Saat ini rasanya hampir tidak ada komputer yang tidak tersambung ke jaringan/internet, baik itu melalui modem dialup, modem ADSL, maupun dedicated LAN. Hal ini menunjukkan pengaruh globalization di dalam beberapa dekade ini, dimana salah satu imbasnya adalah masuknya kita ke dalam 'internet society' - sebuah komunitas global yang terhubung melalui internet.

Hal ini tentu saja memberikan banyak pengaruh positif seperti makin cepatnya tersebarnya informasi dari satu negara ke negara lain, makin lancarnya transaksi bisnis lintas negara, dll. Dari sisi mikro, kini telah merupakan hal yang umum bila perusahaan berlangganan koneksi internet dedicated. Dengan berlangganan internet dedicated, maka selain lebih ekonomis, perusahaan pun dapat lebih leluasa dan cepat di dalam mengakses informasi/kesempatan bisnis lewat internet. Namun hal ini juga memberikan dampak negatif, atau mungkin lebih tepat kalau kita memakai istilah 'tantangan'.

Mengapa tantangan? Sebab dibandingkan sewaktu munculnya era internet di tahun 1990an, kini internet telah menjadi lingkungan yang sangat kejam. Tidak perduli apakah kita admin yang baru belajar ataupun yang sudah pengalaman, kita harus selalu waspada. Waspada dalam hal apa? Di dalam konteks ini adalah waspada di dalam mengatur siapa/apa yang boleh/tidak boleh mengakses masuk/keluar network kita. Bisa dibayangkan apa yang akan terjadi bila ada cracker yang berhasil membobol server kita. Mulai dari deface website, abuse bandwidth, sampai penghapusan data. Ini berarti kita harus selalu menjaga keamanan network dan server2 kita.

Ada banyak cara yang harus dilakukan di dalam menjaga keamanan network dan server, namun di tulisan kali ini kita akan konsentrasi membahas dari sisi firewall. Apa itu firewall? Seperti arti harafiah katanya, yaitu: 'tembok api'. Di firewall ini kita melakukan proses penyaringan trafik network apa dan bagaimana yang kita perbolehkan/larang. Di dalam konsep networking, semua service networking (seperti web, ftp, mail, dns, dll) berjalan melalui jalur2 yang kita namakan 'port'. Masing2 service tersebut memiliki jalurnya sendiri, yaitu port2 dengan nomor tersendiri, seperti service:
- web ---> port tcp 80, 445
- ftp ---> port tcp 20, 21
- mail ---> port tcp 25, 110
- dns ---> port tcp/udp 53
- Dll, lihat daftar lengkapnya di file /etc/services

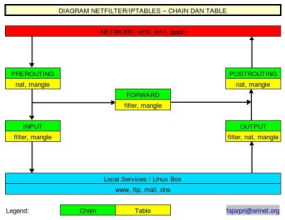
Dua pendekatan setup firewall
Di mailing list sering ada yang bertanya: "Port apa saja sih yang harus kita TUTUP?" Ini adalah pendekatan 'negative list', dimana secara DEFAULT semua port kita BUKA, baru kemudian satu per satu kita TUTUP port yang diinginkan.

Pendekatan kedua adalah: 'positive list', yaitu dimana secara DEFAULT semua port di TUTUP, dan baru kemudian satu per satu kita BUKA port yang diinginkan.

Sebenarnya bagaimana sih cara bekerja iptables sebagai firewall? Seperti dapat kita lihat di gambar 1, di tengah2 bawah adalah server Linux kita. Di atas adalah Network, baik local maupun internet. Di gambar itu juga terlihat ada 5 buah kotak berwarna hijau kuning.

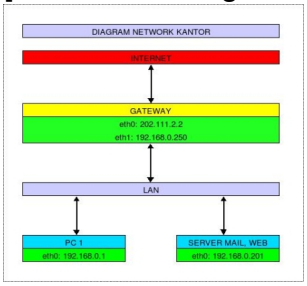
Kotak-kotak ini melambangkan titik/lokasi tempat kita bisa melakukan filtering maupun manipulasi terhadap paket network yang sedang lewat.

[Gambar 1, Diagram Netfilter]



Wah cukup rumit yah. Memang mungkin sebaiknya kita membahas contoh penggunaan iptables menggunakan cerita. Kita gunakan contoh gambar 2. Disini ceritanya kita berperan sebagai seorang admin Linux di kantor. Kantor kita berlangganan internet dedicated dan kita diminta melakukan:
1. Mengamankan gateway dari kemungkinan serangan baik dari luar maupun dalam.
2. Secara default user tidak dapat melakukan koneksi ke gateway dan internet.
3. Sharing internet.
4. Membuat transparent proxy di gateway.
5. Mengatur agar kita bisa membuat sebuah web dan mail server yang terlindungi di belakang gateway.

[Gambar 2, Diagram Network Kantor]



Demikianlah secuplik isinya. Panduan lengkap setebal **18 halaman** ini dapat di download dari menu di sebelah:
Download > Artikel > Linux Admin > Sort berdasarkan submit date > adm_iptables_praktis.pdf

Jangan lupa login/register dahulu untuk mendownload.
Selamat belajar :)