Linux Firewall

Mengal Firewall dan Iptables

Firewall dapat digambarkan sebagai suatu sistem yang digunakan untuk membatasi ataupun mengatur hak akses dari suatu segmen jaringan ke segmen jaringan yang lain, biasanya firewall digunkan untuk membatasi antara jaringan Wide Area Network(WAN) dan Local Area Network (LAN), firewall umumnya digunakan untuk menentukan kebijakan apa saja yang boleh di akses dari jaringan luar (WAN) kedalam (LAN) dan apa yang tidak boleh dan juga sebaliknya yang bertujuan untuk meningkatkan sistem keamanan, firewall umumnya merupakan sistem yang terdedikasi (dedicated) yang juga berfungsi sebagai pintu gerbang (gateway) jaringan internet, dalam kehidupan nyata firewall dapat digambarkan sebagai pintu masuk pada sebuah bangunan, di pintulah akan diatur siapa saja yang boleh dan siapa saja yang tidak boleh memasuki gedung tersebut.

Iptables merupkana modual kernel linux yang digunakan untuk memfilter paket-paket data, Iptables disertakan ke dalam kernel linux mulai versi 2.4 ke atas. Konfigurasi sederhana pada Iptables setidaknya menangani 3 aturan yang juga disebut *chain*, paket-paket yang masuk dinamakan chain INPUT, paket yang diteruskan oleh sistem dinamakan chain FORWARD dan paket keluar dinamakan chain OUTPUT.

Kita dapat menyalakan ataupun menghentikan service Iptables menggunakn perintah service berikut

```
/bin/sbin/service iptables start
/sservice iptables stop
```

atau kita juga dapat menggunakan init scipt

```
/etc/init.d/iptables start
/etc/inint.d/iptables stop
```

Agar service iptables berjalan secara otomatis setiap kali sistem kita dihidupkan, maka kita dapat menggunakan perintah chkconfig

```
/sbin/chkconfig iptables on
```

Muhammad Rifqi
http://masrifqi.staff.ugm.ac.id

Beberapa opsi iptables yang sering digunakan adalah sebagai berikut

-A : Menambahkan (add) aturan atau *chain*

-i : Menyisipkan (insert) turan ke baris firewall paling atas

-D : Menghapus (delete) aturan yang telah dibuat

-s : Alama sumber (source)

-d : Alamat tujuan (destination)

-j : Jump paket ke keputusan routing apabila paket yang dimaksud cocok

-L : Menampilkan rules

Pengenalan Rules IPtables

Berikut adalah contoh kasus Iptables, pada contoh pertama ini kita akan menolak semu koneksi ke sistem linux kita

```
/sbin/iptables -A INPUT -j DROP
/sbin/iptables -t filter -A INPUT -j DROP
```

Catatan :

Pada baris kedua perintah iptables diatas mempunyai arti yang sama dengan perintah iptables baris petama karena secara default iptables menyertakan *-t filter* sebagai tabel default.

Pada contoh selanjutnya kita akan membuata rules iptables untuk mengizinkan koneksi masuk ke sistem kita

```
/sbin/iptables -A INPUT -j ACCEPT
```

berikut adalah contoh rules iptables untuk menolak atau mengizinkan koneksi dari IP tertentu

```
/sbin/iptables -A INPUT -p tcp -s 192.168.1.100 -j DROP
/sbin/iptables -A INPUT -p tcp -s 192.168.1.100 -j ACCEPT
```

Pada penggunaan sehari-hari mungkin kita membutuhkan kebijakan firewall yang akan menolak koneksi dari suatu host hanya pada port-port tertentu saja, dab berikut adalah contoh iptables untuk menolak koneksi dari ip tertentu dan menuju port tertentu

```
/sbin/iptables -A INPUT -p tcp -s 192.168.1.100 --dport 80 -j DROP
```

menolak koneksi dari satu jaringan ke port tertentu

```
/sbin/iptables -A INPUT -p tcp -s 192.168.1.0/24 –dport 80 -j DROP
```

Berikut dalah contoh rules Iptbles untuk menolak koneksi menuju port icmp

/sbin/iptables -A INPUT -p icmp -j DROP

dengan menggunakan rues diatas maka semua koneksi menuju port icmp akan di tolak, dengan efeknya client kita tidak dapan melakukan ping ke mesin kita.

Pada iptables kita juga dapat membuat pengecualian, sebagai contoh apabila kita akan menolak semua koneksi masuk kecuali dari host 192.168.1.10, maka berikut adalah rules iptablesnya

```
/sbin/iptables -A INPUT ! -s 192.168.1.10 -j DROP
```

Pada iptables kita juga dimungkinkan untuk menolak koneksi dari suatu host atau network ke beberapa port sekaligus, berikut adalah contoh rules iptales untuk menolak koneksi dari suatu host menuju beberpa port tertentu

```
/sbin/iptables -A INPUT -p tcp -s 192.168.1.1 -m multiport --dport 21,80,443 -j DROP
```

Contoh lain menolak koneksi berdasarkan range port, semisal kita akan menolak semua koneksi masuk mulai dari port 1000 sampai dengan port 5000

```
/sbin/iptables -A INPUT -p tcp -m multiport --dport 1000:5000 -j DROP
```

Network Address Translation (NAT)

Network Address Translator (NAT) adalah salah satu fitur yang telah di dukung oleh iptables, adapun NTA sendiri dapat dibagi menjadi dua yaitu Source NAT (SNAT) dan Destionation NAT (DNAT) adapun penjelasanya adalah sebagai berikut:

1. Source NAT (SNAT)

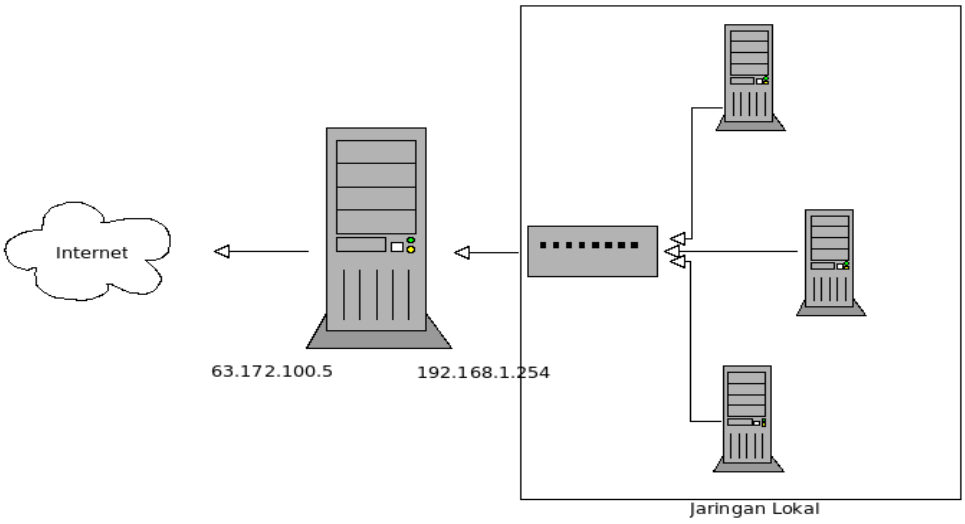
   SNAT adalah metode yang digunakan untuk menyembunyikan alamat asal paket dengan melakukan pemetaan alamat asal paket yang akan menuju jaringan eksernal ke suatu IP address

2. Destination NAT (DNAT)

DNAT merupakan merupakan kebalikan dari SNAT, jika pada SNAT alamat yang disembunyikan adalah alamat asal maka pada DNAT alamat yng disembunyikan adalah alamat tujuan, fungsi ini biasanya banyak digunakan untuk fungsi DMZ (Demilitary Zone).

- Network Address Translation (NAT) dan Masquerade

Salah satu dukungan fungsi yag telah tersedia pada IP Tables adalah IP Masquerder yng merupakan versi lain dari Network Address Translation (NAT), yaitu merupakan metode yang dapat mengizinkan beberapa host yang tidak mempunyai ip public atau tidak mempunyai blok ip dari jaringan eksternal dapat terkoneksi dengan jaringan internet. Carakerjanya adalah server masquerader atau yag sering di sebut sebagai gateway menjalankn fungsi masquerader dengan IP Tables untuk membuat host-host yang berada pada jaringan lokal terkoneksi dengan internet dan IP address yang terbaca dalah IP dari komputer gateway, berikut adalah gambaran dari fungsi masquerade



Gambar 1 (Masquerade)

Berikut adalah contoh penggunaan IP Masquerade menggunakan IP Tables

```
/sbin/iptables -A POSTROUTING -t nat -s 192.168.1.0/24 -o eth0
-j MASQUERADE
```

Baris diatas berarti server gateway akan mengizinkan jaringan lokal dengan ip 192.168.1.0/24 untuk bisa menggunkan internet yang di masquerader dengan IP gateway pada interface eth0.

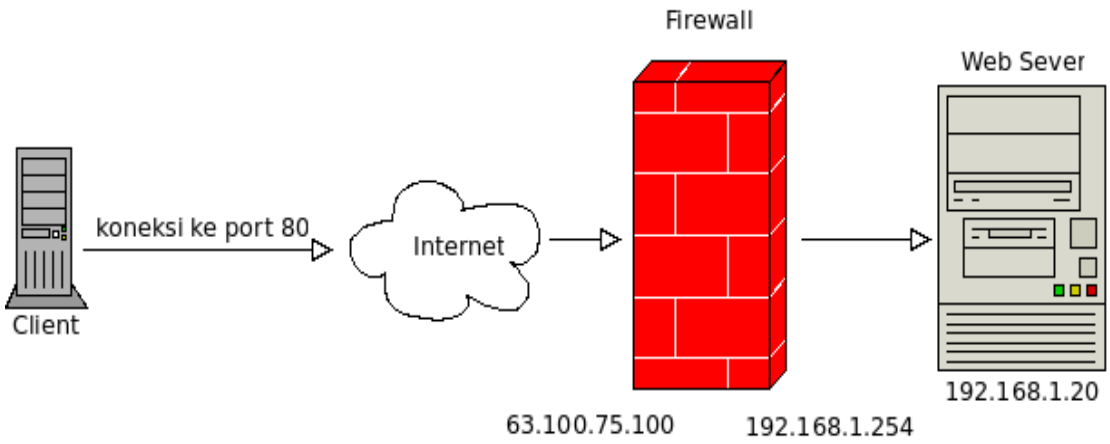
Selain menggunakan metode masquerade ip tables juga dapat menjalankan fungsi NAT dengan manggunakan fungsi SNAT, dan berikut adalah contoh penggunaan NAT menggunakan SNAT

```
/sbin/iptables -t nat -A POSTROUTING -o eth0 -s 192.168.1.0/24
-j SNAT --to-source 63.172.100.5
```

1. penggunaan fungsi di atas akan menghasilkan hasil yang sama, yaitu fungsi NAT, hanya saja ketika kita menggunakan koneksi internet Dial-up atau koneksi yang menggunakan ip dynamic maka kita tidak dapat menggunaan fungsi masquerader, maka kita dapat menggunakan metode SNAT.

- Demiliterized Zone (DMZ) menggunakan DNAT

  Seperti yang telah disinggung sebelumnya, IPTables mempunyai fitur yang sangat berguna yaitu Destination NAT (DNAT) dan fungsi DNAT ini digunakan ketika kita akan membangun jaringan Demilitarized Zone (DMZ), DMZ biasanya digunakan untuk alasan keamanan, semisal untuk mengamankan webserver, cara kerjanya adalah sebagai berikut, mesin firewall menggunakan dua antar muka jaringan (ethernet), salah satu ethernet menggunakan IP Public dan ethernet yang lain menggunakan ip privat yang terhubung dengan jaringan lokal yang berada di belakng frewall, setiap permintaan koneksi dari client menuju ke port 80 (web) pada firewall akan di teruskan ke komputer webserver yang berada pada jaringan lokal di belakang mesin firewall, DMZ dapat memberikan perlindungan kemananan lebih kepda mesin web server karena client tidak dapat mengakses langsung mesin web server tersebut, berikut dalah gambar skema jaringan DMZ



Gambar Skema DMZ

Berikut adalah contoh rules IPTables untuk fungsi Demiliterized Zone (DMZ) yang berfungsi meneruskan paket (forwarding) port 80 dari komputer client ke komputer webserver dengan tujuan port 80

```
/sbin/iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 80 -j DNAT
--to 192.168.1.20:80
```

Dengan menggunakan perintah di atas maka setiap koneksi yang menuju firewall dan port tujuan 80 (http) maka akan di teruskan (di forward) menuju host 192.168.1.20 port 80 (http)

Redirection

Redirection merupakan fungsi yang telah didukung oleh iptables, fungsi ini biasanya digunakan untuk membuat proxy server, setiap koneksi yang menuju port 80 akan di redirek ke port squid 3128 sehingga semua koneksi web akan di request dari port proxy, berikut adalah contoh redirectio untuk mebuat proxy server bisa berfungsi menjadi tranparent proxy

```
/sbin/iptables -t nat -A PREROUTING -s 192.168.1.0/24 -d 0/0 -p tcp
--dport 80 -j REDIRECT --to-ports 3128
```

degan rules di atas maka setiap koneksi dari client jringan LAN 192.168.1.0/24 akan di redirect ke port proxy port 3128, contoh lain rules redirection untuk proxy server

```
/sbin/iptables -t nat -A PREROUTING -s 192.168.1.0/24 -d 0/0 -p tcp --dport 80 -j REDIRECT --to-ports 8080
```

Blok Koneksi Berdasarkan MAC

Pada beberapa kondisi blocking koneksi dengan menggunakan IP Address kadang masih mengalami kegagalan karena komputer client dapat saja mengganti IP Address dengan mudah, dan salah satu solusi untuk kebijakan keamanan dalam menolak koneksi adalah dengan blocking menggunakan blocking *Media Access Control* (MAC) berikut adalah contoh blocking berdasarkan alamat MAC

```
/sbin/iptables -A INPUT -m mac --mac-source 00:15:F9:D0:75:2E -j DROP
```

dengan menggunakan rules Iptables di atas maka komputer dengan alamat mac tidak akan dapat terkoneksi ke mesin firewalling, contoh lain penggunaan blocking berdasarkan alamat MAC

```
/sbin/iptables -A INPUT -m mac --mac-source 00:15:E9:F0:58:2F -p tcp --dport 80 -j DROP
```

atau kita juga bisa menggabungkan antara blocking berdsarkan IP Address dan juga almat MAC, berikut adalah contoh rulsenya

```
/sbin/iptables -A INPUT -s 192.168.1.10 -m mac –mac-source 00:15:E9:F0:58:2F -p tcp –dport 80 -j DROP
```

Connection Limit

Dengan menegunakan Iptables kita juga dapat memberi batasan jumlah koneksi pada suatu port, misalkan kita membatasi jumlah koneksi maksimal yang boleh tersambung dengan port ssh (22) kita batasi hanya 2 kkoneksi, jika jumlah koneksi sudah mencapai nilai yag telah kita tentukan sebelumnya maka koneksi akan kita tolak (reject), dan berikut adalah rules iptablenya

```
/sbin/iptables -A INPUT -p tcp --syn --dport 22 -m connlimit --connlimit-above 2 -j REJECT
```

berikut dalah contoh lain dari penggunaan opsi connection limit, pada contoh berikut kita kna embatasi koneksi secara simultan maksimal yang di izinkan kepada client IP kelas C (netmsk 24)

```
/sbin/iptables -A INPUT -p tcp --syn --dport 80 -m connlimit --connlimit-above 16 --connlimit-mask 24 -j REJECT
```

Berikut dlah contoh rules lengkap iptables

```
#!/bin/bash
# default input policy DROP, default out policy ACCEPT
/sbin/iptables -P INPUT DROP
/sbin/iptables -P OUTPUT ACCEPT
# ijinkan koneksi ke port ssh
/sbin/iptables -A INPUT -p tcp --dport 22 -j ACCEPT
# ijinkan koneksi ke port 53 (named)
/sbin/iptables -A INPUT -p tcp --dport 53 -j ACCEPT
# ijinkan koneksi ke port 80 dan 443
/sbin/iptables -A INPUT -p tcp -m multiport --dport 80,443 -j ACCEPT
# ijinkan koneksi ping
/sbin/iptables -A INPUT -p icmp -j ACCEPT
```