Dalam mengatur alur lalulintas data dalam suatu jarigan tentu dibutuhkan proses Routing. Dimana Proses Routing ini sangat berpengaruh terhadap kontinuitas dan alur kerja sistem secara berkesinambungan.

Hal ini akan menjadi sangat penting karena ketika terjadi masalah dalam jaringan maka yang paling utama dilakukan cross check terhadap jaringan tersebut adalah PROSES ROUTING. Dibawah ini merupakan salah satu SCRIPT ROUTING yang dapat digunakan oleh sistem operasi linux apapun yaitu :

```
#! /bin/sh
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -F
iptables -t nat -F


###################
# DROP ALL INPUT CHAINS #
###################
iptables -P INPUT DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i eth0 -j ACCEPT
iptables -A INPUT -i eth1 -j ACCEPT


iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -i eth1 -p tcp --dport 80 -j ACCEPT


iptables -A INPUT -i eth0 -p tcp --dport 21 -j ACCEPT
iptables -A INPUT -i eth1 -p tcp --dport 21 -j ACCEPT
```

```
iptables -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -i eth1 -p tcp --dport 22 -j ACCEPT

iptables -A INPUT -i eth0 -p tcp --dport 53 -j ACCEPT
iptables -A INPUT -i eth1 -p tcp --dport 53 -j ACCEPT

iptables -A INPUT -i eth0 -p icmp -j ACCEPT
iptables -A INPUT -i eth1 -p icmp -j ACCEPT

iptables -A INPUT -p tcp --dport 110 -j ACCEPT
iptables -A INPUT -p tcp --sport 110 -j ACCEPT

iptables -A INPUT -p tcp --dport 143 -j ACCEPT
iptables -A INPUT -p tcp --sport 143 -j ACCEPT

iptables -A INPUT -p tcp --dport 111 -j ACCEPT
iptables -A INPUT -p tcp --sport 111 -j ACCEPT

iptables -A INPUT -p tcp --dport 993 -j ACCEPT
iptables -A INPUT -p tcp --sport 993 -j ACCEPT

iptables -A INPUT -p tcp --dport 995 -j ACCEPT
iptables -A INPUT -p tcp --sport 995 -j ACCEPT

iptables -A INPUT -p tcp --dport 25 -j ACCEPT
iptables -A INPUT -p tcp --sport 25 -j ACCEPT

iptables -A INPUT -p tcp -i eth0 --dport 10000 -j ACCEPT
```

```
iptables -A INPUT -p tcp -i eth1 --dport 10000 -j ACCEPT



iptables -A INPUT -p tcp --dport 443 -j ACCEPT
iptables -A INPUT -p udp --dport 443 -j ACCEPT



######################
# IP PUBLIC TO INTERNET OPEN #
######################
ip addr add 118.98.xxx.xxx/29 brd + dev eth0
iptables -A INPUT -s 118.98.xxx.xxx/29 -j ACCEPT
iptables -A INPUT -d 118.98.xxx.xxx/29 -j ACCEPT



######################
# IP PUBLIC TO INTERNET OPEN #
######################



iptables -A INPUT -s 118.97.xxx.xxx/29 -j ACCEPT
iptables -A INPUT -d 118.97.xxx.xxx/29 -j ACCEPT



iptables -A INPUT -s 192.168.90.1/24 -j ACCEPT
iptables -A INPUT -d 192.168.90.1/24 -j ACCEPT



####################
# IP TO BACKBONE INTERNAL  #
####################
ip addr add 172.30.100.26/27 brd + dev eth0
iptables -A INPUT -s 172.30.100.26/27 -j ACCEPT
iptables -A INPUT -d 172.30.100.26/27 -j ACCEPT



ip addr add 172.30.110.26/27 brd + dev eth0
iptables -A INPUT -s 172.30.110.26/27 -j ACCEPT
iptables -A INPUT -d 172.30.110.26/27 -j ACCEPT
```

```
#echo "search pkbmcyber.net" > /etc/resolv.conf
#echo "nameserver 192.168.1.254" >> /etc/resolv.conf
#echo "nameserver 202.134.1.10" >> /etc/resolv.conf



###################################
#                                 DMZ                                 #
###################################



#iptables -t nat -A PREROUTING -p tcp --dport 1080 -d 118.97.xxx.xxx -j DNAT --to-destination
172.30.110.27:80
#iptables -t nat -A PREROUTING -p tcp --dport 1000 -d 118.97.xxx.xxx -j DNAT --to-destination
172.30.110.27:10000
#iptables -t nat -A PREROUTING -p tcp --dport 1022 -d 118.97.xxx.xxx -j DNAT --to-destination
172.30.110.27:22



iptables -t nat -A PREROUTING -p tcp --dport 1010  -d 118.97.xxx.xxx -j DNAT --to-destination
172.30.100.10:80
#iptables -t nat -A PREROUTING -p tcp --dport 7788  -d 118.97.xxx.xxx -j DNAT
--to-destination 10.55.55.253:8291
#iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
#iptables -t nat -A POSTROUTING -o eth3 -j MASQUERADE
#iptables -t nat -A POSTROUTING -p tcp -d 10.32.25.2 --dport 80 -j MASQUERADE
iptables -t nat -A POSTROUTING -d 172.30.100.10 -j MASQUERADE



#####################################################################



#iptables -t nat -A POSTROUTING -s 10.75.31.0/24 ! -d 10.75.0.0/16 -p tcp -o ppp0 -j
MASQUERADE
#iptables -t nat -A POSTROUTING -s 10.75.31.0/24 ! -d 10.75.0.0/16 -p icmp -o ppp0 -j
MASQUERADE
```

```
#iptables -t nat -A POSTROUTING --out-interface ppp0 --jump MASQUERADE
#iptables -A INPUT -p tcp --dport 80 -i ppp0 -j ACCEPT
#iptables -A INPUT -p tcp -s 64.57.102.34 --dport 80 -i ppp0 -j ACCEPT
#iptables -A INPUT -p icmp -j ACCEPT
#iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE



#iptables -t nat -A POSTROUTING -s 192.168.0.0/16 -o ppp0 -j MASQUERADE
#iptables -A FORWARD -s 192.168.0.0/16 -o ppp0 -j ACCEPT
#iptables -A FORWARD -d 192.168.0.0/16 -m state --state ESTABLISHED,RELATED -i ppp0 -j
ACCEPT



#iptables -t nat -A POSTROUTING -d 127.0.0.0/8 -j ACCEPT
#iptables -t nat -A POSTROUTING -d 192.168.0.0/24 -j ACCEPT
#iptables -t nat -A POSTROUTING -j SNAT --to 203.0.113.1



##############################################
#                    SAMPLE IPTABLES FOR PPPOE                    #
##############################################



#iptables -F
#iptables -t nat -F
#iptables -t mangle -F #ignore if you get an error here
#iptables -X #deletes every non-builtin chain in the table



#iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
#iptables -A INPUT -m state --state NEW -i ! ppp0 -j ACCEPT
# only if both of the above rules succeed, use
#iptables -P INPUT DROP



#iptables -A FORWARD -i ppp0 -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
#iptables -A FORWARD -i eth0 -o ppp0 -j ACCEPT
```

```
#iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE



#iptables -A FORWARD -i ppp0 -o ppp0 -j REJECT



##############################################
#                                DROP MAC ADDRESS                                #
##############################################



#iptables -A INPUT -m mac --mac-source 94:39:e5:af:1b:c7 -j DROP
#iptables -A INPUT -s 10.0.100.15 -m mac --mac-source 94:39:e5:af:1b:c7 -p all -i eth3 -j
DROP
#iptables -A FORWARD -s 10.0.100.15 -m mac --mac-source 94:39:e5:af:1b:c7 -i eth3 -j DROP



#iptables -A FORWARD -m mac --mac-source 94:39:e5:af:40:ff -i eth3 -j DROP
#iptables -A FORWARD -m mac --mac-source cc:af:78:d2:50:21 -i eth3 -j DROP
#iptables -A FORWARD -m mac --mac-source 1c:6f:65:8b:19:67 -i eth3 -j DROP



##############################################



#IP MYNET 135.24.1.254 MAC ADDR => 00:13:46:3B:02:E1 (1)
#iptables -A INPUT -s 10.0.100.15 -m mac --mac-source 94:39:e5:af:1b:c7 -p all -i eth3 -j
DROP
#iptables -A INPUT -s 135.24.1.254 -m mac --mac-source 00:13:46:3B:02:E1 -p all -i eth2 -j
ACCEPT
#iptables -A INPUT -s 135.24.1.254 -m mac --mac-source 00:13:46:3B:02:E1 -p all -i eth5 -j
ACCEPT
#iptables -A INPUT -s 135.24.1.254 -m mac --mac-source 00:13:46:3B:02:E1 -p all -i eth6 -j
ACCEPT
#iptables -A INPUT -s 135.24.1.254 -m mac --mac-source 00:13:46:3B:02:E1 -p all -i eth7 -j
ACCEPT
#iptables -A INPUT -s 135.24.1.254 -m mac --mac-source 00:13:46:3B:02:E1 -p all -i eth8 -j
ACCEPT
#iptables -A INPUT -s 135.24.1.254 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
#iptables -A FORWARD -s 135.24.1.254 -m mac --mac-source 00:13:46:3B:02:E1 -i eth0 -j
ACCEPT
#iptables -A FORWARD -s 135.24.1.254 -m mac --mac-source 00:13:46:3B:02:E1 -i eth5 -j
ACCEPT
#iptables -A OUTPUT -d 10.0.100.15 -o eth3 -j DROP
#iptables -A FORWARD -d 135.24.1.254 -o eth0 -j ACCEPT



#################
#  BLOK MAC ADDRESS  #
#################



#iptables -A INPUT -m mac --mac-source 00:23:cd:1e:43:73 -j DROP
#iptables -A FORWARD -p tcp -m mac --mac-source 00:23:cd:1e:43:73 -j DROP



#iptables -A INPUT -m mac --mac-source 00:02:6f:47:1d:f8 -j DROP
#iptables -A FORWARD -p tcp -m mac --mac-source 00:02:6f:47:1d:f8 -j DROP



###############
# FORWARD CHAIN  #
###############
#iptables -P FORWARD DROP
#iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
#iptables -A FORWARD -s 202.62.22.111 -i eth2 -j ACCEPT
#iptables -A FORWARD -d 202.62.22.111 -i eth2 -j ACCEPT
#iptables -A FORWARD -s 202.62.22.196 -j ACCEPT
#iptables -A FORWARD -d 202.62.22.196 -j ACCEPT
#iptables -A FORWARD -s 10.4.18.254 -j ACCEPT
#iptables -A FORWARD -d 10.4.18.254 -j ACCEPT
iptables -A FORWARD -p udp --sport 69 -j DROP
iptables -A FORWARD -p udp --dport 69 -j DROP
iptables -A FORWARD -p tcp --sport 135 -j DROP
iptables -A FORWARD -p tcp --dport 135 -j DROP
iptables -A FORWARD -p udp --sport 137 -j DROP
iptables -A FORWARD -p udp --dport 137 -j DROP
iptables -A FORWARD -p udp --sport 138 -j DROP
iptables -A FORWARD -p udp --dport 138 -j DROP
iptables -A FORWARD -p tcp --sport 139 -j DROP
iptables -A FORWARD -p tcp --dport 139 -j DROP
```

```
iptables -A FORWARD -p tcp --sport 445 -j DROP
iptables -A FORWARD -p tcp --dport 445 -j DROP
iptables -A FORWARD -p tcp --sport 593 -j DROP
iptables -A FORWARD -p tcp --dport 593 -j DROP
iptables -A FORWARD -p tcp --sport 4444 -j DROP
iptables -A FORWARD -p tcp --dport 4444 -j DROP
iptables -A FORWARD -p tcp --dport 6660 -j DROP
iptables -A FORWARD -p tcp --dport 6661 -j DROP
iptables -A FORWARD -p tcp --dport 6662 -j DROP
iptables -A FORWARD -p tcp --dport 6663 -j DROP
iptables -A FORWARD -p tcp --dport 6664 -j DROP
iptables -A FORWARD -p tcp --dport 6665 -j DROP
iptables -A FORWARD -p tcp --dport 6668 -j DROP
iptables -A FORWARD -p tcp --dport 7000 -j DROP
iptables -A FORWARD -p tcp --dport 7001 -j DROP
iptables -A FORWARD -p tcp --dport 7002 -j DROP




###################################
#IP yang di izinkan tapi tidak boleh menggunakan DDL#
###################################



#for port in  6346:6348 gnutella-svc
#do
#iptables -A FORWARD -s 172.17.10.1/24 -p tcp -i eth1 --dport $port -j DROP
#iptables -A FORWARD -s 172.17.20.254/27 -p tcp -i eth2 --dport $port -j DROP
#iptables -A FORWARD -s 172.17.30.254/27 -p tcp -i eth3 --sport $port -j DROP
#iptables -A FORWARD -s 172.17.40.254/27 -p tcp -i eth4 --sport $port -j DROP
#iptables -A FORWARD -s 172.17.50.254/27 -p tcp -i eth5 --sport $port -j DROP
#done



###############
#  Transparent Proxy  #
###############
#iptables -t nat -A PREROUTING -s 10.0.222.1/27 -i eth3 -p tcp --dport 80 -j REDIRECT
--to-port 3128
#iptables -t nat -A PREROUTING -s 172.17.20.254/27 -i eth2 -p tcp --dport 80 -j REDIRECT
--to-port 3128
#iptables -t nat -A PREROUTING -s 172.17.30.254/27 -i eth3 -p tcp --dport 80 -j REDIRECT
--to-port 3128
```

```
#iptables -t nat -A PREROUTING -s 172.17.40.254/27 -i eth4 -p tcp --dport 80 -j REDIRECT
--to-port 3128
#iptables -t nat -A PREROUTING -s 172.17.50.254/27 -i eth5 -p tcp --dport 80 -j REDIRECT
--to-port 3128
#iptables -t nat -A PREROUTING -s 118.98.218.1/29 -i eth0 -p tcp --dport 80 -j REDIRECT
--to-port 3128



# File Log Book atau catatan tentang sesuatu yang masuk lewat eth1 (Link Internux)
# iptables -A INPUT -i eth1 -j LOG --log-level 5
# iptables -A INPUT -i eth0 -j LOG --log-level 5



##########################################
#                                IP TABLES FOR PPPOE                                #
##########################################



##!/bin/sh



#PATH=/usr/sbin:/sbin:/bin:/usr/bin



## Init table FILTER
#iptables -t filter -F #Flush table
#iptables -t filter -X #Delete personal chains
#iptables -t filter -Z #Idem
#iptables -t filter -P INPUT DROP #Default Rule
#iptables -t filter -P FORWARD DROP #Default Rule
#iptables -t filter -P OUTPUT ACCEPT #Default Rule



## Init table NAT
#iptables -t nat -F
#iptables -t nat -X
#iptables -t nat -Z
#iptables -t nat -P PREROUTING ACCEPT
#iptables -t nat -P OUTPUT ACCEPT
#iptables -t nat -P POSTROUTING ACCEPT
```

```
## Init table MANGLE
#iptables -t mangle -F
#iptables -t mangle -X
#iptables -t mangle -Z
#iptables -t mangle -P PREROUTING ACCEPT
#iptables -t mangle -P INPUT ACCEPT
#iptables -t mangle -P OUTPUT ACCEPT
#iptables -t mangle -P FORWARD ACCEPT
#iptables -t mangle -P POSTROUTING ACCEPT


## Accept everything on localhost
#iptables -t filter -A INPUT -i lo -j ACCEPT
#iptables -t filter -A OUTPUT -o lo -j ACCEPT


## Allow everything from local network
#iptables -t filter -A INPUT -s 192.168.25.0/24 -j ACCEPT


## Allow navigation from linux box
#iptables -t filter -A INPUT -i ppp0 -m state –state ESTABLISHED -j ACCEPT
#iptables -t filter -A OUTPUT -o ppp0 -m state –state NEW,ESTABLISHED -j ACCEPT


## NAT local network to internet
#iptables -t filter -A FORWARD -i ppp0 -o eth0 -m state –state ESTABLISHED,RELATED -j
ACCEPT
#iptables -t filter -A FORWARD -i eth0 -o ppp0 -j ACCEPT
#iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE


## Allow SSH on port 443
#iptables -t filter -I INPUT -p tcp –dport 443 -j ACCEPT


## Enable routing
#echo 1 > /proc/sys/net/ipv4/ip_forward
```

##

By : Aliansyah - TKJ CLUB MAKASAR