Praktikum Jaringan Komputer 2

Modul 3

BRIDGE-FIREWALL dengan Netfilter

TUJUAN:

1. Mahasiswa memahami fungsi dari firewall
2. Mahasiswa mampu menggunakan aplikasi netfilter sebagai firewall
3. Mahasiswa mampu menganalisa permasalahan firewall

DASAR TEORI

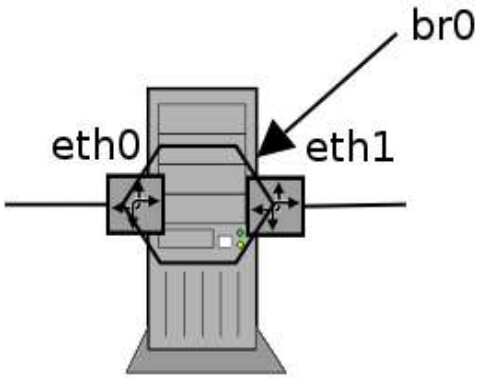
BRIDGE-FIREWALL

Firewall (Gb. 1) merupakan perangkat keamanan dari Teknologi Informasi (TI) , dimana digunakan untuk memperbolehkan data, melarang koneksi atau sebagai proxy berdasarkan ketentuan keamanan (**RULE**).

Gb. 1. Firewall memisahkan zone

Aplikasi firewall di Linux yang digunakan pada layer Network disebut **Netfilter**

Aplikasi firewall digunakan pada PC Router. PC Router difungsikan pada layer 3, tetapi untuk aplikasi firewall sekarang, PC Router difungsikan sebagai bridge (Layer 2). Sehingga nantinya PC Router ini akan tampak transparant.



Gb. 2. Perangkat br0 gabungan dari eth0-eth1

Langkah-langkah membangun PC Router menjadi Bridge (Gb. 2) antara lain:

1. Mempersiapkan 2 Ethernet Card

   Pada PC Router minimal akan menggunakan 2 Ethernet (eth0 dan eth1). Karena untuk memfungsikan bridge, harus menggabungkan beberapa ethernet menjadi 1 perangkat BRIDGE (br0)
2. Mengaktifkan IP Forwarding

   # echo 1 > /proc/sys/net/ipv4/ip_forward
3. Menginstall aplikasi bridge-utils

   # apt-get install bridge-utils
4. Mengaktifkan device bridge (br0)

   # brctl addbr br0
   # brctl addif br0 eth0
   # brctl addif br0 eth1
   # ifconfig eth0 0
   # ifconfig eth1 0
5. Memberikan IP pada perangkat bridge dengan cara static atau dhcp

   # ifconfig br0 10.252.108.100 netmask 255.255.255.0
   atau
   # dhclient br0

NETFILTER

Netfilter merupakan satu set aplikasi yang dapat mengatur kernel linux untuk dapat mencegat dan memanipulasi paket jaringan. Komponen netfilter digunakan sebagai firewall di mesin linux. Untuk menggunakan fungsi netfilter ini diperlukan aplikasi di Linux yang disebut **iptables**.

Iptables memiliki table yang berfungsi untuk menentukan arah putaran paket data. Dimana table tersebut ada 3 yaitu :

1. filter

   Digunakan untuk memilah dan memberikan ijin ACCEPT/DROP pada suatu paket data
2. nat

   Digunakan untuk network address translation
3. mangle

   Digunakan untuk QoS

Untuk praktikum ini kita akan menggunakan table **filter**.

Table filter sendiri memiliki CHAINS (rantai aliran data), yang digunakan untuk memilah aliran paket data. Chains (Gb. 3) tersebut adalah

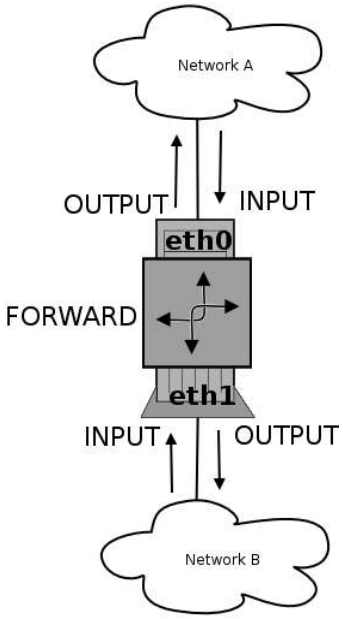
- INPUT

  Digunakan untuk memilah paket data yang masuk ke mesin firewall
- FORWARD

  Digunakan untuk memilah paket data yang melalui mesin firewall dan diroutingkan kembali ke jalur yang lainnya

- OUTPUT

  Digunakan untuk memilah paket data yang keluar dari mesin firewall



Gb. 3. Chains pada table filter

IPTABLES

Iptables memiliki rule yang digunakan untuk memilah data, dan pengecekan terhadap data dibaca dari rule yang paling atas sampai ke bawah.

* Untuk melihat isi dari firewall, dapat menggunakan perintah iptables dengan format

  # iptables -t <TABLE> -nL

contoh :

  # iptables -nL

  # iptables -t nat -nL

* Untuk menghapus isi dari firewall, dapat menggunakan options -F :

  # iptables -t <TABLE> -F

contoh :

  # iptables -F

* Untuk menambahkan suatu rule ke firewall, dapat menggunakan options -A atau -I :

  # iptables -t <TABLE> -I <CHAIN> -p <Protokol> -s <IP-asal/Netmask> -d <IP-tujuan/Netmask> -j <ACCEPT/DROP>

Dimana :

- TABLE, bisa diisikan dengan filter, nat, atau mangle
- CHAIN, apabila tablenya filter bisa diisikan INPUT, OUTPUT, atau FORWARD

- Protokol, bisa diisikan tcp, udp, icmp atau all
- IP-asal, bisa diisikan dengan ip address asal paket (source)
- IP-tujuan, bisa diisikan dengan ip address tujuan paket (destination)
- ACCEPT/DROP, bila ingin mengijinkan data lewat isikan dengan ACCEPT. Bila tidak mengijinkan isikan dengan DROP

contoh :

- Untuk memblok ping ke mesin firewall
  # iptables -t filter -I INPUT -s 0.0.0.0/0 -d 10.252.108.75/32 -p icmp -j DROP

* Untuk menghitung data yang tertangkap oleh firewall dapat dilakukan dengan cara :
  # iptables -nvL

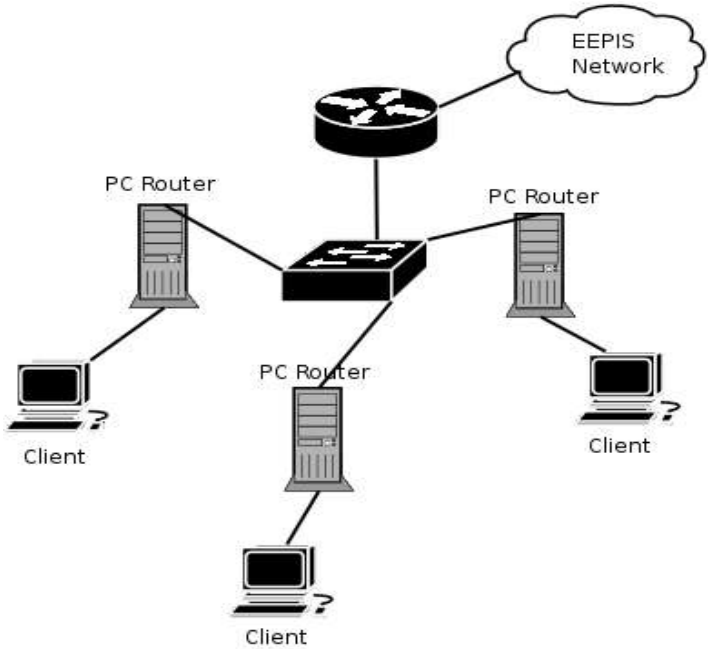
PERALATAN

1. PC Router
2. PC Client
3. Switch

Catat semua langkah dan hasil yang dilakukan pada praktikum laporan sementara !!!

LANGKAH-LANGKAH PRAKTIKUM

1. Siapkan jaringan seperti pada gambar topologi (Gb. 4)



Gb. 4. Topologi Modul 3

2. Tentukan interface mana yang kearah switch dan interface mana yang kearah client. Beri IP dhcp pada interface yang kearah switch dan aktifkan IP-Forwarding

Praktikum Bridge pada Linux

Pada PC Router :

3. Install aplikasi bridge-utils
   # apt-get install bridge-utils
4. Aktifkan mode bridge pada PC Router
   # brctl addbr br0
   # brctl addif br0 eth0
   # brctl addif br0 eth1
   # ifconfig eth0 0
   # ifconfig eth1 0
5. Beri IP pada interface bridge dengan cara DHCP
   # dhclient br0
6. Catat hasil mode bridge dengan perintah ifconfig dan route -n

Pada PC Client

1. Beri IP pada PC Client dengan cara DHCP
   # dhclient
2. Catat ip address dan routing pada PC Client dengan perintah ifconfig dan route -n
3. Lakukan traceroute atau mtr ke arah PC Client pada jaringan yang lain, dan catat hasilnya.

Praktikum Firewall

Persiapan iptables

1. Install aplikasi iptables
   # apt-get install iptables
2. Hapus semua rule iptables pada PC router
   # iptables -F
   # iptables -t nat -F
3. Rubah chain pada firewall menjadi default ACCEPT
   # iptables -P INPUT ACCEPT
   # iptables -P OUTPUT ACCEPT
   # iptables -P FORWARD ACCEPT
4. Catat rule hasil firewall
   # iptables -nL

Memblok jalur ping

1. Lakukan ping dari PC Client ke arah PC Client di jaringan yang beda
2. Lakukan ping ke arah proxy-server EEPIS (202.154.187.7)
3. Lakukan DROP pada PC router supaya PC Client tidak bisa melakukan ping
   # iptables -I FORWARD -s 0.0.0.0/0 -d 0.0.0.0/0 -p icmp -j DROP
4. Catat hasil firewall di PC Router
5. Lakukan ping dari PC Client ke arah PC Client di jaringan yang beda dan juga ke arah

proxy-server EEPIS. Catat hasilnya
6. Lakukan ACCEPT terhadap ping dari PC Client **HANYA** ke arah Proxy-server, dan yang lainnya tetap DROP
7. Catat hasil firewall di PC Router

Memblok jalur WEB
1. Pastikan dari client dapat mengakses ke web http://www.eepis-its.edu dengan web browser (tanpa menggunakan proxy di *preferences* nya)
2. Lakukan DROP supaya PC Client pada masing-masing jaringan tidak dapat mengakses ke web tersebut, dengan cara :
   # iptables -I FORWARD -d 202.154.187.5 -p tcp –dport 80 -j DROP
3. Akses alamat www.eepis-its.edu apakah masih bisa diakses atau tidak
4. Catat hasil rule firewall pada PC Router

Menghitung jumlah koneksi yang tertangkap di firewall
1. Pastikan ada rule di firewall
2. Hitung jumlah paket yang tertangkap pada firewall dengan perintah :
   # iptables -nvL

TUGAS
- Buat program seperti contoh dibawah dan catat tampilan dari program tersebut

```
#!/bin/bash

echo " prot       Source       Destination       Rule"
for i in INPUT FORWARD OUTPUT ;
do
        echo $i
        iptables -nvL $i | grep -v pkts | grep -v Chain | awk '{ printf(" %4s %15s %15s %
8s \n", $4, $8, $9, $3) }'
done
```

REFERENSI

- Wikipedia, http://www.wikipedia.org netfilter firewall
- man iptables
- man brctl

Data Praktikum Modul 3 : Bridge-Firewall dengan Netfilter

NRP :
Nama :
Hari/Tgl :

1. Gambar Topologi, beserta informasi IP address

2. Bridge mode pada PC Router
   # ifconfig

   # route -n

3. PC Client
   # ifconfig

   # route -n

   # mtr

4. Persiapan firewall : iptables -nL

5. Memblok jalur ping : iptables -nL, ping

6. Memblok jalur WEB : iptables -nL, akses ke web http://www.eepis-its.edu

7. Menghitung jumlah koneksi yang tertangkap firewall : iptables -nvL