

Squid, SAMS, Rejik - прокси для домена

Ubuntu 10.4.3 LTS x64

Используемое ПО:

- Squid - прокси-сервер
- SAMS - управление пользователями и настройкаим
- Rejik - блокировка сайтов

SQUID

```
$ sudo apt-get install squid libpcre3 libpcre3-dev
```

Если планируем работать через LDAP - ставим еще и вот эти пакеты:

```
$ sudo apt-get install ldap-utils php5-ldap
```

SAMS

Устанавливаем

Берем с <http://code.google.com/p/sams2/>

Скачиваем последнюю версию SAMS (На настоящий момент версия 1.0.5), для i386 архитектуры процессора выполним это:

```
$ mkdir /usr/src/sams
$ cd /usr/src/sams
$ wget
http://www.nixdev.net/release/sams/packages/xUbuntu_9.10/i386/sams_1.0.5_i386.deb
$ wget
http://www.nixdev.net/release/sams/packages/xUbuntu_9.10/all/sams-doc_1.0.5_all.deb
$ wget
http://www.nixdev.net/release/sams/packages/xUbuntu_9.10/all/sams-web_1.0.5_all.deb
$ sudo dpkg -i sams_1.0.5_i386.deb
```

Если у Вас 64bit система выполняем это:

```
$ mkdir /usr/src/sams
$ cd /usr/src/sams
$ wget
```

```
http://www.nixdev.net/release/sams/packages/xUbuntu_9.10/amd64/sams_1.0.5_amd64.deb
$ wget
http://www.nixdev.net/release/sams/packages/xUbuntu_9.10/all/sams-doc_1.0.5_all.deb
$ wget
http://www.nixdev.net/release/sams/packages/xUbuntu_9.10/all/sams-web_1.0.5_all.deb
$ sudo dpkg -i sams_1.0.5_amd64.deb
```

Редактируем /etc/init.d/sams

Изменяем значение

```
SAMS_ENABLE=true
```

Устанавливаем документацию и веб-интерфейс:

```
$ sudo dpkg -i sams-doc_1.0.5_all.deb
$ sudo dpkg -i sams-web_1.0.5_all.deb
```

Создание базы данных

Для работы SAMS нам необходимо создать пользователя sams в базе данных MySQL:

```
$ mysql -u root -p

GRANT ALL ON squidctrl.* TO sams@localhost IDENTIFIED BY "yourpassword";
GRANT ALL ON squidlog.* TO sams@localhost IDENTIFIED BY "yourpassword";
```

Где yourpassword – пароль root для MySQL.

Настраиваем

Текущая версия SAMS умеет работать с PHP в режиме `safe_mode=On`. Но это требует дополнительной настроек. Для этого отредактируем файл `/etc/php5/apache2/php.ini`. Включаем режим `safe_mode`.

```
safe_mode = On
```

SAMS для некоторых функций WEB интерфейса использует системные команды, например `wbinfo`. В режиме `safe_mode` php блокирует доступ к системным командам. PHP позволяет выполнять системные команды, расположенные в каталоге, заданном параметром `safe_mode_exec_dir`. Поэтому изменяем этот параметр:

```
safe_mode_exec_dir = "/usr/share/sams/bin"
```

Далее разрешаем исполнение системных скриптов из кода PHP. Ищем в файле конфигурации

параметр и убираем из него запрет вызова функций `phpinfo system shell_exec exec`:

```
disable_functions =  
"chdir,dl,ini_get_all,popen,proc_open,passthru,pcntl_exec"
```

В файле `/etc/sams.conf` правим имя пользователя в строке:

```
MYSQLUSER=sams  
MYSQLPASSWORD=yourpasswd
```

Sams - пользователь MySQL, от имени которого будет работать, а `yourpasswd` - пароль пользователя в MySQL:

Создание баз в MySQL для пользователя SAMS

Переходим в каталог `/usr/src/sams-1.0.5/mysql/`:

```
$ cd /usr/share/sams/mysql  
$ mysql -u root -p < sams_db.sql  
$ mysql -u root -p < squid_db.sql
```

Настройка SQUID

Редактируем `/etc/squid/squid.conf`

Ни в коем случае не менять структуру файла и не удалять комментарии.

Указываем порт который будет слушать/обслуживать наш прокси:

```
http_port 3128
```

Включаем кэш:

```
cache_dir ufs /var/spool/squid 100 16 256
```

А также, раскомментировать другие опции работы с кэшем:

```
access_log /var/log/squid/access.log  
pid_filename /var/run/squid.pid
```

Подводные камни

Для установленной версии `php5` и сервера `MySQL-5.1` в WEB интерфейсе будут проблемы с настройками. Необходимо сделать это.

Редактируем /usr/share/sams/src/webconfigtray.php

```
/* function GetHostName()  
* {  
* if (!($value=getenv('SERVER_NAME')))  
* { $value="N.A."; }  
* return($value);  
*}  
*/
```

В файле /usr/share/sams/src/configtray.php закоментировать таким образом следующие строчки.

```
/* function GetHostName()  
* {  
* if (!($value=getenv('SERVER_NAME')))  
* { $value="N.A."; }  
* return($value);  
*}  
*/
```

Авторизация через LDAP

Взято отсюда: <http://sams.perm.ru/doc/ru/adldap.html>

Для того, чтобы система могла авторизоваться в AD необходимо в файле /etc/sams.conf настроить поддержку AD:

LDAPSERVER=activedirectoryserver - имя или ip адрес сервера AD
LDAPBASEDN=domain.name - домен, поддерживаемый AD.
LDAPUSER=username - пользователь, входящий в группу AD администраторов домена (Domain Administrator), от имени которого SAMS будет работать с AD
LDAPUSERPASSWD=passwd - пароль пользователя
LDAPUSERSGROUP=Users - группа, содержащая пользователей в AD (обычно это Users)

Проверка функционирования доступа к AD

Для настройки авторизации пользователей в AD необходимо в дереве настроек WEB интерфейса SAMS выбрать пункт «Администрирование SAMS», далее в нижнем фрейме нажать кнопку «Настройки SAMS». В открывшемся диалоге выбираем способ авторизации пользователей «Active Directory». Далее нажимаем кнопку «Тестировать ответ PDC». В открывшемся окне будет выведен список пользователей, зарегистрированных в AD.

Если список пользователей не выведен, то проверьте настройки доступа к ldap в sams.conf, проверьте, является ли пользователь, от имени которого вы запрашиваете информацию в AD членом группы администраторов домена.

Далее запускаем хелпер и проверяем как он авторизует пользовател в AD:

```
$ /usr/lib/squid/ldap_auth -u cn -b "cn=Users,dc=your,dc=domain"
```

```
activedirectoryserver
```

далее вводим:

```
имяпользователя пароль (через пробел)
```

и смотрим, что выдает хелпер:

OK - авторизация пользователя в AD прошла успешно, ERR - ошибка авторизации пользователя в AD

Если вы получили ошибку авторизации - читаем `man ldap_auth` и документацию по авторизации squid в AD в интернете. Есть различные способы настроить авторизацию пользователей SQUID в AD, всех их здесь я приводить не буду.

Конфигурируем SQUID на работу с авторизацией в Ad

В файл `/etc/squid/squid.conf` добавляем строки:

К сожалению, мне удалось осуществить при помощи хелпера `squid_ldap_auth` только basic авторизацию. Это означает, что браузер, при первом запросе пользователя, всегда запрашивает login и пароль.

```
auth_param basic program /usr/lib/squid/ldap_auth -u cn -b
"cn=Users,dc=your,dc=domain" activedirectoryserver
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
```

Настраиваем SAMS

Идем в секцию WEB interface settings (значок инструменты)

- Выставляем язык: `russian utf-8`
- Показывать графики в отчетах *
- Создавать PDF отчеты с помощью `fpdf` (если это нужно, требуется установить пакет `php-fpdf`)
- Остальные функции выставляете по вкусу, и по документации, благо она на русском, поэтому проблем не возникнет.

Идем в секцию Администрирование SAMS:

- Уровень детализации записей в журнале - 1
- Выбираем домен (по умолчанию WORKGROUP)
- В настройках авторизации выставляем - IP
- Обязательно ставим галочку - «Обрабатывать логи squid» и выставляем интересующий нас промежуток
- Не использовать редиректор (при настройке Режика чуть ниже изменим эту настройку)
- Включаем ограничение скорости пользователей

- И выставляем промежуток времени для хранения отчетов о посещенных ресурсах по своему усмотрению

ВАЖНО!!! Вместо <http://IP/sams/icon/classic/blank.gif> писать в обоих строчках <http://localhost/sams/icon/classic/blank.gif>). Не забудьте поставить галочку «Обрабатывать логи SQUID», иначе статистика не будет собираться. Сохраняемся.

Переходим SAMS → «Шаблоны пользователей»: Удаляем все существующие группы пользователей и шаблоны пользователей.

Теперь добавляем пользователей: SAMS → «Пользователи», нажимаем внизу «Загрузить всех пользователей домена Active Directory» или «Добавить пользователя». Тут главное - не забыть поставить галочку «Пользователь активен». И потом сохраняем изменения: SAMS → SQUID → «Реконфигурировать SQUID».

Rejik

Ставим из PPA

Есть вариант поставить пакет из PPA - это лучше и проще чем собирать из исходников. И система чище будет.

```
$ sudo apt-add-repository ppa:infra-it.ru/updates
$ sudo apt-get update
$ sudo apt-get install rejik
```

Собираем пакет из исходников

Если хочется поставить из исходников, делаем по описанию.

Загружаем файлы

```
$ mkdir /usr/src/rejik
$ cd /usr/src/rejik
$ wget http://rejik.ru/download/redirector-3.2.8.tgz
$ wget http://rejik.ru/download/squid-like-www-ru.tgz
$ wget http://www.rejik.ru/download/banlists-2.x.x.tgz
```

Распаковываем

```
$ tar xvf redirector-3.2.8.tgz
$ tar xvf squid-like-www-ru.tgz
$ tar xvf banlists-2.x.x.tgz
```

Компилируем

Перед началом компиляции необходимо внести изменения в файл Makefile:

Папка, где будет находиться наш rejik. В Ubuntu принято, что все рабочие файлы лежат в /usr/lib, поэтому меняем

```
INSTALL_PATH=/usr/local/rejik3
```

на

```
INSTALL_PATH=/usr/lib/rejik
```

Теперь изменяем

```
SQUID_USER=nobody  
SQUID_GROUP=nogroup
```

на пользователя, от имени которого работает Squid. Это можно посмотреть так:

```
$ cat /etc/squid/squid.conf | grep cache_effective  
cache_effective_user proxy  
cache_effective_group proxy
```

В Debian/Ubuntu это пользователь proxy:proxy

Итак, все должно выглядеть как:

```
SQUID_USER=proxy  
SQUID_GROUP=proxy
```

Все, пора компилировать.

```
$ make  
$ sudo make install
```

Копируем файлы

Для работы rejik требует файлы бан-листов. Если их не будет - rejik упадет.

```
$ sudo cp banlists /usr/lib/rejik  
$ sudo chown -R proxy:proxy /usr/lib/rejik
```

Настраиваем файл конфигурации rejik

Если ставим из пакета - файл конфигурации лежит в /etc/rejik, если самостоятельно - то по указанному пути, в моем случае это /usr/lib/rejik

Создаем файл конфигурации:

```
$ cp redirector.conf.dist redirector.conf
```

Логи работы я хочу хранить вместе с логами Squid - так удобнее.

```
error_log /var/log/squid/redirector.err  
change_log /var/log/squid/redirector.log
```

Создаю пустые файлы для логов и даю на них правильные права:

```
$ cd /var/log/squid  
$ sudo touch redirector.log redirector.err  
$ sudo chown proxy:proxy redirector.log redirector.err
```

Если нужны какие-то еще настройки - делаем их.

Проверяем работу

```
$ cd /usr/lib/rejik/tools/  
$ ./check_redirector
```

Если появилась надпись

```
http://127.0.0.1/ban/porno.html 127.0.0.1/- - GET
```

значит все хорошо работает.

Если не работает - проверяем папки и права на них, как правило это помогает.

Подключаем rejik к Squid

Добавляем в /etc/squid/squid.conf

```
url_rewrite_program /usr/lib/rejik/redirector /usr/lib/rejik/redirector.conf
```

Настраиваем SAMS

SAMS → Администрирование SAMS → Настройка SAMS

Редиректор: Rejik

SAMS → SQUID → Реконфигурирование SQUID → Реконфигурировать

Запускаем сервисы

```
$ sudo service squid start  
$ sudo service sams start
```

И проверяем логи - все ли у нас запустилось и все ли заработало.

[squid](#), [sams](#), [rejik](#), [самс](#), [режик](#), [настройка](#), [прокси](#)

From:

<https://wiki.rtzra.ru/> - RTzRa's hive

Permanent link:

<https://wiki.rtzra.ru/software/squid/squid-corporate>

Last update: **2017/05/09 18:34**

