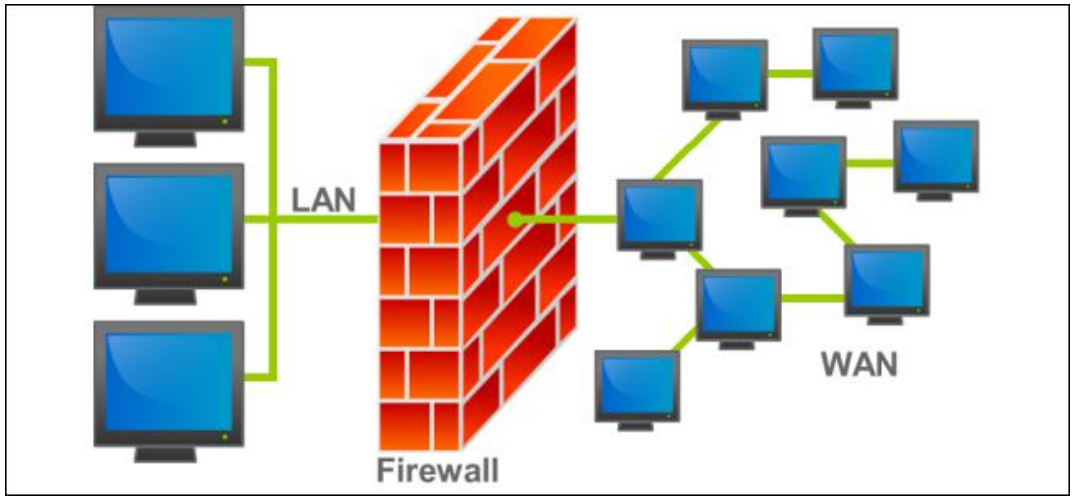
Linux Server

"Firewall"

Pemateri : 1. alfian
2. iqbal

Apa itu Firewall ?

Firewall adalah sebuah sistem yang didesain untuk mencegah akses yang tidak sah dari jaringan luar atau dalam



Firewall dapat dibedakan menjadi

1. **Dedicated Firewall**
   Firewall yang berupa perangkat keras. Contoh : Cisco PIX Firewall
2. **Server Based Firewall**
   Firewall yang berupa sistem operasi jaringan (Linux, Unix) yang menjalankan fungsi firewall
3. **Integrated Firewall**
   Firewall yang ditambahkan pada suatu perangkat jaringan
4. **Personal Firewall**
   Firewall yang dipasangkan di personal PC, dapat berupa Software bawaan OS, Antivirus dll.

Keuntungan dan Manfaat Firewall

1. Dapat mengamankan data dari serangan jaringan luar
2. Dapat memfilter sebuah paket” yang keluar masuk jaringan
3. Dapat mencegah suatu akses yang tidak diinginkan untuk masuk/keluar jaringan

Mengenal IPTABLES, Firewall pada Linux

Linux sudah dilengkapi dengan aplikasi firewall, fungsi firewall dijalankan oleh *iptables,*

Mengenal Tabel Pada Firewall

Iptables memiliki 3 buah fungsi dasar yang masing-masing memiliki kegunaan tersendiri.
Iptables dilengkapi 3 tabel fungsi yaitu

1. **Mangle**
   Untuk memanipulasi paket data
2. **Filter**
   Untuk memfilter sebuah paket
3. **Nat**
   Untuk melakukan Network address translation

Mengenal Chain Pada Firewall

Chain adalah sebuah aturan pada setiap table.

kegunaan chain untuk menetukan jenis trafik yang akan di-manage pada fitur firewall dan setiap fungsi pada firewall seperti Filter Rule, NAT, Mangle memiliki opsi chain yang berbeda.

Chain Pada Tabel Mangle :

1. **Prerouting**
2. **Postrouting**
3. **Input**
4. **Output**
5. **Forward**

Mengenal Chain Pada Firewall

Chain Pada Tabel Filter :

1. Input

Digunakan untuk memproses trafik paket data yang masuk ke dalam router melalui interface yang ada di router dan memiliki tujuan IP Address berupa ip yang terdapat pada router.

2. Output

Digunakan untuk memproses trafik paket data yang keluar dari router. Dengan kata lain merupakan kebalikan dari 'Input'. Jadi trafik yang berasal dari dalam router itu sendiri dengan tujuan jaringan Public maupun jaringan Local.

3. Forward

Digunakan untuk memproses trafik paket data yang hanya melewati router. Misalnya trafik dari jaringan public ke local atau sebaliknya dari jaringan local ke public.

Mengenal Chain Pada Firewall

Chain Pada Tabel Nat:

1. Prerouting

Merupakan sebuah koneksi yang akan masuk kedalam router dan melewati router. Berbeda dengan input yang mana hanya akan menangkap trafik yang masuk ke router. Trafik yang melewat router dan trafik yang masuk kedalam router dapat ditangkap di chain prerouting.

2. Postrouting

Kebalikan dari prerouting, postrouting merupakan koneksi yang akan keluar dari router, baik untuk trafik yang melewati router ataupun yang keluar dari router.

Mengenal Target dan Jump Pada Firewall

Setiap paket yang kriterianya sama dengan chain yang sudah ditentukan, maka paket tersebut akan menjalankan Jump atau mengeksekusi paket tersebut. Jump dapat berupa DROP (buang) atau ACCEPT (menerima)

Berbagai Jenis Jump

- ACCEPT
  - Menerima paket
- DROP
  - Membuang paket
- LOG
  - Membuat log dari informasi paket
- REJECT
  - Paket akan diblok dan memberikan balasan ke host pengirim
- DNAT
  - Destination IP address dari paket yang akan dikirimkan
- SNAT
  - Source IP address dari paket yang dikirim
- MASQUERADE
  - Source IP Address dari paket akan dirubah

Sintaks IPTABLES

- **-t <table>**
  mendefinisikan tabel yang akan digunakan, bila tidak ditulis maka default tabel = filter
- **-j <target>**
  mendefinisikan jump/action yang akan digunakan
- **-A**
  menambahkan chain baru sesudah chain terakhir
- **-F (Flush)**
  Menghapus semua chain firewall
- **-p <protocol_type>**
  mencocokan protokol apa yang digunakan (TCP, UDP, ICMP dll)
- **-s <ip_address>**
  mencocokan source IP address pada paket data
- **-d <ip_address>**
  mencocokan destination IP address pada paket data
- **-i <interface_name>**
  mencocokan input Interface dimana paket akan diterima
- **-o <interface_name>**
  mencocokan input Interface dimana paket akan dikirim

Cek apakah iptables sudah terinstall atau belum

```
fossil@fossil:~$ sudo apt list | grep iptables

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

arno-iptables-firewall/stable 2.0.1.f-1 all
golang-github-coreos-go-iptables-dev/stable 0.1.0-1 all
iptables/stable,now 1.6.0+snapshot20161117-6 amd64 [installed]
iptables-converter/stable 0.9.8-1 all
iptables-converter-doc/stable 0.9.8-1 all
iptables-dev/stable 1.6.0+snapshot20161117-6 all
iptables-nftables-compat/stable 1.6.0+snapshot20161117-6 amd64
iptables-optimizer/stable 0.9.14-1 all
iptables-optimizer-doc/stable 0.9.14-1 all
iptables-persistent/stable 1.0.4+nmu2 all
libiptables-chainmgr-perl/stable 1.6-1 all
libiptables-parse-perl/stable 1.6-1 all
python-iptables/stable 0.11.0-4 amd64
python-iptables-doc/stable 0.11.0-4 all
python3-iptables/stable 0.11.0-4 amd64
```

Cek apakah iptables sudah terinstall atau belum

```
fossil@fossil:~$ sudo iptables
iptables v1.6.0: no command specified
Try `iptables -h' or 'iptables --help' for more information.
fossil@fossil:~$ sudo iptables -h
iptables v1.6.0

Usage: iptables -[ACD] chain rule-specification [options]
       iptables -I chain [rulenum] rule-specification [options]
       iptables -R chain rulenum rule-specification [options]
       iptables -D chain rulenum [options]
       iptables -[LS] [chain [rulenum]] [options]
       iptables -[FZ] [chain] [options]
       iptables -[NX] chain
       iptables -E old-chain-name new-chain-name
       iptables -P chain target [options]
       iptables -h (print this help information)
```

menghapus paket iptables

```
fossil@fossil:~$ sudo apt purge iptables
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libecap3
Use 'sudo apt autoremove' to remove it.
The following packages will be REMOVED:
  iptables*
0 upgraded, 0 newly installed, 1 to remove and 98 not upgraded.
After this operation, 1,565 kB disk space will be freed.
Do you want to continue? [Y/n]
```

memasang paket iptables

```
fossil@fossil:~$ sudo apt install iptables
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libecap3
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  iptables
```

untuk melihat konfigurasi firewall yang dijalankan

```
fossil@fossil:~$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
fossil@fossil:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

membuat konfigurasi firewall(iptables) permanent

```
fossil@fossil:~$ sudo iptables-save > /etc/iptables.up.rules
bash: /etc/iptables.up.rules: Permission denied
fossil@fossil:~$ sudo su
root@fossil:/home/fossil# cd
root@fossil:~# iptables-save > /etc/iptables.up.rules
root@fossil:~# nano /etc/network/if-pre-up.d/iptables
```

```
  GNU nano 2.7.4        File: /etc/network/if-pre-up.d/iptables        Modified

#!/bin/sh
/sbin/iptables-restore < /etc/iptables.up.rules
```

membuat konfigurasi firewall(iptables) permanent

```
root@fossil:~# ls -l /etc/network/if-pre-up.d/iptables
-rw-r--r-- 1 root root 58 Mar 22 18:36 /etc/network/if-pre-up.d/iptables
root@fossil:~# chmod +x /etc/network/if-pre-up.d/iptables
root@fossil:~# ls -l /etc/network/if-pre-up.d/iptables
-rwxr-xr-x 1 root root 58 Mar 22 18:36 /etc/network/if-pre-up.d/iptables
```

melihat konfigurasi tabel filter

```
fossil@fossil:~$ sudo iptables -t filter -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

melihat konfigurasi tabel nat

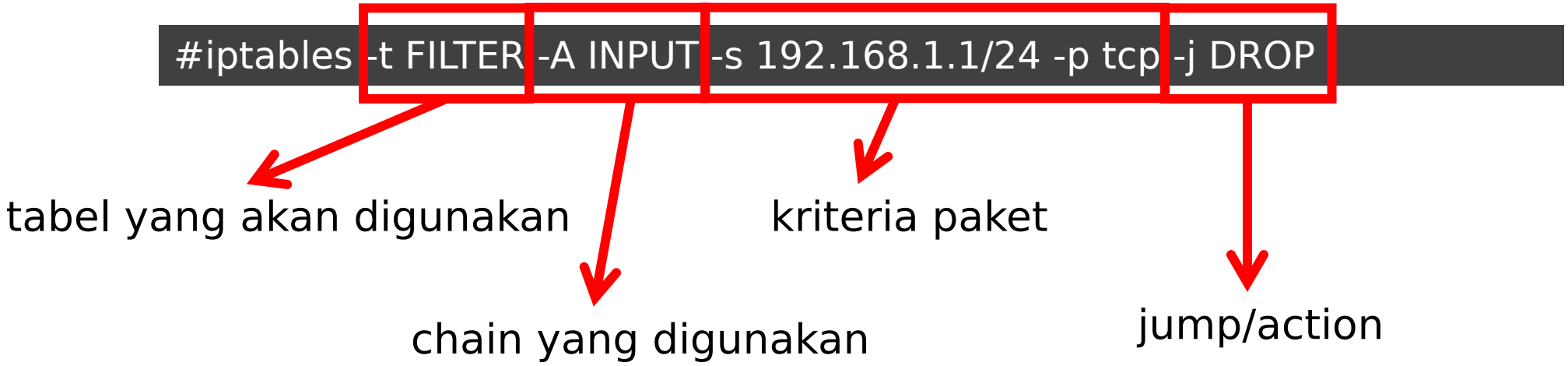
```
fossil@fossil:~$ sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
```

Contoh penulisan IPTABLES



Challenge

1. Buatlah sebuah Firewall untuk memblokir PING dari host ke SERVER
2. Buatlah sebuah Firewall untuk menghubungkan jaringan lokal ke public
3. Buatlah sebuah firewall untuk memblokir akses ke SERVER