

KJK-Projek

Router Debian

Firewall (Debian)

Setup awal

```
1 apt update
2 apt install iptables-persistent
```

Hasil Uji coba

```
1 Setting up iptables-persistent (1.0.23) ...
2 root@Firewall:~# ip route show
3 default via 192.168.122.1 dev eth0 metric 2096
4 192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.1
5 192.168.2.0/24 dev eth2 proto kernel scope link src 192.168.2.1
6 192.168.3.0/24 dev eth3 proto kernel scope link src 192.168.3.1
7 192.168.4.0/24 dev eth4 proto kernel scope link src 192.168.4.1
8 192.168.5.0/24 dev eth5 proto kernel scope link src 192.168.5.1
9 192.168.6.0/24 via 192.168.2.2 dev eth2
10 192.168.7.0/24 via 192.168.3.2 dev eth3
11 192.168.8.0/24 via 192.168.4.2 dev eth4
12 192.168.9.0/24 via 192.168.5.2 dev eth5
13 192.168.122.0/24 dev eth0 proto kernel scope link src 192.168.122.83
14 root@Firewall:~#
```

```
1  #
2  # This is a sample network config, please uncomment lines to configure tl
3  #
4
5  # Uncomment this line to load custom interface files
6  # source /etc/network/interfaces.d/*
7
8  # DHCP config for eth0
9  auto eth0
10 iface eth0 inet dhcp
11 up echo nameserver 192.168.122.1 > /etc/resolv.conf
12
13 # Static config for eth1
14 auto eth1
15 iface eth1 inet static
16     address 192.168.1.1
17     netmask 255.255.255.0
18
19 # Static config for eth2
20 auto eth2
21 iface eth2 inet static
22     address 192.168.2.1
23     netmask 255.255.255.0
24
25
26 # Static config for eth3
27 auto eth3
28 iface eth3 inet static
29     address 192.168.3.1
30     netmask 255.255.255.0
31
32 # Static config for eth4
33 auto eth4
34 iface eth4 inet static
35     address 192.168.4.1
36     netmask 255.255.255.0
37
38
39 # Static config for eth5
40 auto eth5
41 iface eth5 inet static
42     address 192.168.5.1
43     netmask 255.255.255.0
```

Router Mahasiswa

```
1  #
2  # This is a sample network config, please uncomment lines to configure tl
3  #
4
5  # Uncomment this line to load custom interface files
6  # source /etc/network/interfaces.d/*
7
8  # Static config for eth0
9  auto eth0
10 iface eth0 inet static
11     address 192.168.2.2
12     netmask 255.255.255.0
13     gateway 192.168.2.1
14     up echo nameserver 192.168.122.1 > /etc/resolv.conf
15
16 # Static config for eth1
17 auto eth1
18 iface eth1 inet static
19     address 192.168.6.1
20     netmask 255.255.255.0
```

Router Akademik

```
1  #
2  # This is a sample network config, please uncomment lines to configure tl
3  #
4
5  # Uncomment this line to load custom interface files
6  # source /etc/network/interfaces.d/*
7
8  # Static config for eth0
```

```
9   auto eth0
10  iface eth0 inet static
11      address 192.168.3.2
12      netmask 255.255.255.0
13      gateway 192.168.3.1
14      up echo nameserver 192.168.122.1 > /etc/resolv.conf
15
16  # Static config for eth1
17  auto eth1
18  iface eth1 inet static
19      address 192.168.7.1
20      netmask 255.255.255.0
```

Admin

```
1  #
2  # This is a sample network config, please uncomment lines to configure tl
3  #
4
5  # Uncomment this line to load custom interface files
6  # source /etc/network/interfaces.d/*
7
8  # Static config for eth0
9  auto eth0
10  iface eth0 inet static
11      address 192.168.1.2
12      netmask 255.255.255.0
13      gateway 192.168.1.1
14      up echo nameserver 192.168.122.1 > /etc/resolv.conf
15
```

Router riset

```
1  #
2  # This is a sample network config, please uncomment lines to configure tl
3  #
```

```
4
5 # Uncomment this line to load custom interface files
6 # source /etc/network/interfaces.d/*
7
8 # Static config for eth0
9 auto eth0
10 iface eth0 inet static
11     address 192.168.4.2
12     netmask 255.255.255.0
13     gateway 192.168.4.1
14     up echo nameserver 192.168.122.1 > /etc/resolv.conf
15
16
17 # Static config for eth1
18 auto eth1
19 iface eth1 inet static
20     address 192.168.8.1
21     netmask 255.255.255.0
```

Router Guest

```
1 #
2 # This is a sample network config, please uncomment lines to configure tl
3 #
4
5 # Uncomment this line to load custom interface files
6 # source /etc/network/interfaces.d/*
7
8 # Static config for eth0
9 auto eth0
10 iface eth0 inet static
11     address 192.168.5.2
12     netmask 255.255.255.0
13     gateway 192.168.5.1
14     up echo nameserver 192.168.122.1 > /etc/resolv.conf
15
16
17 # Static config for eth1
18 auto eth1
19 iface eth1 inet static
20     address 192.168.9.1
21     netmask 255.255.255.0
```

Client

MHS 1

```
1  #
2  # This is a sample network config, please uncomment lines to configure tl
3  #
4
5  # Uncomment this line to load custom interface files
6  # source /etc/network/interfaces.d/*
7
8  # Static config for eth0
9  auto eth0
10 iface eth0 inet static
11     address 192.168.6.2
12     netmask 255.255.255.0
13     gateway 192.168.6.1
14     up echo nameserver 192.168.122.1 > /etc/resolv.conf
15
```

MHS 2

```
1  #
2  # This is a sample network config, please uncomment lines to configure tl
3  #
4
5  # Uncomment this line to load custom interface files
6  # source /etc/network/interfaces.d/*
7
8  # Static config for eth0
9  auto eth0
10 iface eth0 inet static
11     address 192.168.6.3
12     netmask 255.255.255.0
```

```
13         gateway 192.168.6.1
14         up echo nameserver 192.168.122.1 > /etc/resolv.conf
15
```

Akademik 1

```
1  #
2  # This is a sample network config, please uncomment lines to configure tl
3  #
4
5  # Uncomment this line to load custom interface files
6  # source /etc/network/interfaces.d/*
7
8  # Static config for eth0
9  auto eth0
10 iface eth0 inet static
11     address 192.168.7.2
12     netmask 255.255.255.0
13     gateway 192.168.7.1
14     up echo nameserver 192.168.122.1 > /etc/resolv.conf
15
16
```

Akademik 2

```
1  #
2  # This is a sample network config, please uncomment lines to configure tl
3  #
4
5  # Uncomment this line to load custom interface files
6  # source /etc/network/interfaces.d/*
7
8  # Static config for eth0
9  auto eth0
10 iface eth0 inet static
11     address 192.168.7.3
12     netmask 255.255.255.0
13     gateway 192.168.7.1
```

```
14         up echo nameserver 192.168.122.1 > /etc/resolv.conf
15
```

Riset 1

```
1  #
2  # This is a sample network config, please uncomment lines to configure tl
3  #
4
5  # Uncomment this line to load custom interface files
6  # source /etc/network/interfaces.d/*
7
8  # Static config for eth0
9  auto eth0
10 iface eth0 inet static
11     address 192.168.8.2
12     netmask 255.255.255.0
13     gateway 192.168.8.1
14     up echo nameserver 192.168.122.1 > /etc/resolv.conf
```

Riset 2

```
1  #
2  # This is a sample network config, please uncomment lines to configure tl
3  #
4
5  # Uncomment this line to load custom interface files
6  # source /etc/network/interfaces.d/*
7
8  # Static config for eth0
9  auto eth0
10 iface eth0 inet static
11     address 192.168.8.3
12     netmask 255.255.255.0
13     gateway 192.168.8.1
```



```
14          up echo nameserver 192.168.122.1 > /etc/resolv.conf
```

Guest 1

```
1  #
2  # This is a sample network config, please uncomment lines to configure tl
3  #
4
5  # Uncomment this line to load custom interface files
6  # source /etc/network/interfaces.d/*
7
8  # Static config for eth0
9  auto eth0
10 iface eth0 inet static
11     address 192.168.9.2
12     netmask 255.255.255.0
13     gateway 192.168.9.1
14     up echo nameserver 192.168.122.1 > /etc/resolv.conf
```

Guest 2

```
1  #
2  # This is a sample network config, please uncomment lines to configure tl
3  #
4
5  # Uncomment this line to load custom interface files
6  # source /etc/network/interfaces.d/*
7
8  # Static config for eth0
9  auto eth0
10 iface eth0 inet static
11     address 192.168.9.2
12     netmask 255.255.255.0
13     gateway 192.168.9.1
14     up echo nameserver 192.168.122.1 > /etc/resolv.conf
```

Bandit 1

```
1  #
2  # This is a sample network config, please uncomment lines to configure tl
3  #
4
5  # Uncomment this line to load custom interface files
6  # source /etc/network/interfaces.d/*
7
8
9  # DHCP config for eth0
10 auto eth0
11 iface eth0 inet dhcp
12     up echo nameserver 192.168.0.1 > /etc/resolv.conf
13
```

Bandit 2

```
1  #
2  # This is a sample network config, please uncomment lines to configure tl
3  #
4
5  # Uncomment this line to load custom interface files
6  # source /etc/network/interfaces.d/*
7
8  # Static config for eth0
9  auto eth0
10 iface eth0 inet static
11     address 192.168.6.3
12     netmask 255.255.255.0
13     gateway 192.168.6.1
14     up echo nameserver 192.168.122.1 > /etc/resolv.conf
```

Firewall

```
1 root@Firewall:~# ls
2 firewall.sh iptables-rules.txt
3 root@Firewall:~# cat firewall.sh
4 #!/bin/sh
5
6 WAN="eth0"
7 ADM="eth1"
8 MHS="eth2"
9 AKD="eth3"
10 RST="eth4"
11 GST="eth5"
12
13 # 1. Atur kebijakan default
14 iptables -P INPUT DROP
15 iptables -P FORWARD DROP
16 iptables -P OUTPUT ACCEPT # Izinkan trafik keluar dari firewall itu send:
17
18 # 2. Izinkan koneksi yang sudah ada/terkait
19 iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
20 iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
21
22 # 3. Aktifkan NAT (Masquerading) untuk semua yang keluar ke WAN
23 iptables -t nat -A POSTROUTING -o $WAN -j MASQUERADE
24
25 # ===== ATURAN ZONA GUEST (GST) =====
26 # Izinkan GST -> WAN (Hanya Web & DNS)
27 iptables -A FORWARD -i $GST -o $WAN -p udp --dport 53 -j ACCEPT
28 iptables -A FORWARD -i $GST -o $WAN -p tcp --dport 53 -j ACCEPT
29 iptables -A FORWARD -i $GST -o $WAN -p tcp --dport 80 -j ACCEPT
30 iptables -A FORWARD -i $GST -o $WAN -p tcp --dport 443 -j ACCEPT
31 # (Trafik GST ke zona internal lain otomatis di-DROP oleh kebijakan defai
32
33 # ===== ATURAN ZONA MAHASISWA (MHS) =====
34 # Izinkan MHS -> WAN (Hanya Web & DNS)
35 iptables -A FORWARD -i $MHS -o $WAN -p udp --dport 53 -j ACCEPT
36 iptables -A FORWARD -i $MHS -o $WAN -p tcp --dport 53 -j ACCEPT
37 iptables -A FORWARD -i $MHS -o $WAN -p tcp --dport 80 -j ACCEPT
38 iptables -A FORWARD -i $MHS -o $WAN -p tcp --dport 443 -j ACCEPT
39 # Izinkan MHS -> AKD (Hanya Web)
40 iptables -A FORWARD -i $MHS -o $AKD -p tcp --dport 80 -j ACCEPT
41 iptables -A FORWARD -i $MHS -o $AKD -p tcp --dport 443 -j ACCEPT
42
43 # ===== ATURAN ZONA AKADEMIK (AKD) =====
```

```

44 # Izinkan AKD -> WAN (Semua)
45 iptables -A FORWARD -i $AKD -o $WAN -j ACCEPT
46 # Izinkan AKD -> MHS (Semua)
47 iptables -A FORWARD -i $AKD -o $MHS -j ACCEPT
48
49 # ===== ATURAN ZONA Riset (RST) =====
50 # Izinkan RST -> WAN (Semua)
51 iptables -A FORWARD -i $RST -o $WAN -j ACCEPT
52 # (Trafik RST ke zona internal lain otomatis di-DROP)
53
54 # ===== ATURAN ZONA ADMIN (ADM) =====
55 # Izinkan ADM -> SEMUA ZONA (Termasuk WAN)
56 iptables -A FORWARD -i $ADM -j ACCEPT
57
58 # Izinkan Ping (ICMP) dari semua zona internal (opsional, untuk tes)
59 iptables -A INPUT -i $ADM -p icmp -j ACCEPT
60 iptables -A INPUT -i $MHS -p icmp -j ACCEPT
61 iptables -A INPUT -i $AKD -p icmp -j ACCEPT
62 iptables -A INPUT -i $RST -p icmp -j ACCEPT
63 # (Kita sengaja tidak izinkan GUEST ping ke firewall)
64
65 # Izinkan SSH & HTTPS HANYA dari zona ADM
66 iptables -A INPUT -i $ADM -p tcp --dport 22 -j ACCEPT
67 iptables -A INPUT -i $ADM -p tcp --dport 443 -j ACCEPT
68
69 # Izinkan loopback (penting untuk internal OS)
70 iptables -A INPUT -i lo -j ACCEPT
71
72
73 root@Firewall:~#

```

Firewall-Rev1

```

1 #!/bin/bash
2 set -eou pipefail
3
4 # ===== Interface & Subnet (192.168.x.x) =====
5 WAN_IF="eth0"
6 ADM_IF="eth1"; ADM_NET="192.168.1.0/24"
7 MHS_IF="eth2"; MHS_NET="192.168.2.0/24"
8 AKD_IF="eth3"; AKD_NET="192.168.3.0/24"
9 RST_IF="eth4"; RST_NET="192.168.4.0/24"
10 GST_IF="eth5"; GST_NET="192.168.5.0/24"
11

```

```

12 # Service ports
13 WEB_PORTS="80,443"
14 DNS_PORT=53
15
16 # ===== Sistem & Reset =====
17 echo 1 > /proc/sys/net/ipv4/ip_forward
18
19 iptables -t nat -F; iptables -t mangle -F; iptables -F; iptables -X
20 iptables -P INPUT DROP; iptables -P FORWARD DROP; iptables -P OUTPUT ACCEPT
21
22 # ===== Chains utilitas =====
23 iptables -N LOG_DROP
24 iptables -A LOG_DROP -m limit --limit 5/min -j LOG --log-prefix "DROP "
25 iptables -A LOG_DROP -j DROP
26
27 # ===== Basic hygiene =====
28 iptables -A INPUT -i lo -j ACCEPT
29 iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
30 iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
31 iptables -A INPUT -m state --state INVALID -j LOG --log-prefix "INVALID
32 iptables -A INPUT -m state --state INVALID -j DROP
33 iptables -A FORWARD -m state --state INVALID -j DROP
34
35 # ===== Anti-spoofing =====
36 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
37     iptables -A INPUT -i "$WAN_IF" -s "$NET" -j LOG --log-prefix "SPOOF WAN
38     iptables -A INPUT -i "$WAN_IF" -s "$NET" -j DROP
39     iptables -A FORWARD -i "$WAN_IF" -s "$NET" -j DROP
40 done
41
42 # Lateral anti-spoof
43 iptables -A INPUT -i "$ADM_IF" -s "$ADM_NET" -j ACCEPT
44 iptables -A INPUT -i "$ADM_IF" ! -s "$ADM_NET" -j DROP
45 iptables -A INPUT -i "$MHS_IF" -s "$MHS_NET" -j ACCEPT
46 iptables -A INPUT -i "$MHS_IF" ! -s "$MHS_NET" -j DROP
47 iptables -A INPUT -i "$AKD_IF" -s "$AKD_NET" -j ACCEPT
48 iptables -A INPUT -i "$AKD_IF" ! -s "$AKD_NET" -j DROP
49 iptables -A INPUT -i "$RST_IF" -s "$RST_NET" -j ACCEPT
50 iptables -A INPUT -i "$RST_IF" ! -s "$RST_NET" -j DROP
51 iptables -A INPUT -i "$GST_IF" -s "$GST_NET" -j ACCEPT
52 iptables -A INPUT -i "$GST_IF" ! -s "$GST_NET" -j DROP
53
54 # ===== NAT Masquerading =====
55 iptables -t nat -A POSTROUTING -o "$WAN_IF" -j MASQUERADE
56
57 # ===== ICMP FIX: Outbound & Reply =====
58 # Izinkan ICMP outbound dari SEMUA zona internal ke WAN
59 iptables -A FORWARD -i "$ADM_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
60 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r

```

```

61 iptables -A FORWARD -i "$AKD_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
62 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
63 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
64
65 # Izinkan ICMP reply kembali (echo-reply dari WAN ke internal)
66 iptables -A FORWARD -i "$WAN_IF" -o "$ADM_IF" -p icmp --icmp-type echo-r
67 iptables -A FORWARD -i "$WAN_IF" -o "$MHS_IF" -p icmp --icmp-type echo-r
68 iptables -A FORWARD -i "$WAN_IF" -o "$AKD_IF" -p icmp --icmp-type echo-r
69 iptables -A FORWARD -i "$WAN_IF" -o "$RST_IF" -p icmp --icmp-type echo-r
70 iptables -A FORWARD -i "$WAN_IF" -o "$GST_IF" -p icmp --icmp-type echo-r
71
72 # Rate limit ICMP ke firewall (anti-ICMP flood)
73 iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/se
74 iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
75
76 # ===== TCP/UDP Rules (Existing) =====
77 # ADMIN -> semua
78 iptables -A FORWARD -i "$ADM_IF" -j ACCEPT
79
80 # MAHASISWA -> Internet (HTTP/HTTPS/DNS)
81 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp -m multiport --dpor
82 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -
83 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -
84
85 # AKADEMIK -> Internet (full)
86 iptables -A FORWARD -i "$AKD_IF" -o "$WAN_IF" -j ACCEPT
87
88 # AKADEMIK -> Riset (full)
89 iptables -A FORWARD -i "$AKD_IF" -o "$RST_IF" -j ACCEPT
90
91 # RISET/IoT -> Internet (HTTPS only)
92 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport 443 -j ACCE
93 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -
94 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -
95
96 # RISET/IoT -> Admin (monitoring ports)
97 iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p udp --dport 514 -j ACCE
98 iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p tcp -m multiport --dpor
99
100 # RISET/IoT -> Akademik (full)
101 iptables -A FORWARD -i "$RST_IF" -o "$AKD_IF" -j ACCEPT
102
103 # GUEST -> Internet (HTTP/HTTPS/DNS)
104 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp -m multiport --dpor
105 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -
106 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -
107
108 # SSH brute-force protection
109 iptables -N SSHSCAN

```

```

110 iptables -A INPUT -i "$ADM_IF" -p tcp --dport 22 -m state --state NEW -j
111 iptables -A SSHSCAN -m recent --set --name SSH --rsource
112 iptables -A SSHSCAN -m recent --update --seconds 60 --hitcount 4 --name !
113 iptables -A SSHSCAN -m recent --update --seconds 60 --hitcount 4 --name !
114 iptables -A INPUT -i "$ADM_IF" -p tcp --dport 22 -j ACCEPT
115
116 # ===== Logging drops =====
117 iptables -A INPUT -j LOG_DROP
118 iptables -A FORWARD -j LOG_DROP
119

```

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

```

1  #!/bin/bash
2  set -euo pipefail
3
4  # ===== Interface & Subnet (192.168.x.x) =====
5  WAN_IF="eth0"
6  ADM_IF="eth1"; ADM_NET="192.168.1.0/24"
7  MHS_IF="eth2"; MHS_NET="192.168.2.0/24"
8  AKD_IF="eth3"; AKD_NET="192.168.3.0/24"
9  RST_IF="eth4"; RST_NET="192.168.4.0/24"
10 GST_IF="eth5"; GST_NET="192.168.5.0/24"
11
12 # LAB subnet spesifik (dalam zona Riset)
13 LAB_NET="192.168.8.0/24" # Riset3 sebagai Lab
14 LAB_ROUTER_IP="192.168.8.4" # Router Riset
15
16 # Service ports
17 WEB_PORTS="80,443"
18 DNS_PORT=53
19 LAB_PORTS="22,80,443" # SSH, HTTP, HTTPS untuk lab access
20
21 # ===== Sistem & Reset =====
22 echo 1 > /proc/sys/net/ipv4/ip_forward
23
24 iptables -t nat -F; iptables -t mangle -F; iptables -F; iptables -X
25 iptables -P INPUT DROP; iptables -P FORWARD DROP; iptables -P OUTPUT ACCI
26
27 # ===== Chains utilitas =====
28 iptables -N LOG_DROP
29 iptables -A LOG_DROP -m limit --limit 5/min -j LOG --log-prefix "DROP "

```

```

30 iptables -A LOG_DROP -j DROP
31
32 # ===== Basic hygiene =====
33 iptables -A INPUT -i lo -j ACCEPT
34 iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
35 iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
36 iptables -A INPUT -m state --state INVALID -j LOG --log-prefix "INVALID
37 iptables -A INPUT -m state --state INVALID -j DROP
38 iptables -A FORWARD -m state --state INVALID -j DROP
39
40 # ===== Anti-spoofing =====
41 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
42     iptables -A INPUT -i "$WAN_IF" -s "$NET" -j LOG --log-prefix "SPOOF WAI
43     iptables -A INPUT -i "$WAN_IF" -s "$NET" -j DROP
44     iptables -A FORWARD -i "$WAN_IF" -s "$NET" -j DROP
45 done
46
47 # Lateral anti-spoof
48 iptables -A INPUT -i "$ADM_IF" -s "$ADM_NET" -j ACCEPT
49 iptables -A INPUT -i "$ADM_IF" ! -s "$ADM_NET" -j DROP
50 iptables -A INPUT -i "$MHS_IF" -s "$MHS_NET" -j ACCEPT
51 iptables -A INPUT -i "$MHS_IF" ! -s "$MHS_NET" -j DROP
52 iptables -A INPUT -i "$AKD_IF" -s "$AKD_NET" -j ACCEPT
53 iptables -A INPUT -i "$AKD_IF" ! -s "$AKD_NET" -j DROP
54 iptables -A INPUT -i "$RST_IF" -s "$RST_NET" -j ACCEPT
55 iptables -A INPUT -i "$RST_IF" ! -s "$RST_NET" -j DROP
56 iptables -A INPUT -i "$GST_IF" -s "$GST_NET" -j ACCEPT
57 iptables -A INPUT -i "$GST_IF" ! -s "$GST_NET" -j DROP
58
59 # ===== NAT Masquerading =====
60 iptables -t nat -A POSTROUTING -o "$WAN_IF" -j MASQUERADE
61
62 # ===== ICMP FIX: Outbound & Reply =====
63 # Izinkan ICMP outbound dari SEMUA zona internal ke WAN
64 iptables -A FORWARD -i "$ADM_IF" -o "$WAN_IF" -p icmp --icmp-type echo-rq
65 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p icmp --icmp-type echo-rq
66 iptables -A FORWARD -i "$AKD_IF" -o "$WAN_IF" -p icmp --icmp-type echo-rq
67 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-rq
68 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-rq
69
70 # Izinkan ICMP reply kembali
71 iptables -A FORWARD -i "$WAN_IF" -o "$ADM_IF" -p icmp --icmp-type echo-rq
72 iptables -A FORWARD -i "$WAN_IF" -o "$MHS_IF" -p icmp --icmp-type echo-rq
73 iptables -A FORWARD -i "$WAN_IF" -o "$AKD_IF" -p icmp --icmp-type echo-rq
74 iptables -A FORWARD -i "$WAN_IF" -o "$RST_IF" -p icmp --icmp-type echo-rq
75 iptables -A FORWARD -i "$WAN_IF" -o "$GST_IF" -p icmp --icmp-type echo-rq
76
77 # Rate limit ICMP ke firewall
78 iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/sec

```



```

79 iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
80
81 # ===== KEBIJAKAN LAB (Riset3) =====
82
83 # MAHASISWA -> Lab (LIMITED: SSH, HTTP, HTTPS, Ping)
84 iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d "$LAB_NET" -p tcp -m multiport --dports 22,80,443 -j ACCEPT
85 iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d "$LAB_NET" -p icmp --icmp-type echo-request -j ACCEPT
86
87 # AKADEMIK -> Lab (FULL access)
88 iptables -A FORWARD -i "$AKD_IF" -o "$RST_IF" -d "$LAB_NET" -j ACCEPT
89
90 # ADMIN -> Lab (FULL access, sudah diatur di bawah)
91
92 # Lab -> Internet (HTTPS+DNS) - sama seperti RST
93 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport 443 -j ACCEPT
94 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j ACCEPT
95 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j ACCEPT
96
97 # Lab -> Admin (monitoring ports)
98 iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p udp --dport 514 -j ACCEPT
99 iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p tcp -m multiport --dports 22,80,443 -j ACCEPT
100
101 # Lab -> Akademik (FULL)
102 iptables -A FORWARD -i "$RST_IF" -o "$AKD_IF" -j ACCEPT
103
104 # ===== KEBIJAKAN ZONA LAIN (TETAP SAMA) =====
105
106 # ADMIN -> semua
107 iptables -A FORWARD -i "$ADM_IF" -j ACCEPT
108
109 # MAHASISWA -> Internet (HTTP/HTTPS/DNS)
110 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp -m multiport --dports 80,443 -j ACCEPT
111 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j ACCEPT
112 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j ACCEPT
113
114 # AKADEMIK -> Internet (full)
115 iptables -A FORWARD -i "$AKD_IF" -o "$WAN_IF" -j ACCEPT
116
117 # AKADEMIK -> Riset (full)
118 iptables -A FORWARD -i "$AKD_IF" -o "$RST_IF" -j ACCEPT
119
120 # RISET/IoT -> Internet (HTTPS+DNS)
121 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport 443 -j ACCEPT
122 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j ACCEPT
123 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j ACCEPT
124
125 # RISET/IoT -> Admin (monitoring)
126 iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p udp --dport 514 -j ACCEPT
127 iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p tcp -m multiport --dports 22,80,443 -j ACCEPT

```

```

128
129 # Riset/IoT -> Akademik (full)
130 iptables -A FORWARD -i "$RST_IF" -o "$AKD_IF" -j ACCEPT
131
132 # GUEST -> Internet (HTTP/HTTPS/DNS)
133 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp -m multiport --dport $DNS_PORT -j ACCEPT
134 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j ACCEPT
135 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j ACCEPT
136
137 # SSH brute-force protection
138 iptables -N SSHSCAN
139 iptables -A INPUT -i "$ADM_IF" -p tcp --dport 22 -m state --state NEW -j SSHSCAN
140 iptables -A SSHSCAN -m recent --set --name SSH --rsource
141 iptables -A SSHSCAN -m recent --update --seconds 60 --hitcount 4 --name SSH -j REJECT
142 iptables -A SSHSCAN -m recent --update --seconds 60 --hitcount 4 --name SSH -j REJECT
143 iptables -A INPUT -i "$ADM_IF" -p tcp --dport 22 -j ACCEPT
144
145 # ===== Logging drops =====
146 iptables -A INPUT -j LOG_DROP
147 iptables -A FORWARD -j LOG_DROP
148
149 echo "Firewall zone-based with Lab access (Riset3) activated."

```

Firewall Rev-3

```

1  #!/bin/bash
2  set -e
3
4  # ===== Interface & Subnet (192.168.x.x) =====
5  WAN_IF="eth0"
6  ADM_IF="eth1"; ADM_NET="192.168.1.0/24"
7  MHS_IF="eth2"; MHS_NET="192.168.2.0/24"
8  AKD_IF="eth3"; AKD_NET="192.168.3.0/24"
9  RST_IF="eth4"; RST_NET="192.168.4.0/24"
10 GST_IF="eth5"; GST_NET="192.168.5.0/24"
11
12 # LAB host spesifik (hanya 192.168.8.4)
13 LAB_HOST="192.168.8.4" # Riset3 sebagai Lab
14 BLOCKED_HOSTS="192.168.8.2,192.168.8.3" # Host yang diblokir untuk Mahasiswa
15
16 # Service ports
17 WEB_PORTS="80,443"
18 DNS_PORT=53
19 LAB_PORTS="22,80,443" # SSH, HTTP, HTTPS untuk lab access
20

```

```

21 # ===== Sistem & Reset =====
22 echo 1 > /proc/sys/net/ipv4/ip_forward
23
24 iptables -t nat -F; iptables -t mangle -F; iptables -F; iptables -X
25 iptables -P INPUT DROP; iptables -P FORWARD DROP; iptables -P OUTPUT ACCEPT
26
27 # ===== Chains utilitas =====
28 iptables -N LOG_DROP
29 iptables -A LOG_DROP -m limit --limit 5/min -j LOG --log-prefix "DROP "
30 iptables -A LOG_DROP -j DROP
31
32 # ===== Basic hygiene =====
33 iptables -A INPUT -i lo -j ACCEPT
34 iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
35 iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
36 iptables -A INPUT -m state --state INVALID -j LOG --log-prefix "INVALID
37 iptables -A INPUT -m state --state INVALID -j DROP
38 iptables -A FORWARD -m state --state INVALID -j DROP
39
40 # ===== Anti-spoofing =====
41 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
42     iptables -A INPUT -i "$WAN_IF" -s "$NET" -j LOG --log-prefix "SPOOF WAN
43     iptables -A INPUT -i "$WAN_IF" -s "$NET" -j DROP
44     iptables -A FORWARD -i "$WAN_IF" -s "$NET" -j DROP
45 done
46
47 # Lateral anti-spoof
48 iptables -A INPUT -i "$ADM_IF" -s "$ADM_NET" -j ACCEPT
49 iptables -A INPUT -i "$ADM_IF" ! -s "$ADM_NET" -j DROP
50 iptables -A INPUT -i "$MHS_IF" -s "$MHS_NET" -j ACCEPT
51 iptables -A INPUT -i "$MHS_IF" ! -s "$MHS_NET" -j DROP
52 iptables -A INPUT -i "$AKD_IF" -s "$AKD_NET" -j ACCEPT
53 iptables -A INPUT -i "$AKD_IF" ! -s "$AKD_NET" -j DROP
54 iptables -A INPUT -i "$RST_IF" -s "$RST_NET" -j ACCEPT
55 iptables -A INPUT -i "$RST_IF" ! -s "$RST_NET" -j DROP
56 iptables -A INPUT -i "$GST_IF" -s "$GST_NET" -j ACCEPT
57 iptables -A INPUT -i "$GST_IF" ! -s "$GST_NET" -j DROP
58
59 # ===== NAT Masquerading =====
60 iptables -t nat -A POSTROUTING -o "$WAN_IF" -j MASQUERADE
61
62 # ===== ICMP FIX: Outbound & Reply =====
63 # Izinkan ICMP outbound dari SEMUA zona internal ke WAN
64 iptables -A FORWARD -i "$ADM_IF" -o "$WAN_IF" -p icmp --icmp-type echo-request
65 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p icmp --icmp-type echo-request
66 iptables -A FORWARD -i "$AKD_IF" -o "$WAN_IF" -p icmp --icmp-type echo-request
67 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-request
68 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-request
69

```

```

70 # Izinkan ICMP reply kembali
71 iptables -A FORWARD -i "$WAN_IF" -o "$ADM_IF" -p icmp --icmp-type echo-r
72 iptables -A FORWARD -i "$WAN_IF" -o "$MHS_IF" -p icmp --icmp-type echo-r
73 iptables -A FORWARD -i "$WAN_IF" -o "$AKD_IF" -p icmp --icmp-type echo-r
74 iptables -A FORWARD -i "$WAN_IF" -o "$RST_IF" -p icmp --icmp-type echo-r
75 iptables -A FORWARD -i "$WAN_IF" -o "$GST_IF" -p icmp --icmp-type echo-r
76
77 # Rate limit ICMP ke firewall
78 iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/se
79 iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
80
81 # ===== KEBIJAKAN LAB (Riset3) - HOST SPECIFIC =====
82
83 # BLOKIR Mahasiswa -> 192.168.8.2 dan 192.168.8.3
84 iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d 192.168.8.2 -j LOG --lo
85 iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d 192.168.8.2 -j DROP
86 iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d 192.168.8.3 -j LOG --lo
87 iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d 192.168.8.3 -j DROP
88
89 # IZINKAN Mahasiswa -> Lab 192.168.8.4 (LIMITED: SSH, HTTP, HTTPS, Ping)
90 iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d "$LAB_HOST" -p tcp -m mi
91 iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d "$LAB_HOST" -p icmp --i
92
93 # AKADEMIK -> Lab (FULL access) - diatur di bawah via AKADEMIK->Riset
94 # ADMIN -> Lab (FULL access) - diatur di bawah via ADMIN->all
95
96 # ===== KEBIJAKAN ZONA LAIN (TETAP SAMA) =====
97
98 # ADMIN -> semua
99 iptables -A FORWARD -i "$ADM_IF" -j ACCEPT
100
101 # MAHASISWA -> Internet (HTTP/HTTPS/DNS)
102 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp -m multiport --dpor
103 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -
104 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -
105
106 # AKADEMIK -> Internet (full)
107 iptables -A FORWARD -i "$AKD_IF" -o "$WAN_IF" -j ACCEPT
108
109 # AKADEMIK -> Riset (full)
110 iptables -A FORWARD -i "$AKD_IF" -o "$RST_IF" -j ACCEPT
111
112 # RISET/IoT -> Internet (HTTPS+DNS)
113 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport 443 -j ACCE
114 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -
115 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -
116
117 # RISET/IoT -> Admin (monitoring)
118 iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p udp --dport 514 -j ACCE

```

```

119 iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p tcp -m multiport --dport
120
121 # Riset/IoT -> Akademik (full)
122 iptables -A FORWARD -i "$RST_IF" -o "$AKD_IF" -j ACCEPT
123
124 # GUEST -> Internet (HTTP/HTTPS/DNS)
125 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp -m multiport --dport
126 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j
127 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j
128
129 # SSH brute-force protection
130 iptables -N SSHSCAN
131 iptables -A INPUT -i "$ADM_IF" -p tcp --dport 22 -m state --state NEW -j
132 iptables -A SSHSCAN -m recent --set --name SSH --rsource
133 iptables -A SSHSCAN -m recent --update --seconds 60 --hitcount 4 --name !
134 iptables -A SSHSCAN -m recent --update --seconds 60 --hitcount 4 --name !
135 iptables -A INPUT -i "$ADM_IF" -p tcp --dport 22 -j ACCEPT
136
137 # ===== Logging drops =====
138 iptables -A INPUT -j LOG_DROP
139 iptables -A FORWARD -j LOG_DROP
140
141 echo "Firewall zone-based with Lab access (Riset3) activated."

```

Firewall (System logging,seperti IDS/IPS)

```

1  #!/bin/bash
2  set -euo pipefail
3
4  # ===== Interface & Subnet (192.168.x.x) =====
5  WAN_IF="eth0"
6  ADM_IF="eth1"; ADM_NET="192.168.1.0/24"
7  MHS_IF="eth2"; MHS_NET="192.168.2.0/24"
8  AKD_IF="eth3"; AKD_NET="192.168.3.0/24"
9  RST_IF="eth4"; RST_NET="192.168.4.0/24"
10 GST_IF="eth5"; GST_NET="192.168.5.0/24"
11
12 # LAB host spesifik
13 LAB_HOST="192.168.8.4"
14 BLOCKED_HOSTS="192.168.8.2,192.168.8.3"
15
16 # Service ports
17 WEB_PORTS="80,443"

```

```
18 DNS_PORT=53
19 LAB_PORTS="22,80,443"
20
21 # ===== Sistem & Reset =====
22 echo 1 > /proc/sys/net/ipv4/ip_forward
23
24 iptables -t nat -F; iptables -t mangle -F; iptables -F; iptables -X
25 iptables -P INPUT DROP; iptables -P FORWARD DROP; iptables -P OUTPUT ACCEPT
26
27 # ===== Chains utilitas =====
28 iptables -N LOG_DROP
29 iptables -A LOG_DROP -m limit --limit 10/min -j LOG --log-prefix "DROP "
30 iptables -A LOG_DROP -j DROP
31
32 # Chain khusus untuk deteksi serangan
33 iptables -N ATTACK_DETECT
34 iptables -A ATTACK_DETECT -m limit --limit 5/min -j LOG --log-prefix "ATTACK_DETECT "
35 iptables -A ATTACK_DETECT -j DROP
36
37 # ===== Basic hygiene =====
38 iptables -A INPUT -i lo -j ACCEPT
39 iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
40 iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
41 iptables -A INPUT -m state --state INVALID -j LOG --log-prefix "INVALID_IP "
42 iptables -A INPUT -m state --state INVALID -j DROP
43 iptables -A FORWARD -m state --state INVALID -j DROP
44
45 # ===== Anti-spoofing & Logging =====
46 for NET in 192.168.0.0/16 10.0.0.0/8 172.16.0.0/12 127.0.0.0/8 169.254.0.0/16
47 do
48     iptables -A INPUT -i "$WAN_IF" -s "$NET" -j LOG --log-prefix "SPOOF_AT_$NET "
49     iptables -A INPUT -i "$WAN_IF" -s "$NET" -j DROP
50     iptables -A FORWARD -i "$WAN_IF" -s "$NET" -j DROP
51 done
52
53 # Lateral anti-spoof dengan logging
54 iptables -A INPUT -i "$ADM_IF" -s "$ADM_NET" -j ACCEPT
55 iptables -A INPUT -i "$ADM_IF" ! -s "$ADM_NET" -j LOG --log-prefix "SPOOF_AT_$ADM_NET "
56 iptables -A INPUT -i "$ADM_IF" ! -s "$ADM_NET" -j DROP
57
58 iptables -A INPUT -i "$MHS_IF" -s "$MHS_NET" -j ACCEPT
59 iptables -A INPUT -i "$MHS_IF" ! -s "$MHS_NET" -j LOG --log-prefix "SPOOF_AT_$MHS_NET "
60 iptables -A INPUT -i "$MHS_IF" ! -s "$MHS_NET" -j DROP
61
62 iptables -A INPUT -i "$AKD_IF" -s "$AKD_NET" -j ACCEPT
63 iptables -A INPUT -i "$AKD_IF" ! -s "$AKD_NET" -j LOG --log-prefix "SPOOF_AT_$AKD_NET "
64 iptables -A INPUT -i "$AKD_IF" ! -s "$AKD_NET" -j DROP
65
66 iptables -A INPUT -i "$RST_IF" -s "$RST_NET" -j ACCEPT
67 iptables -A INPUT -i "$RST_IF" ! -s "$RST_NET" -j LOG --log-prefix "SPOOF_AT_$RST_NET "
```

```

67 iptables -A INPUT -i "$RST_IF" ! -s "$RST_NET" -j DROP
68
69 iptables -A INPUT -i "$GST_IF" -s "$GST_NET" -j ACCEPT
70 iptables -A INPUT -i "$GST_IF" ! -s "$GST_NET" -j LOG --log-prefix "SPOOL
71 iptables -A INPUT -i "$GST_IF" ! -s "$GST_NET" -j DROP
72
73 # ===== NAT Masquerading =====
74 iptables -t nat -A POSTROUTING -o "$WAN_IF" -j MASQUERADE
75
76 # ===== ICMP FIX & Logging =====
77 # Izinkan ICMP outbound dan log percobaan flood
78 iptables -A FORWARD -i "$ADM_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
79 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
80 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
81 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
82 iptables -A FORWARD -i "$AKD_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
83 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
84 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
85 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
86 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p icmp --icmp-type echo-r
87
88 # Izinkan ICMP reply
89 iptables -A FORWARD -i "$WAN_IF" -o "$ADM_IF" -p icmp --icmp-type echo-r
90 iptables -A FORWARD -i "$WAN_IF" -o "$MHS_IF" -p icmp --icmp-type echo-r
91 iptables -A FORWARD -i "$WAN_IF" -o "$AKD_IF" -p icmp --icmp-type echo-r
92 iptables -A FORWARD -i "$WAN_IF" -o "$RST_IF" -p icmp --icmp-type echo-r
93 iptables -A FORWARD -i "$WAN_IF" -o "$GST_IF" -p icmp --icmp-type echo-r
94
95 # Rate limit ICMP ke firewall
96 iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/se
97 iptables -A INPUT -p icmp --icmp-type echo-request -j LOG --log-prefix "
98 iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
99
100 # ===== PORT SCAN DETECTION =====
101 # Deteksi NULL scan (TCP flags ALL NONE)
102 iptables -A INPUT -p tcp --tcp-flags ALL NONE -j LOG --log-prefix "NULL_
103 iptables -A INPUT -p tcp --tcp-flags ALL NONE -j ATTACK_DETECT
104
105 # Deteksi SYN-FIN scan (invalid combination)
106 iptables -A INPUT -p tcp --tcp-flags SYN,FIN SYN,FIN -j LOG --log-prefix
107 iptables -A INPUT -p tcp --tcp-flags SYN,FIN SYN,FIN -j ATTACK_DETECT
108
109 # Deteksi XMAS scan (FIN,URG,PSH)
110 iptables -A INPUT -p tcp --tcp-flags FIN,URG,PSH FIN,URG,PSH -j LOG --lo
111 iptables -A INPUT -p tcp --tcp-flags FIN,URG,PSH FIN,URG,PSH -j ATTACK_DI
112
113 # ===== KEBIJAKAN LAB (Riset3) =====
114
115 # BLOKIR Mahasiswa -> 192.168.8.2 dan 192.168.8.3 dengan logging

```

```

116 iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d 192.168.8.2 -j LOG --log
117 iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d 192.168.8.2 -j DROP
118 iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d 192.168.8.3 -j LOG --log
119 iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d 192.168.8.3 -j DROP
120
121 # IZINKAN Mahasiswa -> Lab 192.168.8.4 (LIMITED: SSH, HTTP, HTTPS, Ping)
122 iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d "$LAB_HOST" -p tcp -m multi
123 iptables -A FORWARD -i "$MHS_IF" -o "$RST_IF" -d "$LAB_HOST" -p icmp --icmp
124
125 # ===== KEBIJAKAN ZONA LAIN =====
126
127 # ADMIN -> semua
128 iptables -A FORWARD -i "$ADM_IF" -j ACCEPT
129
130 # MAHASISWA -> Internet (HTTP/HTTPS/DNS) dengan rate limit
131 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp -m multiport --dports
132 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp -m multiport --dports
133 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp -m multiport --dports
134 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j
135 iptables -A FORWARD -i "$MHS_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j
136
137 # AKADEMIK -> Internet (full)
138 iptables -A FORWARD -i "$AKD_IF" -o "$WAN_IF" -j ACCEPT
139
140 # AKADEMIK -> Riset (full)
141 iptables -A FORWARD -i "$AKD_IF" -o "$RST_IF" -j ACCEPT
142
143 # RISET/IoT -> Internet (HTTPS+DNS)
144 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport 443 -j ACCEPT
145 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j
146 iptables -A FORWARD -i "$RST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j
147
148 # RISET/IoT -> Admin (monitoring)
149 iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p udp --dport 514 -j ACCEPT
150 iptables -A FORWARD -i "$RST_IF" -o "$ADM_IF" -p tcp -m multiport --dports
151
152 # RISET/IoT -> Akademik (full)
153 iptables -A FORWARD -i "$RST_IF" -o "$AKD_IF" -j ACCEPT
154
155 # GUEST -> Internet (HTTP/HTTPS/DNS) dengan rate limit ketat
156 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp -m multiport --dports
157 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp -m multiport --dports
158 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp -m multiport --dports
159 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p udp --dport $DNS_PORT -j
160 iptables -A FORWARD -i "$GST_IF" -o "$WAN_IF" -p tcp --dport $DNS_PORT -j
161
162 # SSH brute-force protection dengan logging
163 iptables -N SSHSCAN
164 iptables -A INPUT -i "$ADM_IF" -p tcp --dport 22 -m state --state NEW -j

```



```
165 iptables -A SSHSCAN -m recent --set --name SSH --rsource
166 iptables -A SSHSCAN -m recent --update --seconds 60 --hitcount 4 --name :
167 iptables -A SSHSCAN -m recent --update --seconds 60 --hitcount 4 --name :
168 iptables -A INPUT -i "$ADM_IF" -p tcp --dport 22 -j ACCEPT
169
170 # ===== Logging drops =====
171 iptables -A INPUT -j LOG_DROP
172 iptables -A FORWARD -j LOG_DROP
173
174 echo "Firewall IDS/IPS activated with comprehensive logging."
175
```

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 & Rourn 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
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:~#

```

```

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

```
1 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