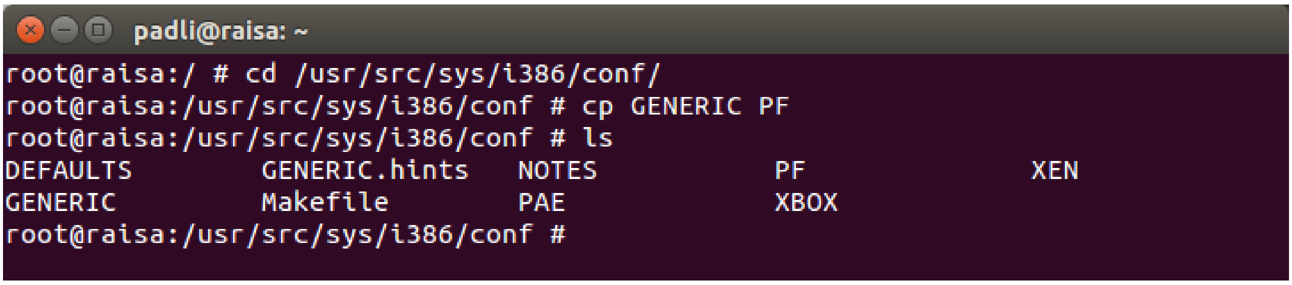
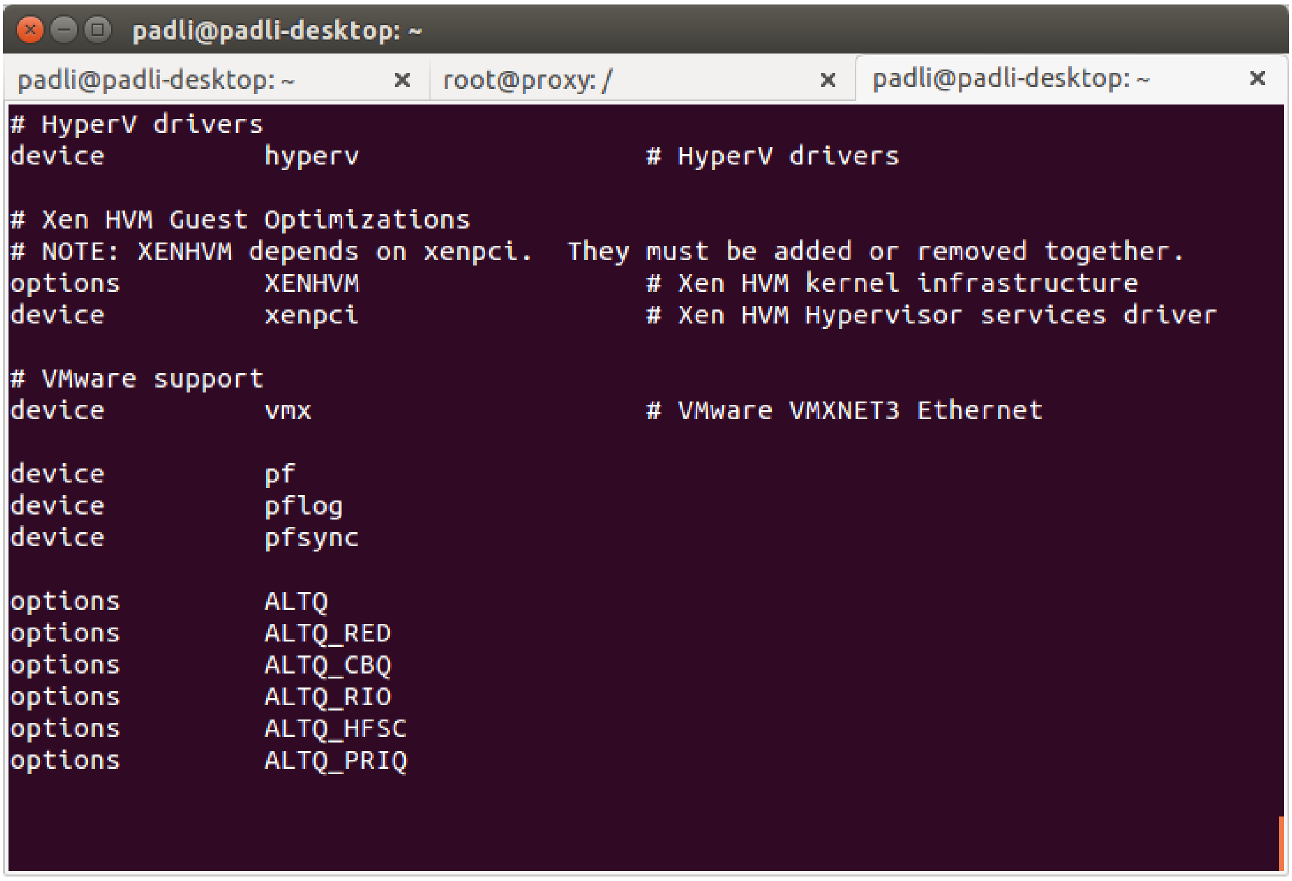
ROUTER + FIREWALL PF (PACKET FILTER)

1. kompile kernel freebsd “cd /usr/src/sys/i386/conf” & copy kernel “cp GENERIC PF”



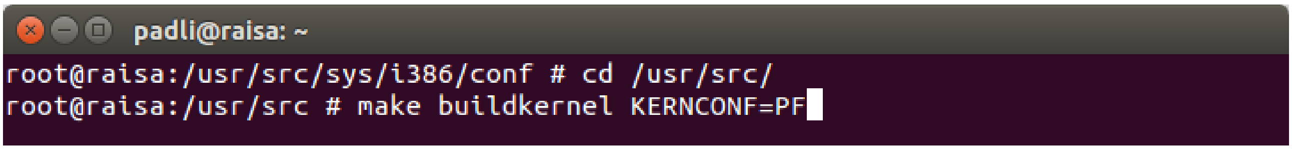
```
root@raisa:/ # cd /usr/src/sys/i386/conf/
root@raisa:/usr/src/sys/i386/conf # cp GENERIC PF
root@raisa:/usr/src/sys/i386/conf # ls
DEFAULTS        GENERIC.hints   NOTES           PF              XEN
GENERIC         Makefile        PAE             XBOX
root@raisa:/usr/src/sys/i386/conf #
```

2. edit kernel PF “vi PF” tambahkan pf dan ALTQ

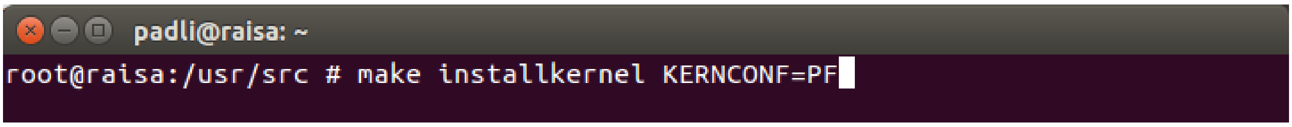


```
# HyperV drivers
device          hyperv                  # HyperV drivers

# Xen HVM Guest Optimizations
# NOTE: XENHVM depends on xenpci.  They must be added or removed together.
options         XENHVM                  # Xen HVM kernel infrastructure
device          xenpci                  # Xen HVM Hypervisor services driver

# VMware support
device          vmx                     # VMware VMXNET3 Ethernet

device          pf
device          pflog
device          pfsync

options         ALTQ
options         ALTQ_RED
options         ALTQ_CBQ
options         ALTQ_RIO
options         ALTQ_HFSC
options         ALTQ_PRIQ
```

3. pindah dir “cd /usr/src” & build kernel “make buildkernel KERNCONF=PF” & install kernel “make installkernel KERNCONF=PF” & restart komputer

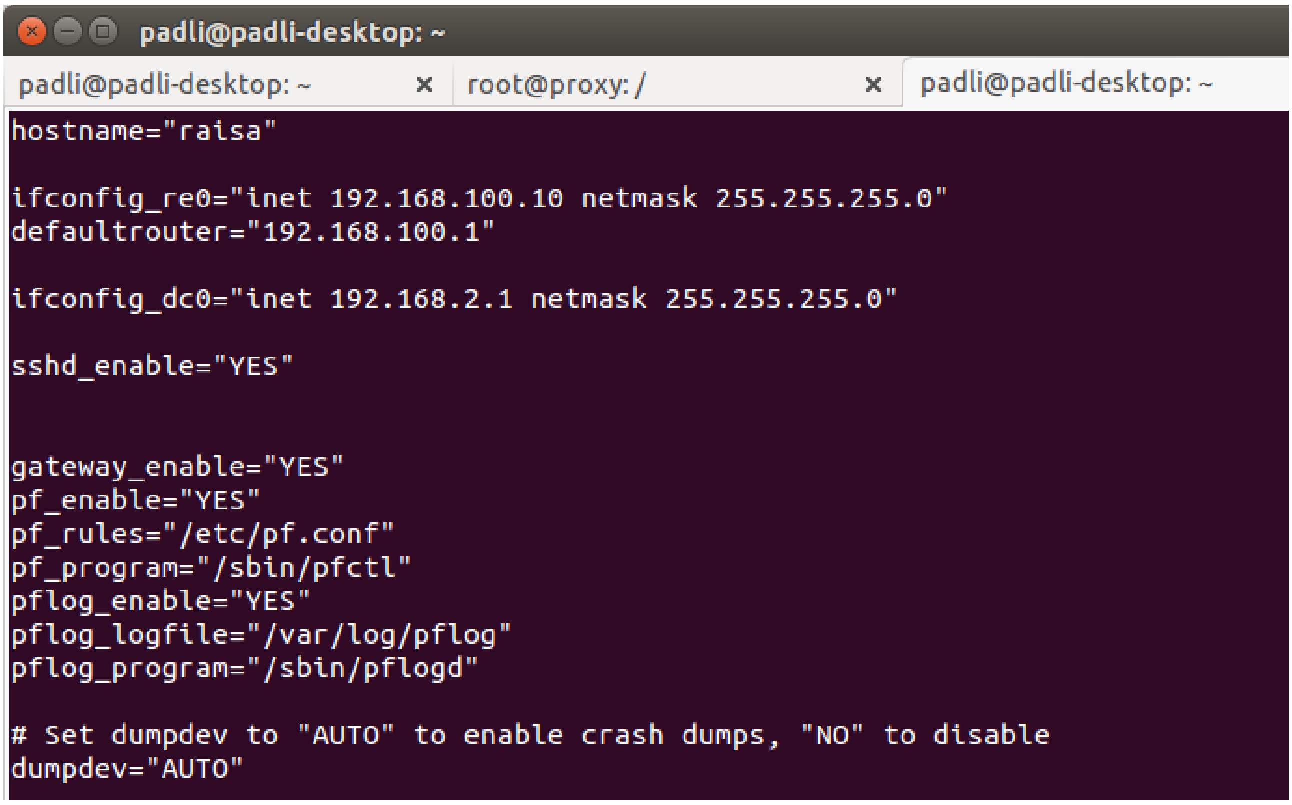


```
root@raisa:/usr/src/sys/i386/conf # cd /usr/src/
root@raisa:/usr/src # make buildkernel KERNCONF=PF
```



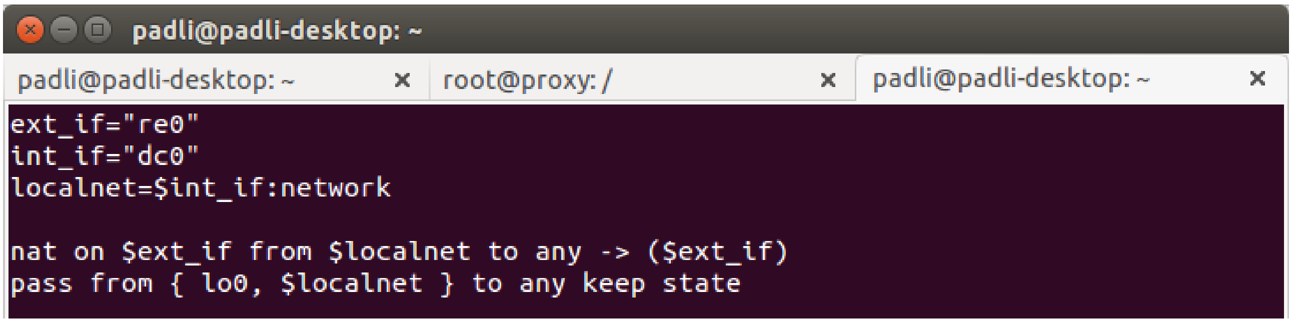
```
root@raisa:/usr/src # make installkernel KERNCONF=PF
```

4. edit “vi /etc/rc.conf” tambahkan baris



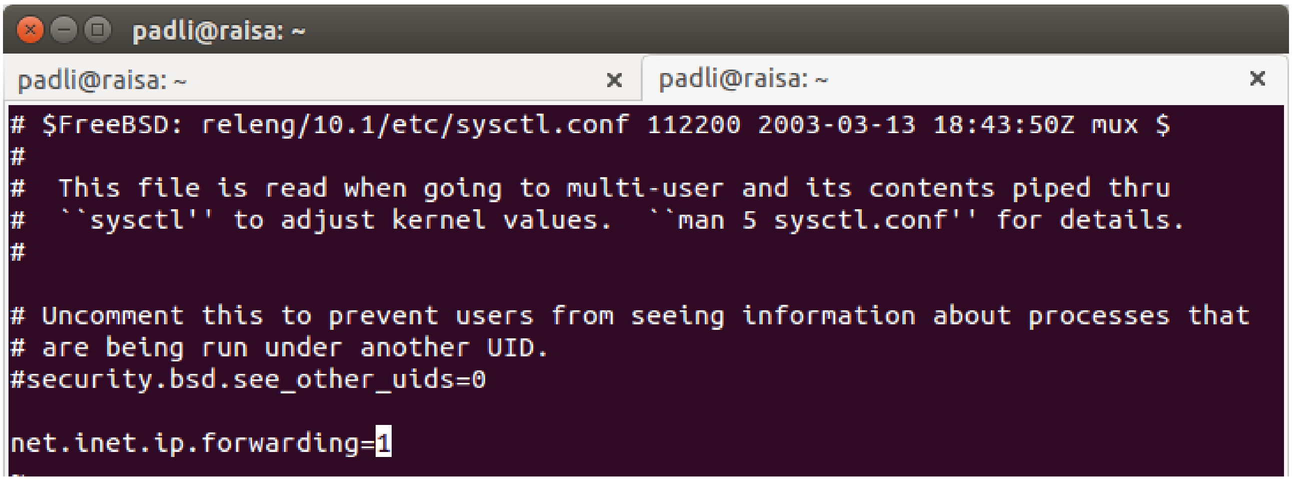
```
hostname="raisa"

ifconfig_re0="inet 192.168.100.10 netmask 255.255.255.0"
defaultrouter="192.168.100.1"

ifconfig_dc0="inet 192.168.2.1 netmask 255.255.255.0"

sshd_enable="YES"


gateway_enable="YES"
pf_enable="YES"
pf_rules="/etc/pf.conf"
pf_program="/sbin/pfctl"
pflog_enable="YES"
pflog_logfile="/var/log/pflog"
pflog_program="/sbin/pflogd"

# Set dumpdev to "AUTO" to enable crash dumps, "NO" to disable
dumpdev="AUTO"
```

5. edit “vi /etc/pf.conf” tambahkan baris ini dan restart pf “pfctl -f /etc/pf.conf” config sesuaikan dengan kebutuhan



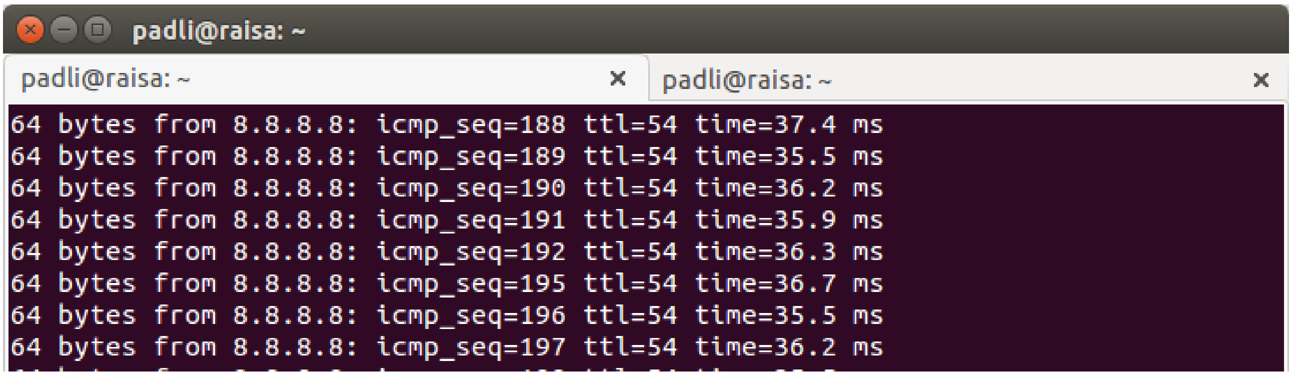
```
ext_if="re0"
int_if="dc0"
localnet=$int_if:network

nat on $ext_if from $localnet to any -> ($ext_if)
pass from { lo0, $localnet } to any keep state
```

6. edit “vi /etc/sysctl.conf” tambahkan baris



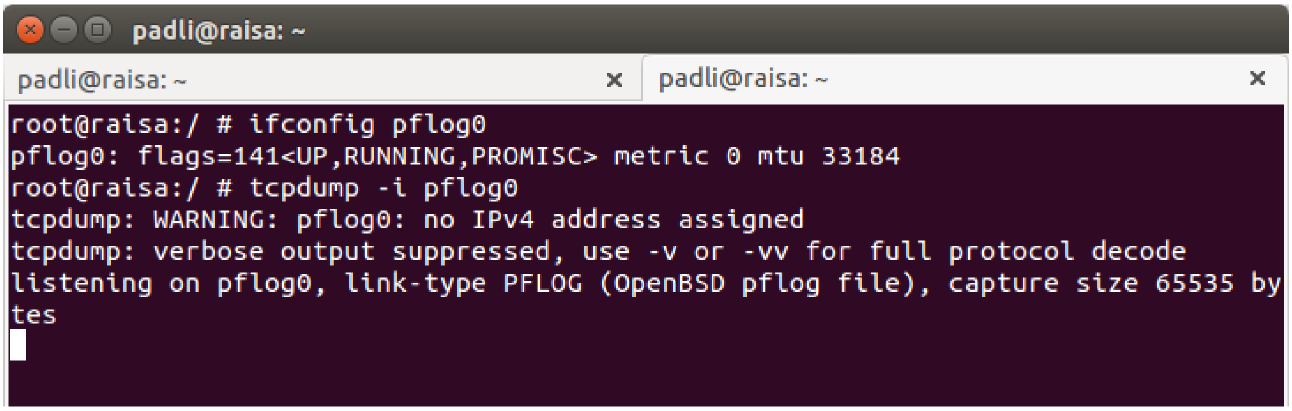
```
# $FreeBSD: releng/10.1/etc/sysctl.conf 112200 2003-03-13 18:43:50Z mux $
#
#  This file is read when going to multi-user and its contents piped thru
#  ``sysctl'' to adjust kernel values.  ``man 5 sysctl.conf'' for details.
#

# Uncomment this to prevent users from seeing information about processes that
# are being run under another UID.
#security.bsd.see_other_uids=0

net.inet.ip.forwarding=1
```

7. tes ping dari client

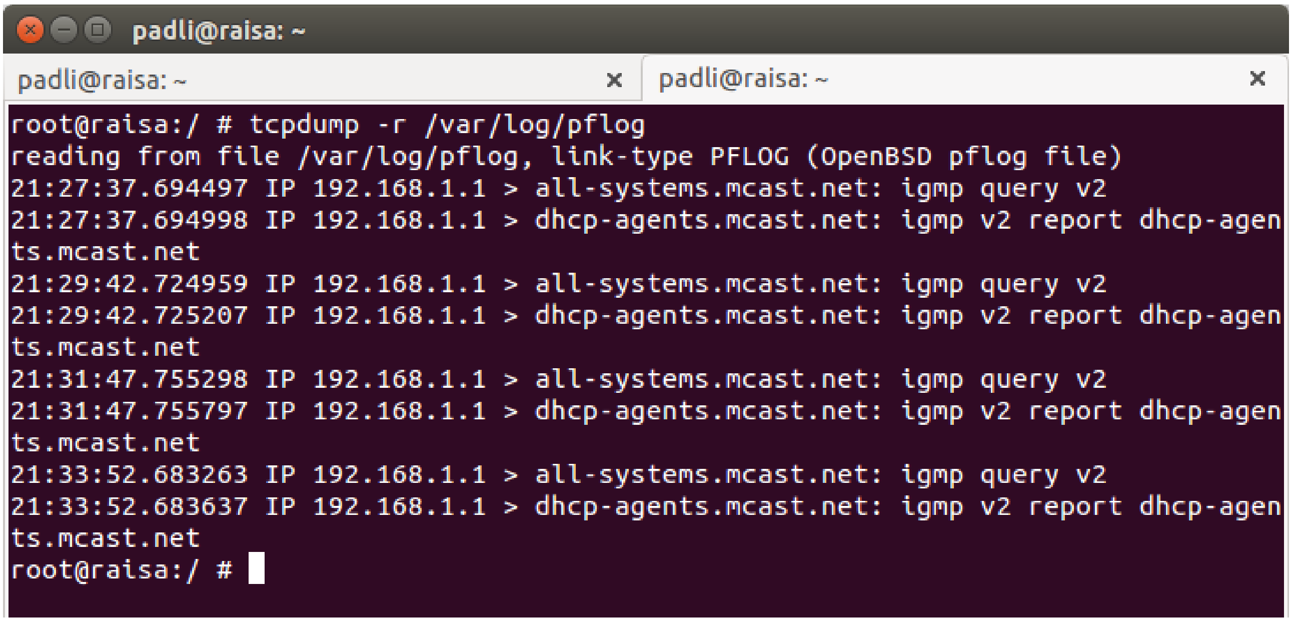


```
64 bytes from 8.8.8.8: icmp_seq=188 ttl=54 time=37.4 ms
64 bytes from 8.8.8.8: icmp_seq=189 ttl=54 time=35.5 ms
64 bytes from 8.8.8.8: icmp_seq=190 ttl=54 time=36.2 ms
64 bytes from 8.8.8.8: icmp_seq=191 ttl=54 time=35.9 ms
64 bytes from 8.8.8.8: icmp_seq=192 ttl=54 time=36.3 ms
64 bytes from 8.8.8.8: icmp_seq=195 ttl=54 time=36.7 ms
64 bytes from 8.8.8.8: icmp_seq=196 ttl=54 time=35.5 ms
64 bytes from 8.8.8.8: icmp_seq=197 ttl=54 time=36.2 ms
```

8. cek pflog “ifconfig pflog0” & “tcpdump -i pflog0” & “tcpdump -r /var/log/pflog”

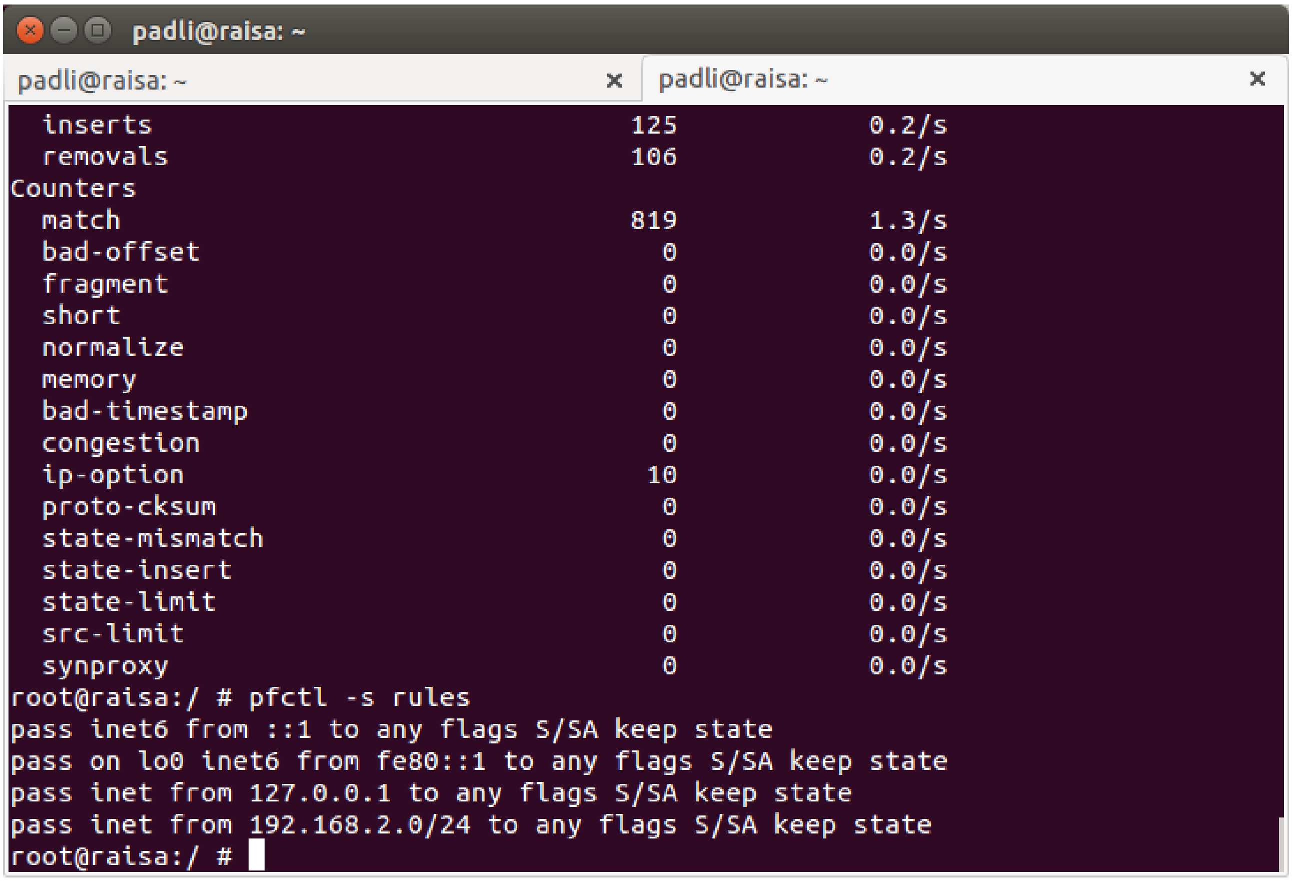


```
root@raisa:/ # ifconfig pflog0
pflog0: flags=141<UP,RUNNING,PROMISC> metric 0 mtu 33184
root@raisa:/ # tcpdump -i pflog0
tcpdump: WARNING: pflog0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on pflog0, link-type PFLOG (OpenBSD pflog file), capture size 65535 by
tes
```



```
root@raisa:/ # tcpdump -r /var/log/pflog
reading from file /var/log/pflog, link-type PFLOG (OpenBSD pflog file)
21:27:37.694497 IP 192.168.1.1 > all-systems.mcast.net: igmp query v2
21:27:37.694998 IP 192.168.1.1 > dhcp-agents.mcast.net: igmp v2 report dhcp-agen
ts.mcast.net
21:29:42.724959 IP 192.168.1.1 > all-systems.mcast.net: igmp query v2
21:29:42.725207 IP 192.168.1.1 > dhcp-agents.mcast.net: igmp v2 report dhcp-agen
ts.mcast.net
21:31:47.755298 IP 192.168.1.1 > all-systems.mcast.net: igmp query v2
21:31:47.755797 IP 192.168.1.1 > dhcp-agents.mcast.net: igmp v2 report dhcp-agen
ts.mcast.net
21:33:52.683263 IP 192.168.1.1 > all-systems.mcast.net: igmp query v2
21:33:52.683637 IP 192.168.1.1 > dhcp-agents.mcast.net: igmp v2 report dhcp-agen
ts.mcast.net
root@raisa:/ #
```

8. tambahan “pfctl -s info” “pfctl -s rules”



```
  inserts                              125             0.2/s
  removals                             106             0.2/s
Counters
  match                                819             1.3/s
  bad-offset                             0             0.0/s
  fragment                               0             0.0/s
  short                                  0             0.0/s
  normalize                              0             0.0/s
  memory                                 0             0.0/s
  bad-timestamp                          0             0.0/s
  congestion                             0             0.0/s
  ip-option                             10             0.0/s
  proto-cksum                            0             0.0/s
  state-mismatch                         0             0.0/s
  state-insert                           0             0.0/s
  state-limit                            0             0.0/s
  src-limit                              0             0.0/s
  synproxy                               0             0.0/s
root@raisa:/ # pfctl -s rules
pass inet6 from ::1 to any flags S/SA keep state
pass on lo0 inet6 from fe80::1 to any flags S/SA keep state
pass inet from 127.0.0.1 to any flags S/SA keep state
pass inet from 192.168.2.0/24 to any flags S/SA keep state
root@raisa:/ # 
```