ulog-acctd – подсчет и детализация трафика

Ищем по RPM-пакетам на этом сайте: http://rpm.pbone.net/index.php3?stat=3&search=ulog-acctd&srodzaj=3 и переходим по ссылке напротив нашей версии ОС (у меня CentOS 6.9 i386, но подошла на 6.5)

```
# wget ftp://ftp.pbone.net/mirror/rnd.rajven.net/centos/7.0.1406/os/x86_64/ulog-acctd-0.4.3-7cnt7.x86_64.rpm
# rpm -Uhv ulog-acctd-0.4.3-7cnt7.x86_64.rpm
```

Конфигурационный файл чрезвычайно прост, там нужно указать multicast group (указанный в правиле iptables), формат лога. Он находится в /etc, немного поправим его:

```
# vi /etc/ulog-acctd.conf

multicast groups=4

accounting file=/var/log/ulog-acctd/account.log
dump file=/var/log/ulog-acctd/dump
debug file=/var/log/ulog-acctd/debug.log
```

Все остальное по умолчанию.

Для того чтобы демон начал получать пакеты нужно добавить соответствующее правило в iptables:

```
# ULOG-ACCTD
iptables -A INPUT -j ULOG --ulog-nlgroup 4 --ulog-cprange 48 --ulog-qthreshold 10 --ulog-prefix "INPUT"
iptables -A FORWARD -j ULOG --ulog-nlgroup 4 --ulog-cprange 48 --ulog-qthreshold 10 --ulog-prefix "FORWARD"
iptables -A OUTPUT -o $if_wan -j ULOG --ulog-nlgroup 4 --ulog-cprange 48 --ulog-qthreshold 10 --ulog-prefix "OUTPUT"
```

Здесь мы добавляем в цепочку **FORWAD** (пакеты проходящие через маршуризатор) отправлять все пакеты в target ULOG, задать им

префикс ‘FORWARD’ (чтобы можно было различать статистику полученную с разных правил) –ulog-nlgroup 4 – номер multicast group, в которую будут посылаться заголовки пакетов.

```
tst.tst-amo.net.ua  1561299321  17  185.25.183.91  27142
192.168.0.10 54286 1 174 "enp2s0" "enp3s1" "FORWARD"
tst.tst-amo.net.ua  1561299314  17  185.25.183.91  27088
192.168.0.10 54286 1 173 "enp2s0" "enp3s1" "FORWARD"
tst.tst-amo.net.ua  1561299314  17  185.25.183.93  27174
192.168.0.10 54286 1 174 "enp2s0" "enp3s1" "FORWARD"
tst.tst-amo.net.ua  1561299325  17  185.25.181.77  27088
192.168.0.10 54286 1 181 "enp2s0" "enp3s1" "FORWARD"
tst.tst-amo.net.ua  1561299316  17  185.25.183.91  27119
192.168.0.10 54286 1 174 "enp2s0" "enp3s1" "FORWARD"
tst.tst-amo.net.ua  1561299318  17  185.25.183.93  27206
192.168.0.10 54286 1 176 "enp2s0" "enp3s1" "FORWARD"
tst.tst-amo.net.ua  1561299320  17  185.25.183.93  27085
192.168.0.10 54286 1 175 "enp2s0" "enp3s1" "FORWARD"
```

Ulog-acctd должен быть настроен на прослушивание этой группы. –ulog-cprange 48 – количество байт из пакета передаваемых в userspace. При этом может возникнуть ситуация, когда при наличии в пакете большого количества флагов заголовок может ‘не влезть’, тогда пакет будет не посчитан. В syslog будет выдано сообщение “Short IP header. Increase copy range to RANGE” по которому можно будет обнаружить и исправить эту ситуацию. Если же cprange настолько мало, что даже не может вместить ip адрес, то в лог дополнительно будет помещено сообщение ‘copy range is too short to even capture IP headers. ALL IP PACKETS WILL BE DROPPED!’ –ulog-qthreshold 10 сколько пакетов должно собрать ядро прежде чем передать данные о них в user-space.

Если прописать правило в цепочку **INPUT**, то мы получим статистику по входящим в роутер пакетам (адрес назначения которых – роутер)

```
tst.tst-amo.net.ua 1561299331 17 192.168.1.1 138 192.168.1.255
138 1 229 "enp2s0" "-" "INPUT"
tst.tst-amo.net.ua  1561299327  17  192.168.0.10  27005
```

```
255.255.255.255 27015 14 854 "enp3s1" "-" "INPUT"
```

Запускаем:

```
# systemctl start ulog-acctd
```

Статистику смотрим в

```
/var/log/ulog-acctd
```

Столбцы согласно описанию идут в таком порядке:

```
# Accounting format, specified with a format string with similar
# syntax to printf(3)
#
# %h hostname
# %t timestamp
# %p protocol
# %s source IP
# %S source port
# %d destination IP
# %D destination port
# %P packets
# %b bytes
# %i incoming interface
# %o outgoing interface
# %f prefix
#
# \t tab
# \n newline
# \\ literal \
# \" literal "
# \% literal %
# %% literal %
```

Данные можно втянуть, например, в Exel:

```
=UnixTime / 86400 + 25569 - 4 / 24
```

Для ежедневной ротации логов проверить присутсвие файла /etc/logrotate.d/ulog-acctd и прав 644 или 444:

```
# cat /etc/logrotate.d/ulog-acctd
```

```
/var/log/ulog-acctd/account.log  /var/log/ulog-acctd/debug.log
{
    weekly
    rotate 5
    copytruncate
    compress
    notifempty
    missingok
    sharedscripts
    prerotate
         if [ -e /var/run/ulog-acctd.pid ]; then kill -TSTP
`cat /var/run/ulog-acctd.pid`; fi
    endscript
    postrotate
          if [ -e /var/run/ulog-acctd.pid ]; then kill -CONT
`cat /var/run/ulog-acctd.pid`; fi
    endscript
}
```

https://www.opennet.ru/base/net/ulog_traf.txt.html

Простой учёт трафика на Linux средствами iptables + ulog-acctd

https://www.e-reading.club/chapter.php/79424/70/Andreasson_-_Iptables_Tutorial_1.1.19.html

https://it.wikireading.ru/14371