



SQUID + SAMS - гибкость в управлении доступом

Опубликовано muff в Вт, 2010-03-16 14:01



Настроен очередной маршрутизатор... Как бы работа уже завершена. Но "высокое начальство" решает, что нужно полностью контролировать трафик. Для контроля контента только один вариант - прокси-сервер. Выбор остановился на довольно мощном инструменте - SQUID. Тем более, что к нему можно "прикрутить" такой инструмент, как [SAMS \(Squid Account Manager Sams\)](#) [1].

Но обо всем по порядку...

Будем отталкиваться от того, что [Apache](#) [2], [PHP5](#) [2] и [MySQL](#) [3] уже установлены и настроены.

Приступим непосредственно к установке прокси-сервера Squid

```
# cd /usr/ports/www/squid && make install clean && rehash
```

Опции сборки устанавливаю следующие:

Options for squid 2.7.7_4

```
[ ] SQUID_KERB_AUTH      Install Kerberos authentication helpers[ ] SQUID_LDAP_AUTH
  Install LDAP authentication helpers[ ] SQUID_NIS_AUTH      Install NIS/YP auth
  entication helpers[ ] SQUID_SASL_AUTH      Install SASL authentication helpers[X] SQ
UID_DELAY_POOLS      Enable delay pools[X] SQUID_SNMP          Enable SNMP support[X]
  SQUID_CARP          Enable CARP support[X] SQUID_SSL          Enable SSL support
  for reverse proxies[X] SQUID_PINGER        Install the icmp helper[ ] SQUID_DNS_HE
  LPER              Use the old 'dnsserver' helper[ ] SQUID_HTCP          Enable HTCP support[
  ] SQUID_VIA_DB      Enable forward/via database[ ] SQUID_CACHE_DIGESTS  Enable c
  ache digests[X] SQUID_WCCP          Enable Web Cache Coordination Prot. v1[ ] SQUID
  _WCCPV2            Enable Web Cache Coordination Prot. v2[ ] SQUID_STRICT_HTTP  Be st
  rictly HTTP compliant[X] SQUID_IDENT      Enable ident (RFC 931) lookups[ ] SQUI
  D_REFERERER_LOG    Enable Referer-header logging[ ] SQUID_USERAGENT_LOG  Enable User-A
  gent-header logging[X] SQUID_ARP_ACL      Enable ACLs based on ethernet address[ ]
  SQUID_PF           Enable transparent proxying with PF[ ] SQUID_IPFILTER      En
  able transp. proxying with IPfilter[ ] SQUID_FOLLOW_XFF      Follow X-Forwarded-For h
  eaders[ ] SQUID_AUFS          Enable the aufs storage scheme[ ] SQUID_COSS
  Enable the COSS storage scheme[X] SQUID_KQUEUE          Use kqueue(2) instead of po
  ll(2)[X] SQUID_LARGEFILE      Support log and cache files >2GB[ ] SQUID_STACKTRACES
  Create backtraces on fatal errors
```

Создадим SWAP:

```
# squid -z
2010/03/16 19:42:23| Creating Swap Directories
```

Добавим Squid в /etc/rc.conf



```
# echo '# Proxy-server' >> /etc/rc.conf
# echo 'squid_enable="YES"' >> /etc/rc.conf
```

Собственно, запуск Squid:

```
# sh /usr/local/etc/rc.d/squid start
Starting squid.
```

Проверяем, есть ли Squid в процессах:

```
# ps -ax | grep squid
3675 ?? ls 0:00.00 /usr/local/sbin/squid -D
3677 ?? S 0:00.37 (squid) -D (squid)
```

Squid запущен и работает. Приступим к установке и настройке непосредственно SAMS.

```
# cd /usr/ports/www/sams && make install clean && rehash
```

По завершению установки скопируем предложенный пример конфигурационного файла непосредственно в файл конфигурации:

```
# cp /usr/local/etc/sams.conf.sample /usr/local/etc/sams.conf
```

Далее правим конфигурационный файл до следующего состояния:

```
# cat /usr/local/etc/sams.conf

[client]

# имя базы данных, где SAMS хранит информацию, полученную из логов SQUID
SQUID_DB=squidlog

# имя базы данных SAMS
SAMS_DB=squidctrl

# адрес хоста, где стоит MySQL
MYSQLHOSTNAME=localhost

# имя пользователя MySQL, от имени которого будет работать SAMS
MYSQLUSER=sams

# пароль этого пользователя в MySQL
MYSQLPASSWORD=you_password_here

# версия установленного MySQL-сервера
MYSQLVERSION=5.0

# Имя файла логов SQUID
SQUIDCACHEFILE=access.log

# путь к директории, где лежит конфиг SQUID
SQUIDROOTDIR=/usr/local/etc/squid

# путь к директории, где лежит файл логов SQUID
SQUIDLOGDIR=/var/squid/logs

# путь к кэшу SQUID

# необходим для работы функции восстановления файлов из кэша SQUID
SQUIDCACHEDIR=/var/spool/squid
```



```
# путь, куда установлен SAMS
SAMSPATH=/usr/local

# путь, где лежит SQUID
SQUIDPATH=/usr/local/sbin

# Если вы хотите использовать NTLM или AD авторизацию,
# и у вас есть имена пользователей на руссокм языке,
# необходимо присутствие этого пункта:
RECODECOMMAND=iconv -f KOI8-R -t 866 %finp > %fout

# путь к редиректору REJIK
REJIKPATH=/usr/local/rejik

# Команда, выполняемая при нажатии на кнопку SAMS "Shutdown proxy server"
# Данная команда добавлена для удобства удаленного выключения прокси сервера.
SHUTDOWNCOMMAND=/sbin/shutdown -h now
# Номер прокси-сервера SQUID, зарегистрированного в SAMS.

# SAMS поддерживает возможность управления несколькими прокси серверами SQUID
# (на данный момент только команда на реконфигурирование).

CACHENUM=0
```

Дальнейшая настройка будет производиться из веб-интерфейса. Чтобы "добраться" к нему, необходимо добавить следующий блок в httpd.conf:

```
Alias /sams "/usr/local/share/sams/"

<Directory "/usr/local/share/sams/">
AllowOverride AuthConfig
Options Indexes MultiViews
Order allow,deny
Allow from all
</Directory>
```

Также необходимо, чтобы PHP работал в Safe Mode. Для этого в php.ini выставляем следующие переменные:

```
safe_mode = On
safe_mode_exec_dir = "/usr/local/share/sams/bin"
```

Проверим, не допустили ли мы ошибок при конфигурировании, и если все в порядке, то перезапускаем демон httpd:

```
# apachectl configtest
Syntax OK
# apachectl graceful
```

Далее открываем браузер, и в строке адреса набиваем http://IP_proxy_server/sams/install.php [4]



В результате в окно браузера будет выведено окно, в котором необходимо заполнить параметры коннекта к базе MySQL, а также данные для создания аккаунта доступа к БД SAMS.

SAMS installations

MySQL Hostname:

MySQL login:

MySQL password:

Create SAMS MySQL user

SAMS MySQL user:

SAMS MySQL user password:

Create Database

SAMS documentation

[english](#)

[russian](#)

После заполнения формы, жмем кнопку "Create Database" и наблюдаем за работой скрипта. По завершению создания таблиц, будет выведено приглашение перейти в админ-панель SAMS:



SAMS installations

File squid_db.sql opened

Please wait, database createst may take up to 30 minutes.....

Database successfully generated

File sams_db.sql opened

Please wait, database createst may take up to 30 minutes.....

Database successfully generated

SAMS databases created

Please wait, create SAMS MySQL user...

SAMS MySQL user created

Starting SAMS webinterface

Добавляем в /etc/rc.conf строку запуска SAMS:

```
# echo '# Squid Account Manager Sams' >> /etc/rc.conf  
# echo 'sams_enable="YES"' >> /etc/rc.conf
```

Собственно, запуск SAMS

```
# sh /usr/local/etc/rc.d/sams start  
Starting sams.
```

Приступим к конфигурированию через веб-интерфейс. Для этого в строке браузера введем следующий URL: http://IP_proxy_servera/sams/ [4]

Результат - на скриншоте:



The screenshot shows the SAMS web interface. On the left is a navigation tree with 'SAMS' selected. The main area displays a tree of users: 'Администраторы SAMS', 'Пользователи', 'Администраторы', 'Пользователи', and 'user'. The 'user' node is circled in red. A message says 'look up the Internet work statistics' and 'You are welcome!'. Below the message, it says 'To look up the internet work statistics choose the left user frame under which you authorize in the windows domain (or enter in the browser to work in the internet), and enter the password'. At the bottom, there is a 'User' label and a small icon.

Для авторизации ждем на иконку пользователей, которую можно рассмотреть внизу скриншота. По умолчанию логин **Admin**, пароль **qwerty**.

Для начала настроим панель "под себя". Для этого переходим в раздел "WEB interface settings" и ждем иконку изменения настроек (гаечный ключ внизу страницы). Для себя я выставил переменные в следующие значение (на прилагаемом скриншоте):



WEB-interface settings

Settings of the SAMS web interface

Language:	Russian KOI8-R
Allow the users access to your own statistics:	
on daily traffic	<input checked="" type="checkbox"/>
on URL visiting	<input checked="" type="checkbox"/>
Icon set	bumper
Show users tree	<input checked="" type="checkbox"/>
Show users as	Family Name
Kilobyte size of your ISP (byte)	1024
Megabyte size of your ISP (byte)	1048576
Create diagrams	<input checked="" type="checkbox"/>
Create PDF reports:	Do not create

Save changes

Дальнейшая настройка - уже в зависимости от конфигурации сети. Я же только напишу



перечень пунктов, которые нужно поочередно настроить:

1. Настройка SAMS
2. Шаблоны пользователей
3. Пользователи -> Добавить пользователя
4. Локальные домены
5. Реконфигурирование SQUID

Наведу пример настройки с авторизацией по IP-адресу.

Настройка SAMS

SAMS -> Администрирование SAMS -> Настройка SAMS

<p>Подсчет трафика пользователей:</p> <p>Считать трафик: [Полный]</p> <p>Преобразовывать DNS имена []</p> <p>Уровень детализации записей в журнале [3]</p> <p>Домен по умолчанию (оставляем пустым)</p> <p>Выберите скрипт, используемый для отправки сообщения при отключении пользователей: [NONE]</p> <p>Введите адрес администратора, на который следует посылать сообщения [admin [at] domain [dot] com]</p> <p>Настройка авторизации пользователя:</p> <p>Способ аутентификации пользователя: [IP]</p> <p>Настройка samsdaemon</p> <p>Проверять наличие команды на реконфигурирование squid каждые [5] секунд</p> <p>Обрабатывать логи SQUID [X]</p> <p>используя: [Запускать обработчик логов через N минут]</p> <p>обрабатывать через [1] минут</p> <p>Автоматически очищать счетчики трафика пользователей [X]</p> <p>Путь к wbinfo: [/usr/bin]</p> <p>Файл перенаправления запроса [http://your.ip.address/sams/icon/classic/blank.gif]</p> <p>Путь к каталогу, где лежат файлы запрета запроса [http://your.ip.address/sams/messages]</p> <p>Редиректор [встроенный SAMS]</p> <p>Включить ограничение скорости доступа пользователей (delaypool) [X]</p> <p>Сохранять данные о трафике в базе за последние [6] месяцев</p> <p>[Сохранить изменения]</p>
--



SAMS -> Шаблоны пользователей

Создание нового шаблона

Название шаблона: **[Users]**

Объем трафика пользователя шаблона по умолчанию (Mb): **[0]**

Скорость канала для всего шаблона (byte/s): **[100000000]**

Скорость канала для всего шаблона (byte/s): **[1250000]**

Способ авторизации пользователей **[IP]**

Период лимита трафика **[месяц]**

Дни недели

Пн Вт Ср Чт Пт Сб Вск

[x][x][x][x][x][x][x]

Временной период

0 : 00 - 23 : 59

[Добавить шаблон]

SAMS -> Шаблоны пользователей -> Users

Перенаправление запроса

[x] Banners

[x] Counters

Доступ запрещен ко всем URL

Запрет доступа

[x] Chats

[x] Porno

[x] Localdomains

Объем трафика пользователя шаблона по умолчанию (Mb): **[0]**

Скорость канала для всего шаблона (byte/s): **[100000000]**

Скорость канала для отдельного пользователя (byte/s): **[1250000]**

Период лимита трафика **[месяц]**

Дни недели

Пн Вт Ср Чт Пт Сб Вск



[x][x][x][x][x][x][x]

Временной период

0 : 00 - 23 : 59

[Сохранить изменения]

Пользователи -> Добавить пользователя

Пользователь: **[user0]**

Домен: **[оставляем пустым]**

Пароль для просмотра статистики пользователем: **[hard_password]**

IP адрес/маска: **[client_ip_adress]** / **[255.255.255.255]**

Имя: **[Username_here]**

Отчество: **[Username_here]**

Фамилия: **[Username_here]**

Группа: **[Users]**

Разрешенный трафик (Мб) **[0]**

Пользователь активен: **[x]**

Шаблон: **[Users]**

[Добавить пользователя]

Локальные домены

писок содержит домены, данные по доступу к которым пользователей НЕ ЗАНОСЯТСЯ в базу логов SQUID. Трафик пользователей по этим доменам не учитывается.

пример:

linux.perm.ru - трафик с домена linux.perm.ru в базу не вносится

192.168.0.10 - трафик с хоста 192.168.0.10 в базу не вносится

192.168.0.0/24 или 192.168.0.0/255.255.255.0 - трафик с подсети 192.168.0.x в базу не вносится

SQUID -> Реконфигурирование SQUID -> Реконфигурировать

Последний штрих... Добавим последней строкой в конфигурационный файл Squid:

```
redirect_program /usr/local/bin/samsredir
```

Перезапускаем Squid, чтобы изменения вступили в силу.

```
# sh /usr/local/etc/rc.d/squid restart
```



Далее в web-интерфейсе управления задаем список URL, доступ к которым должен быть заблокирован, реконфигурируем Squid и наслаждаемся результатом:

ДОСТУП ЗАПРЕЩЕН !



Пользователь **phantom**

Доступ к данному URL запрещен

Access denied

P.S. Обработка "напильником"

После окончательной настройки, выяснилось, что не работает запрет доступа по типу расширения файла. Уточнил у всезнающего гугля, и оказалось, что данная проблема существует не только у меня. Как вариант решения проблемы - создать списки "Запрета доступа по регулярным выражениям". Например, чтобы запретить доступ к файлам формата mp3, необходимо добавить следующее регулярное выражение:

```
\.+V.+\.mp3([\W_]|$)
```

В "System Information" не отображается использование памяти и свопа:

	Total	Used	Free
Memory			
Swap			

Как оказалось, это следствие того, что SAMS изначально предназначался для Linux. "Лечится" это следующими действиями.

Изменение запросов free на top:

1. Правим /usr/local/share/sams/bin/freemem до следующего состояния:

```
# cat /usr/local/share/sams/bin/freemem

#!/bin/sh

STR=`top | grep Mem:`
echo $STR
```

2. Правим /usr/local/share/sams/bin/freeswap до следующего состояния:



```
# cat /usr/local/share/sams/bin/freeswap
```

```
#!/bin/sh
```

```
STR=`top | grep Swap:`  
echo $STR
```

3. Правим /usr/local/share/sams/src/configtray.php:

До редактирования:

```
# ***** Пропущено ***** #
```

```
$a=explode(" ",$value);  
for($i=1;$i<4;$i++)  
{  
    $mem[$i-1]=$a[$i];  
}  
$a=explode(" ",$swapvalue);  
for($i=1;$i<4;$i++)  
{  
    $swap[$i-1]=$a[$i];  
}
```

```
# ***** Пропущено ***** #
```

После редактирования:

```
# ***** Пропущено ***** #
```

```
$a=explode(" ",$value);  
for($i=1;$i<4;$i++)  
{  
    $mem[0]=$a[1]+$a[3]+$a[5]+$a[11]; //total mem  
    $mem[1]=$a[1]; //Used mem  
    $mem[2]=$a[11]; //Free mem  
}  
$a=explode(" ",$swapvalue);  
for($i=1;$i<4;$i++)  
{  
    $swap[0]=$a[1]; //total swap  
    $swap[1]=$a[3]; //used swap  
    $swap[2]=$a[5]; //free swap  
}
```

```
# ***** Пропущено ***** #
```

Результат (у меня сдвинулись и некоректно отображаются поля свапа, поскольку: Swap: 2048M Total, 2048M Free):

	Total	Used	Free
Memory	486	105M	52M
Swap	2048M	2048M	

Squid поддерживает так называемый "прозрачный" режим. То есть так, что не приходится настраивать каждого клиента отдельно, а можно завернуть всех на прокси принудительно.



Для этого требуется внести изменения в настройки Squid и файрволл ipfw. Сначала изменим настройки Squid, для этого в `/usr/local/etc/squid/squid.conf`, найдем строку:

```
http_port 3128
```

и заменим ее на

```
http_port 3128 transparent
```

Для того, чтобы изменения вступили в силу, перестартуем Squid:

```
# sh /usr/local/etc/rc.d/squid restart
```

Настройка ipfw сводится к добавлению следующего правила:

```
ipfw add 15 fwd 127.0.0.1,3128 tcp from 192.168.0.0/24 to not me dst-port 80 in recv fxp0
```

где

- у меня номер правила 15, у Вас может быть другой;
- 127.0.0.1,3128 - сокет локалхоста, на котором запущен squid;
- 192.168.0.0/24 - адрес локальной сети, которую нужно "завернуть" в проксю;
- fxp0 - интерфейс, который "смотрит" в локальную сеть.

ВАЖНО! Наткнулся на интересный баг. Если имя пользователя начинается с большой буквы, **Username** например, то Squid для этого пользователя не считает трафик (считается ли трафик, когда встречается большая буква в середине или конце логина не проверял). Если же имя пользователя написано строчными буквами - все нормально.

Источник (получено 2026-04-09 00:18):

<http://muff.kiev.ua/content/squid-sams-gibkost-v-upravlenii-dostupom>

Ссылки:

- [1] http://sams.perm.ru/index.php?option=com_content&task=view&id=15&Itemid=31
- [2] <http://muff.kiev.ua/node/22>
- [3] <http://muff.kiev.ua/node/24>
- [4] http://ip_proxy_servera/sams/install.php