Laporan Pendahuluan Keamanan Data

Firewall

oleh Dimas Rizky H.P. – 2110141011 – 3 D4 IT A

**Konsep Firewall**

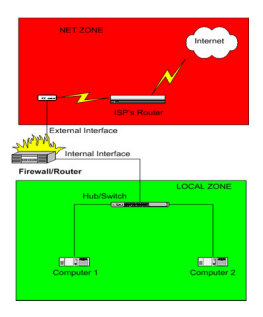
Firewall merupakan salah satu layer pertahanan(security) yang mengatur koneksi komputer dengan jaringan eksternal melalui analisa dan interogasi setiap traffic, packet dan port-port yang diatur dengan rule yang ada.

Firewall bekerja dengan cara, menyaring, membatasi dan menolak paket yang keluar masuk melewati firewall itu sendiri. Konfigurasi sederhana dari firewall adalah sebagai berikut

* Jaringan Lokal <==> Firewall <==> Internet (Jaringan publik)
* Jaringan A <==> Firewall <==> Jaringan B

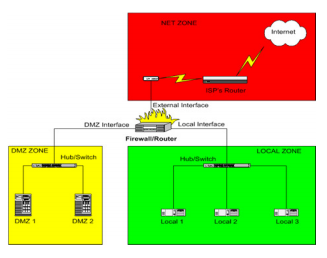
Firewall dapat dibangun dengan beberapa topologi, diantaranya adalah topologi tanpa DMZ atau dengan menggunakan DMZ

* Basic Two-interface Firewall (No DMZ)



*Gambar 1.0 No DMZ topologi*

* + Menghubungkan jaringan dengan ISP menggunakan DSL, Cable modem, ISDN, Dial-up, dll
  + Menyediakan internet connection sharing dari single public IP address pada local network menggunakan SNAT/Masquerading
  + SNAT (source NAT) atau masquerading adalah translasi IP address dari local ke public pada sisi IP source disertai dengan translasi port source, sehingga satu alamat IP public dapat digunakan secara bersama sama dengan banyak local address
* Three-interface Firewall (Dengan DMZ)



*Gambar 1.1 Three-interface firewall*

* + Menyediakan koneksi internet secara sharing menggunakan satu atau lebih public IP address
  + Memiliki DMZ (Demilitari Zone) yang berisi server yang dapat diakses oleh internet (jaringan publik)
  + Jika server terkena serangan, firewall dan jaringan local tidak akan tersentuh
  + DMZ memisahkan antara server dan jaringan lokal yang ada
  + Dengan DMZ, internet dapat mengakses server, namun tidak dapat mengakses jaringan local. Jaringan local dapat mengakses internet dan juga dapat mengakses server

**Tipe Firewall**

* Packet filtering

Memfilter paket berdasarkan sumber tujuan dan atribut paket (filter berdasarkan IP dan Port). Yang difilter antara lain IP, TCP, UDP dan ICMP header serta port number

* Application layer (Proxy Firewall)

Memfilter berdasarkan content packet

* Circuit level gateway

Filter berdasarkan sesi komunikasi dengan pengawasan sesi handshake

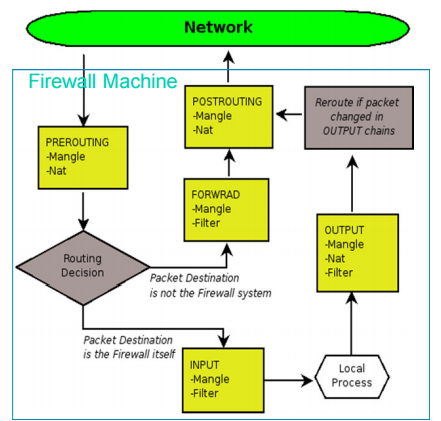
* Statefull multilayer inspection firewall

Merupakan kombinasi antara tiga firewall diatas

**IPTABLES**

Iptables merupakan netadmin command line tool pada linux yang menyediakan koneksi ke kernel untuk mengatur stateless dan statefull firewall serta konfigurasi NAT.

Prinsip kerjanya adalah paket masuk diproses berdasarkan tujuan lalu dicocokan berdasarkan tabel policy yang dipunyai firewall apakah di accept ataukah di drop



*Gambar 3.1 prinsip kerja firewall*

Jika destinasi packet bukan sistem firewall, maka yang dilakukan firewall adalah melakukan routing packet tersebut. Namun jika destinasi packet tersebut adalah firewall, maka packet tersebut akan di filter dan di proses hingga nantinya akan di reroute jika paket berganti

Ada beberapa sintaks Iptables yang dapat digunakan, antara lain adalah

* -A, menambah satu aturan baru dan ditempatkan pada posisi terakhir
* -D, menghapus rule
* -l, menambah aturan baru yang penempatannya dapat disisipkan sesuai dengan nomor yang di spesifikan
* -R, mengganti rule
* -F, menghapus seluruh rule
* -L, melihat rule

Iptables juga memiliki match, artinya aturan untuk menentukan/mendefinisikan host/mac yang aturannya diaplikasikan.

* Mac address, matching packet berdasarkan nomor MAC address
* Multiport, mendefinisikan banyak port
* State, mendefinisikan state dari koneksi

Target/Jump iptables, merupakan rule yang mengatur akan diapakan atau jump apa yang akan digunakan untuk rule yang spesifik

* ACCEPT, setiap packet langsung diterima
* DROP, packet datang langsung dibuang
* REJECT, packet yang ditolak akan dikrimi pesan ICMP error
* SNAT, sumber packet dirubah, biasanya yang memiliki koneksi internet
* DNAT, merubah tujuan alamat packet, biasanya jika server memiliki IP lokal, sehingga keamanannya lebih tinggi pada jaringan lokal milik server
* MASQUERADE, memungkinkan untuk berbagi koneksi internet dimana nomor IP nya terbatas, digunakan sebagai mapping IP lokal ke IP publik
* REDIRECT, digunakan untuk transparent proxy
* LOG, melakukan pencatatan tehadap aktifitas firewall yang ada dan dapat dibuka di /etc/syslog.conf