

ПОДСЧЕТ ТРАФИКА С ПОМОЩЬЮ NETAMS



Существует большое количество программ, предназначенных для подсчета трафика и сбора статистики. Сегодня мы рассмотрим одну из них, которая, на мой взгляд, будет одинаково интересна и новичкам, и специалистам.

КИРИЛЛ ТИХОНОВ

NeTAMS – Network Traffic Accounting and Management System (www.netams.com) предназначена для контроля и учета сетевого трафика, проходящего через сервер. Работает под управлением операционных систем FreeBSD (4.3 и старше) и Linux (ядро 2.4 или выше и iptables).

Краткие характеристики:

- Работа с БД MySQL, PostgreSQL, unix hash.
- Контроль доступа, квот и прав пользования.
- Вывод статистики прямым запросом или через веб-интерфейс.
- Управление посредством соединения клиентом telnet на некий tcp-порт сервера.
- Веб-интерфейс для отображения статистики.

Установку программы нельзя назвать тривиальной. В качестве сервера будем использовать Linux, поскольку с ним, в отличие от FreeBSD, возникает большинство проблем. Сервер является маршрутизатором с 2 сетевыми картами, одна смотрит в Интернет, другая – в локальную сеть.

Нам понадобится пакетный фильтр iptables и входящая в него библиотека libipq. Библиотека libipq добавляет цель QUEUE, т.е. очередь. Забегая вперед, скажу, что весь трафик заворачивается с помощью QUEUE в системную очередь, из которой пакеты берет NeTAMS, анализирует и отдает обратно.

Скачиваем пакетный фильтр с www.netfilter.org, распаковываем и компилируем (предполагается, что текущее ядро лежит в /usr/src/linux):

```
# tar xvfj iptables-1.2.9.tar.bz2
# cd iptables-1.2.9
# make KERNEL_DIR=/usr/src/linux
# make install
# make install-devel
```

Последняя строка позволяет установить библиотеку libipq. Скачиваем NeTAMS с www.netams.org, последняя версия на момент написания статьи 3.1(1801), и распаковываем:

```
# tar xvfz netams-3.1.1801.tar.gz
# cd netams-3.1.1801
# vi Makefile
```

Скрипта configure здесь нет, поэтому редактируем Makefile. Он хорошо документирован, поэтому разобраться в опциях не составляет труда. Для начала комментируем все, относящееся к FreeBSD, а именно строки 13, 14, 17, 25, 26. После этого раскомментируем строки, относящиеся к Linux: строки 34 и 35. Далее выбираем тип БД: DB1 (unix hash), MySQL или PostgreSQL и раскомментируем относящиеся к ним строки. Само собой, используемая БД должна быть уже установлена и настроена. Мы выбираем MySQL. Поскольку мы используем iptables-1.2.9, то надо раскомментировать строку 50.

Далее правим пути к конфигурационному файлу и логам (строки 56, 57) и компилируем:

```
# make
```

Результатом компиляции будут 2 файла: netams – сама программа и netamsctl – утилита для автоматизации выполнения повседневных работ. Цели install в Makefile нет, поэтому устанавливаем вручную:

```
# cp src/netams /usr/local/bin
# cp src/netamsctl /usr/local/bin
```

Отлично, программа установлена. Но прежде чем мы начнем писать конфигурационный файл, настроим MySQL.

В принципе необходимости ручного создания БД нет. При первом запуске NeTAMS создаст ее сам. Однако сделать это возможно только под пользователем с правами администратора MySQL. Мы же заведем отдельного пользователя с именем netamsuser и паролем passwd и вручим ему права на доступ к БД.

Итак:

```
# mysql -u root -p
Enter password:
```

Создаем базу netams, в которую NeTAMS будет писать данные:

```
mysql> create database netams;
mysql> connect netams;
```

Вручаем права пользователю netams-user:

```
mysql> grant SELECT,INSERT,DELETE,UPDATE,CREATE \
on netams.* to netamsuser;
mysql> grant SELECT,INSERT,DELETE,UPDATE,CREATE \
on netams.* to netamsuser@localhost;
```

и задаем пароль пользователя netamsuser:

```
mysql> connect mysql;
mysql> set password for \
'netamsuser'@'localhost'=password('passwd');
mysql> set password for 'netamsuser'@'%'=password('passwd');
```

Для того чтобы внесенные изменения вступили в силу, обновляем активные привилегии и выходим:

```
mysql> flush privileges;
mysql> exit
```

Все, БД готова к приему данных от NeTAMS. Начнем писать конфигурационный файл /etc/netams.cfg:

```
debug none
user name admin real-name Admin email root@localhost \
password 123 permit all

service server 0
login any
listen 20001
max-conn 6
```

При запуске программа с такой конфигурацией ничего считать не будет. К ней можно только подключиться с помощью telnet и просмотреть конфигурацию.

Разберем файл построчно. Строка debug none отключает вывод отладочной информации. Следующая строка определяет пользователя:

- user name admin – логин;
- real-name Admin – реальное имя;
- email root@localhost – email;
- password 123 – пароль (незашифрованный);
- permit all – разрешено все.

Следующая строка начинает описание сервиса server. Этот сервис обеспечивает возможность подключения к работающей программе с помощью telnet:

- service server 0 – начало описания сервиса. Каждый сервис должен иметь номер. Это нужно для того, чтобы можно было описать несколько одинаковых сервисов. Например, несколько сервисов storage, которые будут хранить разную информацию в разных БД.
- login any – пустить всех.
- listen 20001 – слушать tcp-порт 20001.
- max-conn 6 – максимальное число одновременных подключений.

Запустим программу:

```
# netams -ld
```

К ней можно подключиться, набрав:

```
telnet netams_host 20001
```

Далее надо ввести логин и пароль – в нашем случае admin и 123. Введя «?», можно получить справку по командам.

Теперь займемся подсчетом трафика.

В уже созданный файл допишем еще несколько сервисов, после чего он примет вид:

```
debug none
user name admin real-name Admin email root@localhost \
password 123 permit all

service server 0
login any
listen 20001
max-conn 6

service processor 0
lookup-delay 10
policy acct name all-ip target ip
restrict all pass local pass
unit host name linux-gw ip 195.x.x.x acct-policy all-ip
storage 1 all

service storage 1
type mysql
user netamsuser
```

```
password passwd

service data-source 1
type ip-traffic

service html 1
path /var/www/localhost/netams
run lmin
client-pages all
```

Разберем написанное. Обращаю внимание, что в пределах одного сервиса пустые строки недопустимы. Дело в том, что с точки зрения NeTAMS после пустой строки должно идти начало нового сервиса, и в случае обнаружения пустой строки, за которой не идет определение сервиса, NeTAMS будет аварийно завершать работу.

- service processor 0 – ядро системы, в нем определяются объекты, по которым будет идти учет.
- policy acct name all-ip target ip – определяет политику, по которой будет производиться подсчет трафика, в данном случае политика с именем all-ip (параметр name) будет считать весь IP-трафик. Параметр target может принимать следующие значения:
 - ip – весь IP-трафик;
 - icmp – весь icmp-трафик;
 - tcp – весь tcp-трафик;
 - udp – весь udp-трафик;
 - tcp-http – весь tcp-трафик, входящий или исходящий, порты которого 80, 808, 8080, 3128, 442;
 - tcp-ports – весь tcp-трафик на указанные порты;
 - udp-ports – весь udp-трафик на указанные порты.
- unit host name linux-gw ip 195.x.x.x acct-policy all-ip – определяет объект, для которого будет производиться подсчет трафика. В данном случае объект host с именем linux-gw, IP-адресом 195.x.x.x (внешний адрес маршрутизатора) и определенной выше политикой all-ip. Таким образом, с помощью этого правила мы считаем весь IP-трафик, поступающий из Интернета на наш маршрутизатор.
- storage 1 all – передает все данные сервису storage 1.
- service storage 1 – сервис, определяющий тип и параметры доступа к БД, в которой будет сохраняться статистика.
- service data-source 1 – обеспечивает поступление данных о трафике внутрь программы. В данном случае определен источник данных ip-traffic. Этот источник работает с системной очередью, в которую с помощью iptables попадают пакеты.
- service html 1 – организует автоматическое периодическое создание статических html-страниц, содержащих информацию о прошедшем трафике. Периодичность создания задается параметром run, в данном случае она равна 1 минуте.

Теперь запускаем программу в режиме демона:

```
# netams
```

и определим правила iptables, с помощью которых данные будут поступать в программу:

```
$IPTABLES -t mangle -A POSTROUTING -p all -j QUEUE
$IPTABLES -t mangle -A PREROUTING -p all -j QUEUE
```

Здесь есть один очень важный момент. Дело в том, что с помощью приведенных выше правил iptables все входящие и исходящие пакеты поступают в системную очередь, откуда их будет брать NeTAMS. Однако если в момент активизации iptables NeTAMS не будет запущен, пакеты будут поступать в системную очередь и пропадать там, т.к. не будет программы, которая отправит их обратно. В результате пропадает коннект до сервера. Поэтому в процессе отладки надо либо сидеть за консолью сервера, либо в случае удаленного администрирования тренироваться на icmp-трафике (в сервисе processor 0 поменять значение параметра policy target ip на target icmp, и в правилах iptables аналогично заменить -p all на -p icmp). А порядок запуска такой: сначала запускаем NeTAMS, потом iptables. Соответственно порядок остановки обратный – сначала останавливаем iptables, потом NeTAMS.

Каждый объект имеет свой уникальный шестнадцатеричный идентификатор (OID), который является ключом в базе данных. Он генерируется автоматически после первого запуска, поэтому чтобы статистика не пропала, после запуска программы надо подключиться к ней с помощью telnet и выполнить команду save. Она перезапишет netams.cfg, добавив в него сгенерированные OID. Таким образом, наш файл будет выглядеть так:

```
#NeTAMS version 3.1(1801.7) compiled by root@localhost
#configuration built Thu Apr 1 09:25:23 2004
#begin
#global variables configuration
debug none
user oid 01327B name admin real-name "Admin"
  crypted $1$$GmbL3iXOMZR57QuGDLv.L1
schedule oid 08FFFF time lmin- action "html"

#services configuration

service server 0
login any
listen 20001
max-conn 6

service processor 0
lookup-delay 10
policy acct oid 036633 name all-ip target ip
restrict all pass local pass
unit host 022EB1 name linux-gw ip 195.x.x.x
  acct-policy all-ip
storage 1 all

service storage 1
type mysql
user netamsuser
password passwd

service data-source 1
type ip-traffic

service html 1
path /var/www/localhost/netams
run lmin
client-pages all
```

Мы рассмотрели простейший случай подсчета трафика от провайдера до шлюза. В документации, поставляемой с программой, настройка описана более детально. Например, для каждого пользователя в локальной сети можно настроить квоту, при превышении которой NeTAMS автоматически отключит доступ в Интернет. К тому же на сайте www.netams.com есть русскоязычный форум, в котором можно найти ответы на любой возникший вопрос.