Indra Dermawan (13294025)

BEBERAPA ARSITEKTUR FIREWALL

Indra Dermawan

Dosen: Onno W. Purbo

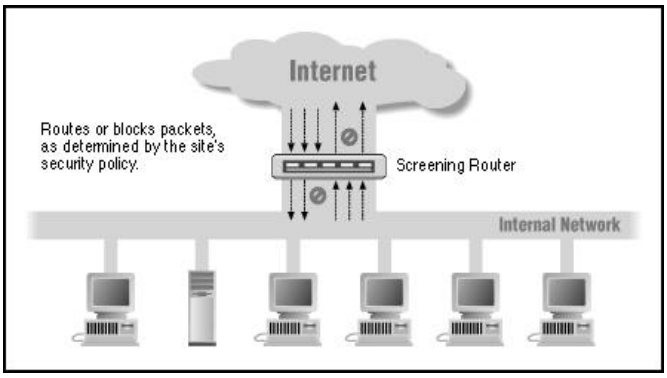
Perkembangan Internet dan jaringan internal yang semakin pesat menuntut adanya pengamanan terhadap jaringan internal dari kemungkinan adanya serangan dari jaringan eksternal. Salah satu cara yang banyak digunakan adalah dengan menggunakan firewall.

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. Firewall dapat berupa hardware dalam bentuk router atau komputer, atau software yang menjalankan sistem gateway, atau kombinasi keduanya. Dalam artikel ini akan dijelaskan komponen-komponen dasar dan beberapa arsitektur yang banyak digunakan dalam membuat suatu firewall.

Ada dua pendekatan utama yang digunakan dalam membuat firewall, yaitu : packet filtering dan proxy server.

Packet Filtering

Sistem packet filtering melakukan packet routing antara jaringan internal dengan jaringan eksternal secara selektif. Sistem ini melewatkan atau memblok packet data yang lewat sesuai dengan aturan yang telah ditentukan. Router pada sistem ini disebut screening router.



Gambar 1. Packet filtering dengan menggunakan screening router

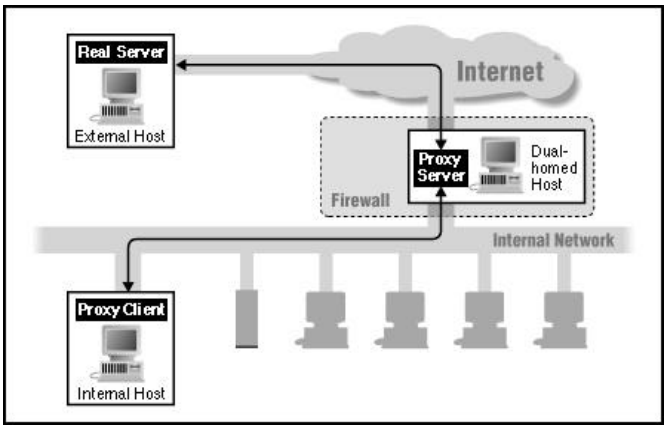
Untuk mengetahui bagaimana cara kerja packet filtering, kita harus mengetahui perbedaan antara router biasa dengan sebuah screening router. Router biasa hanya melihat alamat IP tujuan dari suatu packet data dan mengarahkannya ke jalur yang terbaik agar packet data tersebut sampai ke tujuannya. Bila router tidak dapat melakukannya, packet data akan dikembalikan ke sumbernya.

Screening router tidak hanya menentukan apakah router dapat melewatkan suatu packet data atau tidak, tetapi juga menerapkan suatu aturan yang akan menentukan apakah packet data tersebut akan dilewatkan atau tidak. Pemfilteran ini didasarkan pada :

1. IP sumber dan IP tujuan dari packet data
2. Port sumber dan port tujuan dari data
3. Protokol yang digunakan (TCP, UDP, ICMP, dan sebagainya)
4. Tipe pesan ICMP

Proxy Server

Proxy server adalah aplikasi khusus atau program server yang berjalan pada host firewall; baik pada dual-homed host yang memiliki sebuah interface ke jaringan internal dan interface lain ke jaringan eksternal, atau pada bastion host yang memiliki akses ke Internet dan dapat diakses oleh mesin internal. Program ini menangani request-request untuk service-service Internet dari user dan melewatkannya ke service yang sebenarnya. Proxy menyediakan koneksi pengganti dan bertindak selaku gateway terhadap service-service tersebut. Oleh karena itu proxy sering juga disebut gateway level aplikasi.



Gambar 2. Penggunaan proxy server pada dual-home host

Proxy server menghubungkan user pada jaringan internal dengan service pada Internet. User dan service tersebut tidak berkomunikasi secara langsung. Masing-masing berhubungan dengan proxy dan proxy yang menangani hubungan antara user dan service di belakang layar.

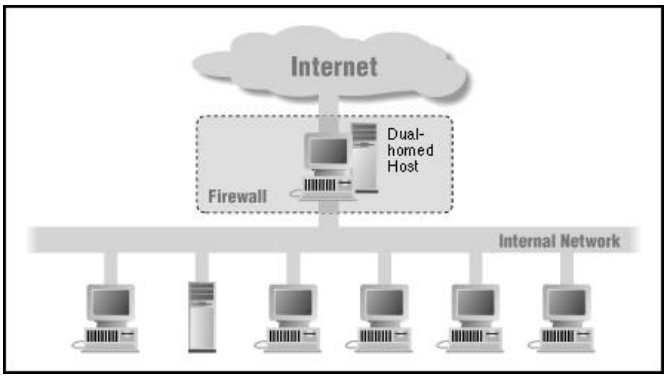
Proxy server dapat membatasi apa yang dapat dilakukan oleh user, karena proxy dapat memutuskan apakah suatu request dari user diperbolehkan atau ditolak.

Arsitektur Firewall

Ada beberapa arsitektur firewall. Pada artikel ini hanya akan dijelaskan beberapa diantaranya, yaitu : dual-homed host architecture, screened host architecture, dan screened subnet architecture.

1. Arsitektur Dual-Homed Host

Arsitektur Dual-home host dibuat disekitar komputer dual-homed 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.

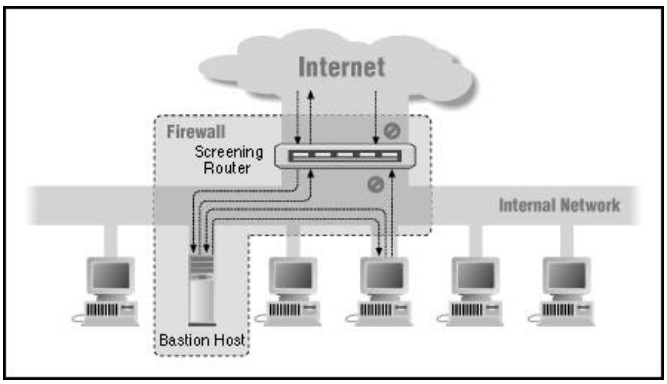


Gambar 3. Arsitektur dual-homed host

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. Arsitektur Screened Host

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.

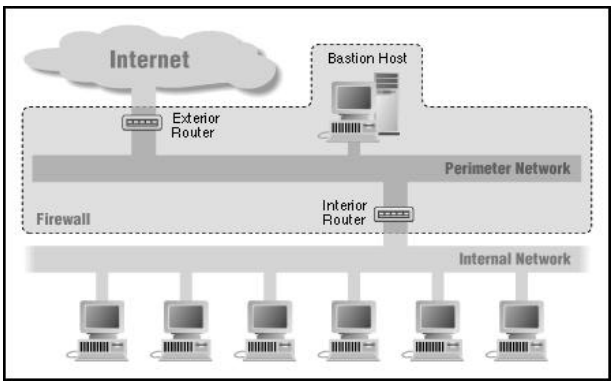


Gambar 4. Arsitektur screened host

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. Arsitektur Screened Subnet

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.



Gambar 5. Arsitektur screened subnet

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). Untuk menembus jaringan internal dengan tipe arsitektur screened subnet, seorang intruder harus melewati dua buah router tersebut sehingga jaringan internal akan relatif lebih aman.

Ada beberapa site yang menyediakan software firewall secara gratis, antara lain :

1. Firewall untuk Windows NT (Guardian Internet Firewall), dapat di download dari :
   http://www2.firewallnt.com/firewallnt/ntfirewalls.html
   http://www.lanoptic.com/lanoptics/downforml.cfm,
   http://www2.firewallnt.com/firewallnt/html/downloads.cfm
2. Keterangan tentang firewall untuk Linux, dapat dilihat di :
   http://metalab.unc.edu/linux/HOWTO/Firewall-HOWTO.html
   software firewall yang dijelaskan adalah filtering firewall IPFWADM (IP Firewall Administration Tools), TIS proxy server dan SICKS proxy server . Di sini juga dijelaskan proses instalasi dan konfigurasinya.