KJK-Projek

Router Debian

Firewall (Debian)

Setup awal

```
apt update
apt install iptables-persistent
```

Hasil Uji coba

```
Setting up iptables-persistent (1.0.23) ...
root@Firewall:~# ip route show
default via 192.168.122.1 dev eth0 metric 2096
192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.1
192.168.2.0/24 dev eth2 proto kernel scope link src 192.168.2.1
192.168.3.0/24 dev eth3 proto kernel scope link src 192.168.3.1
192.168.4.0/24 dev eth4 proto kernel scope link src 192.168.4.1
192.168.5.0/24 dev eth5 proto kernel scope link src 192.168.5.1
192.168.6.0/24 via 192.168.2.2 dev eth2
192.168.7.0/24 via 192.168.3.2 dev eth3
192.168.8.0/24 via 192.168.4.2 dev eth4
192.168.9.0/24 via 192.168.5.2 dev eth5
192.168.122.0/24 dev eth0 proto kernel scope link src 192.168.122.83
root@Firewall:~#
```

```
#
# This is a sample network config, please uncomment lines to configure th
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# DHCP config for eth0
auto eth0
iface eth0 inet dhcp
up echo nameserver 192.168.122.1 > /etc/resolv.conf

# Static config for eth1
auto eth1
iface eth1 inet static
        address 192.168.1.1
        netmask 255.255.255.0

# Static config for eth2
auto eth2
iface eth2 inet static
        address 192.168.2.1
        netmask 255.255.255.0


# Static config for eth3
auto eth3
iface eth3 inet static
        address 192.168.3.1
        netmask 255.255.255.0

# Static config for eth4
auto eth4
iface eth4 inet static
        address 192.168.4.1
        netmask 255.255.255.0


# Static config for eth5
auto eth5
iface eth5 inet static
        address 192.168.5.1
        netmask 255.255.255.0
```

Router Mahasiswa

```
#
# This is a sample network config, please uncomment lines to configure th
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
        address 192.168.2.2
        netmask 255.255.255.0
        gateway 192.168.2.1
        up echo nameserver 192.168.122.1 > /etc/resolv.conf

# Static config for eth1
auto eth1
iface eth1 inet static
        address 192.168.6.1
        netmask 255.255.255.0
```

Router Akademik

```
#
# This is a sample network config, please uncomment lines to configure th
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
```

```
auto eth0
iface eth0 inet static
        address 192.168.3.2
        netmask 255.255.255.0
        gateway 192.168.3.1
        up echo nameserver 192.168.122.1 > /etc/resolv.conf

# Static config for eth1
auto eth1
iface eth1 inet static
        address 192.168.7.1
        netmask 255.255.255.0
```

Admin

```
#
# This is a sample network config, please uncomment lines to configure th
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
        address 192.168.1.2
        netmask 255.255.255.0
        gateway 192.168.1.1
        up echo nameserver 192.168.122.1 > /etc/resolv.conf

```

Router riset

```
#
# This is a sample network config, please uncomment lines to configure th
#
```

```

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
        address 192.168.4.2
        netmask 255.255.255.0
        gateway 192.168.4.1
        up echo nameserver 192.168.122.1 > /etc/resolv.conf


# Static config for eth1
auto eth1
iface eth1 inet static
        address 192.168.8.1
        netmask 255.255.255.0
```

Router Guest

```
#
# This is a sample network config, please uncomment lines to configure t
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
        address 192.168.5.2
        netmask 255.255.255.0
        gateway 192.168.5.1
        up echo nameserver 192.168.122.1 > /etc/resolv.conf


# Static config for eth1
auto eth1
iface eth1 inet static
        address 192.168.9.1
        netmask 255.255.255.0
```

Client

MHS 1

```
#
# This is a sample network config, please uncomment lines to configure tl
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
        address 192.168.6.2
        netmask 255.255.255.0
        gateway 192.168.6.1
        up echo nameserver 192.168.122.1 > /etc/resolv.conf

```

MHS 2

```
#
# This is a sample network config, please uncomment lines to configure tl
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
        address 192.168.6.3
        netmask 255.255.255.0
        gateway 192.168.6.1
        up echo nameserver 192.168.122.1 > /etc/resolv.conf

```

Akademik 1

```
#
# This is a sample network config, please uncomment lines to configure th
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
        address 192.168.7.2
        netmask 255.255.255.0
        gateway 192.168.7.1
        up echo nameserver 192.168.122.1 > /etc/resolv.conf


```

Akademik 2

```
#
# This is a sample network config, please uncomment lines to configure th
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
        address 192.168.7.3
        netmask 255.255.255.0
        gateway 192.168.7.1
        up echo nameserver 192.168.122.1 > /etc/resolv.conf

```

Riset 1

```
#
# This is a sample network config, please uncomment lines to configure th
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
        address 192.168.8.2
        netmask 255.255.255.0
        gateway 192.168.8.1
        up echo nameserver 192.168.122.1 > /etc/resolv.conf
```

Riset 2

```
#
# This is a sample network config, please uncomment lines to configure th
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
        address 192.168.8.3
        netmask 255.255.255.0
        gateway 192.168.8.1
        up echo nameserver 192.168.122.1 > /etc/resolv.conf
```

Guest 1

```
#
# This is a sample network config, please uncomment lines to configure t
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
        address 192.168.9.2
        netmask 255.255.255.0
        gateway 192.168.9.1
        up echo nameserver 192.168.122.1 > /etc/resolv.conf
```

Guest 2

```
#
# This is a sample network config, please uncomment lines to configure t
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
        address 192.168.9.2
        netmask 255.255.255.0
        gateway 192.168.9.1
        up echo nameserver 192.168.122.1 > /etc/resolv.conf
```

Bandit 1

```
#
# This is a sample network config, please uncomment lines to configure th
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*


# DHCP config for eth0
auto eth0
iface eth0 inet dhcp
        up echo nameserver 192.168.0.1 > /etc/resolv.conf

```

Bandit 2

```
#
# This is a sample network config, please uncomment lines to configure th
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
auto eth0
iface eth0 inet static
        address 192.168.6.3
        netmask 255.255.255.0
        gateway 192.168.6.1
        up echo nameserver 192.168.122.1 > /etc/resolv.conf
```

Scripting

Firewall

```
root@Firewall:~# ls
firewall.sh  iptables-rules.txt
root@Firewall:~# cat firewall.sh
#!/bin/sh

WAN="eth0"
ADM="eth1"
MHS="eth2"
AKD="eth3"
RST="eth4"
GST="eth5"

# 1. Atur kebijakan default
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT # Izinkan trafik keluar dari firewall itu sendi

# 2. Izinkan koneksi yang sudah ada/terkait
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# 3. Aktifkan NAT (Masquerading) untuk semua yang keluar ke WAN
iptables -t nat -A POSTROUTING -o $WAN -j MASQUERADE

# ====== ATURAN ZONA GUEST (GST) ======
# Izinkan GST -> WAN (Hanya Web & DNS)
iptables -A FORWARD -i $GST -o $WAN -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -i $GST -o $WAN -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -i $GST -o $WAN -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i $GST -o $WAN -p tcp --dport 443 -j ACCEPT
# (Trafik GST ke zona internal lain otomatis di-DROP oleh kebijakan defau

# ====== ATURAN ZONA MAHASISWA (MHS) ======
# Izinkan MHS -> WAN (Hanya Web & DNS)
iptables -A FORWARD -i $MHS -o $WAN -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -i $MHS -o $WAN -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -i $MHS -o $WAN -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i $MHS -o $WAN -p tcp --dport 443 -j ACCEPT
# Izinkan MHS -> AKD (Hanya Web)
iptables -A FORWARD -i $MHS -o $AKD -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i $MHS -o $AKD -p tcp --dport 443 -j ACCEPT

# ====== ATURAN ZONA AKADEMIK (AKD) ======
# Izinkan AKD -> WAN (Semua)
iptables -A FORWARD -i $AKD -o $WAN -j ACCEPT
# Izinkan AKD -> MHS (Semua)
iptables -A FORWARD -i $AKD -o $MHS -j ACCEPT

# ====== ATURAN ZONA RISET (RST) ======
# Izinkan RST -> WAN (Semua)
iptables -A FORWARD -i $RST -o $WAN -j ACCEPT
# (Trafik RST ke zona internal lain otomatis di-DROP)

# ====== ATURAN ZONA ADMIN (ADM) ======
# Izinkan ADM -> SEMUA ZONA (Termasuk WAN)
iptables -A FORWARD -i $ADM -j ACCEPT

# Izinkan Ping (ICMP) dari semua zona internal (opsional, untuk tes)
iptables -A INPUT -i $ADM -p icmp -j ACCEPT
iptables -A INPUT -i $MHS -p icmp -j ACCEPT
iptables -A INPUT -i $AKD -p icmp -j ACCEPT
iptables -A INPUT -i $RST -p icmp -j ACCEPT
# (Kita sengaja tidak izinkan GUEST ping ke firewall)

# Izinkan SSH & HTTPS HANYA dari zona ADM
iptables -A INPUT -i $ADM -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -i $ADM -p tcp --dport 443 -j ACCEPT

# Izinkan loopback (penting untuk internal OS)
iptables -A INPUT -i lo -j ACCEPT


root@Firewall:~#
```

Firewall-Rev1

```
#!/bin/bash
set -euo pipefail

# ================== Interface & Subnet (192.168.x.x) ==================
WAN_IF="eth0"
ADM_IF="eth1"; ADM_NET="192.168.1.0/24"
MHS_IF="eth2"; MHS_NET="192.168.2.0/24"
AKD_IF="eth3"; AKD_NET="192.168.3.0/24"
RST_IF="eth4"; RST_NET="192.168.4.0/24"
GST_IF="eth5"; GST_NET="192.168.5.0/24"

```

```
# Service ports
WEB_PORTS="80,443"
DNS_PORT=53

# ================== Sistem & Reset ==================
echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -F; iptables -t mangle -F; iptables -F; iptables -X
iptables -P INPUT DROP; iptables -P FORWARD DROP; iptables -P OUTPUT ACC

# ================== Chains utilitas ==================
iptables -N LOG_DROP
iptables -A LOG_DROP -m limit --limit 5/min -j LOG --log-prefix "DROP "
iptables -A LOG_DROP -j DROP

# ================== Basic hygiene ==================
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -m state --state INVALID -j LOG --log-prefix "INVALID
iptables -A INPUT -m state --state INVALID -j DROP
iptables -A FORWARD -m state --state INVALID -j DROP

# ================== Anti-spoofing ==================
for NET in 192.168.0.0/16 10.0.0.0/8 172.16.0.0/12 127.0.0.0/8 169.254.0
  iptables -A INPUT -i "$WAN_IF" -s "$NET" -j LOG --log-prefix "SPOOF WA
  iptables -A INPUT -i "$WAN_IF" -s "$NET" -j DROP
  iptables -A FORWARD -i "$WAN_IF" -s "$NET" -j DROP
done

# Lateral anti-spoof
iptables -A INPUT -i "$ADM_IF" -s "$ADM_NET" -j ACCEPT
iptables -A INPUT -i "$ADM_IF" ! -s "$ADM_NET" -j DROP
iptables -A INPUT -i "$MHS_IF" -s "$MHS_NET" -j ACCEPT
iptables -A INPUT -i "$MHS_IF" ! -s "$MHS_NET" -j DROP
iptables -A INPUT -i "$AKD_IF" -s "$AKD_NET" -j ACCEPT
iptables -A INPUT -i "$AKD_IF" ! -s "$AKD_NET" -j DROP
iptables -A INPUT -i "$RST_IF" -s "$RST_NET" -j ACCEPT
iptables -A INPUT -i "$RST_IF" ! -s "$RST_NET" -j DROP
iptables -A INPUT -i "$GST_IF" -s "$GST_NET" -j ACCEPT
iptables -A INPUT -i "$GST_IF" ! -s "$GST_NET" -j DROP

# ================== NAT Masquerading ==================
iptables -t nat -A POSTROUTING -o "$WAN_IF" -j MASQUERADE

# ================== ICMP FIX: Outbound & Reply ==================
# Izinkan ICMP outbound dari SEMUA zona internal ke WAN
iptables -A FORWARD -i "$ADM_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$AKD_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r

# Izinkan ICMP reply kembali (echo-reply dari WAN ke internal)
iptables -A FORWARD -i "$WAN_IF" -o "$ADM_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$WAN_IF" -o "$MHS_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$WAN_IF" -o "$AKD_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$WAN_IF" -o "$RST_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$WAN_IF" -o "$GST_IF" -p icmp --icmp-type echo-r

# Rate limit ICMP ke firewall (anti-ICMP flood)
iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/se
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

# ================== TCP/UDP Rules (Existing) ==================
# ADMIN -> semua
iptables -A FORWARD -i "$ADM_IF" -j ACCEPT

# MAHASISWA -> Internet (HTTP/HTTPS/DNS)
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp -m multiport --dpor
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j

# AKADEMIK -> Internet (full)
iptables -A FORWARD -i "$AKD_IF" -o "$WAN_IF" -j ACCEPT

# AKADEMIK -> Riset (full)
iptables -A FORWARD -i "$AKD_IF" -o "$RST_IF" -j ACCEPT

# RISET/IoT -> Internet (HTTPS only)
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport 443 -j ACCE
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j

# RISET/IoT -> Admin (monitoring ports)
iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p udp --dport 514 -j ACCE
iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p tcp -m multiport --dpor

# RISET/IoT -> Akademik (full)
iptables -A FORWARD -i "$RST_IF" -o "$AKD_IF" -j ACCEPT

# GUEST -> Internet (HTTP/HTTPS/DNS)
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp -m multiport --dpor
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j

# SSH brute-force protection
iptables -N SSHSCAN
iptables -A INPUT -i "$ADM_IF" -p tcp --dport 22 -m state --state NEW -j
iptables -A SSHSCAN -m recent --set --name SSH --rsource
iptables -A SSHSCAN -m recent --update --seconds 60 --hitcount 4 --name
iptables -A SSHSCAN -m recent --update --seconds 60 --hitcount 4 --name
iptables -A INPUT -i "$ADM_IF" -p tcp --dport 22 -j ACCEPT

# ================== Logging drops ==================
iptables -A INPUT -j LOG_DROP
iptables -A FORWARD -j LOG_DROP

```

Firewall Rev-2 (Routing mahasiswa bisa ke jalur Riset)

```
#!/bin/bash
set -euo pipefail

# ================== Interface & Subnet (192.168.x.x) ==================
WAN_IF="eth0"
ADM_IF="eth1"; ADM_NET="192.168.1.0/24"
MHS_IF="eth2"; MHS_NET="192.168.2.0/24"
AKD_IF="eth3"; AKD_NET="192.168.3.0/24"
RST_IF="eth4"; RST_NET="192.168.4.0/24"
GST_IF="eth5"; GST_NET="192.168.5.0/24"

# LAB subnet spesifik (dalam zona Riset)
LAB_NET="192.168.8.0/24"  # Riset3 sebagai Lab
LAB_ROUTER_IP="192.168.8.4"  # Router Riset

# Service ports
WEB_PORTS="80,443"
DNS_PORT=53
LAB_PORTS="22,80,443"  # SSH, HTTP, HTTPS untuk lab access

# ================== Sistem & Reset ==================
echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -F; iptables -t mangle -F; iptables -F; iptables -X
iptables -P INPUT DROP; iptables -P FORWARD DROP; iptables -P OUTPUT ACC

# ================== Chains utilitas ==================
iptables -N LOG_DROP
iptables -A LOG_DROP -m limit --limit 5/min -j LOG --log-prefix "DROP "
iptables -A LOG_DROP -j DROP

# ================== Basic hygiene ==================
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -m state --state INVALID -j LOG --log-prefix "INVALID
iptables -A INPUT -m state --state INVALID -j DROP
iptables -A FORWARD -m state --state INVALID -j DROP

# ================== Anti-spoofing ==================
for NET in 192.168.0.0/16 10.0.0.0/8 172.16.0.0/12 127.0.0.0/8 169.254.0
  iptables -A INPUT -i "$WAN_IF" -s "$NET" -j LOG --log-prefix "SPOOF WA
  iptables -A INPUT -i "$WAN_IF" -s "$NET" -j DROP
  iptables -A FORWARD -i "$WAN_IF" -s "$NET" -j DROP
done

# Lateral anti-spoof
iptables -A INPUT -i "$ADM_IF" -s "$ADM_NET" -j ACCEPT
iptables -A INPUT -i "$ADM_IF" ! -s "$ADM_NET" -j DROP
iptables -A INPUT -i "$MHS_IF" -s "$MHS_NET" -j ACCEPT
iptables -A INPUT -i "$MHS_IF" ! -s "$MHS_NET" -j DROP
iptables -A INPUT -i "$AKD_IF" -s "$AKD_NET" -j ACCEPT
iptables -A INPUT -i "$AKD_IF" ! -s "$AKD_NET" -j DROP
iptables -A INPUT -i "$RST_IF" -s "$RST_NET" -j ACCEPT
iptables -A INPUT -i "$RST_IF" ! -s "$RST_NET" -j DROP
iptables -A INPUT -i "$GST_IF" -s "$GST_NET" -j ACCEPT
iptables -A INPUT -i "$GST_IF" ! -s "$GST_NET" -j DROP

# ================== NAT Masquerading ==================
iptables -t nat -A POSTROUTING -o "$WAN_IF" -j MASQUERADE

# ================== ICMP FIX: Outbound & Reply ==================
# Izinkan ICMP outbound dari SEMUA zona internal ke WAN
iptables -A FORWARD -i "$ADM_IF" -o "$WAN_IF" -p icmp --icmp-type echo-re
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p icmp --icmp-type echo-re
iptables -A FORWARD -i "$AKD_IF" -o "$WAN_IF" -p icmp --icmp-type echo-re
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-re
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-re

# Izinkan ICMP reply kembali
iptables -A FORWARD -i "$WAN_IF" -o "$ADM_IF" -p icmp --icmp-type echo-re
iptables -A FORWARD -i "$WAN_IF" -o "$MHS_IF" -p icmp --icmp-type echo-re
iptables -A FORWARD -i "$WAN_IF" -o "$AKD_IF" -p icmp --icmp-type echo-re
iptables -A FORWARD -i "$WAN_IF" -o "$RST_IF" -p icmp --icmp-type echo-re
iptables -A FORWARD -i "$WAN_IF" -o "$GST_IF" -p icmp --icmp-type echo-re

# Rate limit ICMP ke firewall
iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/se
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

# ================== KEBIJAKAN LAB (Riset3) ==================

# MAHASISWA -> Lab (LIMITED: SSH, HTTP, HTTPS, Ping)
iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d "$LAB_NET" -p tcp -m mul
iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d "$LAB_NET" -p icmp --ic

# AKADEMIK -> Lab (FULL access)
iptables -A FORWARD -i "$AKD_IF" -o "$RST_IF" -d "$LAB_NET" -j ACCEPT

# ADMIN -> Lab (FULL access, sudah diatur di bawah)

# Lab -> Internet (HTTPS+DNS) - sama seperti RST
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport 443 -j ACCE
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j

# Lab -> Admin (monitoring ports)
iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p udp --dport 514 -j ACCE
iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p tcp -m multiport --dpor

# Lab -> Akademik (FULL)
iptables -A FORWARD -i "$RST_IF" -o "$AKD_IF" -j ACCEPT

# ================== KEBIJAKAN ZONA LAIN (TETAP SAMA) ==================

# ADMIN -> semua
iptables -A FORWARD -i "$ADM_IF" -j ACCEPT

# MAHASISWA -> Internet (HTTP/HTTPS/DNS)
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp -m multiport --dpor
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j

# AKADEMIK -> Internet (full)
iptables -A FORWARD -i "$AKD_IF" -o "$WAN_IF" -j ACCEPT

# AKADEMIK -> Riset (full)
iptables -A FORWARD -i "$AKD_IF" -o "$RST_IF" -j ACCEPT

# RISET/IoT -> Internet (HTTPS+DNS)
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport 443 -j ACCE
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j

# RISET/IoT -> Admin (monitoring)
iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p udp --dport 514 -j ACCE
iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p tcp -m multiport --dpor
```

```

# RISET/IoT -> Akademik (full)
iptables -A FORWARD -i "$RST_IF" -o "$AKD_IF" -j ACCEPT

# GUEST -> Internet (HTTP/HTTPS/DNS)
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp -m multiport --dpor
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -

# SSH brute-force protection
iptables -N SSHSCAN
iptables -A INPUT -i "$ADM_IF" -p tcp --dport 22 -m state --state NEW -j
iptables -A SSHSCAN -m recent --set --name SSH --rsource
iptables -A SSHSCAN -m recent --update --seconds 60 --hitcount 4 --name
iptables -A SSHSCAN -m recent --update --seconds 60 --hitcount 4 --name
iptables -A INPUT -i "$ADM_IF" -p tcp --dport 22 -j ACCEPT

# ================= Logging drops =================
iptables -A INPUT -j LOG_DROP
iptables -A FORWARD -j LOG_DROP

echo "Firewall zone-based with Lab access (Riset3) activated."
```

Firewall Rev-3

```
#!/bin/bash
set -euo pipefail

# ================= Interface & Subnet (192.168.x.x) =================
WAN_IF="eth0"
ADM_IF="eth1"; ADM_NET="192.168.1.0/24"
MHS_IF="eth2"; MHS_NET="192.168.2.0/24"
AKD_IF="eth3"; AKD_NET="192.168.3.0/24"
RST_IF="eth4"; RST_NET="192.168.4.0/24"
GST_IF="eth5"; GST_NET="192.168.5.0/24"

# LAB host spesifik (hanya 192.168.8.4)
LAB_HOST="192.168.8.4"  # Riset3 sebagai Lab
BLOCKED_HOSTS="192.168.8.2,192.168.8.3"  # Host yang diblokir untuk Maha

# Service ports
WEB_PORTS="80,443"
DNS_PORT=53
LAB_PORTS="22,80,443"  # SSH, HTTP, HTTPS untuk lab access

```

```
# ================== Sistem & Reset ==================
echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -F; iptables -t mangle -F; iptables -F; iptables -X
iptables -P INPUT DROP; iptables -P FORWARD DROP; iptables -P OUTPUT ACC

# ================== Chains utilitas ==================
iptables -N LOG_DROP
iptables -A LOG_DROP -m limit --limit 5/min -j LOG --log-prefix "DROP "
iptables -A LOG_DROP -j DROP

# ================== Basic hygiene ==================
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -m state --state INVALID -j LOG --log-prefix "INVALID
iptables -A INPUT -m state --state INVALID -j DROP
iptables -A FORWARD -m state --state INVALID -j DROP

# ================== Anti-spoofing ==================
for NET in 192.168.0.0/16 10.0.0.0/8 172.16.0.0/12 127.0.0.0/8 169.254.0
  iptables -A INPUT -i "$WAN_IF" -s "$NET" -j LOG --log-prefix "SPOOF WA
  iptables -A INPUT -i "$WAN_IF" -s "$NET" -j DROP
  iptables -A FORWARD -i "$WAN_IF" -s "$NET" -j DROP
done

# Lateral anti-spoof
iptables -A INPUT -i "$ADM_IF" -s "$ADM_NET" -j ACCEPT
iptables -A INPUT -i "$ADM_IF" ! -s "$ADM_NET" -j DROP
iptables -A INPUT -i "$MHS_IF" -s "$MHS_NET" -j ACCEPT
iptables -A INPUT -i "$MHS_IF" ! -s "$MHS_NET" -j DROP
iptables -A INPUT -i "$AKD_IF" -s "$AKD_NET" -j ACCEPT
iptables -A INPUT -i "$AKD_IF" ! -s "$AKD_NET" -j DROP
iptables -A INPUT -i "$RST_IF" -s "$RST_NET" -j ACCEPT
iptables -A INPUT -i "$RST_IF" ! -s "$RST_NET" -j DROP
iptables -A INPUT -i "$GST_IF" -s "$GST_NET" -j ACCEPT
iptables -A INPUT -i "$GST_IF" ! -s "$GST_NET" -j DROP

# ================== NAT Masquerading ==================
iptables -t nat -A POSTROUTING -o "$WAN_IF" -j MASQUERADE

# ================== ICMP FIX: Outbound & Reply ==================
# Izinkan ICMP outbound dari SEMUA zona internal ke WAN
iptables -A FORWARD -i "$ADM_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$AKD_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r

```

```
# Izinkan ICMP reply kembali
iptables -A FORWARD -i "$WAN_IF" -o "$ADM_IF" -p icmp --icmp-type echo-re
iptables -A FORWARD -i "$WAN_IF" -o "$MHS_IF" -p icmp --icmp-type echo-re
iptables -A FORWARD -i "$WAN_IF" -o "$AKD_IF" -p icmp --icmp-type echo-re
iptables -A FORWARD -i "$WAN_IF" -o "$RST_IF" -p icmp --icmp-type echo-re
iptables -A FORWARD -i "$WAN_IF" -o "$GST_IF" -p icmp --icmp-type echo-re

# Rate limit ICMP ke firewall
iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/sec
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

# ================== KEBIJAKAN LAB (Riset3) - HOST SPECIFIC ============

# BLOKIR Mahasiswa -> 192.168.8.2 dan 192.168.8.3
iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d 192.168.8.2 -j LOG --log
iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d 192.168.8.2 -j DROP
iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d 192.168.8.3 -j LOG --log
iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d 192.168.8.3 -j DROP

# IZINKAN Mahasiswa -> Lab 192.168.8.4 (LIMITED: SSH, HTTP, HTTPS, Ping)
iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d "$LAB_HOST" -p tcp -m mu
iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d "$LAB_HOST" -p icmp --ic

# AKADEMIK -> Lab (FULL access) - diatur di bawah via AKADEMIK->Riset
# ADMIN -> Lab (FULL access) - diatur di bawah via ADMIN->all

# ================== KEBIJAKAN ZONA LAIN (TETAP SAMA) ==================

# ADMIN -> semua
iptables -A FORWARD -i "$ADM_IF" -j ACCEPT

# MAHASISWA -> Internet (HTTP/HTTPS/DNS)
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp -m multiport --dport
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j

# AKADEMIK -> Internet (full)
iptables -A FORWARD -i "$AKD_IF" -o "$WAN_IF" -j ACCEPT

# AKADEMIK -> Riset (full)
iptables -A FORWARD -i "$AKD_IF" -o "$RST_IF" -j ACCEPT

# RISET/IoT -> Internet (HTTPS+DNS)
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport 443 -j ACCEP
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j

# RISET/IoT -> Admin (monitoring)
iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p udp --dport 514 -j ACCEP
iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p tcp -m multiport --dport

# RISET/IoT -> Akademik (full)
iptables -A FORWARD -i "$RST_IF" -o "$AKD_IF" -j ACCEPT

# GUEST -> Internet (HTTP/HTTPS/DNS)
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp -m multiport --dport
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j

# SSH brute-force protection
iptables -N SSHSCAN
iptables -A INPUT -i "$ADM_IF" -p tcp --dport 22 -m state --state NEW -j
iptables -A SSHSCAN -m recent --set --name SSH --rsource
iptables -A SSHSCAN -m recent --update --seconds 60 --hitcount 4 --name S
iptables -A SSHSCAN -m recent --update --seconds 60 --hitcount 4 --name S
iptables -A INPUT -i "$ADM_IF" -p tcp --dport 22 -j ACCEPT

# ================== Logging drops ==================
iptables -A INPUT -j LOG_DROP
iptables -A FORWARD -j LOG_DROP

echo "Firewall zone-based with Lab access (Riset3) activated."
```

Firewall (System logging,seperti IDS/IPS)

```
#!/bin/bash
set -euo pipefail

# ================== Interface & Subnet (192.168.x.x) ==================
WAN_IF="eth0"
ADM_IF="eth1"; ADM_NET="192.168.1.0/24"
MHS_IF="eth2"; MHS_NET="192.168.2.0/24"
AKD_IF="eth3"; AKD_NET="192.168.3.0/24"
RST_IF="eth4"; RST_NET="192.168.4.0/24"
GST_IF="eth5"; GST_NET="192.168.5.0/24"

# LAB host spesifik
LAB_HOST="192.168.8.4"
BLOCKED_HOSTS="192.168.8.2,192.168.8.3"

# Service ports
WEB_PORTS="80,443"
```

```
DNS_PORT=53
LAB_PORTS="22,80,443"

# ================== Sistem & Reset ==================
echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -F; iptables -t mangle -F; iptables -F; iptables -X
iptables -P INPUT DROP; iptables -P FORWARD DROP; iptables -P OUTPUT ACC

# ================== Chains utilitas ==================
iptables -N LOG_DROP
iptables -A LOG_DROP -m limit --limit 10/min -j LOG --log-prefix "DROP "
iptables -A LOG_DROP -j DROP

# Chain khusus untuk deteksi serangan
iptables -N ATTACK_DETECT
iptables -A ATTACK_DETECT -m limit --limit 5/min -j LOG --log-prefix "AT
iptables -A ATTACK_DETECT -j DROP

# ================== Basic hygiene ==================
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -m state --state INVALID -j LOG --log-prefix "INVALID_
iptables -A INPUT -m state --state INVALID -j DROP
iptables -A FORWARD -m state --state INVALID -j DROP

# ================== Anti-spoofing & Logging ==================
for NET in 192.168.0.0/16 10.0.0.0/8 172.16.0.0/12 127.0.0.0/8 169.254.0
  iptables -A INPUT -i "$WAN_IF" -s "$NET" -j LOG --log-prefix "SPOOF_AT
  iptables -A INPUT -i "$WAN_IF" -s "$NET" -j DROP
  iptables -A FORWARD -i "$WAN_IF" -s "$NET" -j DROP
done

# Lateral anti-spoof dengan logging
iptables -A INPUT -i "$ADM_IF" -s "$ADM_NET" -j ACCEPT
iptables -A INPUT -i "$ADM_IF" ! -s "$ADM_NET" -j LOG --log-prefix "SPOO
iptables -A INPUT -i "$ADM_IF" ! -s "$ADM_NET" -j DROP

iptables -A INPUT -i "$MHS_IF" -s "$MHS_NET" -j ACCEPT
iptables -A INPUT -i "$MHS_IF" ! -s "$MHS_NET" -j LOG --log-prefix "SPOO
iptables -A INPUT -i "$MHS_IF" ! -s "$MHS_NET" -j DROP

iptables -A INPUT -i "$AKD_IF" -s "$AKD_NET" -j ACCEPT
iptables -A INPUT -i "$AKD_IF" ! -s "$AKD_NET" -j LOG --log-prefix "SPOO
iptables -A INPUT -i "$AKD_IF" ! -s "$AKD_NET" -j DROP

iptables -A INPUT -i "$RST_IF" -s "$RST_NET" -j ACCEPT
iptables -A INPUT -i "$RST_IF" ! -s "$RST_NET" -j LOG --log-prefix "SPOO
iptables -A INPUT -i "$RST_IF" ! -s "$RST_NET" -j DROP

iptables -A INPUT -i "$GST_IF" -s "$GST_NET" -j ACCEPT
iptables -A INPUT -i "$GST_IF" ! -s "$GST_NET" -j LOG --log-prefix "SPOO
iptables -A INPUT -i "$GST_IF" ! -s "$GST_NET" -j DROP

# ================== NAT Masquerading ==================
iptables -t nat -A POSTROUTING -o "$WAN_IF" -j MASQUERADE

# ================== ICMP FIX & Logging ==================
# Izinkan ICMP outbound dan log percobaan flood
iptables -A FORWARD -i "$ADM_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$AKD_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r

# Izinkan ICMP reply
iptables -A FORWARD -i "$WAN_IF" -o "$ADM_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$WAN_IF" -o "$MHS_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$WAN_IF" -o "$AKD_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$WAN_IF" -o "$RST_IF" -p icmp --icmp-type echo-r
iptables -A FORWARD -i "$WAN_IF" -o "$GST_IF" -p icmp --icmp-type echo-r

# Rate limit ICMP ke firewall
iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/se
iptables -A INPUT -p icmp --icmp-type echo-request -j LOG --log-prefix "
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

# ================== PORT SCAN DETECTION ==================
# Deteksi NULL scan (TCP flags ALL NONE)
iptables -A INPUT -p tcp --tcp-flags ALL NONE -j LOG --log-prefix "NULL_
iptables -A INPUT -p tcp --tcp-flags ALL NONE -j ATTACK_DETECT

# Deteksi SYN-FIN scan (invalid combination)
iptables -A INPUT -p tcp --tcp-flags SYN,FIN SYN,FIN -j LOG --log-prefix
iptables -A INPUT -p tcp --tcp-flags SYN,FIN SYN,FIN -j ATTACK_DETECT

# Deteksi XMAS scan (FIN,URG,PSH)
iptables -A INPUT -p tcp --tcp-flags FIN,URG,PSH FIN,URG,PSH -j LOG --lo
iptables -A INPUT -p tcp --tcp-flags FIN,URG,PSH FIN,URG,PSH -j ATTACK_D

# ================== KEBIJAKAN LAB (Riset3) ==================

# BLOKIR Mahasiswa -> 192.168.8.2 dan 192.168.8.3 dengan logging
```

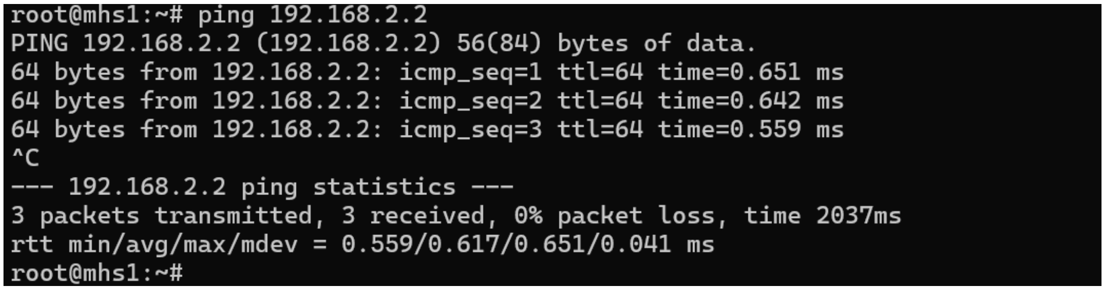
```
iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d 192.168.8.2 -j LOG --log
iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d 192.168.8.2 -j DROP
iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d 192.168.8.3 -j LOG --log
iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d 192.168.8.3 -j DROP

# IZINKAN Mahasiswa -> Lab 192.168.8.4 (LIMITED: SSH, HTTP, HTTPS, Ping)
iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d "$LAB_HOST" -p tcp -m mu
iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d "$LAB_HOST" -p icmp --i

# ================== KEBIJAKAN ZONA LAIN ==================

# ADMIN -> semua
iptables -A FORWARD -i "$ADM_IF" -j ACCEPT

# MAHASISWA -> Internet (HTTP/HTTPS/DNS) dengan rate limit
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp -m multiport --dport
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp -m multiport --dport
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp -m multiport --dport
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j
iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j

# AKADEMIK -> Internet (full)
iptables -A FORWARD -i "$AKD_IF" -o "$WAN_IF" -j ACCEPT

# AKADEMIK -> Riset (full)
iptables -A FORWARD -i "$AKD_IF" -o "$RST_IF" -j ACCEPT

# RISET/IoT -> Internet (HTTPS+DNS)
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport 443 -j ACCEP
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j
iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j

# RISET/IoT -> Admin (monitoring)
iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p udp --dport 514 -j ACCEP
iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p tcp -m multiport --dport

# RISET/IoT -> Akademik (full)
iptables -A FORWARD -i "$RST_IF" -o "$AKD_IF" -j ACCEPT

# GUEST -> Internet (HTTP/HTTPS/DNS) dengan rate limit ketat
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp -m multiport --dport
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp -m multiport --dport
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp -m multiport --dport
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j
iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j

# SSH brute-force protection dengan logging
iptables -N SSHSCAN
iptables -A INPUT -i "$ADM_IF" -p tcp --dport 22 -m state --state NEW -j
iptables -A SSHSCAN -m recent --set --name SSH --rsource
iptables -A SSHSCAN -m recent --update --seconds 60 --hitcount 4 --name
iptables -A SSHSCAN -m recent --update --seconds 60 --hitcount 4 --name
iptables -A INPUT -i "$ADM_IF" -p tcp --dport 22 -j ACCEPT

# ================== Logging drops ==================
iptables -A INPUT -j LOG_DROP
iptables -A FORWARD -j LOG_DROP

echo "Firewall IDS/IPS activated with comprehensive logging."

```

Cara uji coba

```
# Monitor semua serangan
tail -f /var/log/kern.log | grep "ATTACK\|BRUTE\|FLOOD\|SCAN\|BLOCK"

# Monitor per zona
tail -f /var/log/kern.log | grep "MHS->.*BLOCK"   # Mahasiswa mencoba akses ilegal
tail -f /var/log/kern.log | grep "GUEST_FLOOD"    # Guest flood internet
tail -f /var/log/kern.log | grep "SSH_BRUTE"      # Brute force SSH
tail -f /var/log/kern.log | grep "NULL_SCAN"      # Port scanning
```

Hasil Pengujian

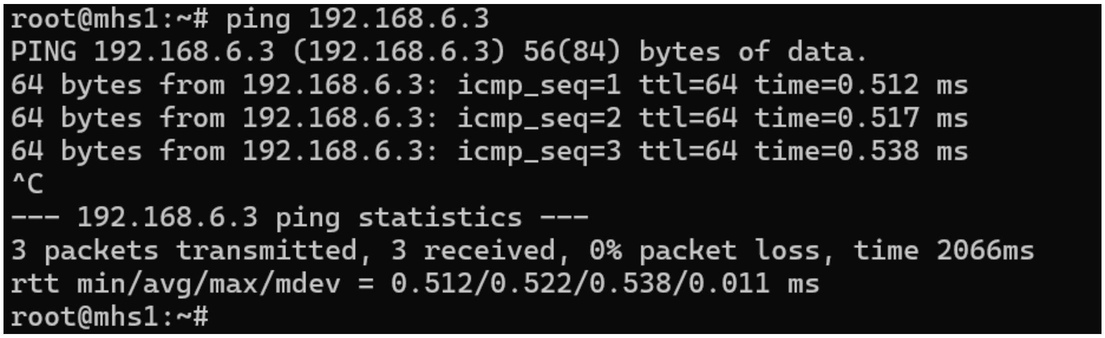
Client & Routern MHS



```
root@mhs1:~# ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=64 time=0.651 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=64 time=0.642 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=64 time=0.559 ms
^C
--- 192.168.2.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2037ms
rtt min/avg/max/mdev = 0.559/0.617/0.651/0.041 ms
root@mhs1:~#
```

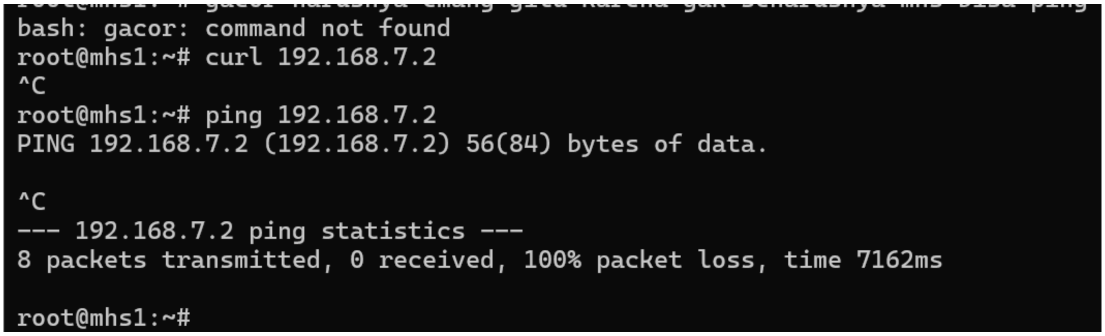
Client MHS1 ping ke routernya

Client MHS1 ping ke MHS lain



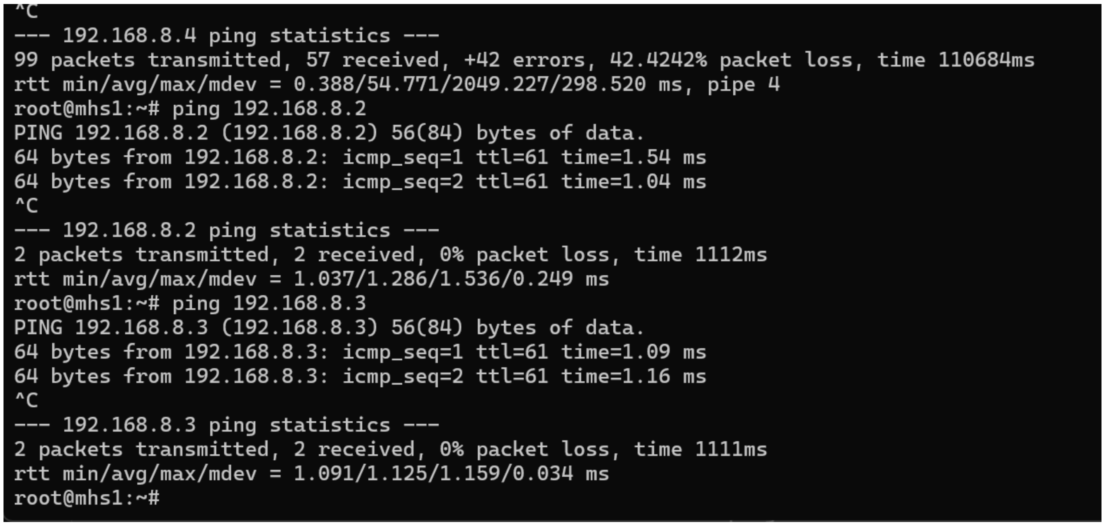
```
root@mhs1:~# ping 192.168.6.3
PING 192.168.6.3 (192.168.6.3) 56(84) bytes of data.
64 bytes from 192.168.6.3: icmp_seq=1 ttl=64 time=0.512 ms
64 bytes from 192.168.6.3: icmp_seq=2 ttl=64 time=0.517 ms
64 bytes from 192.168.6.3: icmp_seq=3 ttl=64 time=0.538 ms
^C
--- 192.168.6.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2066ms
rtt min/avg/max/mdev = 0.512/0.522/0.538/0.011 ms
root@mhs1:~#
```

Client MHS1 -> akademik



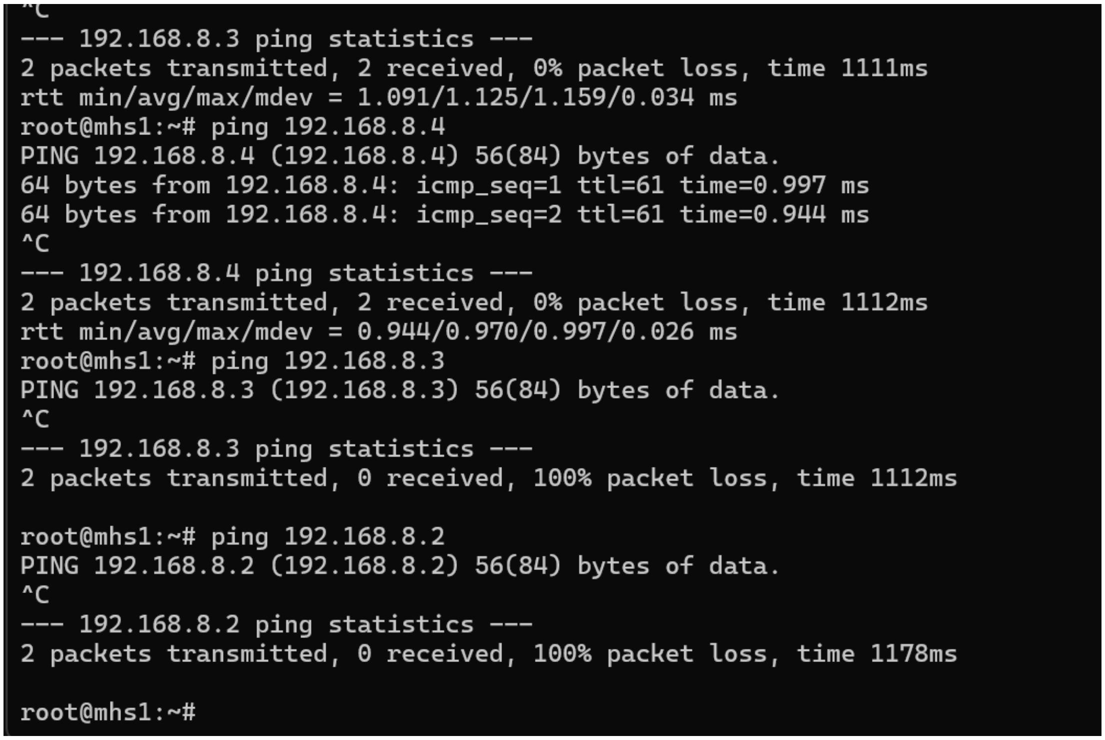
```
root@mhs1:~# gacor harusnya emang gitu karena gak seharusnya mhs bisa ping
bash: gacor: command not found
root@mhs1:~# curl 192.168.7.2
^C
root@mhs1:~# ping 192.168.7.2
PING 192.168.7.2 (192.168.7.2) 56(84) bytes of data.

^C
--- 192.168.7.2 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7162ms

root@mhs1:~#
```

Ini sudah benar karena tidak seharusnya mahasiswa dapat mengakses dari fitur2 atau benefit dari tendik/dosen



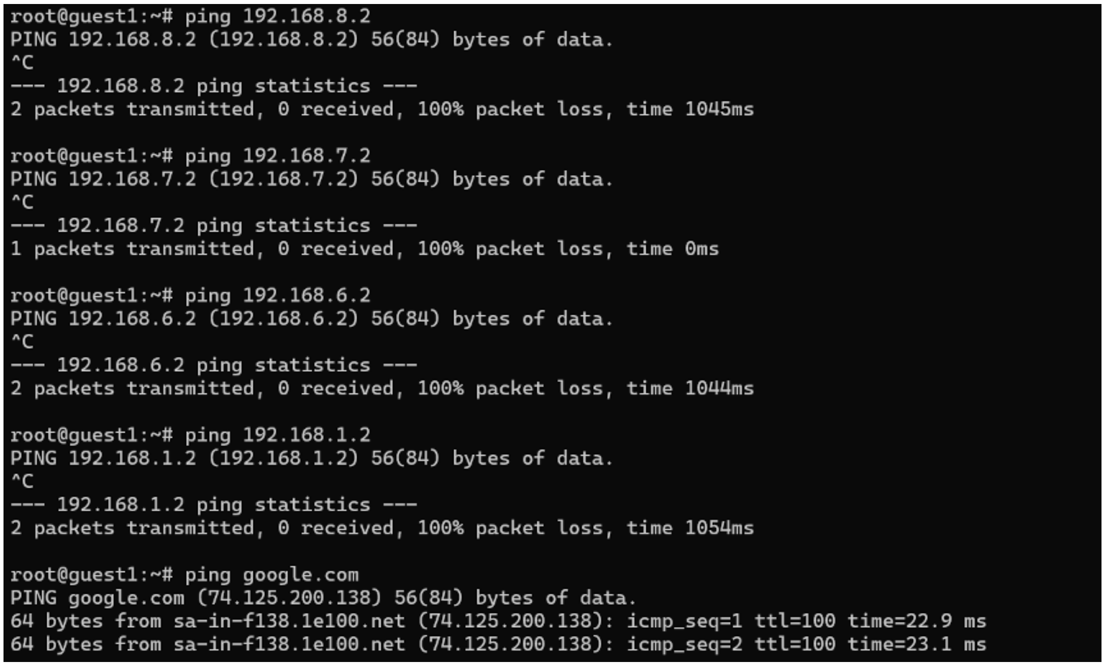
```
^C
--- 192.168.8.4 ping statistics ---
99 packets transmitted, 57 received, +42 errors, 42.4242% packet loss, time 110684ms
rtt min/avg/max/mdev = 0.388/54.771/2049.227/298.520 ms, pipe 4
root@mhs1:~# ping 192.168.8.2
PING 192.168.8.2 (192.168.8.2) 56(84) bytes of data.
64 bytes from 192.168.8.2: icmp_seq=1 ttl=61 time=1.54 ms
64 bytes from 192.168.8.2: icmp_seq=2 ttl=61 time=1.04 ms
^C
--- 192.168.8.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1112ms
rtt min/avg/max/mdev = 1.037/1.286/1.536/0.249 ms
root@mhs1:~# ping 192.168.8.3
PING 192.168.8.3 (192.168.8.3) 56(84) bytes of data.
64 bytes from 192.168.8.3: icmp_seq=1 ttl=61 time=1.09 ms
64 bytes from 192.168.8.3: icmp_seq=2 ttl=61 time=1.16 ms
^C
--- 192.168.8.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1111ms
rtt min/avg/max/mdev = 1.091/1.125/1.159/0.034 ms
root@mhs1:~#
```

Mahasiswa dapat mengakses jaringan lab, namun tidak bisa akses ke riset dan & IoT device (upaya pemblokiran untuk mitigas upaya penyerangan atau tindak illegal)



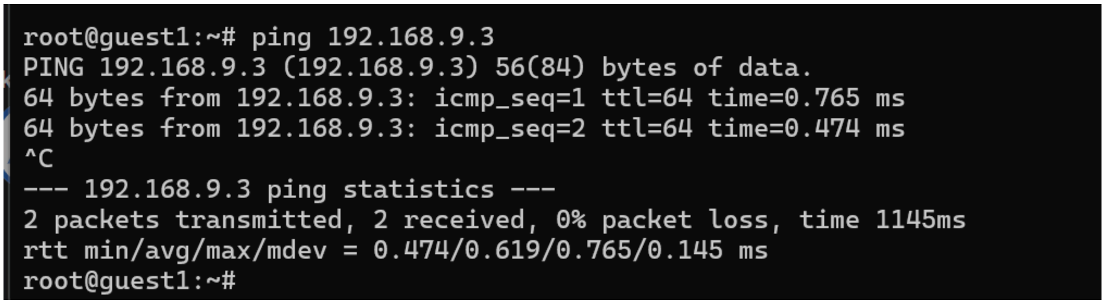
```
^C
--- 192.168.8.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1111ms
rtt min/avg/max/mdev = 1.091/1.125/1.159/0.034 ms
root@mhs1:~# ping 192.168.8.4
PING 192.168.8.4 (192.168.8.4) 56(84) bytes of data.
64 bytes from 192.168.8.4: icmp_seq=1 ttl=61 time=0.997 ms
64 bytes from 192.168.8.4: icmp_seq=2 ttl=61 time=0.944 ms
^C
--- 192.168.8.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1112ms
rtt min/avg/max/mdev = 0.944/0.970/0.997/0.026 ms
root@mhs1:~# ping 192.168.8.3
PING 192.168.8.3 (192.168.8.3) 56(84) bytes of data.
^C
--- 192.168.8.3 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1112ms

root@mhs1:~# ping 192.168.8.2
PING 192.168.8.2 (192.168.8.2) 56(84) bytes of data.
^C
--- 192.168.8.2 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1178ms

root@mhs1:~#
```

Guest



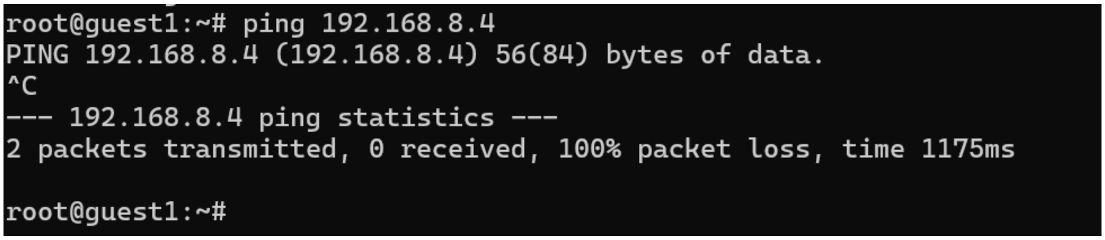
```
root@guest1:~# ping 192.168.8.2
PING 192.168.8.2 (192.168.8.2) 56(84) bytes of data.
^C
--- 192.168.8.2 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1045ms

root@guest1:~# ping 192.168.7.2
PING 192.168.7.2 (192.168.7.2) 56(84) bytes of data.
^C
--- 192.168.7.2 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

root@guest1:~# ping 192.168.6.2
PING 192.168.6.2 (192.168.6.2) 56(84) bytes of data.
^C
--- 192.168.6.2 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1044ms

root@guest1:~# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
^C
--- 192.168.1.2 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1054ms

root@guest1:~# ping google.com
PING google.com (74.125.200.138) 56(84) bytes of data.
64 bytes from sa-in-f138.1e100.net (74.125.200.138): icmp_seq=1 ttl=100 time=22.9 ms
64 bytes from sa-in-f138.1e100.net (74.125.200.138): icmp_seq=2 ttl=100 time=23.1 ms
```

Dari sini Client guest tidak dapat melakukan akses pada internal seperti admin,mahasiswa,akademik,riset, namun guest masih bisa terhubung ke jaringan dengan dibuktikan dapat ping google.com , apt update



```
root@guest1:~# ping 192.168.9.3
PING 192.168.9.3 (192.168.9.3) 56(84) bytes of data.
64 bytes from 192.168.9.3: icmp_seq=1 ttl=64 time=0.765 ms
64 bytes from 192.168.9.3: icmp_seq=2 ttl=64 time=0.474 ms
^C
--- 192.168.9.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1145ms
rtt min/avg/max/mdev = 0.474/0.619/0.765/0.145 ms
root@guest1:~#
```

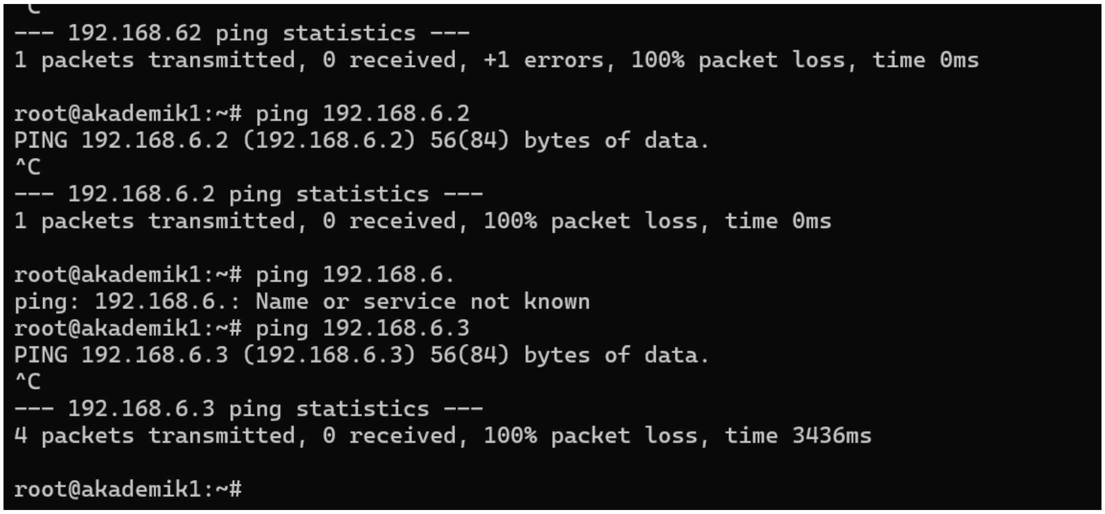
Sesama guest bisa akses networknya



```
root@guest1:~# ping 192.168.8.4
PING 192.168.8.4 (192.168.8.4) 56(84) bytes of data.
^C
--- 192.168.8.4 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1175ms

root@guest1:~#
```

Juga guest tidak bisa ping ke jalur Lab (Riset)

Akademik



```
^C
--- 192.168.62 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

root@akademik1:~# ping 192.168.6.2
PING 192.168.6.2 (192.168.6.2) 56(84) bytes of data.
^C
--- 192.168.6.2 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

root@akademik1:~# ping 192.168.6.
ping: 192.168.6.: Name or service not known
root@akademik1:~# ping 192.168.6.3
PING 192.168.6.3 (192.168.6.3) 56(84) bytes of data.
^C
--- 192.168.6.3 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3436ms

root@akademik1:~#
```

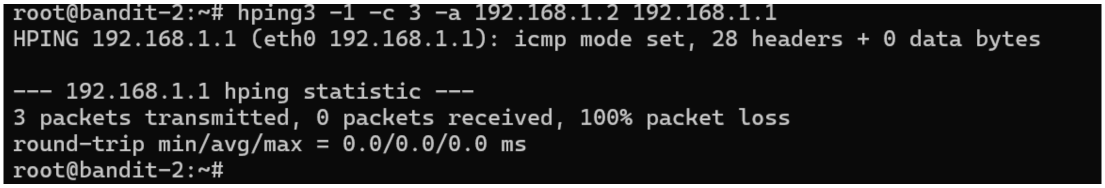
Akademik tidak dapat ping ke mahasiswa (sudah benar), karena menghindari (mitigasi) untuk akses yang tidak sah atau upaya penyerangan jika client MHS terkena retas

---

Security Testing

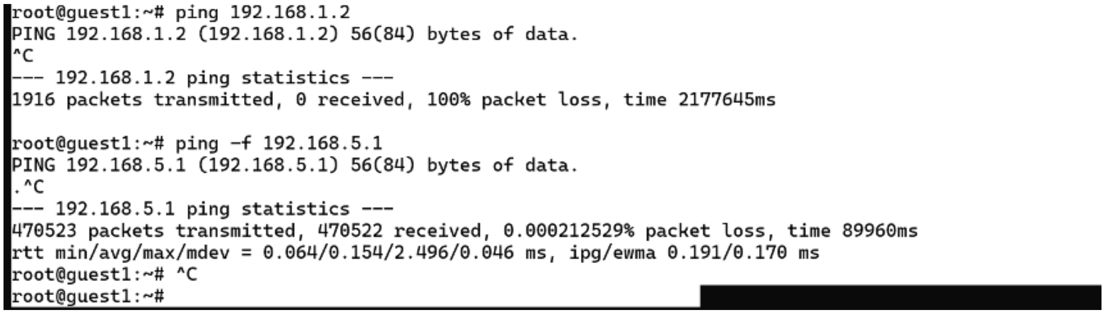
Uji ip spoofing

```
hping3 -1 -c 3 -a 192.168.1.2 192.168.1.1
```

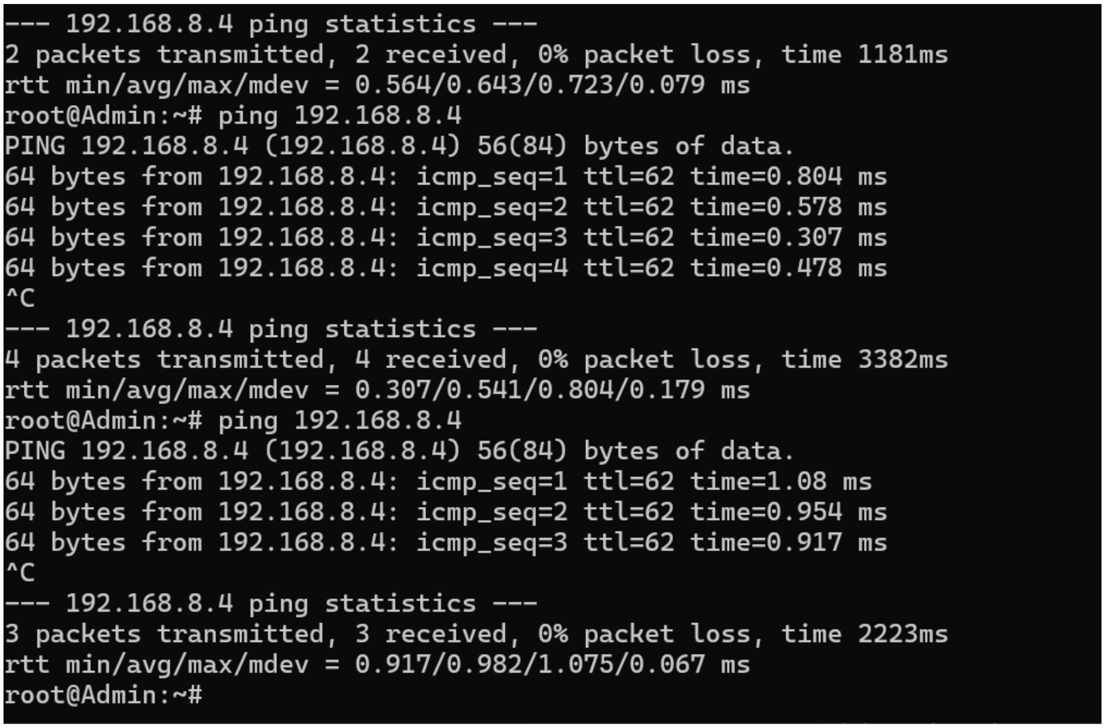


```
root@bandit-2:~# hping3 -1 -c 3 -a 192.168.1.2 192.168.1.1
HPING 192.168.1.1 (eth0 192.168.1.1): icmp mode set, 28 headers + 0 data bytes

--- 192.168.1.1 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@bandit-2:~#
```

Percobaan flooding



```
root@guest1:~# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
^C
--- 192.168.1.2 ping statistics ---
1916 packets transmitted, 0 received, 100% packet loss, time 2177645ms

root@guest1:~# ping -f 192.168.5.1
PING 192.168.5.1 (192.168.5.1) 56(84) bytes of data.
.^C
--- 192.168.5.1 ping statistics ---
470523 packets transmitted, 470522 received, 0.000212529% packet loss, time 89960ms
rtt min/avg/max/mdev = 0.064/0.154/2.496/0.046 ms, ipg/ewma 0.191/0.170 ms
root@guest1:~# ^C
root@guest1:~#
```



```
--- 192.168.8.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1181ms
rtt min/avg/max/mdev = 0.564/0.643/0.723/0.079 ms
root@Admin:~# ping 192.168.8.4
PING 192.168.8.4 (192.168.8.4) 56(84) bytes of data.
64 bytes from 192.168.8.4: icmp_seq=1 ttl=62 time=0.804 ms
64 bytes from 192.168.8.4: icmp_seq=2 ttl=62 time=0.578 ms
64 bytes from 192.168.8.4: icmp_seq=3 ttl=62 time=0.307 ms
64 bytes from 192.168.8.4: icmp_seq=4 ttl=62 time=0.478 ms
^C
--- 192.168.8.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3382ms
rtt min/avg/max/mdev = 0.307/0.541/0.804/0.179 ms
root@Admin:~# ping 192.168.8.4
PING 192.168.8.4 (192.168.8.4) 56(84) bytes of data.
64 bytes from 192.168.8.4: icmp_seq=1 ttl=62 time=1.08 ms
64 bytes from 192.168.8.4: icmp_seq=2 ttl=62 time=0.954 ms
64 bytes from 192.168.8.4: icmp_seq=3 ttl=62 time=0.917 ms
^C
--- 192.168.8.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2223ms
rtt min/avg/max/mdev = 0.917/0.982/1.075/0.067 ms
root@Admin:~#
```

Semua masih normal dan masih bisa ping satu sama lain