Установка NTOP на FreeBSD 6.2

Автор: roygbiv.
Оригинал: http://www.lissyara.su/articles/freebsd/traffic_count/ntop/

Задача: собрать мощный сервер для анализа трафика в сети. Иметь возможность периодически вылавливать и анализировать netflow-статистику с Cisco.
Необходимость возникла из-за незнания "предпочтений" пользователей, и невозможности регулировать аппетиты "топперов" без диаграмм загрузки сети определёнными хостами.
До этого была настроена flow-tools+flowscan+cflowd статистика, которая ловила mirror с главного мартшрутизатора и превращала всё в NetFlow анализируемые пакеты, но захотелось опробовать другие инструменты.

Ожидаемый результат: с помощью данного решения есть возможность без особых трудностей и напряжения серого вещества, да ещё и доступными средствами, собирать и анализировать статистику сети на простейшем оборудовании (любой свитч с mirroring'ом всех портов на один), и строить наглядные графики и таблички "кто-откуда, когда и сколько", но, это решение не позволит вам без доп.знаний СОХРАНЯТЬ статистику. Если вам нужно импортировать данные, либо нужно будет написать скрипты (поддерживается импорт в perl,php и прочее), либо использовать другое решение.
Данная система отображает текущее состояние нагрузки сети, а история в графиках будет жить только до первого перезапуска.
Мне больше от неё и не надо было, т.к. остальное делает вышеуказанная связка flow-tools+flowscan (где посмотреть:1 и 2).

Решение не абсолютное, и использованию подлежит лишь в тех случаях, когда сетевой отдел либо единица управления сетью (в виде ленивого админа) не располагает средствами для покупки как дорогих программных, так и аппаратных решений для анализа трафика и ему нужны графические отчёты для шефа.
Структура реализации: единый центр обмена данными, в котором есть главный маршрутизатор, посылающий зеркалом весь трафик сети на один свой порт, далее, с этого порта принимает и анализирует данные сервер.

Выбор пал на ntop. О нём и его модулях далее пойдёт речь.
Данная статья не рассчитана на профи, прошу не тыкать мне умными замечаниями, кроме конструктивов и замеченными ошибками. Описания настройки Ntop под FreeBSD в сети я не нашёл.
То, что здесь описано, у меня работает.

Оф. сайт программы - http://www.ntop.org/
Ntop - это мощный и довольно тонкоконфигурируемый инструмент для мониторинга

сетей и выявления неполадок.
Распространяется свободно по лицензии GPL, v2 (и поздние).
Возможно управление из командной строки, а так же использование встроенного веб-сервера (умеет ssl).
ntop использует libcap (т.е. сильно грузит CPU для обработки трафика), так что заранее выбирайте сервер помощнее (мой был P4 D 3GHz, 3200MB RAM).

Описание возможностей 3.2 версии (http://www.ntop.org/overview.html):

* Сортировка трафика по большому кол-ву протоколов
* Возможность сортировки данных о трафике по многим критериям
* Отображение сетевой активности (данные о трафике)
* Хранение данных в формате RRD (Round Robin Tool)
* Распознавание особенностей (напр. почтовые адреса) пользователей (детализированное сканирование)
* Пассивное (т.е. без посылки пакетов-запросов) распознавание типов ОС компьютеров
* Отображение распределения IP трафика по протоколам
* Анализ IP трафика и сортировка по источнику/месту назначения
* Отображение структуры и направления IP трафика в виде схем (кто с кем обменивается?)
* Вывод сведений об использовании IP трафика сортировкой по типу протоколов
* Возможность работы в режиме NetFlow/sFlow коллектора для приёма потоков, генерируемых роутерами (Cisco, Juniper) или коммутаторами (Foundry Networks)
* Генерация статистики обмена сетевым трафиком в RMON-подобном формате.

Установку будем производить из портов, как все лентяи.
Символ по ходу лирики - переход на следующую строку (для самых внимательных).
Если не обновляли давно порты: portsnap fetch; portsnap extract

далее, после муторного ожидания ищём пакет ntop: whereis ntop
ntop: /usr/ports/net/ntop

У меня была версия 3.2 (с октября 2005го года не обновлялась), но сейчас вышла 3.3, возможны изменения.
Идём в директорию и собираем пакет, но не делайте make clean! Нам кое-что понадобится из исходников. cd /usr/ports/net/ntop && make install
[X] LOCALE Enable locale (i18n) support. (поддержка интернациализации)
[X] PCAP_PORT Use libpcap from ports. (используем libcap из портов,а не системный)
[ ] XMLDUMP Enable XML Dump support. (не собирается :( )
[X] ASDATA Install AS data. (show traffic by Autonomous System Number,
жрёт доп. память для обработки AS, в большинстве случаев не нужна)
[X] TCPWRAPPER Enable TCP wrapper support

После установки, идём в
/usr/ports/net/ntop/work/ntop-3.2/packages/FreeBSD-ports/net/ntop/files и достаём оттуда sample-config (ntop.conf.sample): cp /usr/ports/net/ntop/work/ntop-3.2/packages/FreeBSD-ports/net/ntop/files/ntop.conf.sample
usr/local/etc/ntop/ntop.conf

И меняем права на файл, а то он какой-то исполняемый, что не есть правильно: chmod -x /usr/local/etc/ntop/ntop.conf

Теперь необходимо проделать операцию создания каталогов для хранения данных ntop. Для этого необходимо создать пользователя (используйте интерактивный # adduser) с ограниченными правами и доступом к выбранной вами папки.
У меня он такой: cat /etc/passwd | grep ntop
ntop:*:2001:2001:ntop manager:/data/netflow/ntop_db:/usr/sbin/nologin

Изменим владельца каталога: chown -R ntop:ntop /data/netflow/ntop_db

Правим конфигурационный файл ntop на своё усмотрение, приведу свой конфиг: cat /usr/local/etc/ntop/ntop.conf
--user ntop # под кем запускать демон
--db-file-path /data/netflow/ntop_db # путь к БД

на каком сетевом интерфейсе слушать (сюда приходит весь mirror-трафик)
--interface rl0

отключить "доверие" MAC-адресам, в случае >
когда у нас данные идут с mirror интерфейса активного оборудования
--no-mac

логи идут не на экран терминала (stdout, по умолчанию), а в syslog
--use-syslog=local3
 # на каком порту слушает встроенный веб-сервер >
(можно ещё --https-3001 вместе с http,
сертификат здесь - /usr/local/etc/ntop/ntop-cert.pem)
--http-server 3000

помогаем программе определить что считать локальным
трафиком (внутренняя сеть будет обособлена для удобства)
--local-subnets 192.168.0.0/16,172.16.192.0/24

можно указать домен для сети, либо программа определит >
его самостоятельно

--domain vasya.ru
--daemon # запускать в виде демона, что под freebsd всегда верно

Полный список команд и вариантов можно посмотреть так: /usr/local/bin/ntop -h

Чтобы логи шли в определённый файл, как мы указали в конфиге, необходимо добавить в syslog.conf следующее: echo '!ntop' >> /etc/syslog.conf
echo 'local3.* /var/log/ntop.log' >> /etc/syslog.conf

и создать этот файл с минимальными правами (чтобы вражище не подсмотрел): touch /var/log/ntop.log && chmod 600 /var/log/ntop.log

Перед запуском всей системы необходимо создать базу и задать пароль администратора: /usr/local/bin/ntop -P /data/netflow/ntop_db -u 2001 -A

где указана папка, которой владеет ntop пользователь с порядковым номером 2001 (мы его таким создали).
Вывод будет примерно таким:Thu May 3 23:31:52 2007 NOTE: Interface merge enabled by default
Thu May 3 23:31:53 2007 Initializing gdbm databases

ntop startup - waiting for user response!

Please enter the password for the admin user:
Please enter the password again:
Thu May 3 23:32:06 2007 Admin user password has been set

Готово, всё настроено и ждёт запуска - для начала сбора статистики и зарисовки диаграмм с графиками для начальника, чтобы учёл старания.
Если у Вас есть сетевой фильтр (firewall), откройте 3000ый tcp порт наружу, а если захотите snmp статистики, то и 161ый udp тоже в режиме keep-state (+163 udp на всякий случай).
Для IPFW это выглядит примерно так (вместе с другими правилами в скрипте): ipfw add allow tcp from me 3000 to 192.168.1.1 via em0

где 192.168.1.1 - IP вашего админского компа, чтобы другим неповадно было, а em0 - сетевая на текущем сервере, где стоит ntop и которая смотрит в ту же сеть, что и админский комп.
Если будете использовать родной скрипт - /usr/local/etc/rc.d/ntop, то не забудьте: echo

'ntop_enable="YES"' >> /etc/rc.conf
echo 'ntop_flags="@/usr/local/etc/ntop/ntop.conf"' >> /etc/rc.conf

И если у вас папка БД программы отличается (как и у меня) от /var/db/, то исправьте проверку на наличие ntop_pw.db файла
в /usr/local/etc/rc.d/ntop скрипте с указанием вашей папки (сами найдёте).
После этого запускаем демона: /usr/local/etc/rc.d/ntop start

и идём в любимый браузер по ссылке http://адресвашегосерверантop:3000
Смотрим и любуемся на потёкшую статистику, а модули в админке подключаем через логин admin и пароль тот, который вводили при создании БД.
Если есть netflow-генерирующий мартшутизаторо-коммутатор или на машине установлен ucd-snmp (net-snmp вроде тоже подойдёт), идём в секцию plugins и включаем там необходимые модули, немножко их настроив:
add netflow device - появляется таблица, где необходимо указать параметры поступающего потока. Здесь всё просто, нужно только иметь доп.сетевую (разумнее), которая ловит netflow, и указать её в конфигурации с дополнительными параметрами.
Так же в админке можно имзенять кучу настроек, тюнинговать существующие и добавлять новые правила фильтрации, дополнять параметрами опции сервера и создавать пользователей для доступа к своей статистике с разными привилегиями.

Если нужно сделать так, чтобы сервер был доступен из-под apache (http://vasya.ru/ntop к примеру), необходимо сделать следующее:
запустить ntop на 3000ом порту (значение можно поменять, конечно же), с параметрами: -w127.0.0.1:3000 -W0 #слушать на http//localhost:3000 и не слушать на https вообще.
Apache должен быть собран с модулями (не все могут быть необходимы, но всё-таки) mod_cgid mod_headers mod_security mod_proxy mod_proxy-http mod_proxy-html proxy_connect.load
proxy_html.load mod_rewrite mod_ssl mod_userdir и поддерживать работу на 443ем порту (ssl).
Секция вирт.хоста в конфиге апача (либо,если версия 2.x,то файла путьдоapache/extra/httpd-vhosts.conf)

```
NameVirtualHost *:443
<VirtualHost *:443>

######          Весь трафик на 443ем порту ( HTTPS )

# поменяйте на свою почту
ServerAdmin webmaster@localhost
SSLEngine On
# поменяйте на путь к вашему сертификату
SSLCertificateFile /etc/apache2/ssl/apache.pem

# измените пути к логам
```

```
ErrorLog /var/log/apache2/error.log
# выберите уровень логирования из предложенных:
# debug, info, notice, warn, error, crit, alert, emerg.
LogLevel warn
CustomLog /var/log/apache2/access.log combined
ServerSignature On
###  PATCH SUGGESTED BY NESSUS ABOUT TRACE ATTACKS
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]

#### NTOP (PROXY проброс) ########
ProxyHTMLLogVerbose On
LogLevel warn
ProxyHTMLExtended On
ProxyRequests Off
<Proxy *>
Order deny,allow
Allow from all
</Proxy>
ProxyPass /ntop/  http://localhost:3000/
ProxyPassReverse /ntop/  http://localhost:3000/
<Location /ntop/>
SetOutputFilter  proxy-html
ProxyHTMLURLMap  / /ntop/
ProxyHTMLURLMap /ntop/plugins/ntop/ /ntop/plugins/
RequestHeader   unset Accept-Encoding
</Location>

</VirtualHost>
```

И перезапустите apache (в моём случае поставлен из портов, версия 2.2.4):
/usr/local/etc/rc.d/apache22 restart

и зайти по адресу https://vasya.ru/ntop/ .

Либо, как другой вариант (редирект с помощью apache-модуля proxy), вкратце:ProxyPass /ntop/ http://localhost:3000/

а в вирт.хостах:
```
RewriteEngine On
RewriteCond %{HTTP_REFERER} vasya.ru/ntop
RewriteCond %{REQUEST_URI} !^/ntop
RewriteRule ^/(.*)$ http://vasya.ru/ntop/$1 [L,P]
```

По идее, всё должно работать, секцию с апачем я пока честно своровал и не пробовал.

На заметку: Ntop 2.1.3 was the last version with the mySQL stuff and is completely unsupported.

При установке руководствовался и откровенно тырил мысли с сайта ntop.org.
Все вопросы к разработчикам, я не при чём, у меня всё работает :)