Traffic Collectors

Программа сбора статистики для последующей ее обработки биллингом.

- NfSen
- ipcad
- Cisco
- traffic2sql

- Классы трафика

NfSen

Nfsen — сборщик и анализатор Netflow с открытым исходным кодом, отображает статистику в веб интерфейсе в виде графиков.

Перед установкой Nfsen должен быть установлен Nfdump

Для установки Nfdump в Ubuntu/Debian

```
apt-get install nfdump
```

В CentOS:

```
sudo yum install nfdump
```

Для продолжение установки Nfsen установим необходимые компоненты:

```
add-apt-repository universe
apt-get install apache2 php libapache2-mod-php librrds-perl librrdp-perl librrd-dev libmailtools-perl build-
essential autoconf rrdtool libio-socket-inet6-perl
```

Скачаем Nfsen и распакуем:

```
mkdir /srv/nfsen
cd /srv/nfsen
wget https://sourceforge.net/projects/nfsen/files/stable/nfsen-1.3.8/nfsen-1.3.8.tar.gz
tar xzfv nfsen-1.3.8.tar.gz
```

Создадим файл конфигурации и откроем его в текстовом редакторе:

```
cd nfsen-1.3.8/etc
cp nfsen-dist.conf nfsen.conf

nano nfsen.conf
```

Если Ubuntu/Debian то в файле **/srv/nfsen/etc/nfsen.conf**

1. Изменить USER, WWWUSER и WWWGROUP на **www-data**
2. В хеше *%sources* указать IP оборудования, которое должно совпадать с IP, указанного в **Настройка > Сервер доступа**

/srv/nfsen/etc/nfsen.conf

```
$BASEDIR = "/srv/nfsen";
$PREFIX  = '/usr/bin';
$USER    = "www-data";
$WWWUSER  = "www-data";
$WWWGROUP = "www-data";

%sources = (
    'upstream1'    => { 'port' => '555', 'col' => '#0000ff', 'IP' =>'195.158.00.000' 'type' => 'netflow' },
    'upstream2'    => { 'port' => '555', 'col' => '#00ff00', 'IP' =>'195.158.00.111' 'type' => 'netflow' },
 );
```

Запустим скрипт установки Nfsen:

```
cd ..
./install.pl ./etc/nfsen.conf
```

Запустим nfsen:

```
/srv/nfsen/bin/nfsen start
```

В конфигурации мы указал upstream1 с портом 555, по этому после запуска nsfsen он автоматически запустит nfcapd на порту 555 и будет писать данные в директорию /srv/nfsen/profiles-data/live/upstream1/.....

Для автозапуска при старте операционной системы выполним команды:

```
ln -s /srv/nfsen/bin/nfsen /etc/init.d/nfsen
update-rc.d nfsen defaults 20
```

Осталось настроить конфигурацию веб сервера либо просто создать символическую ссылку в www директорию (после этого можно будет открыть nfsen в браузере, например http://ixnfo.com/nfsen/nfsen.php):

```
ln -s /srv/nfsen/www/ /var/www/html/nfsen
ln -s /var/www/nfsen/ /var/www/html/nfsen
```

После редактирования конфигурации, например когда нужно добавить или изменить источники, выполним:

```
cd /srv/nfsen/bin
./nfsen reconfig
```

Через некоторое время должны появится данные на графиках, также через tcpdump можно посмотреть приходят ли данные от сенсора:

```
tcpdump port 555 -e -n
```

Убедимся что nfsen запускается при запуске операционной системы:

```
systemctl is-enabled nfsen
systemctl is-enabled nfdump
systemctl enable nfsen
systemctl status nfsen
```

Если в операционной системе установлен flow-tools, то можно отключить его так:

```
systemctl is-enabled flow-capture
systemctl disable flow-capture
systemctl status flow-capture
systemctl stop flow-capture
```

Проверка/редактирование настроек сервиса

nfsen.service

```
vim /etc/systemd/system/nfsen.service
```

Сделать симлинк на файл **traffic2sql**

```
ln -s /usr/abills/Abills/modules/Internet/traffic2sql /usr/abills/libexec/traffic2sql
```

Для сбора данных с Nfsen добавление данных в базу данных нужно добавить вызов файла **traffic2sql** на крон каждый час в **/etc/crontab** . В поле [NAS_IDS] указать NAS_ID. Для проверки вывода данных с потока поставить DEBUG=8.

По умолчанию путь для программы Nfdump указана по адресу '/usr/bin/nfdump'. Если программа установлена по другому пути - можно задать через аргумент FLOW_NFDUMP=/usr/local/bin/nfdump

```
 * */1 * * * root /usr/abills/libexec/traffic2sql [NAS_IDS] NFSEN=1 flowdir=/srv/nfsen/profiles-data/live
/upstream1/
```

Пример:

* */1 * * * root /usr/abills/libexec/traffic2sql 5 NFSEN=1 flowdir=/srv/nfsen/profiles-data/live/upstream1/

flow-tools

Установка flow-tools

ipcad

Установка на FreeBSD и Debian

Запуск скрипта обработки статистики
/etc/crontab

```
 */10 * * * * root /usr/abills/libexec/traffic2sql 8 flowdir=/usr/abills/var/log/ipn/
```

Если у Вас несколько NAS-серверов (коллекторов трафика), то для каждого нужно создать отдельную папку для логов.

Cisco

(aka kir)

```
no ip rcmd domain-lookup
ip rcmd rsh-enable
ip rcmd remote-host firewall 192.168.0.1  root enable
!
ip flow-export source FastEthernet0/1
ip flow-export version 5
ip flow-export destination 192.168.0.1 9996
!
access-list 100 permit 172.19.80.0 0.0.0.255 192.168.0.1
-
access-list 100 dynamic ABILS permit IP any any
-
access-list 100 deny ip any any
  ,     !
!
interface FastEthernet0/1.21
 ip address 192.168.0.1 255.255.255.0
 ip access-group 100 in
      !
!
```

192.168.0.1 - Адрес коллектора для потока Netflow (flow-tools)

Для блокировки и открытия доступа можно использовать скрипт

```
/usr/abills/misc/cisco_access
   ACTION - Allow/Deny
   IP     - Client IP
   debug  - Make debug log
```

/usr/local/etc/sudoers

```
www   ALL = NOPASSWD: /usr/abills/misc/cisco_access
```

traffic2sql

ABillS IPN Traffic collector
Анализатор трафика для модуля IPN

Так как программа анализирует пришедшие за 5 минут пакеты, и потом складывает их в базу при использовании динамических адресов система может не успеть внести трафик последних 5 минут перед разрывом сессии.

Перед использованием см. Установка flow-tools.

Запуск скрипта обработки статистики **/etc/crontab**

```
*/5 * * * * root /usr/abills/libexec/traffic2sql [NAS_IDS] flowdir=/usr/abills/var/log/ipn/
```

Параметры:

```
traffic2sql [NAS_IDS] [Options]
```

Пример вызова для серверов с ID 1,2,3:

```
/usr/abills/libexec/traffic2sql 1,2,3 flowdir=/usr/abills/var/log/ipn/
```

Опции:

NAS_IDS	ID (NAS) серверов доступа. Формат: 1,2,3 или 1-100
log	Расположение файла трафика для trafd
INTERFACE	Интерфейс для trafd
flowdir	Каталог, в который складываются файлы работы flow-capture. После обработки файлов ft* они автоматически удаляются программой traffic2sql.
FLOWTOOLS_IP_AGGREGATION=1	Агрегация потоков по IP адресам. Поднимает скорость анализа.
FLOWTOOLS_FT_BACKUP=dir	Переносить проанализированные файлы в бекапный каталог. Используется для отладки
DEBUG	Режим отладки (1..6) режим 5 и 6 **В БАЗУ ДАННЫЕ НЕ ВНОСИТ**
DETAIL_ONLY	Складывать в базу только детализацию для активных клиентов (присутствующих в /Monitoring), сам подсчет трафика и ведение сессий не производится
UNKNOWN_IP_LOG	Включить учёт адресов, не относящихся к активным пользователям
TCOLLECTOR	Режим глобального коллектора. Складывать весь трафик, полученный от коллектора
AMON_ALIVE	Интервал получения подтверждения активности от AMon. Интервал задаётся в секундах (Значение по умолчанию 120). Если на протяжении 3 интервалов не пришло ни одного пакета активности система закрывает соединение.
daemon	Режим демона (пока в разработке)
FLOW_CAT	Местоположение Flow tools flow-cat
FLOW_PRINT	Местоположение Flow tools flow-print
PREPAID_STORE	Использования отдельной таблицы для хранения значений предоплаченного трафика. Поднимает скорость анализа.
VIRUS_ALERT=1000	Опция разрешает отслеживать заражённые хосты, которые рассылают вирусы. В данной опции указывается количество мелких пакетов размером до 150 байт за единицу времени, при котором хост попадает в чёрный список
LOG_FILE='...'	Файл ведения лога работы анализатора
TRANSACTION=1	Вносить все данные одной транзакцией (ускоряет работу)