


Firewall



Konsep Firewall

- salah satu lapisan pertahanan yang mengatur hubungan komputer dengan dunia luar melalui interogasi setiap traffic, packet, dan port-port yang diatur dengan rule-rule yang ada
- Dilakukan dengan cara :
 - Menyaring
 - membatasi
 - menolak

hubungan /kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya

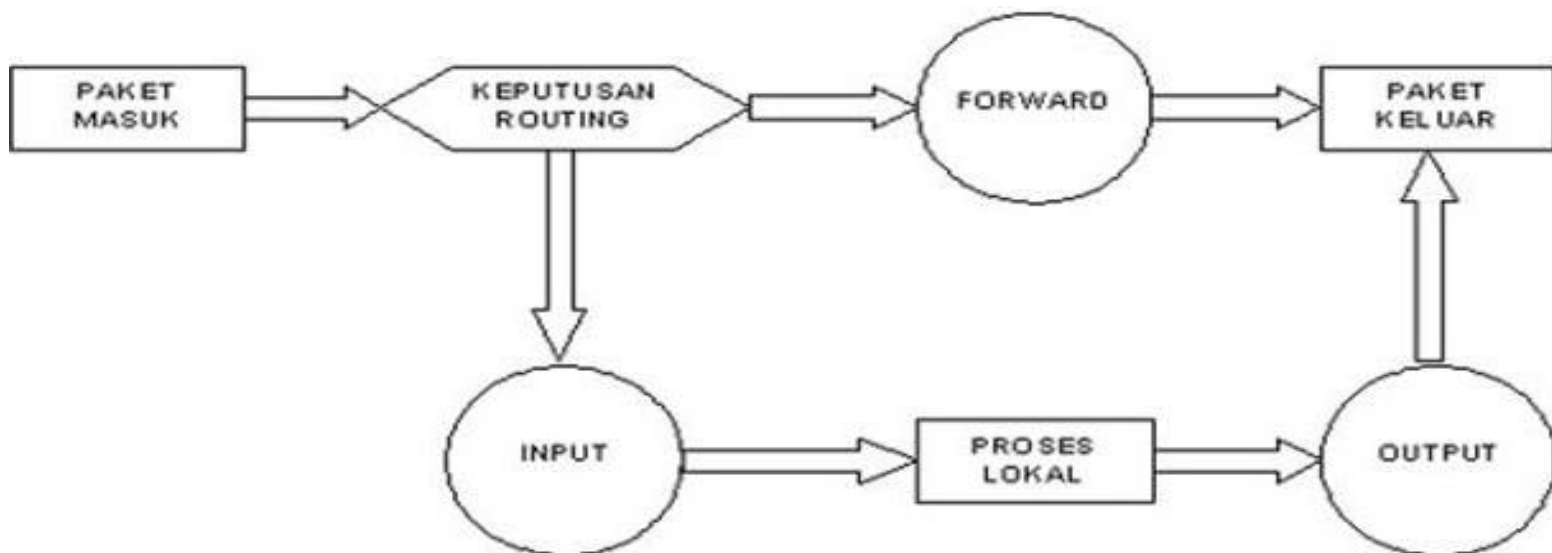
Tipe Firewall

Berdasarkan mekanisme cara kerja :

- Packet Filtering
 - ☞ Memfilter paket berdasarkan sumber, tujuan dan atribut paket (filter berdasar IP dan Port)
- Application Level
 - ☞ Biasa disebut proxy firewall, filter bisa berdasarkan content paket
- Circuit Level Gateway
 - ☞ Filter berdasarkan sesi komunikasi, dengan pengawasan sesi handshake.
 - ☞ Terdapat sesi NEW/ESTABLISH
- Statefull Multilayer Inspection Firewall
 - ☞ Kombinasi dari ketiga tipe firewall diatas

Prinsip Kerja iptables

- Paket masuk diproses berdasarkan tujuan :
 - ☞ Destination IP untuk Firewall → masuk proses input
 - ☞ Destination IP bukan untuk firewall tapi diteruskan → masuk proses FORWARD
- Selanjutnya dicocokkan berdasarkan tabel policy yang dimiliki firewall apakah di-accept atau di-drop



Sintaks IPTABLES

- Opsi
 1. -A, menambah satu aturan baru ditempatkan pada posisi terakhir
`iptables -A INPUT ...`
 1. -D, menghapus rule
`iptables -D INPUT 1`
`iptables -D -s 202.154.178.2 ...`
 2. -I, menambah aturan baru penempatan bisa disisipkan sesuai nomor
`iptables -I INPUT 3 -s 202.154.178.2 -j ACCEPT`
 3. -R, mengganti rule
`iptables -R INPUT 2 -s -s 202.154.178.2 -j ACCEPT`
 4. -F, menghapus seluruh rule
`iptables -F`
 5. -L, melihat Rule
`iptables -L`

Parameter

- -p [!] protocol, protokol yang akan dicek
Iptables -A INPUT -p tcp ...
- -s [!] address/[mask], memeriksa kecocokan sumber paket
Iptables -A INPUT -s 10.252.44.145 ...
- -d [!] address/[mask], memeriksa kecocokan tujuan paket
Iptables -A INPUT -d 202.154.178.2 ...
- -j target, menentukan nasib paket, target misal ACCEPT/DROP/REJECT
Iptables -A INPUT -d 202.154.178 -j DROP
- -i [!] interface_name, identifikasi kartu jaringan tempat masuknya data
Iptables -A INPUT -i etho
- -o [!] interface_name, identifikasi kartu jaringan tempat keluarnya paket
Iptables -A OUTPUT -o eth1

Match iptables

- --mac address, matching paket berdasarkan nomor MAC Address

`Iptables -m mac --mac-address 44:45:53:54:00:FF`

- Multiport, mendefinisikan banyak port

`Iptables -m multiport --source-port 22,25,110,80 -j ACCEPT`

- State, mendefinisikan state dari koneksi

`Iptables -A INPUT -m state --state NEW, ESTABLISH -j ACCEPT`

Target/Jump iptables

- ACCEPT, setiap paket langsung diterima
`Iptables -A INPUT -p tcp -dport 80 -j ACCEPT`
- DROP, paket datang langsung dibuang
`Iptables -A INPUT -p tcp -dport 21 -j DROP`
- REJECT, paket yang ditolak akan dikirim pesan ICMP error
`Iptables -A INPUT -p tcp -dport 21 -j REJECT`
- SNAT, sumber paket dirubah, biasanya yang memiliki koneksi internet
`Iptables -t nat -A POSTROUTING -p tcp -o eth0 -j SNAT --to-source 202.154.178.2`
- DNAT, merubah tujuan alamat paket. Biasanya jika server alamat Ipnya lokal, supaya internet bisa tetap akses diubah ke publik
`Iptables -t nat -A PREROUTING -p tcp -d 202.154.178.2 -dport 80 -j DNAT --to-destination 192.168.1.1`
- MASQUERADE, untuk berbagi koneksi internet dimana no_ipnya terbatas, sebagai mapping ip lokal ke publik
`Iptables -t nat -A POSTROUTING -o eth0 -dport 80 -j MASQUERADE`
- REDIRECT, digunakan untuk transparent proxy
`Iptables -t nat -A PREROUTING -p tcp -d 0/0 -dport 80 -j REDIRECT --to-port 8080`
- LOG, melakukan pencatatan terhadap aktifitas firewall kita, untuk melihat bisa dibuka `/etc/syslog.conf`
`Iptables -A FORWARD -j LOG --log-level-debug`
`Iptables -A FORWARD -j LOG --log-tcp-options`

Firewall Option

- # Mengeluarkan Modul-modul Iptables
- /sbin/modprobe ip_tables
- /sbin/modprobe ip_conntrack
- /sbin/modprobe iptable_filter
- /sbin/modprobe iptable_mangle
- /sbin/modprobe iptable_nat
- /sbin/modprobe ipt_LOG
- /sbin/modprobe ipt_limit
- /sbin/modprobe ipt_state
- /sbin/modprobe ip_conntrack_ftp
- /sbin/modprobe ip_conntrack_irc
- /sbin/modprobe ip_nat_ftp
- /sbin/modprobe ip_nat_irc

Menghapus Rule iptables

- # Menghapus aturan iptables
- \$IPTABLES -F
- \$IPTABLES -t nat -F
- \$IPTABLES -t mangle -F
- # Menghapus nama kolom yg dibuat manual
- \$IPTABLES -X
- \$IPTABLES -t nat -X
- \$IPTABLES -t mangle -X

Packet Filtering Firewall

Modul 5 DoS Rev.doc - Microsoft Word

File Edit View Insert Format Tools Table Window Help Adobe PDF Acrobat

isbat@www: ~/public_html/security

```

--- 10.252.44.178 ping statistics ---
94 packets transmitted, 0 received, 100% packet loss, time 9301ms
www:/home/isbat/public_html/security# ping 10.252.44.178
PING 10.252.44.178 (10.252.44.178) 56(84) bytes of data.
64 bytes from 10.252.44.178: icmp_seq=1 ttl=64 time=0.295 ms
64 bytes from 10.252.44.178: icmp_seq=2 ttl=64 time=0.264 ms
64 bytes from 10.252.44.178: icmp_seq=3 ttl=64 time=0.381 ms
^C
--- 10.252.44.178 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.264/0.313/0.381/0.051 ms
www:/home/isbat/public_html/security# ping 10.252.44.178
PING 10.252.44.178 (10.252.44.178) 56(84) bytes of data.

```

isbat@latihan: ~

```

target    prot opt source      destination
DROP      0    -- localnet/24      anywhere

Chain FORWARD (policy ACCEPT)
target    prot opt source      destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source      destination
latihan:/home/isbat# /sbin/iptables -A INPUT -p icmp -s 10.252.44.145 -j DROP
latihan:/home/isbat# iptables -F
latihan:/home/isbat# /sbin/iptables -A INPUT -p icmp -s 10.252.44.145 -j DROP
latihan:/home/isbat#

```

isbat@latihan: ~

```

17:39:04.807486 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 58686, seq 93, length 64
17:39:05.807553 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 58686, seq 94, length 64
17:39:17.138940 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 59710, seq 1, length 64
17:39:18.138007 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 59710, seq 2, length 64
17:39:19.137200 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 59710, seq 3, length 64
17:39:22.138900 arp reply ftp.pens.edu is-at 00:00:e2:9a:c3:0e (oui Unknown)
17:39:27.570566 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 1, length 64
17:39:28.585373 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 2, length 64
17:39:29.585440 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 3, length 64
17:39:30.585507 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 4, length 64
17:39:31.585573 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 5, length 64
17:39:32.585641 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 6, length 64
17:39:33.585708 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 7, length 64
17:39:34.585775 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 8, length 64
17:39:35.585842 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 9, length 64
17:39:36.585909 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 10, length 64
17:39:37.585976 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 11, length 64
17:39:38.586044 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 12, length 64
17:39:39.586235 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 13, length 64
17:39:40.586302 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 14, length 64
17:39:41.586369 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 15, length 64
17:39:42.586436 IP ftp.pens.edu > latihan.eepis-its.edu: ICMP echo request, id 4159, seq 16, length 64

```

Page 10 Sec 1 10/12 At 9.7" Ln 15 Col 1 REC TRK EXT OVR English (U.S.)

4:42 PM 5/13/2010

Packet Filtering Firewall

```
isbat@latihan: ~  
latihan:/home/isbat# iptables -F  
latihan:/home/isbat# iptables -A INPUT -i eth0 -p tcp -s 10.252.44.145 --dport 21 -j DROP  
latihan:/home/isbat# iptables -L  
Chain INPUT (policy ACCEPT)  
target      prot opt source                destination          tcp dpt:ftp  
DROP        tcp  --  ftp.pens.edu           anywhere             tcp dpt:ftp  
  
Chain FORWARD (policy ACCEPT)  
target      prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source                destination  
latihan:/home/isbat#
```

```
isbat@www: ~/public_html/security  
^C  
ftp> byw  
?Invalid command  
ftp> byw  
?Invalid command  
ftp> bye  
221 Goodbye.  
You have new mail in /var/mail/root  
www:/home/isbat/public_html/security# ftp 10.252.44.178
```

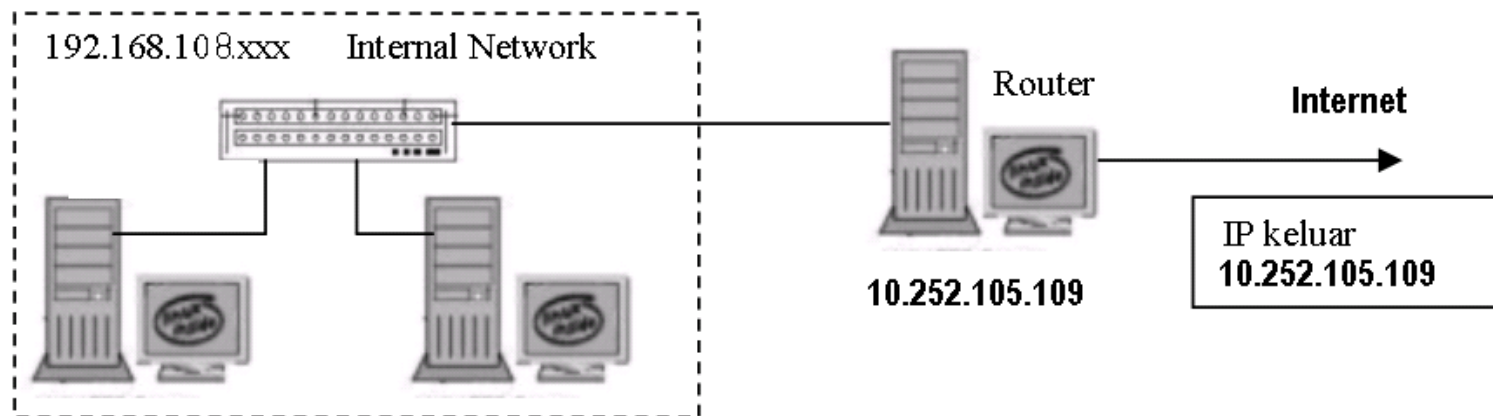
Circuit Level Gateway

```
isbat@latihan: ~  
latihan:/home/isbat# iptables -A INPUT -s 10.252.102.230 -j ACCEPT  
latihan:/home/isbat# iptables -A INPUT -i eth0 -s 0/0 -m state --state ESTABLISH  
-j ACCEPT  
latihan:/home/isbat# iptables -A INPUT -i eth0 -s 10.252.44.145 -m state --state  
NEW -j DROP  
latihan:/home/isbat# iptables -L  
Chain INPUT (policy ACCEPT)  
target      prot opt source                destination  
ACCEPT      0    -- Laptopku.eepis-its.edu anywhere  
ACCEPT      0    -- anywhere              anywhere        state ESTABLISHED  
DROP        0    -- ftp.pens.edu           anywhere        state NEW  
  
Chain FORWARD (policy ACCEPT)  
target      prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source                destination  
latihan:/home/isbat#
```

```
isbat@www: ~/public_html/security  
www:/home/isbat/public_html/security# ftp 10.252.44.178  
  
isbat@www: ~/public_html/security  
www:/home/isbat/public_html/security# ftp 10.252.44.178  
^CYou have new mail in /var/mail/root  
www:/home/isbat/public_html/security# ping 10.252.44.178  
PING 10.252.44.178 (10.252.44.178) 56(84) bytes of data.
```

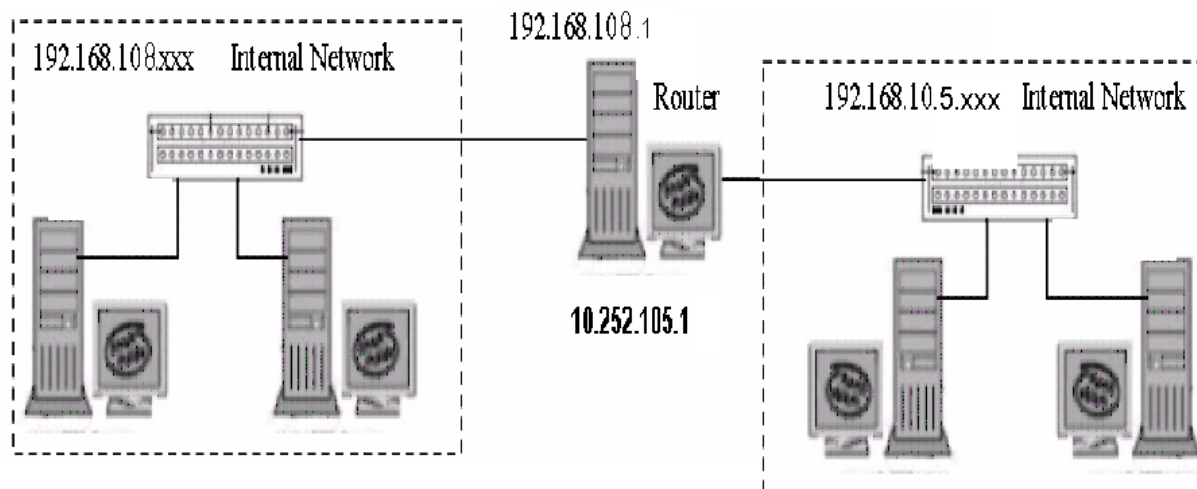
Forward

- `iptables -t nat -A POSTROUTING -s IP_number -d 0/0 -j MASQUERADE`
- `#iptables -A FORWARD -i eth0 -o eth1 -p icmp -s 192.168.108.5 -d 10.252.105.109 -j ACCEPT`
- `#iptables -A FORWARD -i eth1 -o eth0 -p icmp -s 10.252.105.109 -d 192.168.108.5 -j ACCEPT`
- `#iptables -A FORWARD -s 192.168.108.5/24 -d 0/0 -p tcp --dport ftp, -j REJECT`



Studi Kasus 1

- Bangun Jaringan sendiri
- Install web server, FTP Server, dan Telnet pada jaringan 192.168.105.xxx
- Buat jaringan 192.168.108.xxx ada yang bisa akses web, ftp dan telnet dan ada yang tidak
- Buat jaringan 192.168.105.xxx tidak boleh melakukan perintah ping ke 192.168.108.xxx



Studi Kasus 2

