IP Tables

@danangnurfauzi

Pengertian

- Iptables adalah suatu tools dalam sistem operasi linux yang berfungsi sebagai alat untuk melakukan filter (penyaringan) terhadap (trafic) lalulintas data.
- Secara sederhana digambarkan sebagai pengatur lalulintas data.
- Dengan iptables inilah kita akan mengatur semua lalulintas dalam komputer kita, baik yang masuk ke komputer, keluar dari komputer, ataupun traffic yang sekedar melewati komputer kita.

- IPTables packet filtering memiliki tiga aturan (policy), yaitu:

Input

Output

Forward

Input

- Mengatur paket data yang memasuki firewall dari arah intranet maupun internet.
- bisa mengelola komputer mana saja yang bisa mengakses firewall.
- misal: hanya komputer IP 192.168.1.100 yang bisa SSHke firewall dan yang lain tidak boleh.

Output

- Mengatur paket data yang keluar dari firewall ke arah intranet maupun internet.
- Biasanya output tidak diset, karena bisa membatasi kemampuan firewall itu sendiri.

Forward

- Mengatur paket data yang melintasi firewall dari arah internet ke intranet maupun sebaliknya.
- Policy forward paling banyak dipakai saat ini untuk mengatur koneksi internet berdasarkan port, mac address dan alamat IP

Lanjutan ~

- Selain aturan (policy) firewall iptables juga mempunyai parameter yang disebut dengan TARGET, yaitu status yang menentukkan koneksi di iptables diizinkan lewat atau tidak.
- TARGET ada tiga macam yaitu:

Accept

Reject

Drop

Accept ~

- Akses diterima dan diizinkan melewati firewall

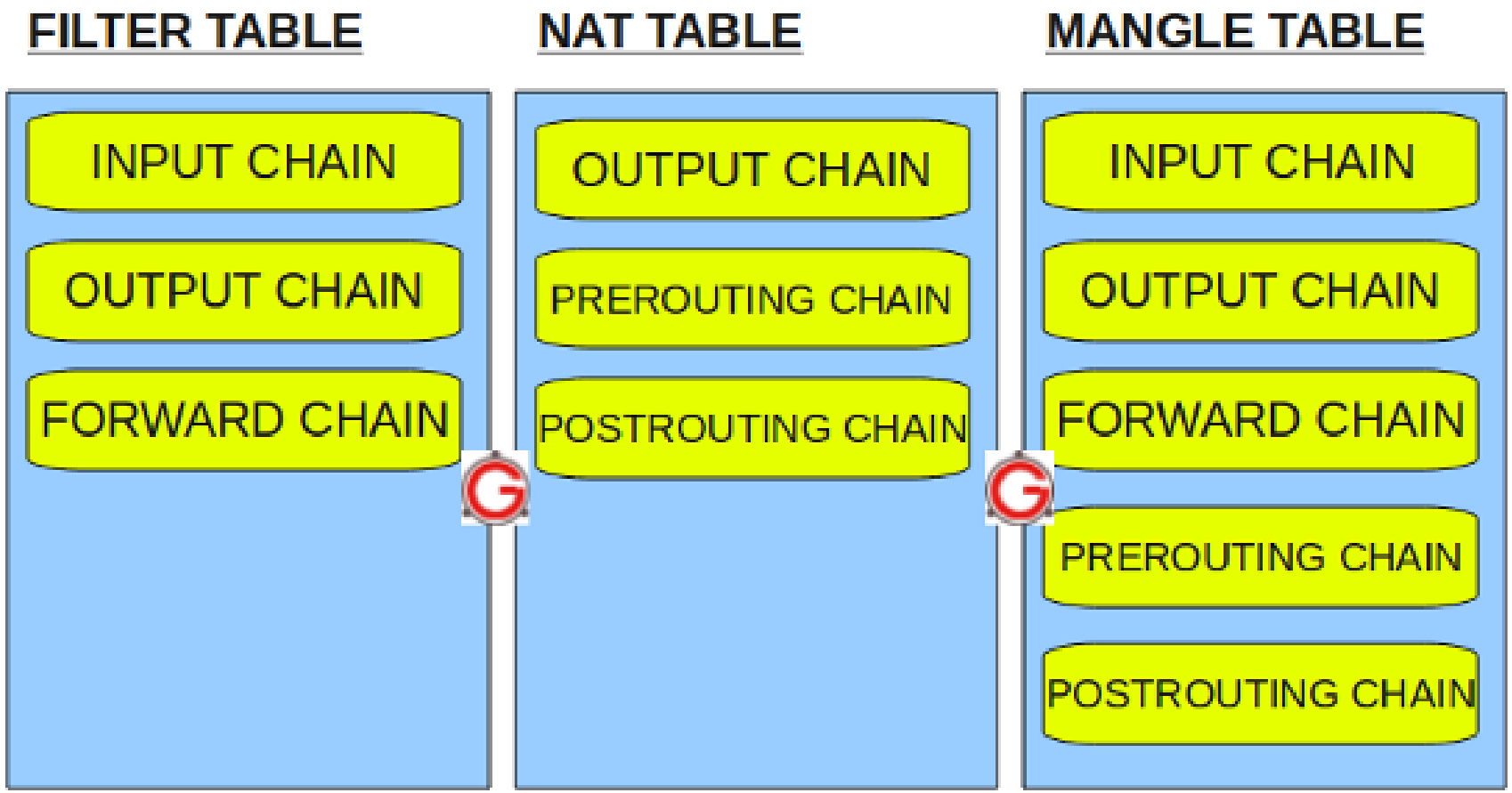
Reject ~

- Akses ditolak, koneksi dari komputer klien yang melewati firewall langsung terputus, biasanya terdapatpesan “Connection Refused”.
- Target Reject tidak menghabiskan bandwidth internet karena akses langsung ditolak

Drop ~

- Akses diterima tetapi paket data langsung dibuang oleh kernel, sehingga pengguna tidak mengetahui kalau koneksinya dibatasi oleh firewall, pengguna melihat seakan – akan server yang dihubungi mengalami permasalahan teknis.
- Pada koneksi internet yang sibuk dengan trafik tinggi Target Drop sebaiknya jangan digunakan.

IP tables and Chain



Filter Table

- tabel yang bertanggung jawab untuk pemfilteran paket. Tabel ini mempunyai 3 rantai (chain) yaitu:

1. Rantai Forward yaitu rantai yang memfilter paket-paket yang akan ke server yang dilindungi oleh firewall. Rantai ini digunakan ketika paket-paket datang dari IP Publik dan bukan dari IP lokal.
2. Rantai Input: yaitu rantai yang memfilter paket-paket yang ditujukan ke firewall.
3. Rantai Output: yaitu rantai yang memfilter paket-paket yang berasal dari firewall.

Nat Table

- yaitu rantai yang bertanggung jawab untuk melakukan Network Address Translation (NAT). NAT yaitu mengganti field asal atau alamat tujuan dari sebuah paket.
- Pada tabel ini terdapat 2 rantai, yaitu:
  1. Rantai Pre-Routing: Merubah paket-paket NAT dimana alamat tujuan dari paket-paket tersebut terjadi perubahan. Biasanya dikenal dengan destination NAT atau DNAT.
  2. Rantai Post-Routing: Merubah paket-paket NAT dimana alamat sumber dari paket-paket tersebut terjadi perubahan. Biasanya dikenal dengan source NAT atau SNAT.

Mangle Table

- tabel yang bertanggung jawab untuk melakukan penghalusan (mangle) paket seperti merubah quality of service (QOS), TTL, dan MARK di header TCP.

Perjalanan Paket yang diforward ke host yang lain

a. Paket berada pada jaringan fisik (Network) dan masuk ke interface jaringan

b. Paket masuk ke rantai PREROUTING pada tabel MANGLE dan tabel NAT

c. Paket mengalami Routing apakah akan diproses oleh host lokal atau diteruskan ke host lain

d. Paket masuk ke rantai FORWARD pada tabel MANGLE dan tabel FILTER

e. Paket masuk ke rantai POSTROUTING pada tabel MANGLE dan tabel NAT

f. Paket keluar menuju ke interface jaringan

g. Paket kembali pada jaringan fisik (Network)

Perjalanan paket yang ditujukan bagi host lokal

a. Paket berada pada jaringan fisik (Network) dan masuk ke interface jaringan

b. Paket masuk ke rantai PREROUTING pada tabel MANGLE dan tabel NAT

c. Paket mengalami Routing

d. Paket masuk ke rantai INPUT pada tabel MANGLE dan tabel FILTER untuk mengalami proses penyaringan

e. Paket akan masuk ke proses lokal (Local Process)

Perjalanan paket yang berasal dari host lokal

a. Aplikasi lokal menghasilkan paket data yang akan dikirimkan melalui jaringan

b. Paket masuk ke rantai OUTPUT pada tabel MANGLE, lalu ke tabel NAT, kemudian ke tabel FILTER

c. Paket mengalami Routing

d. Paket masuk ke rantai POSTROUTING pada tabel MANGLE dan tabel NAT

e. Paket keluar menuju ke interface jaringan

f. Paket kembali pada jaringan fisik (Network)