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.

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

a. **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.
b. **OUTPUT**
   Mengatur paket data yang keluar dari firewall ke arah intranet maupun internet. Biasanya output tidak diset, karena bisa membatasi kemampuan firewall itu sendiri.
c. **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 menentukkan koneksi di iptables diizinkan lewat atau tidak. TARGET ada tiga macam yaitu:

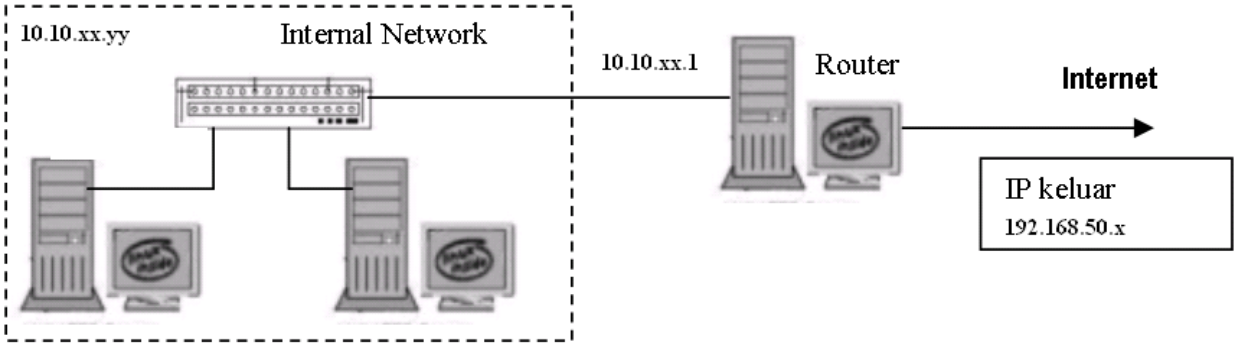
a. **ACCEPT**
   Akses diterima dan diizinkan melewati firewall
b. **REJECT**
   Akses ditolak, koneksi dari komputer klien yang melewati firewall langsung terputus, biasanya terdapat pesan "Connection Refused". Target Reject tidak menghabiskan bandwidth internet karena akses langsung ditolak, hal ini berbeda dengan DROP.
c. **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.

TUGAS PENDAHULUAN

1. Sebutkan dan jelaskan dengan singkat apa yang disebut dengan konsep firewall ?
2. Sebutkan fasilitas iptables yang ada di linux !
3. Jelaskan perbedaan mangle, nat dan filter dari iptables ?

PERCOBAAN

1. Bangun desain jaringan sebagai berikut :



Note :

10.10.xx.yy => xx (1-10) utk nomor kelompok praktikum, yy (1-254) untuk no client
192.168.50.x => gunakan dhclient utk mendapat IP dari server

2. Setting komputer sebagai router (PC1) sbb :
   a. Setting ip_forward
      - `#echo 1 > /proc/sys/net/ipv4/ip_forward`
   b. Setting menggunakan NAT
      - Format penulisan : `# iptables –t nat –A POSTROUTING –o eth0 –s` *`IP_number`* `-d 0/0 -j MASQUERADE`
      - `# iptables –t nat –A POSTROUTING –o eth0 –j MASQUERADE`

      `NB : untuk mengetahui sudah terinstall : # iptables –t nat -nL`
   c. Setting IP
      - `eth0 → 192.168.50.x Mask:255.255.255.0`
      - `eth0:1 → 10.10.1.1 Mask:255.255.255.0 (utk kelompok 1)`
   d. Setting Routing, diambil dari no IP router server
      - `Format : # route add default gw <no_IP_GW>`
      - `# route add default gw 192.168.50.1`

3. Setting komputer client sbb (contoh untuk kelompok 1)
   a. Setting IP

      `# ifconfig eth0 10.10.1.2 netmask 255.255.255.0`
   b. Tambahkan Gateway untuk PC Client

      `# route add default gw 10.10.1.1`

4. Lakukan test konektifitas
   - `ping ke PC router (10.10.x.1)`
   - `ping ke IP Server (192.168.50.1)`

5. Lakukan koneksi di sisi client untuk mengakses web dan ftp dari browser, dan pastikan berhasil.

   Contoh :

   `http://www.eepis-its.edu`
   `ftp://fileserver.eepis-its.edu`

6. Jalankan rule firewall sebagai berikut (blocking ping) :
   a. Blok PC Client supaya tidak bisa ping
      ```
      # iptables –A FORWARD –s 10.10.1.2/24 –d 0/0 –p icmp -j REJECT
      ```
   b. Lihat rule di iptables, catat hasilnya
      ```
      # iptables –nvL
      ```
   c. Cek dengan melakukan ping, catat hasilnya, mana yang berhasil di blok
      ```
      # ping ke PC router (10.10.x.1)
      # ping ke IP Server (192.168.50.1)
      ```
   d. Hapus rule di iptables
      ```
      # iptables –F
      ```
   e. Blok PC Client supaya tidak bisa ping dgn perintah berikut (INPUT)
      ```
      # iptables –A INPUT –s 10.10.1.2/24 –d 0/0 –p icmp -j REJECT
      ```
   f. Ulangi langkah b-d, catat dan bandingkan hasilnya dengan poin 6c.
   g. Blok PC Client supaya tidak bisa ping dgn perintah berikut (DROP)
      ```
      # iptables –A FORWARD –s 10.10.1.2/24 –d 0/0 –p icmp -j DROP
      ```
   h. Ulangi langkah b-d, catat dan bandingkan hasilnya dengan poin 6c.
   i. Apa kesimpulan anda tentang penggunaan perintah INPUT, FORWARD, REJECT dan DROP. Bagaimana agar bisa dilakukan bloking terhadap semua IP di poin 6c.

7. Jalankan rule firewall sebagai berikut (blocking web dan ftp) :
   a. Blok PC Client supaya tidak bisa mengakses web dan ftp di poin 5, cek kembali koneksi di poin 5 dan pastikan berhasil.
      ```
      # iptables –A FORWARD –s 10.10.1.2/24 –p tcp –m multiport --dport
        21,80 -j REJECT
      ```
   b. Lihat rule di iptables, catat hasilnya
      ```
      # iptables –nvL
      ```
   c. Cek koneksi, catat hasilnya
      ```
      http://www.eepis-its.edu
      ftp://fileserver.eepis-its.edu
      ```

8. Lakukan langkah berikut dan analisalah :
   a. Install ftp server dan telnet pada sisi PC Router (firewall) => 10.10.1.1
      ```
      # apt-get install proftpd telnetd
      ```
   b. Lakukan tes koneksi dari client ke PC Router dan pastikan berhasil
      ```
      # telnet 10.10.1.1
      # ftp 10.10.1.1
      ```
   c. Buatlah rule firewall sebagai berikut, dan ujilah rule anda tsb :
      - Drop akses dari client ke ftp server
      - Accept akses dari client ke telnet

9. Bloking dengan menggunakan MAC address
   a. Hapus rule sebelumnya : `# iptables -F`
   b. Catat MAC address di sisi client, dan lakukan perintah berikut di PC Router (firewall)
      ```
      # iptables -A FORWARD -m mac --mac-source 00:30:18:AC:14:41 -d
        0/0 -j REJECT
      ```
   c. Ujilah rule diatas, dan catat hasilnya.

10. Simpan konfigurasi firewall secara permanen
    a. Konfigurasi sbb:

```
# iptables-save > /root/data.fw
# vim /etc/network/interfaces

post-up iptables-restore < /root/data.fw

NB: Tambahkan perintah diatas setelah line eth0
```

    b. Restart komputer :

```
# reboot
```

    c. Cek hasilnya dan catat hasilnya :

```
# iptables -nvL
```

LAPORAN RESMI

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Apa saja command iptables yang dibuat jika kita hanya memperbolehkan ssh yang jalan di jaringan ?
3. Bagaimana jika yang diperbolehkan adalah ssh, web dan email dan yang lainnya ditolak ?

LEMBAR ANALISA

Praktikum Network Security (Konfigurasi Firewall - iptables)
Tanggal Praktikum :
Kelas :
Nama dan NRP :

A. Gambar topologi jaringan beserta dengan IP Addressnya

B. Tes koneksi jaringan untuk poin 4 dan 5

C. Catat dan analisa rule firewall <INPUT, FORWARD, DROP, REJECT> untuk blocking ping (poin 6)

D. Catat dan analisa rule firewall untuk blocking web dan ftp (poin 7)

E. Tuliskan rule firewall pada poin 8

F. Catat dan analisa rule firewall untuk block berdasarkan MAC address (poin 9)