ipcad – подсчет трафика

Установка:

```
# cd /tmp
#                                                    wget
http://rnd.rajven.net/centos/7/os/x86_64/ipcad-3.7.3-5cnt7.x86
_64.rpm
# yum install ipcad-3.7.3-5cnt7.x86_64.rpm -y
```

Правим конфиг:

```
# vi /etc/ipcad.conf

capture-ports enable;
interface "enp3s1" promisc;
#Если нужен маркированный трафик
#interface ulog group 1;
interface tun0 promisc;
aggregate 192.168.113.0/24 strip 32;
aggregate 10.8.0.0/24 strip 32;
aggregate 0.0.0.0/0 strip 32;
rsh enable at 127.0.0.1;
rsh root@127.0.0.1 admin;
rsh user@127.0.0.1 deny;
rsh 127.0.0.1 view-only;
netflow export version 5;
netflow export destination 127.0.0.1 9998;
pidfile = /var/run/ipcad.pid;
dumpfile = /var/log/ipcad/ipcad.dump;
```

Создаем директорию, файл и назначаем права доступа:

```
# mkdir -p /var/log/ipcad && touch /var/log/ipcad/ipcad.dump
&& chmod 600 /var/log/ipcad/ipcad.dump
```

Если маркируем пакеты то дописываем правила iptables для маркировки (после NAT):

```
# IPCAD
iptables -A FORWARD -j ULOG --ulog-nlgroup 1
iptables -A OUTPUT -j ULOG --ulog-nlgroup 1
```

Запуск:

```
# ipcad -rds
```

Значение ключей таково:

- r – при запуске импортируем данные из dumpfile;
- d – запускаем процесс в виде демона (при первом запуске его можно не использовать);
- s – по завершению работы сохранять статистику в dumpfile.

Просмотр статистики:

```
# rsh localhost show ip accounting
```

Полезно периодически сохранять текущую статистику в файл:

```
# rsh localhost dump > /var/log/ipcad/ipcad.`date`
```

Общий синтаксис команд для ipcad выглядит следующим образом:

```
rsh host comand
```

где host – это хост, на котором ведётся статистика, а comand – это сама команда. В рассматриваемом случае значением host является localhost.

По команде:

```
rsh localhost help
```

доступен полный список команд. А именно:

n show ip accounting – показать статистику.
n clear ip accounting – сбросить статистику до контрольной точки. Если контрольная точка не задана, то статистика сбрасывается в ноль.
n show ip accounting checkpoint – показать статистику, сохранённую в контрольных точках.
n clear ip accounting checkpoint – сбросить все контрольные точки.
n show ip cache flow – показать кэш NetFlow.
n show interface <iface> – показать счётчик интерфейса

<iface>.
n dump [<path>] – сохранить текущую статистику в файл <path>. Если <path> не указывать, то статистика сбросится в dumpfile, указанный в конфигурационном файле ipcad.conf.
n restore [<path>] – восстановить статистику.
n import [<path>] – импортировать (добавить) статистику.
n stat – показать текущее состояние работы ipcad.
n show version – показать версию и uptime ipcad.
n shutdown – завершить работу ipcad.

При запуске скрипта возможен вывод варнинга:

```
# /home/$user/bin/ipcad.ch
connect to address ::1: Connection refused
Typing 127.0.0.1...
connect to address ::1: Connection refused
Typing 127.0.0.1...
IP accounting cleared
connect to address ::1: Connection refused
Typing 127.0.0.1...
```

localhost у вас резолвится в

```
host localhost
localhost has address 127.0.0.1
localhost has IPv6 address ::1
```

сначала идет попытка коннектится к ::1:514, там никто не слушает, после rsh делает коннект к 127.0.0.1:514 а там у вас ipcad, трактуйте это не как ошибку а как warning, на работу вашего скрипта это не оказывает никакого влияния.

Если вас это ругань сильно напрягает, то можете заменить в скрипте

rsh localhost на rsh 127.0.0.1

http://www.adodo.ru/blog/linux/95.html

http://www.gentoo.ru/node/11796

http://muff.kiev.ua/content/ipcad-netflow-sobiraem-i-slivaem-statistiku-traffika

https://local.com.ua/forum/topic/81132-ipcad-%D0%BD%D0%B5-%D0%BE%D1%82%D0%B4%D0%B0%D0%B5%D1%82-%D1%81%D1%82%D0%B0%D1%82%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D1%83-%D0%BF%D0%BE-%D1%81%D0%B5%D1%82%D0%B8/

https://www.nixp.ru/articles/11.html

https://forum.netgate.com/topic/72733/%D0%BD%D0%B5-%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0%D0%B5%D1%82-ipcad-%D0%BD%D0%B5-%D0%B7%D0%B0%D0%BF%D1%83%D1%81%D0%BA%D0%B0%D0%B5%D1%82%D1%81%D1%8F

IPCAD installation on CentOS 7