Table of Contents

IPv4 Rules

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]

# Always allow loopback
-A INPUT -i lo -j ACCEPT

# Allow established/related to talk back in
-A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
-A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

# ICMP (ping) from LAN/DMZ (adjust to taste)
-A INPUT -i br2 -p icmp -j ACCEPT
-A INPUT -i br3 -p icmp -j ACCEPT
-A INPUT -i br4 -p icmp -j ACCEPT

# SSH to the router from LAN only (adjust/lock down as needed)
-A INPUT -i br2 -p tcp --dport 22 -j ACCEPT
-A INPUT -i br4 -p tcp --dport 22 -j ACCEPT

# DNS & DHCP to the router from LAN/DMZ (dnsmasq)
-A INPUT -i br2 -p udp --dport 67:68 -j ACCEPT
-A INPUT -i br3 -p udp --dport 67:68 -j ACCEPT
-A INPUT -i br4 -p udp --dport 67:68 -j ACCEPT
-A INPUT -i br2 -p tcp --dport 53 -j ACCEPT
-A INPUT -i br2 -p udp --dport 53 -j ACCEPT
-A INPUT -i br3 -p tcp --dport 53 -j ACCEPT
-A INPUT -i br3 -p udp --dport 53 -j ACCEPT
-A INPUT -i br4 -p tcp --dport 53 -j ACCEPT
-A INPUT -i br4 -p udp --dport 53 -j ACCEPT

# Forwarding policy:
# - LAN -> WAN: allow
# - DMZ -> WAN: allow
# - WLAN -> WAN: allow
# - WAN -> LAN/DMZ: block unless established/related
# - LAN <-> DMZ: default block (tight). Uncomment the next line if you
want LAN to reach DMZ.
-A FORWARD -i br2 -o br0 -j ACCEPT
```

```
-A FORWARD -i br4 -o br0 -j ACCEPT
-A FORWARD -i br3 -o br0 -j ACCEPT
# Allow LAN to reach DMZ (optional)
-A FORWARD -i br2 -o br3 -j ACCEPT
-A FORWARD -i br4 -o br3 -j ACCEPT
# Allow LAN and WLAN to reach each other (optional)
-A FORWARD -i br2 -o br4 -j ACCEPT
-A FORWARD -i br4 -o br2 -j ACCEPT

COMMIT

*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]

# NAT (masquerade) LAN+DMZ out of WAN
-A POSTROUTING -o br0 -j MASQUERADE

# Example: Port-forward 80 on WAN to a DMZ host 192.168.60.10
# (and allow the forward)
#-A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination
192.168.60.10:80
#-A FORWARD -i eth0 -p tcp -d 192.168.60.10 --dport 80 -j ACCEPT

COMMIT
```

```
# manual
sudo iptables -I FORWARD 1 -i br1 -o eth0 -j ACCEPT
sudo iptables -I INPUT 1 -i br1 -p udp --dport 67:68 -j ACCEPT
sudo iptables -I INPUT 1 -i br1 -p udp --dport 53 -j ACCEPT
sudo iptables -I INPUT 1 -i br1 -p tcp --dport 53 -j ACCEPT
sudo iptables -I INPUT 1 -i br1 -p icmp -j ACCEPT
sudo iptables -I INPUT 1 -i br1 -p tcp --dport 22 -j ACCEPT
sudo netfilter-persistent save
```

From:
https://laswitchtech.com/ - **LaswitchTech**

Permanent link:
https://laswitchtech.com/en/projects/router-pi5/documentation/ipv4-rules

Last update: **2025/09/17 20:33**