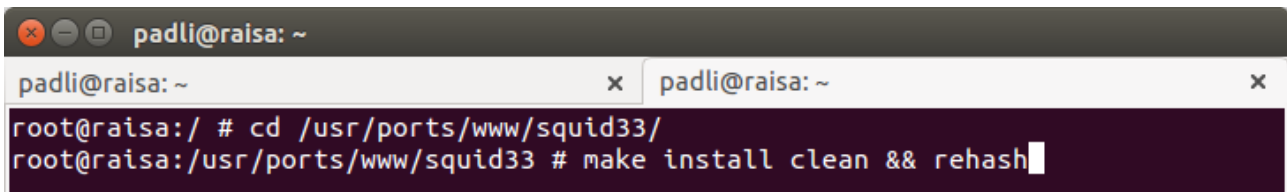


PROXY SQUID+IPFW+SARG

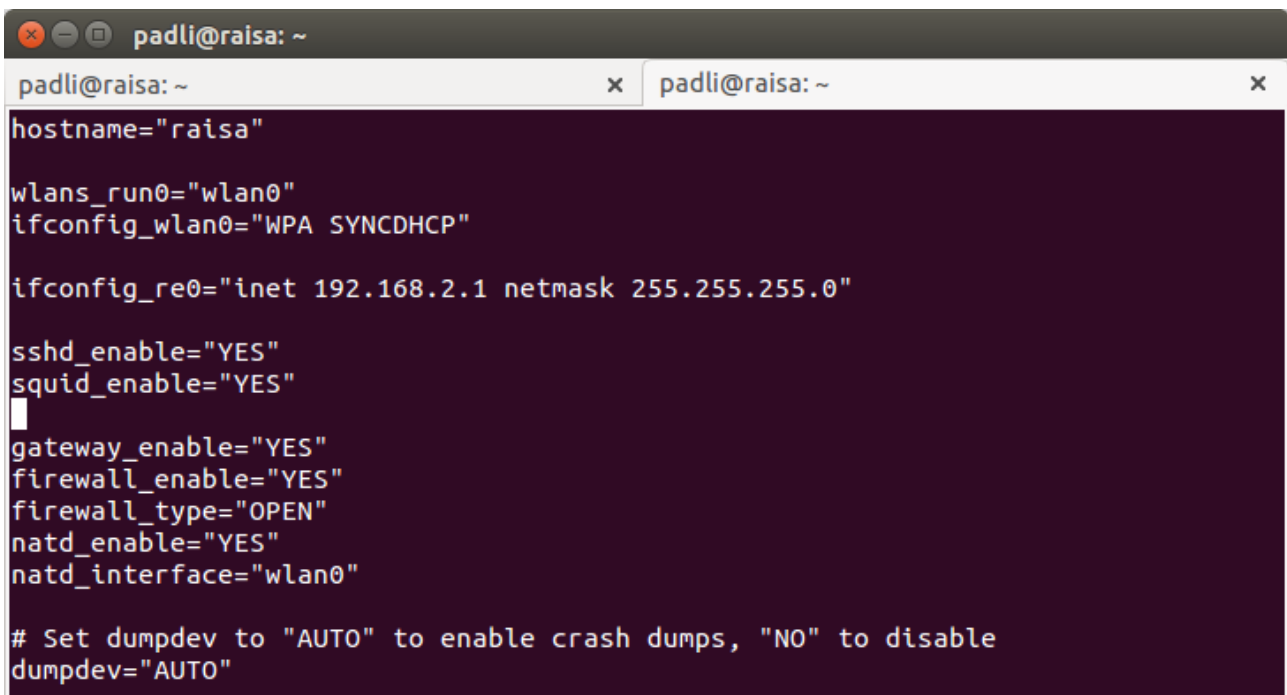
contoh file config squid 33, sarg terlampir

1. "cd /usr/ports/www/squid33", "make install clean && rehash" config sesuaikan dengan kebutuhan.



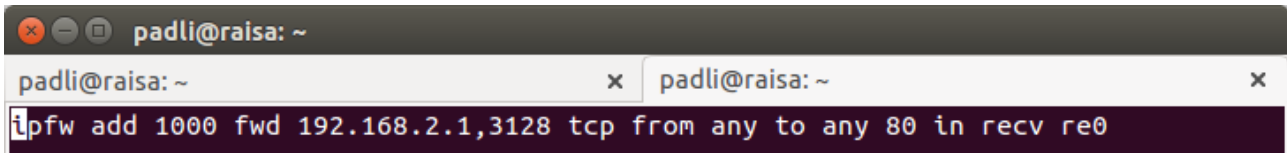
```
padli@raisa: ~  
padli@raisa: ~ x padli@raisa: ~ x  
root@raisa:/ # cd /usr/ports/www/squid33/  
root@raisa:/usr/ports/www/squid33 # make install clean && rehash
```

2. edit "vi /etc/rc.conf" tambahkan baris



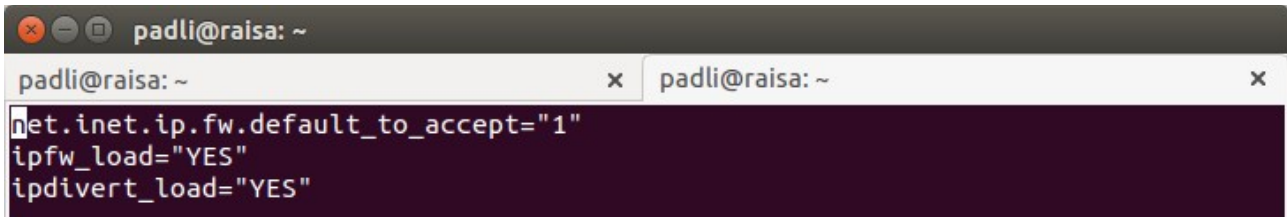
```
padli@raisa: ~  
padli@raisa: ~ x padli@raisa: ~ x  
hostname="raisa"  
  
wlans_run0="wlan0"  
ifconfig_wlan0="WPA SYNCDHCP"  
  
ifconfig_re0="inet 192.168.2.1 netmask 255.255.255.0"  
  
sshd_enable="YES"  
squid_enable="YES"  
  
gateway_enable="YES"  
firewall_enable="YES"  
firewall_type="OPEN"  
natd_enable="YES"  
natd_interface="wlan0"  
  
# Set dumpdev to "AUTO" to enable crash dumps, "NO" to disable  
dumpdev="AUTO"
```

3. edit "vi /etc/rc.local" tambahkan baris



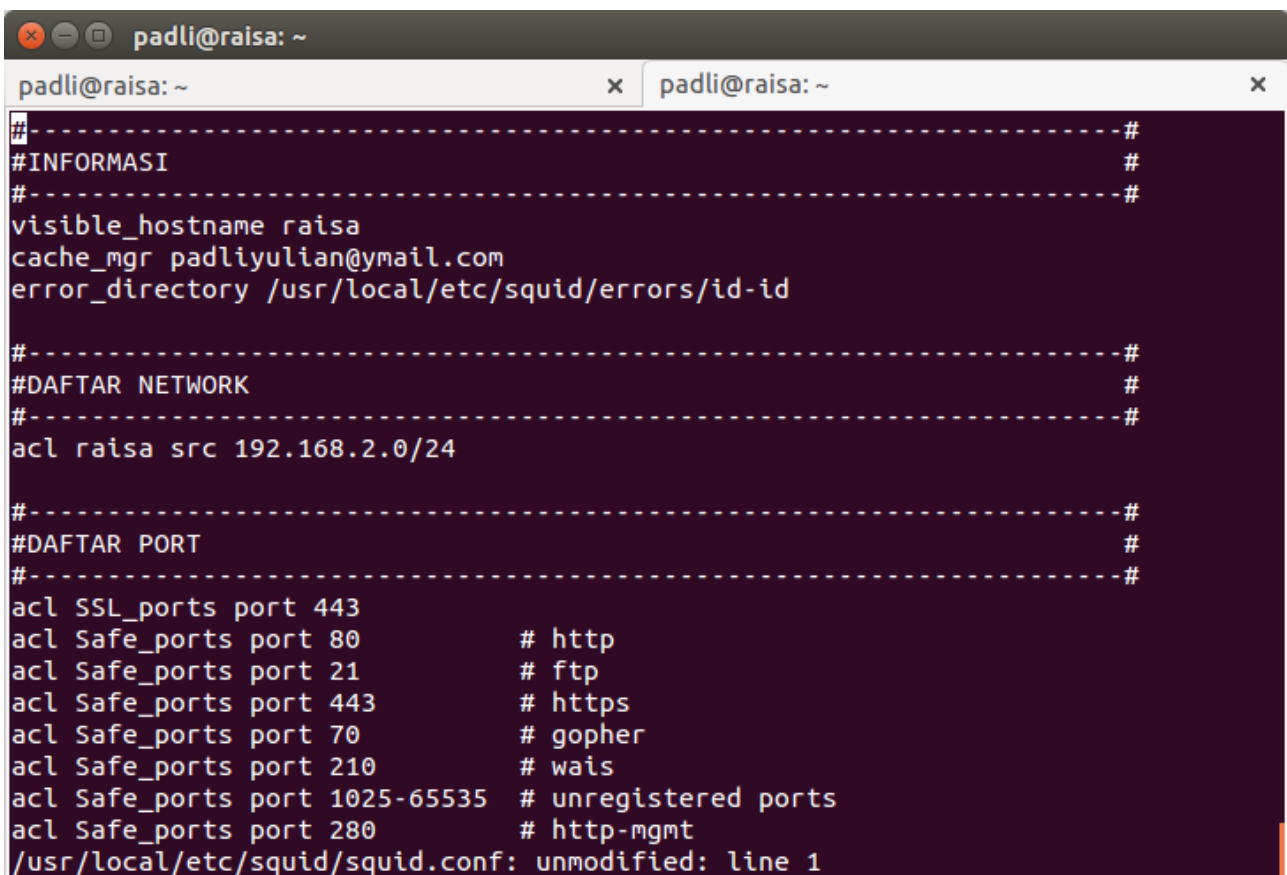
```
padli@raisa: ~  
padli@raisa: ~  
ipfw add 1000 fwd 192.168.2.1,3128 tcp from any to any 80 in recv re0
```

4. edit "vi /boot/loader.conf" tambahkan baris



```
padli@raisa: ~  
padli@raisa: ~  
net.inet.ip.fw.default_to_accept="1"  
ipfw_load="YES"  
ipdivert_load="YES"
```

5. edit "vi /usr/local/etc/squid/squid.conf" config sesuaikan dengan kebutuhan, contoh file config terlampir.

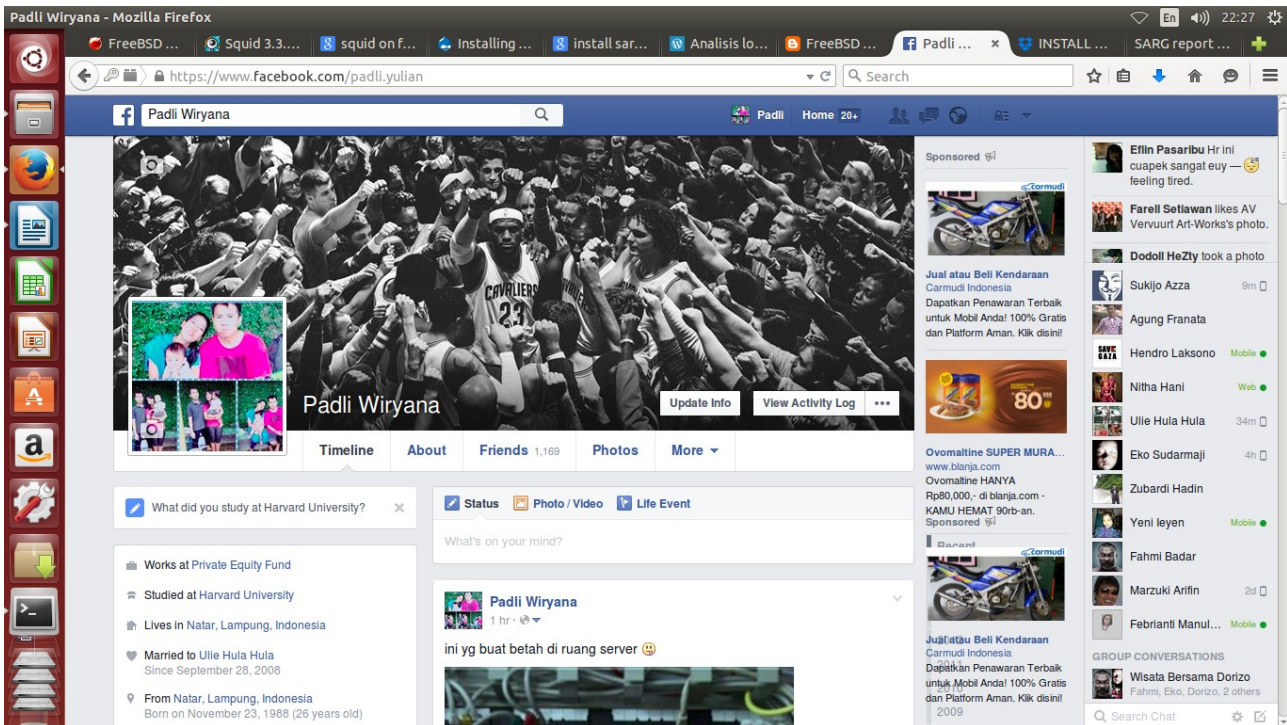


```
padli@raisa: ~  
padli@raisa: ~  
#-----#  
#INFORMASI#  
#-----#  
visible_hostname raisa  
cache_mgr padliyulian@ymail.com  
error_directory /usr/local/etc/squid/errors/id-id  
  
#-----#  
#DAFTAR NETWORK#  
#-----#  
acl raisa src 192.168.2.0/24  
  
#-----#  
#DAFTAR PORT#  
#-----#  
acl SSL_ports port 443  
acl Safe_ports port 80      # http  
acl Safe_ports port 21      # ftp  
acl Safe_ports port 443     # https  
acl Safe_ports port 70      # gopher  
acl Safe_ports port 210     # wais  
acl Safe_ports port 1025-65535 # unregistered ports  
acl Safe_ports port 280     # http-mgmt  
/usr/local/etc/squid/squid.conf: unmodified: line 1
```

6. buat cache dir "squid -z" lalu restart komputer

```
padli@raisa: ~  
padli@raisa: ~  
root@raisa:/ # squid -z
```

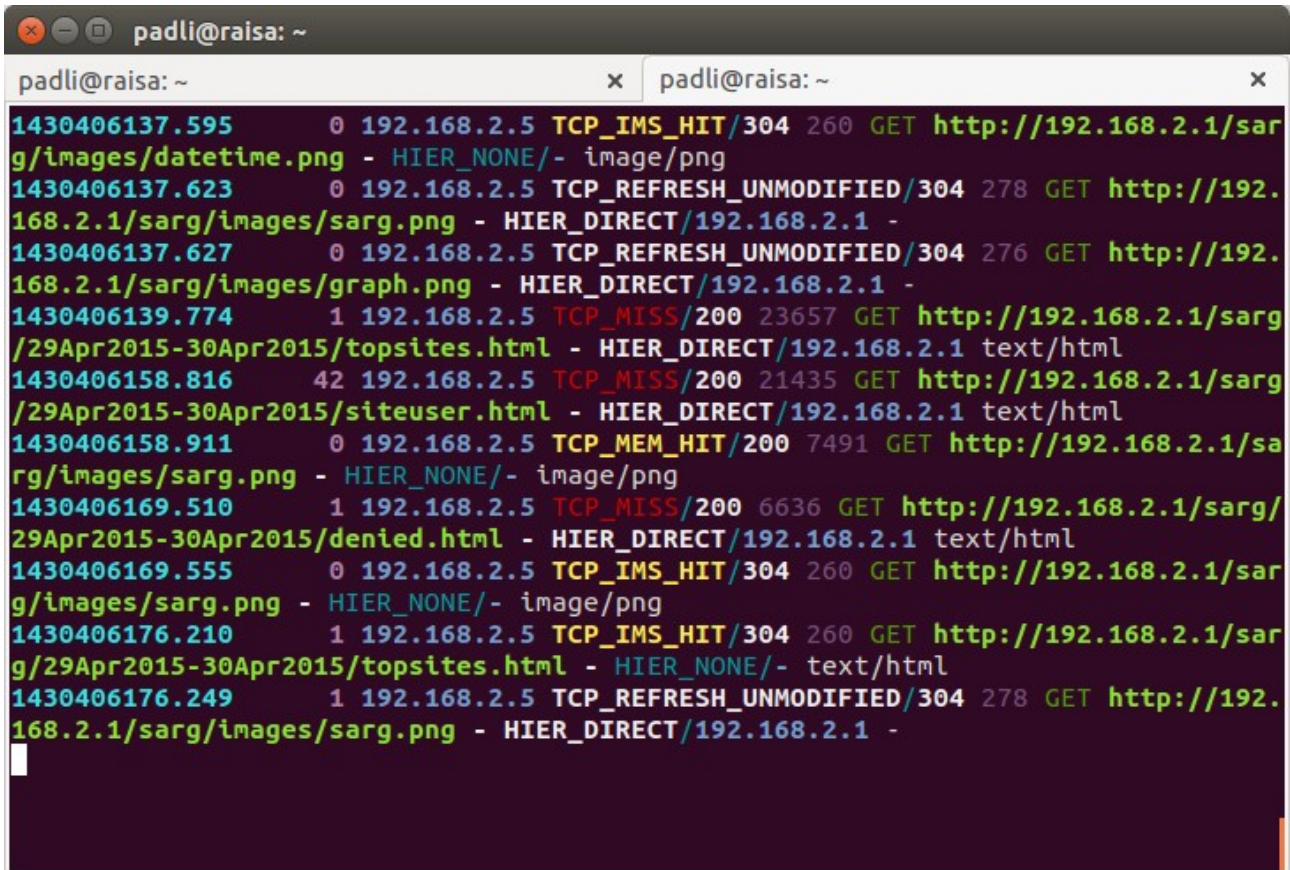
7. tes browsing



8. untuk log akses squid, install ccze "cd /usr/ports/sysutils/ccze", "make install clean && rehash"

```
padli@raisa: ~  
padli@raisa: ~  
root@raisa:/ # cd /usr/ports/sysutils/ccze/  
root@raisa:/usr/ports/sysutils/ccze # make install clean && rehash
```

9. cek log akses squid "tail -f /var/log/squid/access.log | ccze"



```
padli@raisa: ~  
padli@raisa: ~  
1430406137.595      0 192.168.2.5 TCP_IMS_HIT/304 260 GET http://192.168.2.1/sarg/images/datetime.png - HIER_NONE/- image/png  
1430406137.623      0 192.168.2.5 TCP_REFRESH_UNMODIFIED/304 278 GET http://192.168.2.1/sarg/images/sarg.png - HIER_DIRECT/192.168.2.1 -  
1430406137.627      0 192.168.2.5 TCP_REFRESH_UNMODIFIED/304 276 GET http://192.168.2.1/sarg/images/graph.png - HIER_DIRECT/192.168.2.1 -  
1430406139.774      1 192.168.2.5 TCP_MISS/200 23657 GET http://192.168.2.1/sarg/29Apr2015-30Apr2015/topsites.html - HIER_DIRECT/192.168.2.1 text/html  
1430406158.816     42 192.168.2.5 TCP_MISS/200 21435 GET http://192.168.2.1/sarg/29Apr2015-30Apr2015/siteuser.html - HIER_DIRECT/192.168.2.1 text/html  
1430406158.911      0 192.168.2.5 TCP_MEM_HIT/200 7491 GET http://192.168.2.1/sarg/images/sarg.png - HIER_NONE/- image/png  
1430406169.510      1 192.168.2.5 TCP_MISS/200 6636 GET http://192.168.2.1/sarg/29Apr2015-30Apr2015/denied.html - HIER_DIRECT/192.168.2.1 text/html  
1430406169.555      0 192.168.2.5 TCP_IMS_HIT/304 260 GET http://192.168.2.1/sarg/images/sarg.png - HIER_NONE/- image/png  
1430406176.210      1 192.168.2.5 TCP_IMS_HIT/304 260 GET http://192.168.2.1/sarg/29Apr2015-30Apr2015/topsites.html - HIER_NONE/- text/html  
1430406176.249      1 192.168.2.5 TCP_REFRESH_UNMODIFIED/304 278 GET http://192.168.2.1/sarg/images/sarg.png - HIER_DIRECT/192.168.2.1 -
```

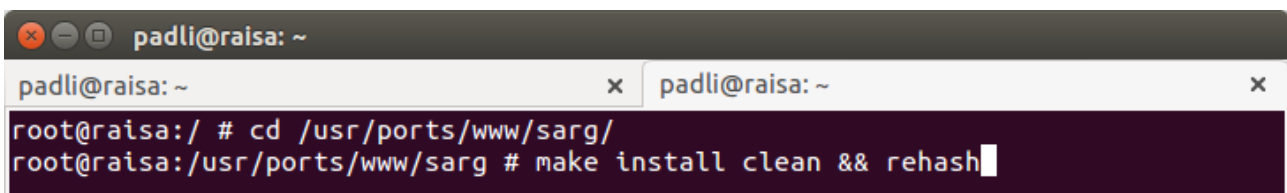
10. lokasi pid squid "/var/run/squid/squid.pid"

11. akses file access.log squid lewat web browser, install dulu nginx dan php56, php56-extensions dan tambahkan ke "vi /etc/rc.conf"



```
padli@raisa: ~  
padli@raisa: ~  
hostname="raisa"  
  
wlans_run0="wlan0"  
ifconfig_wlan0="WPA SYNCDHCP"  
  
ifconfig_re0="inet 192.168.2.1 netmask 255.255.255.0"  
  
sshd_enable="YES"  
squid_enable="YES"  
nginx_enable="YES"  
php_fpm_enable="YES"  
  
gateway_enable="YES"  
firewall_enable="YES"  
firewall_type="OPEN"  
natd_enable="YES"  
natd_interface="wlan0"  
  
# Set dumpdev to "AUTO" to enable crash dumps, "NO" to disable  
dumpdev="AUTO"  
~  
~  
~  
/etc/rc.conf: unmodified: line 1
```

12. install SARG "cd /usr/ports/www/sarg", "make install clean && rehash" config sesuaikan dengan kebutuhan.



```
padli@raisa: ~  
padli@raisa: ~  
root@raisa:/ # cd /usr/ports/www/sarg/  
root@raisa:/usr/ports/www/sarg # make install clean && rehash
```


13. edit "vi /usr/local/etc/sarg/sarg.conf" config sesuaikan dengan kebutuhan, contoh file config sarg terlampir

```
padli@raisa: ~  
padli@raisa: ~  
access_log /var/log/squid/access.log  
graphs yes  
graph_days_bytes_bar_color orange  
title "Squid User Access Reports"  
output_dir /usr/local/www/nginx/sarg  
resolve_ip no  
topuser_sort_field BYTES reverse  
user_sort_field BYTES reverse
```

14. jalankan sarg "/usr/local/bin/sarg"

```
padli@raisa: ~  
padli@raisa: ~  
root@raisa:/ # /usr/local/bin/sarg  
SARG: Records in file: 1098, reading: 100.00%  
SARG: Successful report generated on /usr/local/www/nginx/sarg/2015Apr29-2015Apr30  
root@raisa:/ #
```

15. tes sarg "<http://ip-proxy/sarg>"

SARG report for 2015 Apr 29-2015 Apr 30 - Mozilla Firefox

192.168.2.1/sarg/2015Apr29-2015Apr30/index.html

SARG Squid Analysis Report Generator

Squid User Access Reports
Period: 2015 Apr 29--2015 Apr 30
Sort: Bytes, reverse

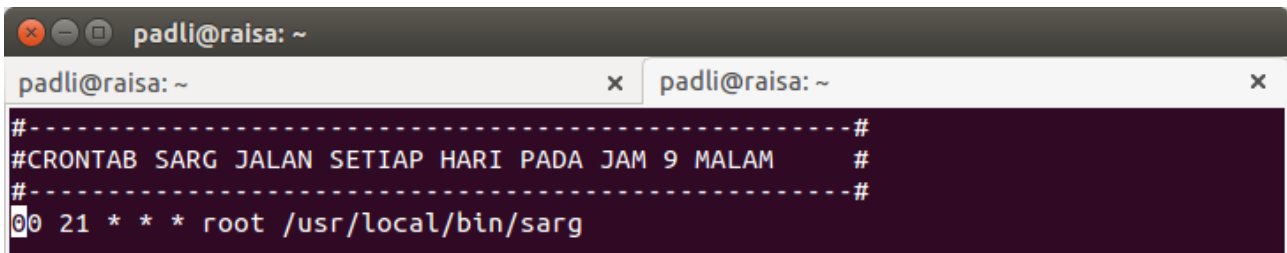
Top users

Top sites
Sites & Users
Denied accesses

NUM	USERID	CONNECT	BYTES	NBYTES	IN-CACHE-OUT	ELAPSED TIME	MILLISEC	%TIME
1	192.168.2.5	1.06K	10.60M	100.00%	1.49%	98.51%	00:27:12	1.632.195
TOTAL		1.06K	10.60M		1.49%	98.51%	00:27:12	1.632.195
AVERAGE		1.06K	10.60M				00:27:12	1.632.195

Generated by sarg-2.3.9 Sep-21-2014 on Apr/30/2015 23:10

16. tambahkan sarg di crontab agar jalan otomatis pada waktu tertentu "crontab -e",
"/etc/rc.d/cron restart"

A terminal window titled 'padli@raisa: ~' with two tabs. The active tab shows the crontab editor. The content is as follows:

```
#-----#  
#CRONTAB SARG JALAN SETIAP HARI PADA JAM 9 MALAM #  
#-----#  
00 21 * * * root /usr/local/bin/sarg
```

The terminal window has a dark background. The title bar shows the user 'padli@raisa' and the home directory '~'. There are two tabs, both labeled 'padli@raisa: ~'. The first tab is active. The content of the terminal is a crontab file being edited. It starts with a header line '#-----#', followed by a comment line '#CRONTAB SARG JALAN SETIAP HARI PADA JAM 9 MALAM #', another header line '#-----#', and then a cron job entry '00 21 * * * root /usr/local/bin/sarg'.

Dok 01/05/2015 : padliyulian@ymail.com