MODUL 3
KONFIGURASI FIREWALL [IPTABLES]

TUJUAN PEMBELAJARAN:

1. Mengenalkan pada mahasiswa tentang konsep dasar firewall
2. Mahasiswa mampu melakukan proses filtering menggunakan iptables

DASAR TEORI

Firewall adalah sistem atau sekelompok sistem yang menetapkan kebijakan kendali akses antara dua jaringan. Secara prinsip, firewall dapat dianggap sebagai sepasang mekanisme : yang pertama memblok lalu lintas, yang kedua mengijinkan lalu lintas jaringan. Firewall dapat digunakan untuk melindungi jaringan anda dari serangan jaringan oleh pihak luar, namun firewall tidak dapat melindungi dari serangan yang tidak melalui firewall dan serangan dari seseorang yang berada di dalam jaringan anda, serta firewall tidak dapat melindungi anda dari program-program aplikasi yang ditulis dengan buruk.
Secara umum, firewall biasanya menjalankan fungsi:

- Analisa dan filter paket
  Data yang dikomunikasikan lewat protokol di internet, dibagi atas paket-paket. Firewall dapat menganalisa paket ini, kemudian memperlakukannya sesuai kondisi tertentu. Misal, jika ada paket a maka akan dilakukan b. Untuk filter paket, dapat dilakukan di Linux tanpa program tambahan.
- Bloking isi dan protokol
  Firewall dapat melakukan bloking terhadap isi paket, misalnya berisi applet Jave, ActiveX, VBScript, Cookie.
- Autentikasi koneksi dan enkripsi
  Firewall umumnya memiliki kemampuan untuk menjalankan enkripsi dalam autentikasi identitas user, integritas dari satu session, dan melapisi transfer data dari intipan pihak lain. Enkripsi yang dimaksud termasuk DES, Triple DES, SSL, IPSEC, SHA, MD5, BlowFish, IDEA dan sebagainya.

Secara konseptual, terdapat dua macam firewall yaitu :

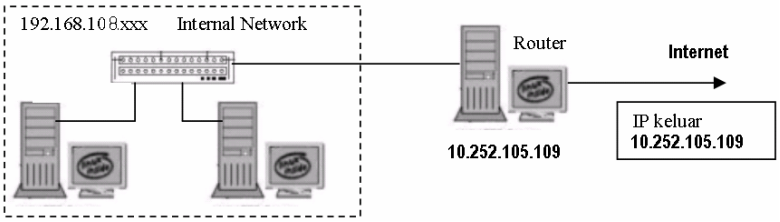
- Network level
  Firewall network level mendasarkan keputusan mereka pada alamat sumber, alamat tujuan dan port yang terdapat dalam setiap paket IP. Network level firewall sangat cepat dan sangat transparan bagi pemakai. Application level firewall biasanya adalah host yang berjalan sebagai proxy server, yang tidak mengijinkan lalu lintas antar jaringan, dan melakukan logging dan auditing lalu lintas yang melaluinya
- Application level.
  Application level firewall menyediakan laporan audit yang lebih rinci dan cenderung lebih memaksakan model keamanan yang lebih konservatif daripada network level

firewall. Firewall ini bisa dikatakan sebagai jembatan. Application-Proxy Firewall biasanya berupa program khusus, misal squid

PERCOBAAN

Percobaan 1

1. Bangun desain jaringan sebagai berikut :



2. Setting komputer sebagai router (PC1) sbb :
   - Setting Ip_forward
     - #echo 1> /proc/sys/net/ipv4/ip_forward
   - Setting IP
     - Eth0 → 192.168.105.109 Bcast:192.168.105.255 Mask:255.255.255.0
     - Eth0:1 → 192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
   - Setting Routing
     - # route add default gw 192.168.105.1

3. Setting komputer client sbb :
   - PC2
     - Setting IP
       - inet addr:192.168.108.10 Bcast:192.168.108.255 Mask:255.255.255.0
   - PC3
     - Setting IP
       - inet addr:192.168.108.5 Bcast:192.168.108.255 Mask:255.255.255.0
   - PC4
     - Setting IP
       - inet addr:192.168.108.20 Bcast:192.168.108.255 Mask:255.255.255.0
   - Setting Gateway untuk PC2, PC3 & PC4
     - route add default gw 192.168.1.1

4. Lakukan test konektifitas
   - Router PC 1
     - ping 192.168.108.10, ping 192.168.108.5, ping 192.168.108.20, ping 192.168.105.1, ping 202.154.187.4
   - PC 2

    - ping 192.168.105.109, ping 192.168.108.5, ping 192.168.108.20, ping 192.168.105.1, ping 202.154.187.4
- PC 3
    - ping 192.168.105.109, ping 192.168.108.10, ping 192.168.108.20, ping 192.168.105.1, ping 202.154.187.4
- PC 4
    - ping 192.168.105.109, ping 192.168.108.10, ping 192.168.108.5, ping 192.168.105.1, ping 202.154.187.4

5. Jalankan rule firewall sebagai berikut :

Blocking

```
[root@localhost /]# iptables -A FORWARD -s 192.168.108.200/24 -d
10.252.105.109/24  -j REJECT
[root@localhost /]# iptables -A FORWARD  -s 192.168.108.200/24 -d
10.252.105.109 -j DROP
```

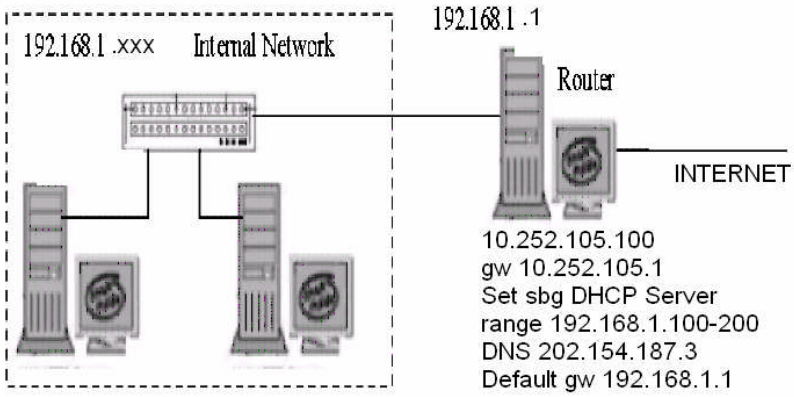
Menghapus rule

```
[root@localhost /]# iptables -D FORWARD  -s 192.168.108.200/24 -d
10.252.105.109 -j DROP
```

Block ping

```
[root@localhost /]# iptables -A FORWARD  -p icmp -s 192.168.108.200/24 -d
10.252.105.109 -j DROP
```

2. Percobaan NAT



Pada komputer router Masuk ke CD #2 Redhat

Pada komputer router Install DHCP Server

```
[root@localhost RPMS]# rpm -ivh dhcp-3.0pl1-23.i386.rpm
warning: dhcp-3.0pl1-23.i386.rpm: V3 DSA signature: NOKEY, key ID db42a60e
Preparing...                ########################################### [100%]
   1:dhcp                   ########################################### [100%]
[root@localhost RPMS]# rpm -ivh dhcp-devel-3.0pl1-23.i386.rpm
```

```
warning: dhcp-devel-3.0pl1-23.i386.rpm: V3 DSA signature: NOKEY, key ID
db42a60ePreparing...                ########################################### [100%]
   1:dhcp-devel              ########################################### [100%]
```

Pada komputer router Konfigurasi dhcp server pada file /etc/dhcpd.conf

Khusus baris dibawah ganti sbb :

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.100 192.168.1.200;
  option domain-name-servers 202.154.187.3;
  option domain-name "eepis-its.edu ";
  option routers 192.168.1.1;
  option broadcast-address 192.168.1.255;
  default-lease-time 600;
  max-lease-time 7200;
}
```

Pada komputer router Jalankan DHCP Server

```
[root@localhost /]# /etc/init.d/dhcpd restart
Shutting down dhcpd:                                [FAILED]
Starting dhcpd:                                  [  OK  ]
```

Selanjutnya hidupkan komputer client pastikan menggunakan sistem DHCP

Pada komputer router buka terminal lain dan jalankan perintah untuk melihat hasil restart DHCP kita

```
[root@localhost /]# tail /var/log/message

Oct 10 07:24:50 localhost dhcpd: dhcpd startup succeeded
```

Jika ada yang meminta IP hasilnya seperti di bawah :

```
Oct 10 07:27:10 localhost dhcpd: DHCPDISCOVER from 00:00:e2:59:8f:d1 via eth1
Oct 10 07:27:11 localhost dhcpd: DHCPOFFER on 192.168.1.200 to 00:00:e2:59:8f:d1
(rpl) via eth1
Oct 10 07:27:11 localhost dhcpd: DHCPREQUEST for 192.168.1.200 (192.168.1.1)
from 00:00:e2:59:8f:d1 (rpl) via eth1
Oct 10 07:27:11 localhost dhcpd: DHCPACK on 192.168.1.200 to 00:00:e2:59:8f:d1
(rpl) via eth1
```

Supaya komputer client bisa routing keluar, maka set server Router kita sbb

Set ip forward menjadi 1

```
[root@localhost /]# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Cek hasil setelah di set 1

```
[root@localhost /]# cat /proc/sys/net/ipv4/ip_forward
1
```

Ketikkan perintah iptables untuk routing

```
[root@localhost /]# iptables -F
[root@localhost /]# iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -d 0/0 -j
MASQUERADE
```

Jalan command berikut pada komputer router

Blocking telnet

Cek Telnet terlebih dahulu

```
[root@localhost /]# telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Red Hat Linux release 9 (Shrike)
Kernel 2.4.20-8 on an i686
login: admin
Password:
Last login: Tue Oct  3 10:12:59 from gis16.eepis-its.edu
You have new mail.
[admin@localhost admin]$
```

Blocking

```
[root@localhost /]# iptables -A FORWARD -s 192.168.1.200/24 -d 10.252.102.22/24 -
i eth1 -j REJECT
[root@localhost /]# iptables -A FORWARD  -s 192.168.1.200/24 -d 202.154.187.3 -i
eth1 -j DROP
```

Menghapus rule

```
[root@localhost /]# iptables -D FORWARD  -s 192.168.1.200/24 -d 202.154.187.3 -i
eth1 -j DROP
```

Block ping

```
[root@localhost /]# iptables -A FORWARD  -p icmp -s 192.168.1.200/24 -d
202.154.187.3 -i eth1 -j DROP
```

Block Web

```
[root@localhost /]# iptables -A FORWARD -p tcp --dport 80 -s 192.168.1.200/24 -i
eth1 -j REJECT
```

Atau jika ada proxynya pada port 3128

```
[root@localhost /]# iptables -A FORWARD -p tcp --dport 3128 -s 192.168.1.200/24 -i
eth1 -j REJECT
```

Praktikum 3 :

a. Jalankan nmap dengan synflood,
b. Pada router jalankan perintah ini dan analisa hasilnya :

Syn-flood protection:

```
# iptables -A FORWARD -p tcp --syn -m limit --limit 1/s
-j ACCEPT
```

```
or
# iptables –N SYN-FLOOD
# iptables –A SYN-FLOOD –m limit ––limit 20/s ––limit-
burst 100 –j RETURN
# iptables –A SYN-FLOOD –j LOG ––log-prefix “SYN-FLOOD:
”
# iptables –A INPUT –p tcp ––syn –j SYN-FLOOD
```

port scanner:

```
# iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST
RST -m limit --limit 1/s -j ACCEPT
```

Ping of death:

```
# iptables -A FORWARD -p icmp --icmp-type echo-request -
m limit --limit 1/s -j ACCEPT
```

```
UDP Attack :
# iptables –N UDP-FLOOD
# iptables –A UDP-FLOOD –m limit ––limit 20/s ––limit-
burst 100 –j RETURN
# iptables –A UDP-FLOOD –j LOG ––log-prefix “UDP-FLOOD:
”
# iptables –A UDP-FLOOD –j DROP
# iptables –A INPUT –p udp –j UDP-FLOOD
```

LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Konfigurasi Firewall [iptables]

Dasar Teori :

Tugas Pendahuluan :

Hasil percobaan :

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Apa command iptables untuk melakukan blocking terhadap http ?
3. Apa command iptables untuk melakukan blocking terhadap MAC address tertentu ?
4. Apa saja command iptables yang dibuat jika kita hanya memperbolehkan ssh yang jalan di jaringan ?
5. Bagaimana jika yang diperbolehkan adalah ssh, web dan email ?
6. Bagaimana untuk blocking command ping ?