Keamanan Sistem dan Jaringan

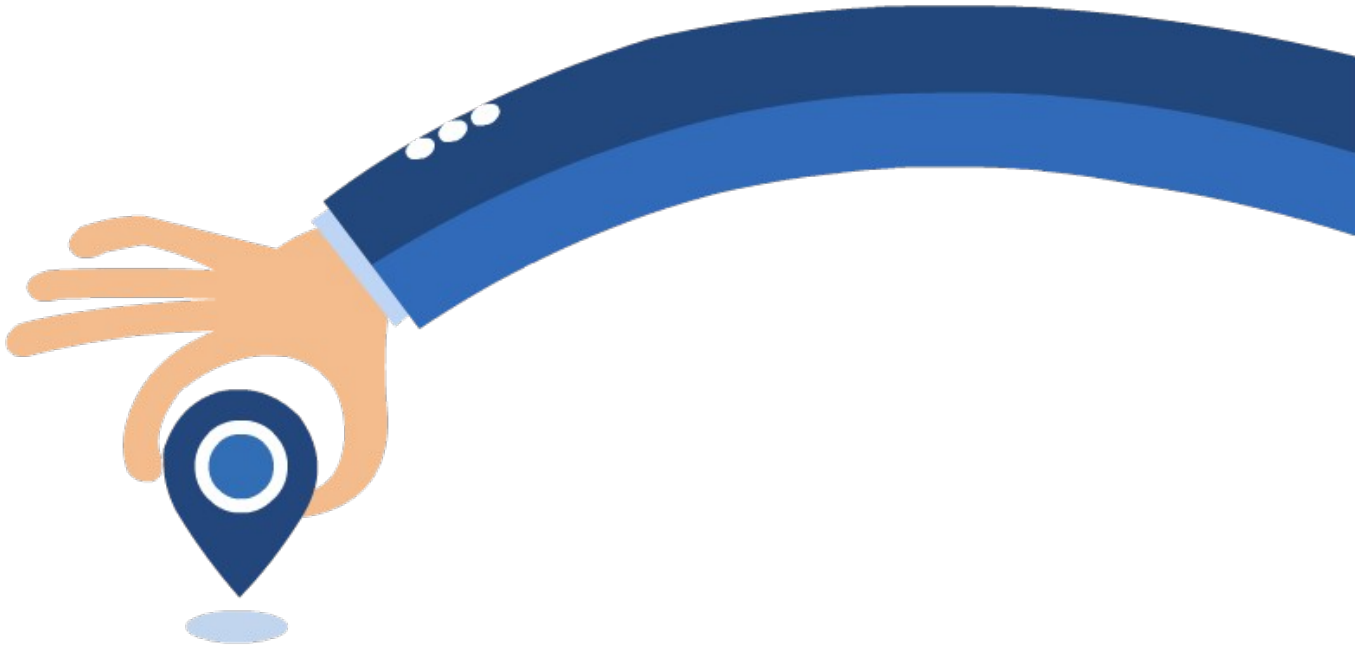
Pertemuan ke-5

Pesantren Teknologi Informasi dan Komunikasi
Jln. Mandor Basar No. 54 RT 01/RW 01 Rangkapanjaya,
Pancoran Mas, Depok 16435 | Telp. (021) 77 88 66 91
Koordinat (-6.386680 S, 106.777305 E)
www.petik.or.id

Pesantren Teknologi Informasi dan Komunikasi

PeTIK

Creates Future Skilled Professionals



Jalan Mandor Basar Nomor 54, RT. 01/001, Rangkapanjaya, Pancoran Mas, Kota Depok 16435

www.petik.or.id 021 7788 6691 info@petik.or.id

Firewall
(iptables)

Pendahuluan

- Firewall adalah suatu mekanisme untuk melakukan filtering paket data, manipulasi paket data serta pengubahan paket-paket data yang datang dari suatu jaringan menuju suatu komputer dalam suatu jaringan.
- Sistem operasi Linux pada kernelnya memiliki sebuah rutin atau fungsi yang dapat melakukan filtering dan manipulasi paket data yang menuju sistem Linux ataupun yang akan keluar dari sistem linux ke jaringan
- Kernel Linux menyediakan default mekanisme firewall pada kernelnya yang sering dikenal dengan Netfilter/iptables

iptables

- Program utiliti yang digunakan untuk mengkonfigurasi Netfilter
- Iptables menggunakan tabel-tabel (filter, nat, mangle) yang berbeda untuk aksi-aksi yang berbeda
- Tabel-tabel tersebut menyimpan daftar rule firewall yang diterapkan
- Tabel yang paling umum digunakan adalah tabel filter dan nat

iptables

- Tabel filter digunakan untuk packet filtering dan tabel nat digunakan untuk melakukan network address translation
- Rule-rule firewall aktual disimpan dalam suatu chains.
- Ada lima buah built-in chains yaitu INPUT, OUTPUT, FORWARD, PREROUTING, dan POSTROUTING
- User dapat mendefinisikan chain sendiri sesuai kebutuhan

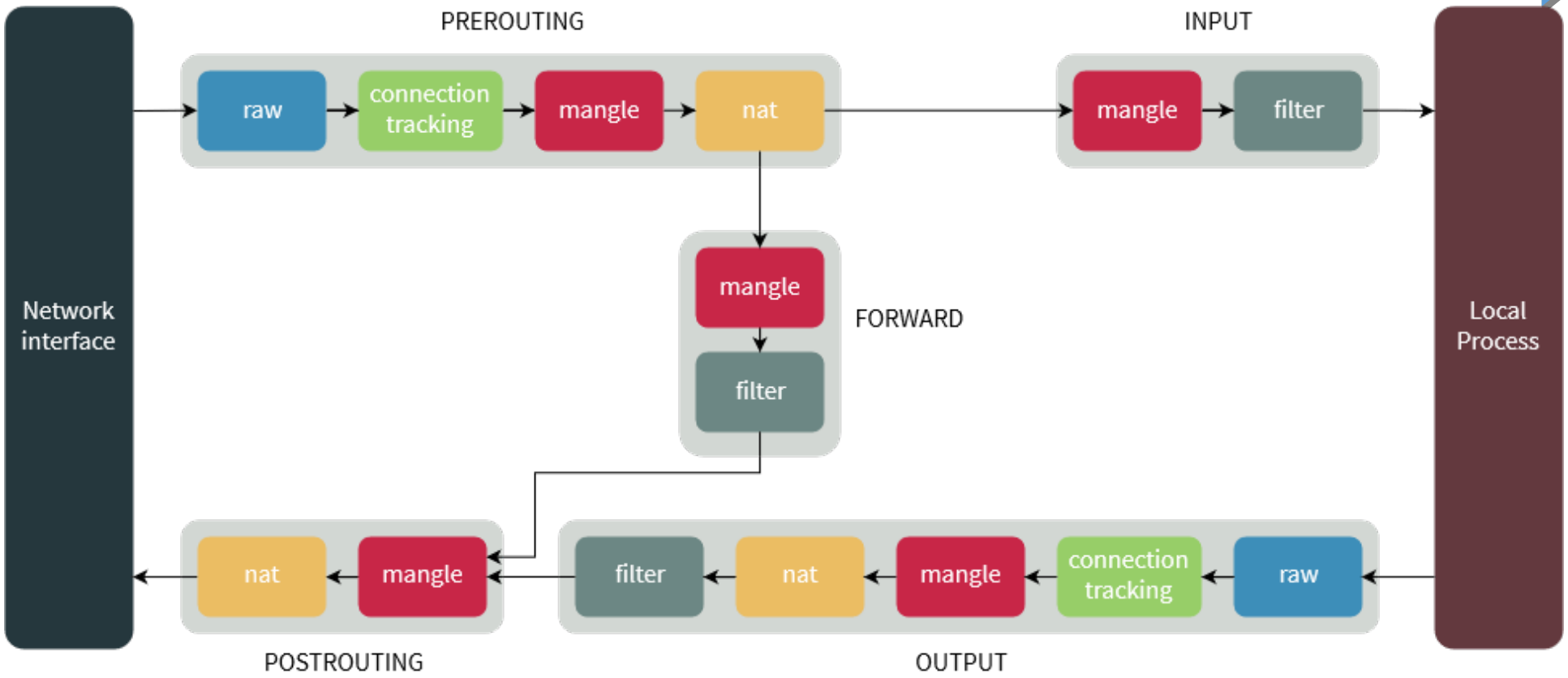
Built-in Chains pada Tabel Filter

- INPUT (untuk paket yg menuju local process)
- FORWARD (untuk paket yg melewati local process)
- OUTPUT (untuk paket yg keluar dari local process)

Built-in Chains pada Tabel NAT

- PREROUTING (paket diubah sebelum masuk ke antarmuka jaringan)
- INPUT (mengubah paket yg menuju local process)
- OUTPUT (mengubah paket yg keluar dari local process)
- POSTROUTING (paket diubah setelah keluar dari antarmuka jaringan)

Packet Flow Diagram



Sintaks Perintah iptables

iptables [-t table] <action> [rule specification] [-j target]

- action, menentukan aksi yang ditampilkan pada table

  -I CHAIN - menambahkan/menyisipkan sebuah rule ke sebuah chain

  -A CHAIN - menambahkan sebuah rule ke sebuah chain pada akhir baris rule

  -D CHAIN - menghapus sebuah rule dari sebuah chain

Sintaks Perintah iptables

-L CHAIN - menampilkan daftar rule dari sebuah chain

-F CHAIN - menghapus semua rule dari sebuah chain

-N CHAIN - membuat chain baru

-P CHAIN - set default policy untuk suatu chain berupa ACCEPT atau DROP

Sintaks Perintah iptables

- rule specification, mendefinisikan rule-rule spesifik yang bersesuaian

  [!] -s <ip-address> - source address paket

  [!] -d <ip-address> - target address paket

  [!] -p <protocol> - protokol (tcp, udp,icmp)

  --dport <port> - port tujuan

  --sport <port> - port sumber

Sintaks Perintah iptables

[!] -o <interface>	-	outgoing interface network
[!] -i <interface>	-	incoming interface network
-m conntrack	-	membolehkan rule filter yg cocok berdasarkan status koneksi. Membolehkan penggunaan opsi --ctstate.

Sintaks Perintah iptables

--ctstate - mendefiniskan daftar status yg cocok dengan rule. Status yg valid:

1. NEW - Koneksi baru.
2. RELATED - Koneksi baru, tetapi terkait dengan koneksi lain yang sudah diizinkan
3. ESTABLISHED - Koneksi sudah terjalin.
4. INVALID - Lalu lintas data tidak dapat diidentifikasi karena alasan tertentu.

Sintaks Perintah iptables

- target, menentukan apa yang akan terjadi dengan paket atau traffic yang sesuai dengan rule.
  - target-target basic (DROP, ACCEPT)
  - target-target extension (LOG,REJECT, CUSTOM CHAIN)

Contoh penggunaan iptables

- Memblok semua paket yang datang dari IP address 192.168.7.254

```
$ sudo iptables -A INPUT -s 192.168.7.254 -j DROP
```

- Memblok semua paket yang ditujukan ke semua ip address kecuali ke ip address 192.168.7.254

```
$ sudo iptables -A OUTPUT ! -d 192.168.7.254 -j DROP
```

- Memblok semua paket dari 192.168.7.251 yang datang pada interface enp0s3

```
$ sudo iptables -A INPUT -s 192.168.7.251 -i enp0s3 -j DROP
```

Contoh penggunaan iptables

- Memblok paket-paket protokol icmp

```
$ sudo iptables -A INPUT -p icmp -j DROP
```

- Memblok paket-paket protokol icmp dengan mengembalikan pesan error default (icmp-port-unreachable)

```
$ sudo iptables -A INPUT -p icmp -j REJECT
```

- Memblok paket-paket protokol icmp dengan mengembalikan pesan error tidak default

```
$ sudo iptables -A INPUT -p icmp -j REJECT –-reject-with icmp-host-prohibited
```

Contoh penggunaan iptables

- Membolehkan paket masuk yang statusnya sudah terkoneksi

```
$ sudo iptables -I INPUT 1 -m conntrack --ctstate
ESTABLISHED,RELATED -j ACCEPT
```

- Memblok semua paket yang ditujukan ke port 80

```
$ sudo iptables -A INPUT -p tcp --dport 80 -j DROP
```

Contoh penggunaan iptables

- Menampilkan daftar rule suatu chain

```
$ sudo iptables -L INPUT
```

- Menampilkan daftar seluruh rule dari semua chain

```
$ sudo iptables -L
```

- Menghapus rule ketiga dari chain INPUT. Gunakan nomor urut rule pada chain tersebut atau gunakan sintaks lengkapnya

```
$ sudo iptables -D INPUT 3
```

```
$ sudo iptables -D INPUT -s 192.168.7.254 -j DROP
```

Contoh penggunaan iptables

- Menghapus seluruh rule (*flush*) pada tabel filter

```
$ sudo iptables -F
```

- Menyimpan rule-rule yang telah didefinisikan ke dalam file

```
$ sudo iptables-save > iptables.rules
```

- Me-*restore* rule-rule dari file

```
$ sudo iptables-restore < iptables.rules
```

Pesantren Teknologi Informasi dan Komunikasi

PeTIK

Creates Future Skilled Professionals

Jalan Mandor Basar Nomor 54, RT. 01/001, Rangkapanjaya,
Pancoran Mas, Kota Depok 16435

www.petik.or.id

021 7788 6691

info@petik.or.id