



IPCad + NetFlow - собираем и "сливаем" статистику траффика

Опубликовано muff в Втр, 2010-02-02 16:14

Собственно есть настроенный сервер статистики. Статистика с маршрутизаторов сливается на сервер по [NetFlow](#) [1] с помощью самописного скрипта и использованием [netgraph](#) [2]. Решил этот скрипт вынести и сливать потоки с помощью ipcad.

Приступаем к установке ipcad из системы портов:

```
# cd /usr/ports/net-mgmt/ipcad && make install clean
```

По завершению установки, следуя инструкциям, добавляем в rc.conf строку запуска:

```
# echo '### IPCAD' >> /etc/rc.conf  
# echo 'ipcad_enable="YES"' >> /etc/rc.conf
```

Далее редактируем конфигурационный файл **/usr/local/etc/ipcad.conf** до следующего содержания:

```
# Опция 'capture-ports' включает/отключает дополнительные поля в статистике,  
# такие, как TCP- и UDP-порты, а также типы ICMP-пакетов. Однако включение  
# данной опции увеличивает потребление памяти, снижает скорость подсчета  
# трафика и, в ряде случаев, искажает вывод через RSH  
  
capture-ports disable;  
  
# Размер буферов, используемых для передачи статистики ядром  
  
buffers = 64k  
  
# Перечень сетевых интерфейсов, на которых считается проходящий трафик.  
# Рассматривается случай шлюза с двумя сетевыми интерфейсами в различные  
# сегменты локальной сети.  
  
interface vlan3;  
interface vlan5;  
  
# Настройки Netflow. Указываем IP-адрес и порт, куда "сливать" статистику.  
  
netflow export destination 192.168.206.66 2002;  
netflow export version 5;  
  
# Задаем путь к файлу, в который по умолчанию будут складываться данные  
# собранной статистики.  
  
dumpfile = ipcad.dump;  
  
# Настройка безопасности. Указываем каталог, относительно которого будем  
# chroot-ить ipcad.  
  
chroot = /tmp/ipcad;  
  
# Путь к pid-файлу.  
  
pidfile = ipcad.pid;
```



```
# Опция 'memory_limit' задает количество памяти для хранения содержимого
# одного потока данных. Синтаксис следующий: memory_limit = <количество>[k|m|e];
# где 'k' -- килобайты, 'm' -- мегабайты, 'e' -- количество строк таблицы # данных.

memory_limit = 10m;
```

Рассмотрим более детально указанные опции:

- **interface** - указываем интерфейсы, на которых считается проходящий трафик;
- **netflow export destination** - указываем, куда "сливать" информацию о проходящем трафике;
- **netflow export version** - указываем версию netflow;
- **dumpfile** - путь к файлу, в который по умолчанию будут складываться данные статистики;
- **chroot** - задаем каталог для chroot;
- **pidfile** - путь к файлу, в котором хранится идентификатор процесса;
- **memory_limit** - количество памяти для хранения содержимого одного потока данных.

Создаем каталог для chroot и пытаемся запустить ipcad:

```
# mkdir /tmp/ipcad
# sh /usr/local/etc/rc.d/ipcad start
Starting ipcad.
Opening vlan3... [LCap] [4096] Initialized as 1
Opening vlan5... [LCap] [4096] Initialized as 2
Configured NetFlow destination at 192.168.206.66:2002
Can't open dump file ipcad.dump
Daemonized.
```

Проверяем, действительно ли запущен процесс:

```
# ps -ax | grep ipcad
54041 ?? S<s  0:00,92 /usr/local/bin/ipcad -rds -c /usr/local/etc/ipcad.conf
```

Ну и проверим, действительно ли сливаются потоки:

```
# tcpdump -ni vlan3 dst port 2002
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vlan3, link-type EN10MB (Ethernet), capture size 96 bytes
16:59:23.458178 IP 192.168.35.64076 > 193.227.206.66.20002: UDP, length 1464
16:59:23.458242 IP 192.168.206.35.64076 > 192.168.206.66.2002: UDP, length 1464
16:59:23.458297 IP 192.168.206.35.64076 > 192.168.206.66.2002: UDP, length 1464
16:59:23.458354 IP 192.168.206.35.64076 > 192.168.206.66.2002: UDP, length 1464
16:59:23.458409 IP 192.168.206.35.64076 > 192.168.206.66.2002: UDP, length 1464
16:59:23.458465 IP 192.168.206.35.64076 > 192.168.206.66.2002: UDP, length 1464
16:59:23.458522 IP 192.168.206.35.64076 > 192.168.206.66.2002: UDP, length 1464
...
```

Поздравляю, все работает...

Источник (получено 2025-07-03 22:31):

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

Ссылки:



[1] <http://xgu.ru/wiki/NetFlow>

[2] <http://ru.wikipedia.org/wiki/Netgraph>