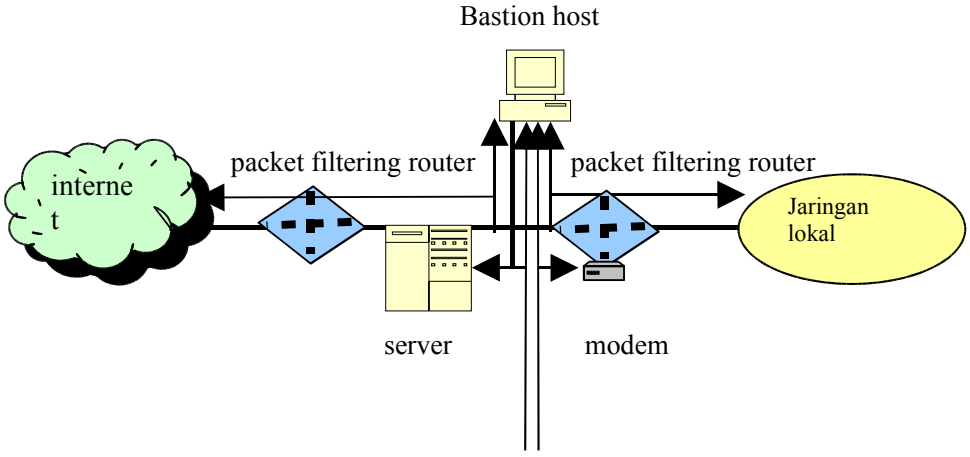


3. Screened subnet firewall

Ini merupakan konfigurasi yang paling tinggi tingkat keamanannya. kenapa? karena pada konfigurasi ini di gunakan 2 buah packet filtering router, 1 diantara internet dan bastion host, sedangkan 1 lagi diantara bastian host dan jaringan local konfigurasi ini membentuk subnet yang terisolasi.

Adapun kelebihannya adalah :

- Terdapat 3 lapisan/tingkat pertahanan terhadap penyususp/intruder .
- Router luar hanya melayani hubungan antara internet dan bastion host sehingga jaringan lokal menjadi tak terlihat (invisible)
- Jaringan lokal tidak dapat mengkonstuksi routing langsung ke internet, atau dengan kata lain , Internet menjadi Invinsible (bukan berarti tidak bisa melakukan koneksi internet).



Langkah-Langkah Membangun firewall

1. Mengidenftifikasi bentuk jaringan yang dimiliki
   Mengetahui bentuk jaringan yang dimiliki khususnya toplogi yang di gunakan serta protocol jaringan, akan memudahkan dalam mendesain sebuah firewall

2. Menentukan Policy atau kebijakan
   Penentuan Kebijakan atau Policy merupakan hal yang harus di lakukan, baik atau buruknya sebuah firewall yang di bangun sangat di tentukan oleh policy/kebijakan yang di terapkan. Diantaranya:

- Menentukan apa saja yang perlu di layani. Artinya, apa saja yang akan dikenai policy atau kebijakan yang akan kita buat
- Menentukan individu atau kelompok-kelompok yang akan dikenakan policy atau kebijakan tersebut
- Menentukan layanan-layanan yang di butuhkan oleh tiap tiap individu atau kelompok yang menggunakan jaringan
- Berdasarkan setiap layanan yang di gunakan oleh individu atau kelompok tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuatnya semakin aman
- Menerapkankan semua policy atau kebijakan tersebut

3. Menyiapkan Software atau Hardware yang akan digunakan
   Baik itu operating system yang mendukung atau software-software khusus pendukung firewall seperti ipchains, atau iptables pada linux, dsb. Serta konfigurasi hardware yang akan mendukung firewall tersebut.

4. Melakukan test konfigurasi
   Pengujian terhadap firewall yang telah selesai di bangun haruslah dilakukan, terutama untuk mengetahui hasil yang akan kita dapatkan, caranya dapat menggunakan tool tool yang biasa dilakukan untuk mengaudit seperti nmap.

**** Bastion Host*** *adalah sistem/bagian yang dianggap tempat terkuat dalam sistem keamanan jaringan oleh administrator.atau dapat di sebuta 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 Bastion host akan menggunakan Sistem operasi yang dapat menangani semua kebutuhan (misal , Unix, linux, NT).*

REFERENSI

1. Stallings, William*, " Cryptography and Network Security , principle and practice: second edition "* , Prentice-Hall,Inc., New Jersey ,1999.
2. Belovin, S. and Cheswick, W., " *Network Firewalls "*, IEEE Communications Magazine, September 1994
3. Smith, R. , *" Internet Crypthography* ", Reading MA: Addison-Wesley, 1997.
4. Semeria, C. , " *Internet Firewalls and Security* ", 3 Com Corp.,1996.
5. Curtin,Matt and Ranum, J. Markus, "*Internet Firewalls: FAQ*" rev 10, 2000.
6. Mulyana, E dan Purbo, Onno W., "*Firewall : Security Internet*".
7. y3dips, "*Firewall"*, ezine-r04 : http://ezine.echo.or.id, Februari, 2004