Автор: Administrator
30.09.2006 17:06 - Обновлено 28.05.2010 12:19

NeTAMS, многофункциональная программа по учету и управлению IP-трафиком (минимальная настройка)

Автор: schizoid.
Оригинал: http://www.lissyara.su/articles/freebsd/traffic_count/netams/

Итак. Вступление. Начало возьмем с оф. сайта данной программы, а именно http://www.netams.com

NeTAMS (Network Traffic Accounting and Monitoring Software) - многофункциональная программа
по учету и управлению IP-трафиком для маршрутизаторов Cisco или компьютеров под управлением Unix (Linux/FreeBSD/Solaris).
Поддерживаются различные методы сбора статистики
(tee/divert/ip_queue/ulog/libpcap/netflow v5 и v9/netgraph),
хранения в базе данных (BerkleyDB/MySQL/PostgresSQL/Oracle/Radius), агрегирования, отображения, оповещения и пр.
Возможно проводить блокировку на базе квот, авторизации, исчерпании баланса (биллинг);
управлять полосой пропускания, контролировать подмену MAC-адреса, делать связь с RADIUS,
создавать гибкие политики учета и фильтрации.

Хочу описать минимальную настройку этой программы, потому что часто после ее упоминания на форуме, народ в аське просит помочь ее настроить. Хотя есть и оф. доки...им этого мало. Ладно, приступим.

Еще раз повторюсь - это пример минимальной настройки! На самом деле прога может много, о чем можно почитать тут: http://netams.com/doc/index.html.

Еще один нюанс. У меня Нетамс стоит уже более 2-х лет, и версия 3.3.5, на сайте же уже доступна последняя стабильная версия: 3.4.1rc1.
Т.к. момент установки я уже не помню, то я поднял виртуальную машину, на которую поставил минимум чего нужно для установки нетамса, поднял его на ней, а уже конфиг и т.д. беру со своего боевого сервака. Т.к. настройка минимальна, то конфиг от более старой версии программы прокатит и на новую.

В качестве базы данных я использую mysql, для заворота трафика на нетамс использую divert в ipfw, поэтому у вас должен быть настроено ядро как минимум с такими опциями:options IPFIREWALL
options IPDIVERT

Итак, mysql-server5.0 и клиент поставились, попробуем начать установку нетамса...чего ему не хватит...
Идем в cd /usr/ports/net-mgmt/netams/
cat distinfo
MD5 (netams-3.4.0rc2.tar.gz) = 3093e50f8ee7a297cb8c2bc6bacd0666
SHA256 (netams-3.4.0rc2.tar.gz) = 7cbfdefa94f075a5dab40613d25738c0e2e40652638338b52632a0efdbc4f68e
SIZE (netams-3.4.0rc2.tar.gz) = 375729

Ага, в портах версия 3.4.0rc2. Ну да Бог с ним. У мну то на самом деле еще моложе :)
#make install
 Options for netams 3.4.0.r2
 [ ] DEBUG Build with debug symbols
 [ ] BW   Build with bandwidth limitation functionality
 [ ] HASH   Build with HASH support

Среди прочих присутствует опция BW   Build with bandwidth limitation functionality

С ее помощью можно будет ограничивать скорость пользователям самим нетамсом. Раньше я ее использовал, потом отказался в сторону pipe в ipfw.
Далее, ставим по-умолчанию.
Что-то долго не мог найти пакет. Но в итоге нашел и все установил:The NeTAMS package has been successfully installed.

Check /usr/local/share/netams and http://www.netams.com for examples.

A sample configuration file has been installed to /usr/local/etc as "netams.cfg.sample". This may be renamed to "netams.cfg" and edited.

In order to use the netamsctl programs, you may copy /usr/local/share/netams/.netamsctl.rc to your home directory and edit it.

By default, CGI scripts are NOT installed, as well as web server is NOT configured.
You should do it yourself, and then copy entire /usr/local/share/netams/cgi/ directory to appropriate place.

And PLEASE READ THE DOCUMENTATION FIRST!
http://www.netams.com

===> Installing rc.d startup script(s)
===> Compressing manual pages for netams-3.4.0.r2
===> Registering installation for netams-3.4.0.r2

===> SECURITY REPORT:
 This port has installed the following files which may act as network
 servers and may therefore pose a remote security risk to the system.
/usr/local/libexec/netams
/usr/local/sbin/ipfw2netflow

 This port has installed the following startup scripts which may cause
 these network services to be started at boot time.
/usr/local/etc/rc.d/netams

 If there are vulnerabilities in these programs there may be a security
 risk to the system. FreeBSD makes no guarantee about the security of
 ports included in the Ports Collection. Please type 'make deinstall'
 to deinstall the port if this is a concern.

 For more information, and contact details about the security
 status of this software, see the following webpage:
http://www.netams.com/

Ну что ж далее по-порядку.[root@ /usr/ports/net-mgmt/netams]# cd /usr/local/etc/
[root@ /usr/local/etc]# cp netams.cfg.sample netams.cfg
[root@ /usr/local/etc]# ee netams.cfg

Конфиг по-умолчанию такой:
!!! Строки взятые в квадратные скобки [...] - нужно писать в одну строку !!!#NeTAMS version 3.4.0 (template config)
#begin
#global variables configuration
debug none
user name admin real-name Admin password aaa email root@localhost permit all

#services configuration

service server 0
login local
listen 20001
max-conn 6

service processor 0
lookup-delay 60
flow-lifetime 180
policy name ip target proto ip
policy name www target proto tcp ports 80 81 8080 3128
policy name mail target proto tcp ports 25 110

```
restrict all pass local pass
unit group name CLIENTS acct-policy ip www mail
unit host name server ip 192.168.0.1 acct-policy ip www mail
[unit user name client1 ip 192.168.0.10 parent CLIENTS email
 client1@domain.ru acct-policy ip www mail]
unit net name LAN ip 192.168.0.0/24 acct-policy ip www mail
storage 1 all

service storage 1
type mysql

service data-source 1
type libpcap
source eth0
rule 11 "ip"

service quota 0
policy ip
notify soft {owner}
notify hard {owner} admin
notify return {owner}
storage 1

service alerter 0
report oid 06100 name rep1 type traffic period day detail simple
smtp-server localhost

service html 0
path /usr/local/www/stat
run 10min
htaccess yes
client-pages all
url http://192.168.0.1/stat/
language ru

service scheduler
oid 08FFFF time 10min action "html"

# $Id: netams.cfg,v 1.12 2006-12-29 18:44:52 anton Exp $
#end
```

Я пока оставил его таким, ничего не меняя.
Далее делаемecho "netams_enable="YES"" >> /etc/rc.conf

стартуем и проверяем нетамс[root@ /usr/local/etc]# /usr/local/etc/rc.d/netams start
Starting netams.
[root@ /usr/local/etc]# sockstat -4l
USER COMMAND PID FD PROTO LOCAL ADDRESS FOREIGN ADDRESS
root netams 15866 4 tcp4 127.0.0.1:20001 *:*
mysql mysqld 15154 10 tcp4 *:3306 *:*
root sendmail 631 3 tcp4 127.0.0.1:25 *:*
root sshd 625 4 tcp4 *:22 *:*
root syslogd 500 7 udp4 *:514 *:*

и того у нас все гут.
Далее делаем все по документации. Мы видим, что нетамс у нас слушается на 20001-м порту.
В конфиге выше была строка:user name admin real-name Admin password aaa email root@localhost permit all

из нее видно что админ нетамса у нас пользователь по имени admin, и пароль его aaa.
заходим телнетом на 20001-й порт[root@ /usr/local/etc]# telnet 127.0.0.1 20001
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
NeTAMS 3.4.0 (3146.1) root@ / Mon Feb 25 01:38:51 UTC 2008

Username: admin
Password:

Далее как гласит дока, пробуем выполнить команды "html", "save", "show version", "show config".
> html

> save

> show version
NeTAMS 3.4.0 (3146.1) root@ / Mon Feb 25 01:38:51 UTC 2008
Run time 1 mins 51.1777 secs
System time: 1 mins 0.3991 secs
Average CPU/system load: 0.36%
Process ID: 15866 RES: 3868K
Memory allocated: 597212 (108), freed (22) (0 NULL) [86 used]
Total objects:
Oids used: 9
NetUnits: 4

```
 Policies: 3
 Services: 10
 Users: 1
 Connections: 1 active, 1 total

Services info:
 Storage ID=1 type mysql wr_q 0/7 rd_q 0/0
 Data-source ID=1 type LIBPCAP source eth0:0 loop 0 average 0 mcsec
 Perf: average skew delay 0 mcsec, PPS: 0, BPS: 0
Alerter 0 queue max: 255, current: 0
 Scheduled tasks: 1

> show config
#NeTAMS 3.4.0 (3146.1) root@ / Mon Feb 25 01:38:51 UTC 2008
#configuration built Mon Feb 25 01:45:38 2008
#begin
#global variables configuration
debug none
language ru
user oid 06260D name admin real-name "Admin" crypted $1$$HpXmjtul/3i1.bf.B27bU.
email root@localhost permit all

#services configuration

service server 0
login local
listen 20001
max-conn 6

service processor
lookup-delay 60
flow-lifetime 180
policy oid 00D9B2 name ip target proto ip
policy oid 09DC4B name www target proto tcp port 80 81 8080 3128
policy oid 07A20C name mail target proto tcp port 25 110
restrict all pass local pass
unit group oid 099818 name CLIENTS acct-policy ip www mail
unit host oid 03C6A3 name server ip 192.168.0.1 acct-policy ip www mail
unit user oid 02D10B name client1 ip 192.168.0.10 email client1@domain.ru parent
CLIENTS acct-policy ip www mail
unit net oid 01988F name LAN ip 192.168.0.0/24 acct-policy ip www mail

service storage 1
type mysql
accept all
```

```
service data-source 1
type libpcap
source eth0
rule 11 "ip"

service quota
policy ip
notify soft owner
notify hard owner
notify return owner

service alerter 0
report oid 06100 name rep1 type traffic period day detail simple
smtp-server localhost

service html
path /usr/local/www/stat
run 10min
url http://192.168.0.1/stat/
htaccess yes
client-pages all
account-pages none

service scheduler
oid 08FFFF time 10min action "html"


#end

>
```

если все так как у меня, то ура, мы установили нетамс :)
Далее я на всякий случай проверил, создал ли он базу.[root@ /usr/local/etc]# mysql
Welcome to the MySQL monitor. Commands end with ; or g.
Your MySQL connection id is 10
Server version: 5.0.51a FreeBSD port: mysql-server-5.0.51a

Type 'help;' or 'h' for help. Type 'c' to clear the buffer.

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
```

```
| netams             |
| test               |
+--------------------+
4 rows in set (0.01 sec)

mysql> use netams;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+------------------+
| Tables_in_netams |
+------------------+
| events           |
| oids             |
| quota            |
| summary          |
+------------------+
4 rows in set (0.01 sec)
```

все хорошо. ну что ж , тогда можно вернуться на реальный сервак и продолжить на нем.

Кроме mysql нам понадобится еще настроенный web-server, я использую apache.
С его помощью пользователи смогут смотреть статистику.
Теперь выкладываю свой конфиг и рассказываю что и зачем.
!!! Строки взятые в квадратные скобки [...] - нужно писать в одну строку !!!#NeTAMS version 3.3.5 (build 2916.1) compiled by root@freeserv.home
#configuration built Thu Nov 16 21:50:15 2006
#begin
#global variables configuration
debug none
language ru
[user oid 02A6F4 name admin real-name "Eugene" crypted $1$$1CXSo9ZU3rRh4yE2MnSlV0
email root@localhost permit all]

#services configuration

service server 0
login local
listen 20001
max-conn 6

service processor
lookup-delay 30

```
flow-lifetime 180
policy oid 0B4940 name ip target proto ip
restrict all drop local pass
[unit net oid 022222 name stah_all ip 10.0.0.0 mask 255.255.255.0 description
 "net 10.0.0.0" password 123 no-local-pass acct-policy ip ]
unit host oid 033333 name server ip 193.16.xx.xx
[unit host oid 000001 name eugene ip 10.0.0.1 description "ip 192.168.10.5"
 email eugene@localhost password 123 acct-policy ip ]
[unit host oid 000002 name agent ip 10.0.0.2 description "ip 192.168.10.18"
 password 123 acct-policy ip ]
[unit host oid 000003 name chetkiller ip 10.0.0.3 description "ip 192.168.10.7"
 password 123 acct-policy ip ]
[unit host oid 000004 name sirius ip 10.0.0.4 description "ip 192.168.10.29"
 password 123 acct-policy ip ]
[unit host oid 000005 name TEAC ip 10.0.0.5 description "ip 192.168.10.40"
 password 123 acct-policy ip ]

service storage 1
type mysql
host localhost
user LOGIN
password PASSWORD
accept all

service data-source 1
type ip-traffic
source divert 199
layer7-detect urls

service login




storage 1
set no name eugene password 123456 inact 3000 abs 0
relogin yes


service monitor 0
monitor to file /usr/tmp/mon_netams.log
monitor unit 000001
monitor unit 000002
monitor unit 000003
monitor unit 000004
monitor unit 000005
```

service quota
policy ip
notify soft {owner}
notify hard {owner} 02A6F4
notify return {owner}

service alerter 0
report oid 06100 name rep1 type traffic period day detail simple
smtp-server localhost

service html
path /usr/local/www/data/stat
run 5min
url http://192.168.10.100/stat/
htaccess yes
client-pages all
account-pages all

service scheduler
oid 08FFFF time 5min action "html"

#end

Итак, по-порядку.
сперва меняем логин/пароль админа нетамса.
!!! Строки взятые в квадратные скобки [...] - нужно писать в одну строку !!![user oid 02A6F4 name admin real-name "Eugene" password SUPERPASS
email root@localhost permit all]

пока он в открытом виде, после рестарта нетамса, но закриптуется.
Также oid можно не ставить, Нетамс его сам поставит.
Далееservice server 0
login local
listen 20001
max-conn 6

Сильна расписывать не буду, т.к. все есть в доке. В кратце: нетамс слушает 20001-й порт,
висит на локалхосте и имеет максимальное число одновременно открытых подключений к процессу 6.

Дальше:
!!! Строки взятые в квадратные скобки [...] - нужно писать в одну строку !!!service

```
processor
lookup-delay 30
flow-lifetime 180
policy oid 0B4940 name ip target proto ip
restrict all drop local pass
[unit net oid 022222 name stah_all ip 10.0.0.0 mask 255.255.255.0 description
 "net 10.0.0.0" password 123 no-local-pass acct-policy ip ]
unit host oid 033333 name server ip 193.16.xx.xx
[unit host oid 000001 name eugene ip 10.0.0.1 description "ip 192.168.10.5"
 email eugene@localhost password 123 acct-policy ip ]
[unit host oid 000002 name agent ip 10.0.0.2 description "ip 192.168.10.18"
 password 123 acct-policy ip ]
[unit host oid 000003 name chetkiller ip 10.0.0.3 description "ip 192.168.10.7"
 password 123 acct-policy ip ]
[unit host oid 000004 name sirius ip 10.0.0.4 description "ip 192.168.10.29"
 password 123 acct-policy ip ]
[unit host oid 000005 name TEAC ip 10.0.0.5 description "ip 192.168.10.40"
 password 123 acct-policy ip  ]
```

Основное, это сервис policy, определяет правило, или политику, по которой для данного объекта (NetUnit) будет производиться фильтрация или подсчет трафика. Т.к. я описываю минимальную конфигурацию, то я использую policy ip, т.е. подсчет всего трафика, не разбивая его по протоколам и портам (нетас это умеет).
Строка restrict all drop local pass, говорит о том, что трафик с ИП-адресов не описанных в конфигурации нетамса пропускаться не будет. По-этому нужно включить и внешний ИП-самого сервера.
далее, я создал один unit, описывающий сеть, а также описал каждого пользователя. Тут подсчет трафика идет по ip из сети 10.0.0.0/24. Опция description позволяет задать любое описание юнита, в моем случае, это ИП-машины пользователя (у меня пользователи имеют статический Ип из сети 192.168.10.0/24, а при подключении по впн им выдается ИП из диапазаона 10.0.0.0/24). Далее идет пароль доступа к страничке со статистикой, ну и указание каким policy мы ограничиваем пользователя, у меня всех ограничиваем полиси ip.

```
далее.service storage 1
type mysql
host localhost
user LOGIN
password PASSWORD
accept all
```

тут описывается собственно хранилище данных. Указываем, что мы используем базу данных mysql, что она находится на этом же хосте, что и нетамс (localhost), а так же указываем логин/пароль к базе нетамса (ведь от рута работать это не есть гут ;))

Что бы установить логин/пароль для базы нетамса, заходим в mysql и даем команду:grant all privileges on netams.* to 'LOGIN'@'localhost' identified by 'PASSWORD';

дальшеservice data-source 1
type ip-traffic
source divert 199
layer7-detect urls

описывается тип и источник данных. В нашем случает тип это ip-traffic, а источник, это divert 199. Т.е. что бы трафик попадал нетамсу, его нужно на него как-то завернуть, я использую правило divert в ipfw. Правила НАТа на НЕТАМС должны обязательно обрамлять правила, которым НАТится сеть в интернет. #NeTAMS-NAT-NeTAMS-out
${fwcmd} 1000 add divert 199 ip from 10.0.0.0/24 to any out xmit ${oif}
${fwcmd} 1100 add divert 8668 ip from 10.0.0.0/24 to any out xmit ${oif}
#NeTAMS-NAT-NeTAMS-in
${fwcmd} 1195 add divert 8668 ip from any to me in recv ${oif}
${fwcmd} 1200 add divert 199 ip from any to 10.0.0.0/24 in recv ${oif}

далееservice monitor 0
monitor to file /usr/tmp/mon_netams.log
monitor unit 000001
monitor unit 000002
monitor unit 000003
monitor unit 000004
monitor unit 000005

сервис monitor, тут я указал размещение файлика mon_netams.log, а так же для каких юнитов ведется сам монитор. Монитор - это лог кто куда ходил. Так же не забудьте описать ротирование этого файла, иначе он может занять все свободное пространство на разделе.

Сервис login и quota, я опишу в следующей статье.
И последнийservice html
path /usr/local/www/data/stat
run 5min
url http://192.168.10.100/stat/
htaccess yes
client-pages all
account-pages all

Сервис html, описывает странички статистики. Здесь мы указываем путь, куда их

генерить, переодичность и url к ним.
Так же описываем тип доступа, в данном случае, включен механизм htaccess, который позволяет разграничить доступ пользователям только к своим страницам статистики исходя из логина/пароля.

Теперь опишем секцию нетамса в апаче:<Directory "/usr/local/www/data/stat/">
 AllowOverride All
 Options None
 Order deny,allow
 Allow from 192.168.10.66 192.168.10.97 192.168.10.45 192.168.10.5 192.168.10.18
 Deny from all
</Directory>

Тут так же с примером разграничения доступа к статистике по ИП-адресам.
Далее делаем stop/start нетамсу, рестартуем апач. И через некоторое время ждем появления статистики по указанному url (http://192.168.10.100/stat/). Тут спросит логин/пароль админа.
(если не хочется ждать, можно зайти телнетом и выполнить команду html).
Для доступа пользователей к своей страничке идем по адресу:
http://192.168.10.100/stat/unit, (где unit - имя пользователя в нетамсе).

Так же есть хорошая примочка у разработчиков. Чтобы каждый раз не ходить телнетом, есть так называемый netamsctl.
netamsctl - примитивный telnet-клиент, позволяющий передать одну или несколько команд для работающего netams. Он работает через обычный TCP-сокет. Открывается соединение, отправляется команда, получается и выводится на экран ответ сервера.
Итак настроим его.# whereis netamsctl
netamsctl: /usr/local/bin/netamsctl /usr/local/man/man8/netamsctl.8.gz
/usr/ports/net-mgmt/netams/work/netams-3.3.5/src/netamsctl

Замечательно, присутствует. В своем домашнем каталоге (пользователя, от которого будет выполняться) создаем файл .netamsctl.rc такого содержания:login=LOGIN
password=PASSWORD
host=localhost

ну и порт, если вы изменили дефолтовый.
Далее работать примерно так:# netamsctl "show version"
host: localhost port: 20001 login: LOGIN password: PASSWORD
cmd: show version
NeTAMS version 3.3.5 (build 2916.1) root@freeserv.home / Sun Jun 25 18:08:46 EEST 2006
Run time: 10 days 5 hours 57 mins 2.4393 secs
System time: 5 hours 57 mins 35.4570 secs
Average CPU/system load: 2.42%

Process ID: 69168 RES: 3620K
Memory allocated: 54495887 (1513554), freed (1503417) (0 NULL) [10137 used]

Total objects:
 Oids used: 75
 NetUnits: 71
 Policies: 1
 Services: 12
 Users: 3
 Connections: 2 active, 49 total
 Scheduled tasks: 1
Alerter 0 queue max: 255, current: 0

Services info:
 Storage ID=1 type MYSQL wr_q 0/288146 rd_q 0/70
 Data-source ID=1 type IP_FILT source divert:199 loop 111323580 average 5 mcsec
 Perf: average skew delay 115 mcsec, PPS: 154, BPS: 42560

Так же возможно задать на исполнение сразу несколько команд, если разделить их комбинацией " && ". Это крайне полезно, если необходимо передать команду какому-нибудь сервису: netamsctl "service processor && unit host name pupkin sys-deny && exit"

Разработчики рекомендуют все юниты заводить именно с помощью netamsctl, затем делать save. При этом нет необходимости рестартовать нетамс.
У меня исторически сложилось так, что я описываю все в конфиге ручками. а затем рестартую нетамс. Мне так удобнее, например для бекапирования, или просто посмотреть предыдущую запись...в общем имхо :)