



PT. Ardelindo 1991, Linux Training & Support Center, Jl. Margonda Raya No. 535 E Depok 16423. Telp. 021-7761121, 021-7774333, 021-78849561 . Fax : 021-7763366.
Email : aples.edu@ardelindo.com, hasan@ardelindo.com

Tutorial

Mastering Iptables Seri 1 dan Seri 2

PT. Ardelindo 1991 menuliskan tutorial-tutorial singkat dan praktis yang dapat digunakan sebagai bahan referensi guna implementasi linux di perusahaan maupun personal.

Artikel lainnya silahkan kunjungi website <http://www.ardelindo.com>

Dokumen ini disusun dengan praktis langsung mengarah pada point masalah. Silahkan mempergunakan dokumen ini dengan semestinya dengan tetap menuliskan penulis aslinya

Oleh :

Ardelindo Team : (Budi Santoso, Hasan)
Date : Januari 2008

email : aples.edu@ardelindo.com, info@ardelindo.com

Mastering IPTables Seri 1

Anda pasti pernah mendengar yang disebut dengan firewall pada jaringan komputer, klo kita jadikan bahasa indonesia berarti tembok api. Aneh dan Lucu, tetapi punya fungsi yang penting untuk melindungi jaringan intranet dari serangan hacker maupun akses ilegal.

Selain meningkatkan keamanan firewall berguna untuk mengatur akses internet yang boleh dipakai pengguna, misalkan pak Joko bisa pakai yahoo messenger dan pak Ali ngga bisa pakai Yahoo Messenger. Nah untuk mengatur akses tadi kita memakai aplikasi firewall linux yaitu iptables.

Firewall adalah perangkat komputer yang kita fungsikan sebagai router untuk memisahkan jaringan intranet dan internet. Firewall memiliki dua kartu jaringan, eth0 berhubungan langsung dengan internet dan eth1 tersambung dengan jaringan LAN / Intranet

Pada Mastering Firewall IPTables Seri - 1 ini kita membahas prinsip dasar firewall iptables, mengelola akses internet berdasarkan alamat IP, port aplikasi dan MAC address. Firewall IPTables packet filtering memiliki tiga aturan (policy), yaitu:

INPUT

Mengatur paket data yang memasuki firewall dari arah intranet maupun internet. kita bisa mengelola komputer mana saja yang bisa mengakses firewall. misal: hanya komputer IP 192.168.1.100 yang bisa SSH ke 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 Selain aturan (policy) firewall iptables juga mempunyai parameter yang disebut dengan TARGET, yaitu status yang menentukan koneksi di iptables diizinkan lewat atau tidak. TARGET ada tiga macam yaitu:

ACCEPT

Akses diterima dan diizinkan melewati firewall

REJECT

Akses ditolak, koneksi dari komputer klien yang melewati firewall langsung terputus, biasanya terdapat pesan "Connection Refused". Target Reject tidak menghabiskan bandwidth internet karena akses langsung ditolak, hal ini berbeda dengan DROP.

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.



Berikut ini contoh penggunaan firewall iptables untuk mengelolak akses internet.

Policy INPUT

IP Firewall = 192.168.1.1
IP Administrator = 192.168.1.100
IP Umum = 192.168.1.200

1. Membatasi port number

```
iptables -A INPUT -i eth1 -s 192.168.1.200 -d 192.168.1.1 -p tcp -dport 22-j REJECT
```

Contoh di atas melarang komputer klien dengan IP 192.168.1.200 mengakses port 22 (ssh) firewall yang memiliki IP 192.168.1.1

Policy FORWARD

1. Membatasi orang mengakses port aplikasi P2P (Limewire, GnuTella & Bearshare)

```
iptables -A FORWARD -p tcp -dport 6340:6350 -j REJECT  
iptables -A FORWARD -p -dport 6340:6350 -j REJECT
```

-p tcp (koneksi menggunakan protokol TCP)
-p udp (koneksi menggunakan protokol UDP)
-dport 6340:6350 (melarang akses port 6340 sampai dengan 6350)

2. Membatasi koneksi satu alamat IP

```
iptables -A FORWARD -s 192.168.1.99 -d 0/0 -j REJECT
```

-d 0/0 berarti ke semua tujuan

3. Membatasi koneksi berdasarkan range IP

```
iptables -A FORWARD -m iprange -src-range 192.168.1.100-192.168.1.150 -d 0/0 -j REJECT
```

4. Membatasi koneksi internet berdasarkan MAC Address

```
iptables -A FORWARD -m mac -mac-source 00:30:18:AC:14:41 -d 0/0 -j REJECT
```

Mastering Firewall IPTables Seri - 2

Network Address Translation

Pada bagian ini kita membahas mengenai Network Address Translation, biasa disebut dengan NAT. Fungsi utama dari NAT adalah untuk melakukan translasi alamat dari satu alamat ke alamat IP yang lain, biasanya dipakai pada internet gateway. Selain melakukan translasi alamat IP, iptables juga bisa melakukan NAT alamat Port aplikasi, bisa disebut juga dengan Port Address Translation (PAT). PAT digunakan untuk membangun beberapa server seperti mail, web, database maupun datacenter yang diakses melalui internet hanya dengan satu alamat IP publik.

Tabel NAT

Selain sebagai IP Filtering / Firewall, iptables juga bisa difungsikan untuk translasi alamat, ditandai dengan opsi `-t nat` pada perintah iptables.

```
iptables -t nat ..
```

prinsip dasar NAT di bagi menjadi dua bagian, yang pertama adalah POSTROUTING, yaitu melakukan NAT paket data yang keluar dari firewall, kebanyakan postrouting dipakai untuk translasi alamat IP. Yang kedua adalah PREROUTING, untuk melakukan NAT paket data yang memasuki firewall, kebanyakan digunakan untuk transparency proxy server dan membangun beberapa server dengan satu IP publik.

POSTROUTING

Translasi alamat yang keluar dari firewall, berarti kita melihat paket data yang keluar dari kartu LAN.

```
iptables -t NAT -A POSTROUTING -o eth0 -s 192.168.1.0/24 -d 0/0 -j SNAT -to 202.154.6.55  
iptables -t NAT -A POSTROUTING -o eth0 -s 192.168.1.0/24 -d 0/0 -j MASQUERADE
```

contoh diatas berarti jaringan subnet 192.168.1.0/24 jika menghubungi web server yang berada di internet dikenali dari IP 202.154.6.55. Target MASQUERADE berarti IP NAT disesuaikan dengan alamat IP kartu LAN eth0, jika IP eth0 dirubah kita tidak perlu merubah settingan iptables.

PREROUTING

Translasi alamat yang memasuki kartu jaringan, kita juga bisa membelokkan paket data ke port tertentu untuk membangun server internet hanya dengan satu IP publik.

```
iptables -t nat -A PREROUTING - eth0 -p tcp -dport 25 -j DNAT -to 192.168.1.20:25  
iptables -t nat -A PREROUTING - eth0 -p tcp -dport 110 -j DNAT -to 192.168.1.20:110  
iptables -t nat -A PREROUTING - eth0 -p tcp -dport 80 -j DNAT -to 192.168.1.30:80
```

Pada contoh diatas kita mempunyai 2 server, 192.168.1.20 (mail server) dan 192.168.1.30 (web server). Koneksi dari internet ke port 25 dan 110 secara otomatis diarahkan ke alamat IP 192.168.1.20 (IP Lokal / LAN). Akses port 80 (web server) diarahkan ke IP lokal 192.168.1.30

List NAT

Untuk melihat NAT yang baru saja kita setting menggunakan perintah:

```
iptables -t nat -L -v  
[root@gw ~]# iptables -t nat -L -v  
Chain PREROUTING (policy ACCEPT 1833K packets, 141M bytes)  
pkts bytes target prot opt in out source destination  
199K 9636K REDIRECT tcp - eth2 any anywhere anywhere tcp dpt:http redir ports 3128
```



```
0 0 REDIRECT      tcp - eth1 any anywhere anywhere tcp dpt:36 redir ports 10000
0 0 REDIRECT      tcp - eth1 any anywhere anywhere tcp dpt:time redir ports 20000
0 0 DNAT          tcp - eth1 any anywhere anywhere tcp dpt:33 to:192.168.1.100:22
```

Menghapus NAT

```
iptables -t nat -F
iptables -t nat -Z
```