

Зргоху: Многофункциональный прокси сервер

Введение

Итак рассмотрим основные возможности [Зргоху](#)

- очень «легкий» прокси сервер, главный демон занимает всего ~135 Кбайт
- модульная структура, т.е. вы можете запустить только необходимый вам вид проксирования, например ftp
- кросс-платформенный, запускается под Windows 9.x/2k/XP, Windows 2k3 server, GNU Linux, FreeBSD, NetBSD, OpenBSD, MacOS, Solaris
- поддержка проксирования http/https, ftp, pop3, smtp, icq/aol
- поддержка SOCKSv4, SOCKSv4.5, SOCKSv5
- портмапинг TCP и UDP протоколов
- использование acl (access control list) для разграничения доступа
- возможность подключать внешние файлы для гибкой настройки acl
- использование лимитов на входящий и исходящий потоки
- возможность задавать лимиты на день/неделю/месяц
- поддержка цепочек прокси серверов
- возможность сохранять log-файл в MySQL, Sqlite, Postgresql через ODBC, а также просматривать статистику через web

Как видно из списка возможностей, назвать Зргоху чистым ftp прокси сервером просто нельзя. Так как он обладает большим количеством возможностей. Но для моей задачи понадобилась возможность проксирования ftp, а также поддержка протокола SOCKS.

Итак в нашем распоряжении следующая система

```
# uname -a
Linux gw1.sys-adm.org.ua 2.6.18-164.el5 #1 SMP Thu Sep 3 03:33:56 EDT 2009
i686 i686 i386 GNU/Linux

# cat /etc/redhat-release
CentOS release 5.3 (Final)
```

В системе есть два интерфейса:

- eth0 - смотрит в локальную сеть
- eth1 - смотрит в мир

Т.е. у нас классический роутер. Наша задача установить и настроить ftp/socks прокси сервер, для возможности использования клиентами в различных программах - icq клиенты, ftp клиенты, торент клиенты, skype и т.д. и т.п.

Установка 3proxy

Данная программа не входит в стандартный репозиторий CentOS 5.x, поэтому вам придется либо самому собрать данный пакет или подключить к себе репозиторий EPEL и установить с него 3proxy. Рассмотрим первый вариант, учитывая, что он не представляет особых проблем. И честно говоря мне не понравилась сборка из EPEL по ряду причин (отсутствие поддержки ODBC, кривой startup скрипт, ошибки в sql скрипте)

```
# cd /usr/src/redhat/SRPMS/
# wget http://www.sys-adm.org.ua/srpms/3proxy-0.6-4.src.rpm
# cd /usr/src/redhat/SPECS
# rpmbuild -ba --target=i686 3proxy.spec
Building target platforms: i686
Building for target i686
Executing(%prep): /bin/sh -e /var/tmp/rpm-tmp.18398
+ umask 022
+ cd /usr/src/redhat/BUILD
...
...
...
Wrote: /usr/src/redhat/SRPMS/3proxy-0.6-4.src.rpm
Wrote: /usr/src/redhat/RPMS/i686/3proxy-0.6-4.i686.rpm
Wrote: /usr/src/redhat/RPMS/i686/3proxy-debuginfo-0.6-4.i686.rpm
Executing(%clean): /bin/sh -e /var/tmp/rpm-tmp.66782
+ umask 022
+ cd /usr/src/redhat/BUILD
+ cd 3proxy-0.6
+ rm -rf /var/tmp/3proxy-0.6-4-root-root
+ exit 0
```

После того, как у нас успешно собрался пакет, устанавливаем его в систему

```
# rpm -ivh /usr/src/redhat/RPMS/i686/3proxy-0.6-4.i686.rpm
Preparing... #####
[100%]
   1:3proxy #####
[100%]
```

У данной программы один конфигурационный файл, который по умолчанию располагается в **/etc/3proxy.conf**. Имя и путь к файлу вы можете указать в **/etc/sysconfig/3proxy**.

```
# cat /etc/sysconfig/3proxy
OPTIONS="/etc/3proxy.conf"
```

Настройка 3proxy

```
#
# /etc/3proxy.conf
```

```
#

# Указываем Зроху запускаться как демон. Данный параметр всегда надо указывать
вначале конфигурационного файла
daemon

# Указываем ip адрес нашего DNS сервера. Если ничего не указать, то будет
использоваться системный из /etc/resolv.conf
nserver 127...1

# Размер кеша
nscache 65535

# Устанавливаем таймауты
timeouts 1 5 30 60 180 1800 15 60

# Путь к log-файлу
# log /var/log/Зроху/Зроху.log

# Формат log-файла
# logformat "- +_L%t.%N.%p %E %U %C:%c %R:%r%0 %I %h %T"

# Указываем, DSN для ODBC. Пользователь, пароль и имя БД мы указываем в
/etc/odbc.ini
log &Зроху,Зроху

# Вставляем информацию в таблицу log. Если вам не нужна данная функция,
закомментируйте эти две строки
# И используйте предыдущие две.
logformat "Linsert into log (time, bytesin, bytesout, username, url, host,
port, service) values ('%Y-%m-%d %H:%M:%S', %I, %0, '%U', '%T', '%n', %r,
'%N');"

# Следующие два параметра нужны только, если вы используете текстовый файл для
хранения логов

# Программа, используемая для архивирования log-файлов
# archiver gz /bin/gzip %F

# Указываем какое количество архивированных файлов хранить
(Зроху.log.1.gz-Зроху.log.5.gz)
# rotate 5

# ip адрес нашего внешнего интерфейса, т.е. eth1. Именно с этим адресом будут все
исходящие пакеты с Зроху
external xxx.xxx.xxx.xxx

# ip адрес внутреннего интерфейса, т.е. eth0. Именно этот адрес нам необходимо будет
прописывать в клиентских программах
internal 192.168.1.1
```

```
# Описываем пользователя admin, который будет использоваться для доступа к веб
интерфейсу
# Формат записи "<имя_пользователя>:<тип_шифрования>:<пароль>"
# CR - md5, строку можно получить с помощью команды тусгрут
users "admin:CR:$1$admin$1kgWpnZpUx.vTroWPXPIB0"

# Описываем admin сервис
# Тип аутентификации strong (login/password)
auth strong

# Сбрасываем acl для следующих сервисов
flush

# Разрешаем доступ только пользователю admin и только с ip 192.168.1.100
allow admin 192.168.1.100

# Количество одновременных соединений к сервису
maxconn 3

# Тип сервиса, а также дополнительные параметры для него.
# admin - консоль администрирования
# -p9090 - слушать порт 9090
# -i127.0.0.1 - привязаться к localhost
admin -p9090 -i192.168.1.1

# Описываем http (ftp over http) прокси сервер
# Тип аутентификации, в нашем случае по ip
auth iponly

# Ограничиваем доступ к сервису для нашей подсети
allow * 192.168.1./24 * *

# Количество одновременных соединений к сервису
maxconn 150

# Тип сервиса, а также дополнительные параметры для него.
# proxy - http прокси сервер
# -p8080 - слушать порт 8080
# -a - прятать информацию о клиенте (использовать анонимный режим)
proxy -p8080 -a

# Описываем "чистый" ftp прокси сервер
# Тип аутентификации, в нашем случае по ip
auth iponly

# Ограничиваем доступ к сервису для нашей подсети
allow * 192.168.1./24 * *

# Количество одновременных соединений к сервису
maxconn 150
```

```
# Тип сервиса, а также дополнительные параметры для него.
# ftppr - ftp прокси сервер, не путайте с ftp over http
# -p2121 слушать порт 2121
ftppr -p2121

# Описываем socks прокси сервер
# Тип аутентификации, в нашем случае по ip
auth iponly

# Ограничиваем доступ к сервису для нашей подсети
allow * 192.168.1./24 * *

# Количество одновременных соединений к сервису
maxconn 150

# Тип сервиса, а также дополнительные параметры для него.
# socks - socks прокси сервер
# -p8888 слушать порт 8888
socks -p8888

# Указываем путь к pid-файлу, позволяет управлять Зроху с помощью сигналов (HUP,
etc)
pidfile /var/run/Зроху.pid

# Пользователь и группа, от которого запускать Зроху (nobody:nobody)
setuid 99
setgid 99
```

Генерируем пароль для пользователя admin

```
# mycrypt admin admin
CR:$1$admin$1kgWpnZpUx.vTroWPXPIB0
```

Для того, чтобы получить полное описание всех параметров выполните следующую команду

```
# man Зроху.cfg
```

Запускаем Зроху

```
# service Зроху start
Starting Зроху: [ OK ]
```

Проверяем, что все наши сервисы запустились и слушают на необходимых интерфейсах

```
# netstat -an | grep 2121
tcp        0      0 192.168.1.1:2121    0.0.0.0:*
LISTEN

# netstat -an | grep 8888
```

```
tcp      0      0 192.168.1.1:8888      0.0.0.0:*
LISTEN

# netstat -an | grep 8080
tcp      0      0 192.168.1.1:8080      0.0.0.0:*
LISTEN

# netstat -an | grep 9090
tcp      0      0 192.168.1.1:9090      0.0.0.0:*
LISTEN
```

Настройка MySQL + ODBC

Если вы сохраняете лог в обычный текстовый файл, можете пропустить эту главу и перейти к тестированию. Итак, мы будем сохранять всю информацию в MySQL. Для этого необходимо установить соответствующий конектор для ODBC.

```
# yum install mysql-connector-odbc
```

После этого, описываем DSN (Database Source Name)

```
#
#/etc/odbc.ini
#

[3proxy]
Description      = MySQL ODBC Driver
Driver           = MySQL
Socket          = /var/lib/mysql/mysql.sock
Server          = localhost
User            = 3proxy
Password        = proxyAdmin
Database        = 3proxy
Option          = 3
```

А также указываем какую библиотеку использовать для связи с MySQL

```
#
#/etc/odbcinst.ini
#

[MySQL]
Description      = MySQL ODBC MyODBC Driver
Driver          = /usr/lib/libmyodbc3.so
FileUsage       = 1
```

После этого нам необходимо создать соответствующую БД. Ниже привожу соответствующий sql скрипт

```
#
# DATABASE: 3proxy
#

CREATE TABLE `log` (
  `time` datetime NOT NULL DEFAULT '0000-00-00 00:00:00',
  `bytesin` INT(11) NOT NULL DEFAULT '0',
  `bytesout` INT(11) NOT NULL DEFAULT '0',
  `username` VARCHAR(20) NOT NULL DEFAULT '',
  `service` VARCHAR(7) NOT NULL DEFAULT '',
  `host` VARCHAR(100) NOT NULL DEFAULT '',
  `port` INT(11) NOT NULL DEFAULT '0',
  `url` VARCHAR(255) NOT NULL DEFAULT ''
) TYPE=MyISAM;

CREATE TABLE `services` (
  `startport` INT(11) NOT NULL DEFAULT '0',
  `endport` INT(11) NOT NULL DEFAULT '0',
  `service` VARCHAR(100) NOT NULL DEFAULT '',
  `description` VARCHAR(100) NOT NULL DEFAULT ''
) TYPE=MyISAM;

CREATE TABLE `timelimit` (
  `datefrom` datetime NOT NULL DEFAULT '0000-00-00 00:00:00',
  `dateto` datetime NOT NULL DEFAULT '0000-00-00 00:00:00'
) TYPE=MyISAM;

INSERT INTO services VALUES (80, 80, 'http', 'Access to Web Server');
INSERT INTO services VALUES (443, 443, 'https', 'Secure Access to Web
Server');

INSERT INTO services VALUES (3128, 3128, 'squid', 'Access to Web server via
external Proxy');
INSERT INTO services VALUES (1080, 1080, 'socks', 'Access to external SOCKS
server');
INSERT INTO services VALUES (5190, 5190, 'ICQ', 'Access to ICQ');
INSERT INTO services VALUES (6666, 6668, 'IRC', 'Access to IRC');

INSERT INTO services VALUES (119, 119, 'NTP', 'Access to news server');
INSERT INTO services VALUES (25, 25, 'smtp', 'Sent Mail');

INSERT INTO services VALUES (, , 'POP3', 'Received Mail');
INSERT INTO services VALUES (, , 'TCPPM', 'Access to external server via TCP
mapping');
INSERT INTO services VALUES (, , 'UDPPM', 'Access to external server via UDP
mapping');
INSERT INTO services VALUES (, , 'PROXY', 'Access to external server via
Proxy');
INSERT INTO services VALUES (, , 'SOCKS4', 'Access to external server via
Socks v4');
INSERT INTO services VALUES (, , 'SOCKS5', 'Access to external server via
```

```
Socks v5');  
INSERT INTO services VALUES (, , 'DNS', 'Name resolution');  
INSERT INTO services VALUES (, , 'undefined', 'Unknown');
```

Теперь нам необходимо создать БД и пользователя в MySQL

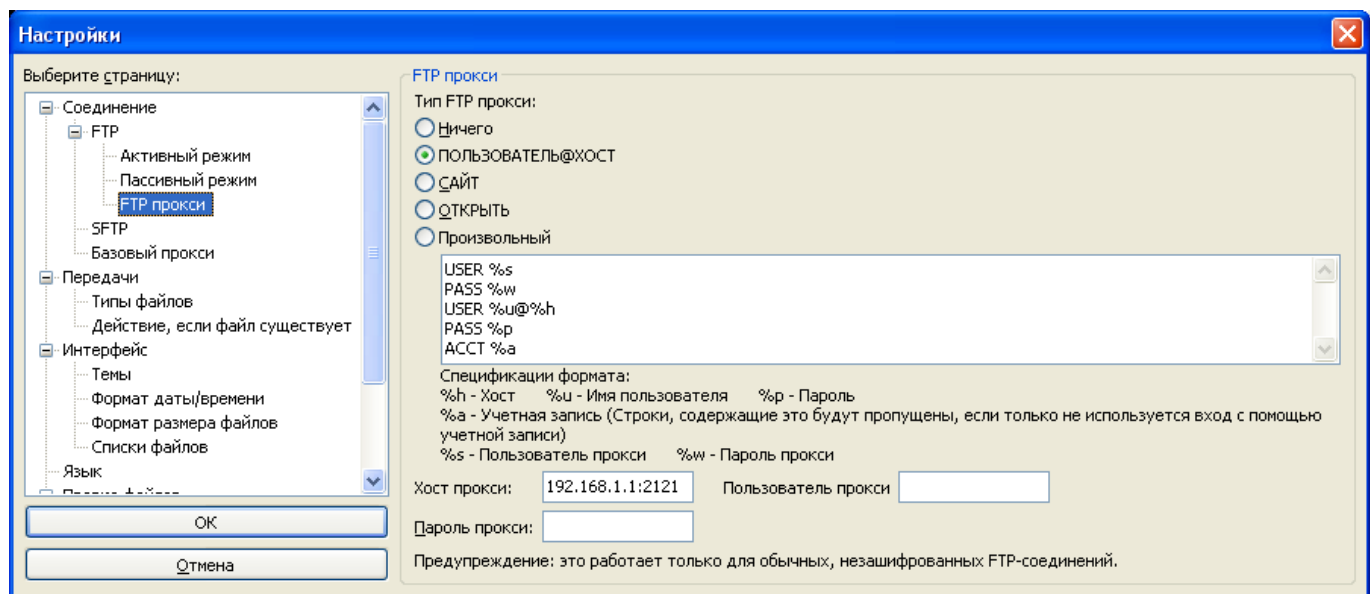
```
mysql> create database 3proxy;  
Query OK, 1 row affected (0.06 sec)  
  
mysql> grant all privileges on 3proxy.* to 3proxy@'%' identified by  
'triproxyAdmin';  
Query OK, 0 rows affected (0.02 sec)  
  
mysql> flush privileges;  
Query OK, 0 rows affected (0.00 sec)  
  
mysql> quit  
Bye
```

После этого заливаем сам скрипт

```
# mysql -u 3proxy -p 3proxy < 3proxy.sql  
Enter password:*****
```

Тестирование

Ну вот собственно и все, позади уже самая сложная часть. Теперь осталось только проверить работу нашего прокси сервера. Для этого воспользуемся клиентом [FileZilla](#).

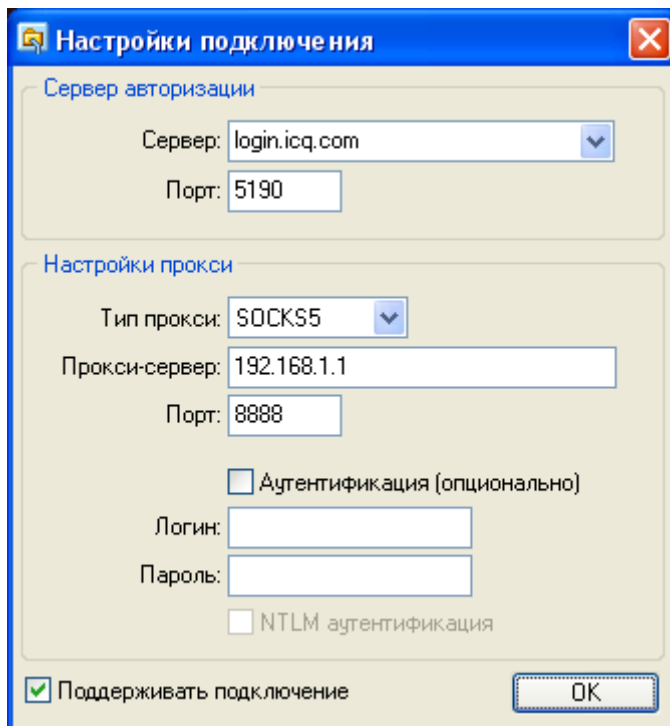


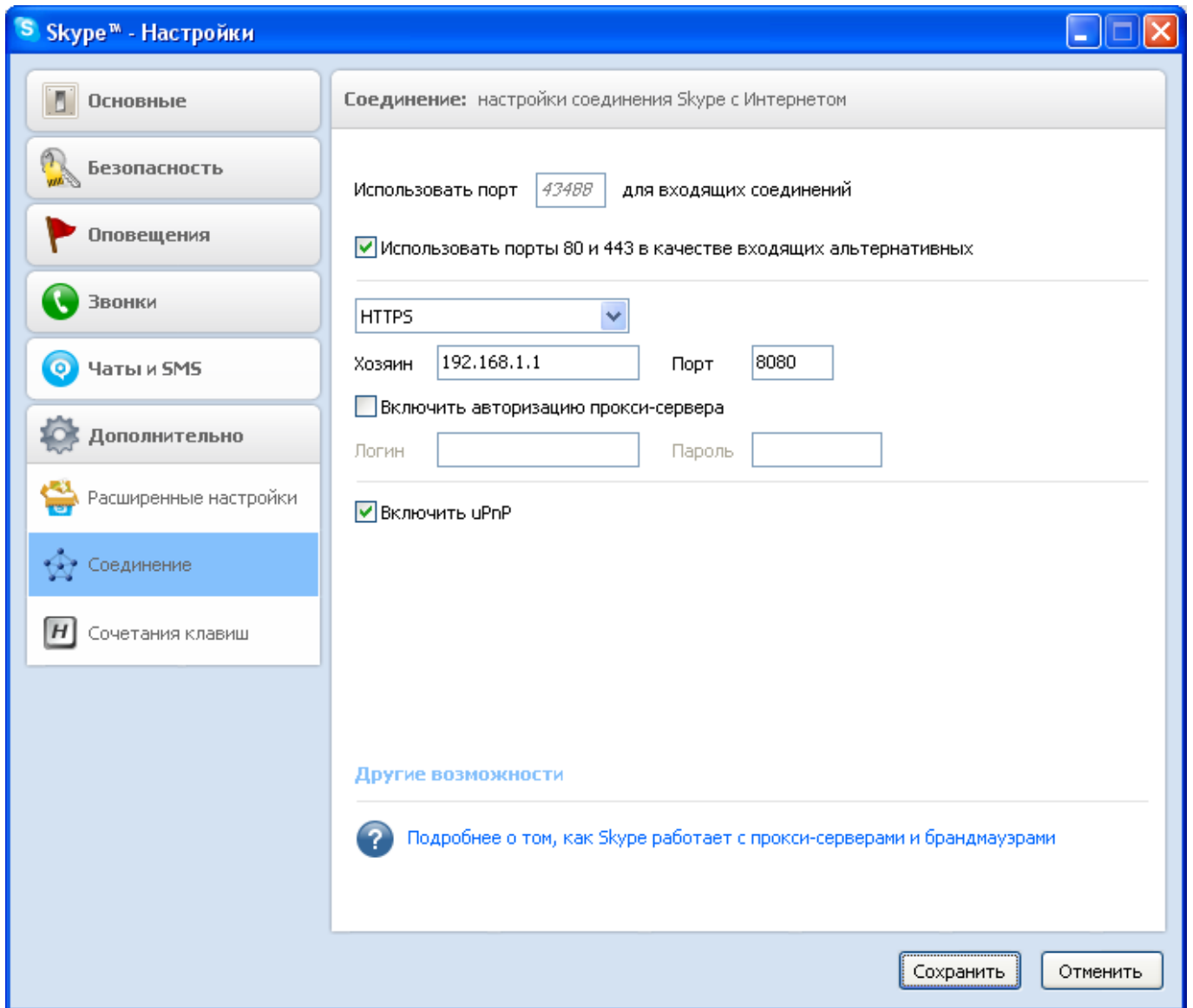
После применения настроек, попробуем закачать любой файл с ftp сервера. И посмотрим логи в MySQL.


```
> select * from log where service='FTPPR' and host='test.sys-  
adm.org.ua';  
+-----+-----+-----+-----+-----+-----+  
-----+-----+-----+-----+-----+  
| time          | bytesin | bytesout | username | service | host  
| port | url          |          |          |          |  
+-----+-----+-----+-----+-----+-----+  
-----+-----+-----+-----+-----+  
| 2009-10-05 19:47:42 | 77 | 37 | - | FTPPR | test.sys-  
adm.org.ua | 21 | alex_hha@test.sys-  
adm.org.ua |  
| 2009-10-05 19:47:43 | 719 | 51 | - | FTPPR | test.sys-  
adm.org.ua | 15035 | LIST |  
| 2009-10-05 19:47:50 | 77 | 37 | - | FTPPR | test.sys-  
adm.org.ua | 21 | alex_hha@test.sys-  
adm.org.ua |  
| 2009-10-05 19:47:50 | 63 | 21 | - | FTPPR | test.sys-  
adm.org.ua | 21 | CWD / |  
| 2009-10-05 19:49:40 | 5921152 | 42 | - | FTPPR | test.sys-  
adm.org.ua | 61439 | RETR dokuwiki.tar.bz2 |  
| 2009-10-05 19:50:43 | 20 | 23 | - | FTPPR | test.sys-  
adm.org.ua | 15035 | |  
+-----+-----+-----+-----+-----+-----+  
-----+-----+-----+-----+-----+  
6 rows in set (0.00 sec)
```

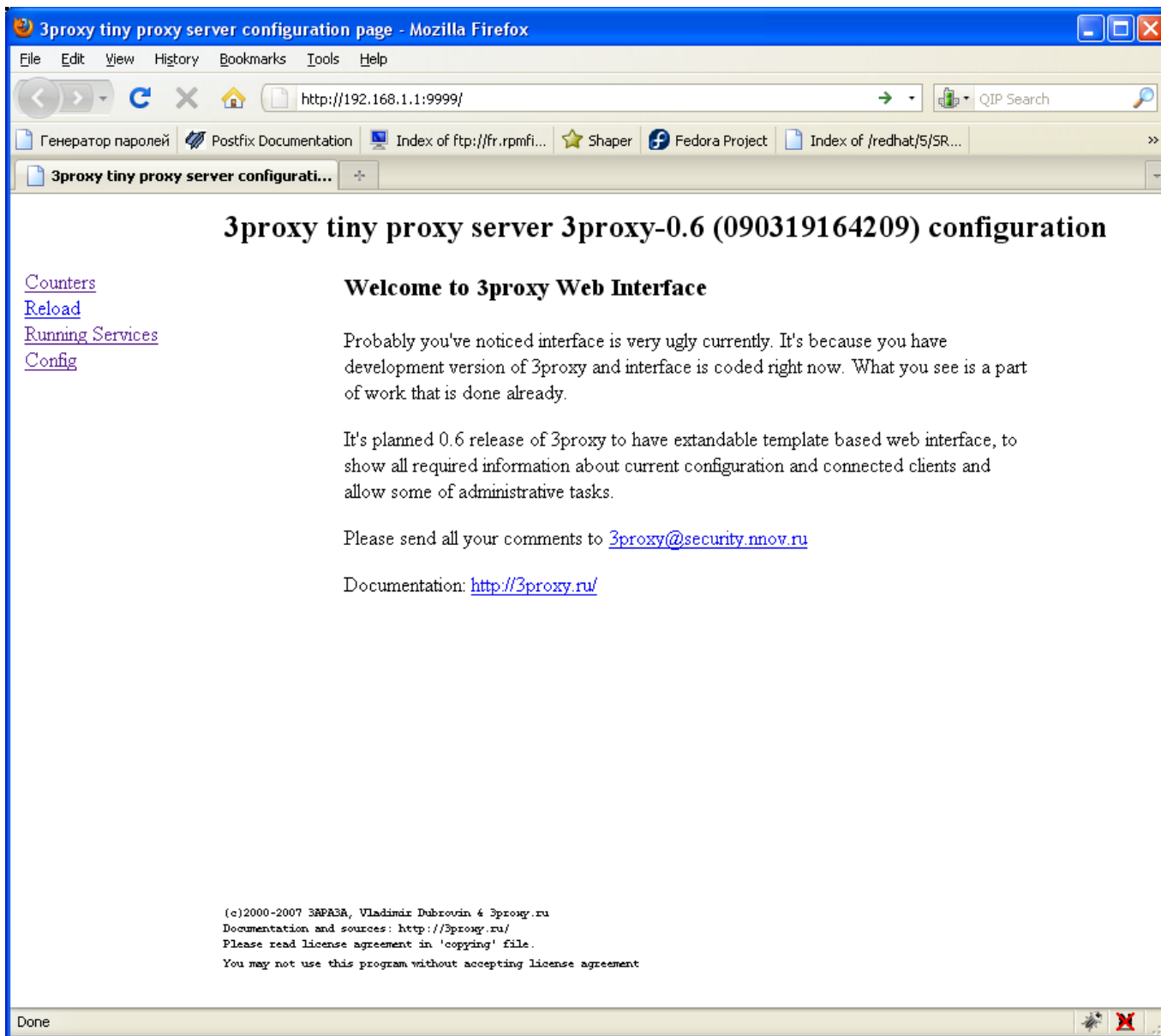
Как видно из логов мы скачали один файл dokuwiki.tar.bz2 размером 5921152 байт. Точно также мы можем использовать ftp over http или socks сервер в настройках FileZilla.

Ниже привожу примеры настроек для qip и skype соответственно.





И единственно что нам осталось проверить - это работа web интерфейса. Для этого открываем в проводнике следующий адрес <http://192.168.1.1:9999/>. На экране должна появиться примерно такая страница



К сожалению на данный момент функционал и дизайн оставляет желать лучшего, возможно в следующих версиях данный сервис будет доведен до ума.

На этом настройку Зроху можно считать завершенной. Для более подробной информацией по настройке обращайтесь на [официальный сайт Зроху](#)

From:
<http://sys-adm.org.ua/> - wiki.sys-adm.org.ua

Permanent link:
<http://sys-adm.org.ua/net/3proxy>

Last update: **2009/10/06 19:39**

