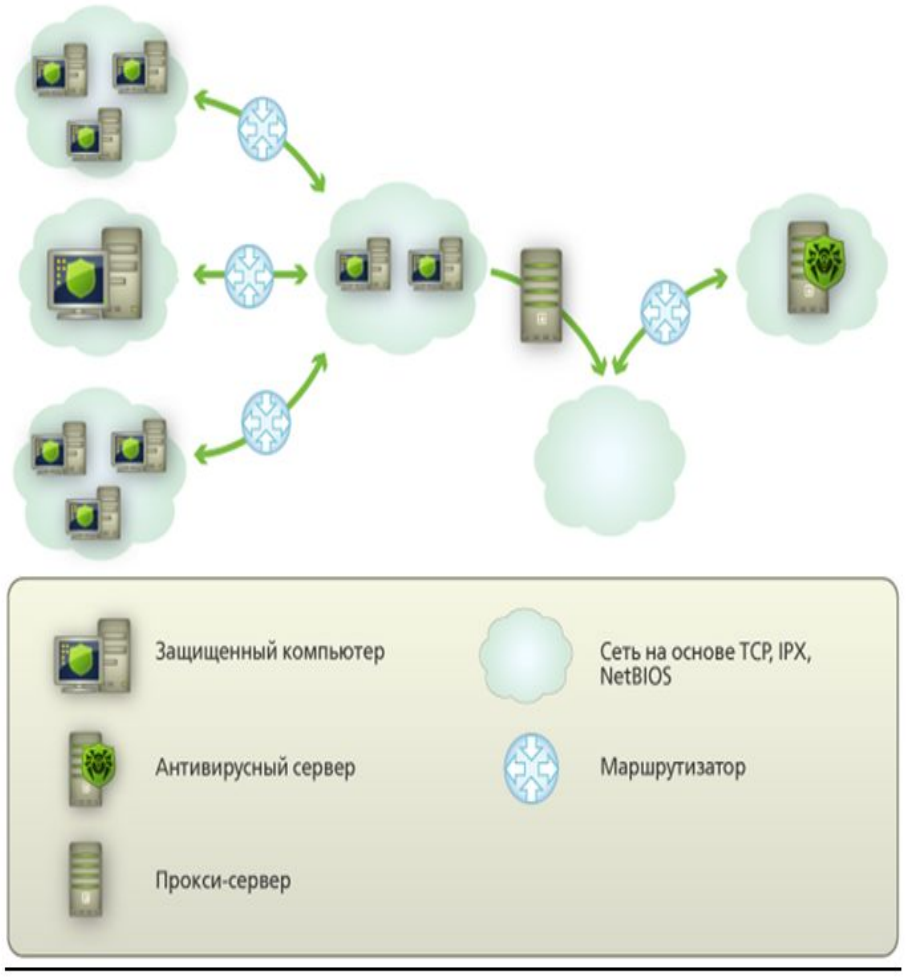
Возможности прокси-сервера SQUID

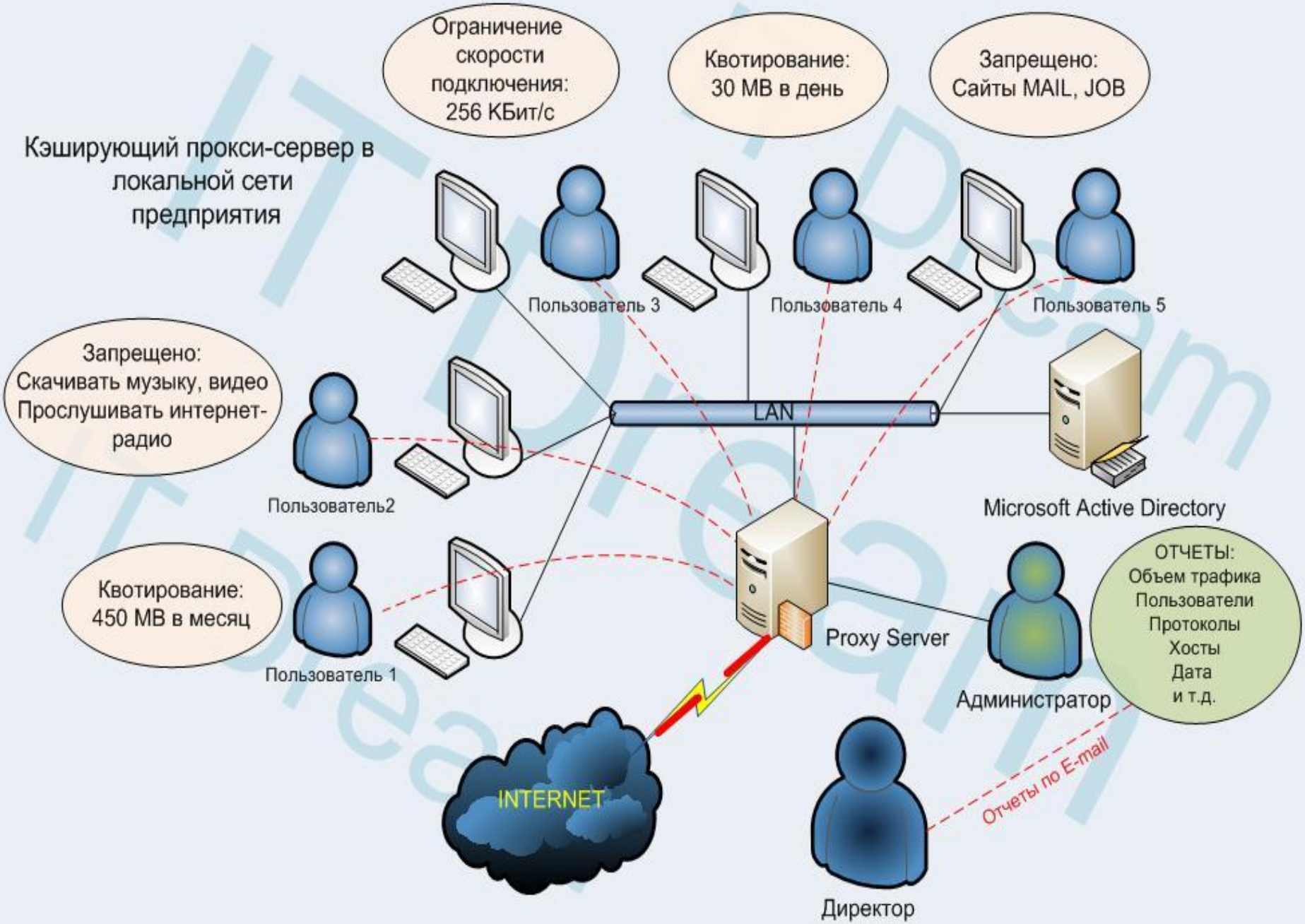


Прокси-сервер (от англ. proxy — «***представитель, уполномоченный***») — служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, e-mail), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша (в случаях, если прокси-сервер имеет свой кэш). В некоторых случаях запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях. Также прокси-сервер позволяет защищать клиентский компьютер от некоторых сетевых атак.

Использование прокси-серверов

Чаще всего прокси-серверы применяются для следующих целей:

1. Обеспечение доступа с компьютеров локальной сети в Интернет.
2. Кэширование данных: если часто происходят обращения к одним и тем же внешним ресурсам, то можно держать их копию на прокси-сервере и выдавать по запросу, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентом запрошенной информации.
3. Сжатие данных: прокси-сервер загружает информацию из Интернета и передаёт информацию конечному пользователю в сжатом виде. Такие прокси-серверы используются в основном с целью экономии внешнего трафика.
4. Защита локальной сети от внешнего доступа: например, можно настроить прокси-сервер так, что локальные компьютеры будут обращаться к внешним ресурсам только через него, а внешние компьютеры не смогут обращаться к локальным вообще (они «видят» только прокси-сервер).
5. Ограничение доступа из локальной сети к внешней: например, можно запретить доступ к определённым веб-сайтам, ограничить использование интернета каким-то локальным пользователям, устанавливать квоты на трафик или полосу пропускания, фильтровать рекламу и вирусы.
6. Анонимизация доступа к различным ресурсам. Прокси-сервер может скрывать сведения об источнике запроса или пользователе. В таком случае целевой сервер видит лишь информацию о прокси-сервере, например, IP-адрес, но не имеет возможности определить истинный источник запроса. Существуют также искажающие прокси-серверы, которые передают целевому серверу ложную информацию об истинном пользователе


Ограничение скорости подключения: 256 КБит/с
Квотирование: 30 MB в день
Запрещено: Сайты MAIL, JOB
Кэширующий прокси-сервер в локальной сети предприятия
Пользователь 3
Пользователь 4
Пользователь 5
Запрещено: Скачивать музыку, видео Прослушивать интернет-радио
LAN
Пользователь2
Microsoft Active Directory
Квотирование: 450 MB в месяц
Пользователь 1
Proxy Server
ОТЧЕТЫ: Объем трафика Пользователи Протоколы Хосты Дата и т.д.
Администратор
INTERNET
Директор
Отчеты по E-mail

Ключевыми типами прокси-серверов, являются:

- пересылающие прокси-серверы (forward proxies);
- прозрачные прокси-серверы (transparent proxies);
- кэширующие прокси-серверы (caching proxies);
- прокси-сервер обеспечения безопасности (security proxies);
- обратные прокси-серверы (reverse proxies).

Пересылающий прокси-сервер является прокси-сервером, который помогает пользователям из одной зоны безопасности выполнять запросы контента из "следующей" зоны, следуя направлению, которое обычно (но не обязательно) является исходящим (это значит, что клиент находится внутри, а сервер где-то в открытом Интернете).

Кэширующие прокси-серверы, как указано в их названии, являются прокси-серверами, которые сконфигурированы на повторное использование кэшированных образов контента, когда это доступно и возможно

Прокси-сервер обеспечения безопасности В качестве необходимой для простых прокси-серверов функциональности прокси-серверы могут быть сконфигурированы для приведения в исполнение политик безопасности. Такие прокси-серверы обеспечения безопасности могут обрабатывать (либо выступать в качестве посредников при обработке) запросы аутентификации и авторизации. В этих случаях аутентификация пользователя клиента и авторизация клиента для доступа к определенному контенту контролируется самим прокси-сервером. Далее мандат безопасности посылается от прокси-сервера к конечным серверам с запросом, а конечный сервер должен быть сконфигурирован на оказание доверия предоставляемому прокси-серверу мандату

Обратные прокси-серверы имеют много общего с пересылающими прокси-серверами: фактически одни и те же продукты могут быть сконфигурированы одним или другим образом либо двумя сразу.

Прокси-сервер Squid

Squid — программный пакет, реализующий функцию ***кэширующего прокси-сервера*** для протоколов HTTP, FTP, Gopher и (в случае соответствующих настроек) HTTPS. Разработан сообществом как программа с открытым исходным кодом (**распространяется в соответствии с GNU GPL**). Все запросы выполняет как один неблокируемый процесс ввода/вывода. Используется в UNIX-like системах и в ОС семейства Windows. Имеет возможность взаимодействия с Active Directory Windows Server путём аутентификации через LDAP, что позволяет использовать разграничения доступа к интернет ресурсам пользователей, которые имеют учётные записи на Windows Server, также позволяет организовать «нарезку» интернет трафика для различных пользователей.

В сочетании с некоторыми межсетевыми экранами и маршрутизаторами Squid может работать в режиме ***прозрачного*** прокси-сервера. В этом режиме маршрутизатор вместо того, чтобы сразу пересылать http-запросы пользователя http-серверу в интернете, перенаправляет их прокси-серверу, который может работать как на отдельном хосте, так и на самом маршрутизаторе. Прокси-сервер обрабатывает запрос (с возможной отдачей содержимого из кэша), это содержимое направляется к запросившему пользователю, для которого оно выглядит как «ответ» сервера, к которому адресовался запрос. Таким образом, пользователь может даже не знать, что все запросы и ответы прошли через прокси-сервер.

Сервер **Squid** развивается в течение уже многих лет. Обеспечивает совместимость с большинством важнейших протоколов Интернета, а также с операционными системами:
GNU/Linux
FreeBSD
OpenBSD
NetBSD
BSDI
Mac OS X
OSF и Digital Unix
IRIX
SunOS/Solaris
NeXTStep
SCO Unix
AIX
HP-UX
Microsoft Windows

Редиректоры

Squid имеет возможность переписывать запрашиваемые URL.
Squid может быть сконфигурирован так, чтобы пропускать входящие URL через процесс редиректора выполняемого как внешний процесс (подобно dnsserver), который возвращает новый URL или пустую строку, обозначающую отсутствие изменений.
Редиректор – не является стандартной частью пакета **Squid.**
Редиректор предоставляет администратору контроль за передвижениями пользователей. Использование редиректора в сочетании с прозрачным проксированием дает простой, но эффективный контроль, над доступом к порно.

Редиректор SAMS

Написан специально для SAMS, напрямую использует информацию, содержащуюся в базе данных. Позволяет включить различное перенапраление запросов для пользователей (регулируется шаблонами пользователей).
Редиректор SAMS обеспечивает:

- ограничение доступа пользователей к SQUID ;
- контроль времени доступа пользователей к SQUID;
- ограничение доступа пользователей к запрещенным ресурсам (или доступ пользователей только к разрешенным ресурсам);
- перенаправление запросов пользователей к баннерам, счетчикам и т.п.

Редиректор SquidGuard

Мощный редиректор с большими возможностями. В состав редиректора входят списки баннерных, порно и пр. доменов.
SAMS добавляет в файл конфигурации SquidGuard Squidguard.conf настройки на списки запрещенных доменов и перенаправления доступа SAMS. Настройки на списки, идущие с SquidGuard не изменяются и не удаляются.
При использовании редиректора SquidGuard в файл Squid.conf заносятся acl, разрешающие доступ всех пользователей к **SQUID**. Ограничение доступа пользователей организовано средствами редиректора.

Squid поддерживает несколько видов идентификации пользователей:

по IP-адресу (или доменному имени узла);

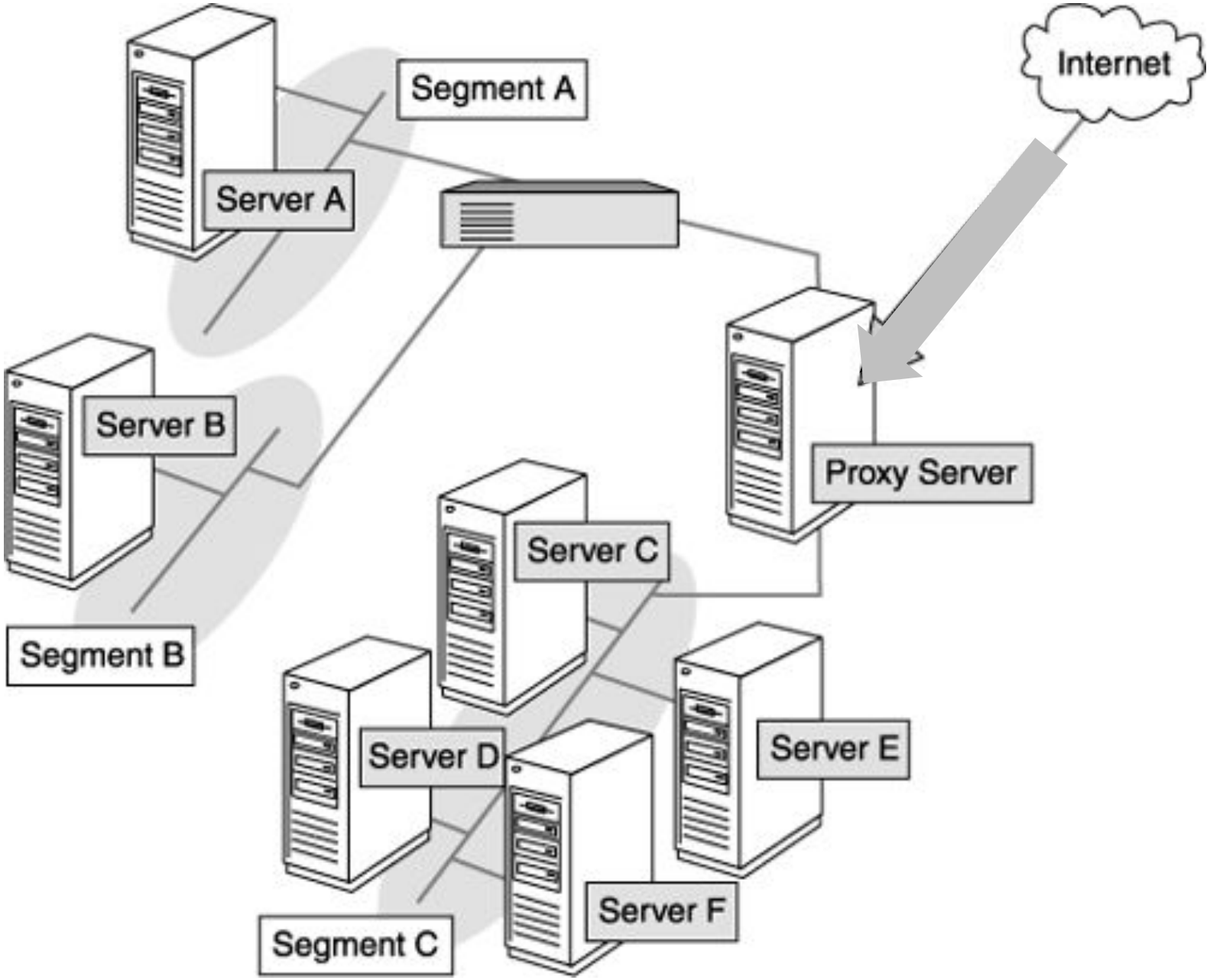
по переданным реквизитам (логин/пароль);

По идентификатору пользовательского агента (браузера);

Для идентификации по логину/паролю возможно использовать:
обычные логин/пароль;

NTLM-авторизацию;

внешние программы авторизации (определяющие формат авторизации).


Internet
Segment A
Server A
Server B
Segment B
Proxy Server
Server C
Server D
Server E
Server F
Segment C

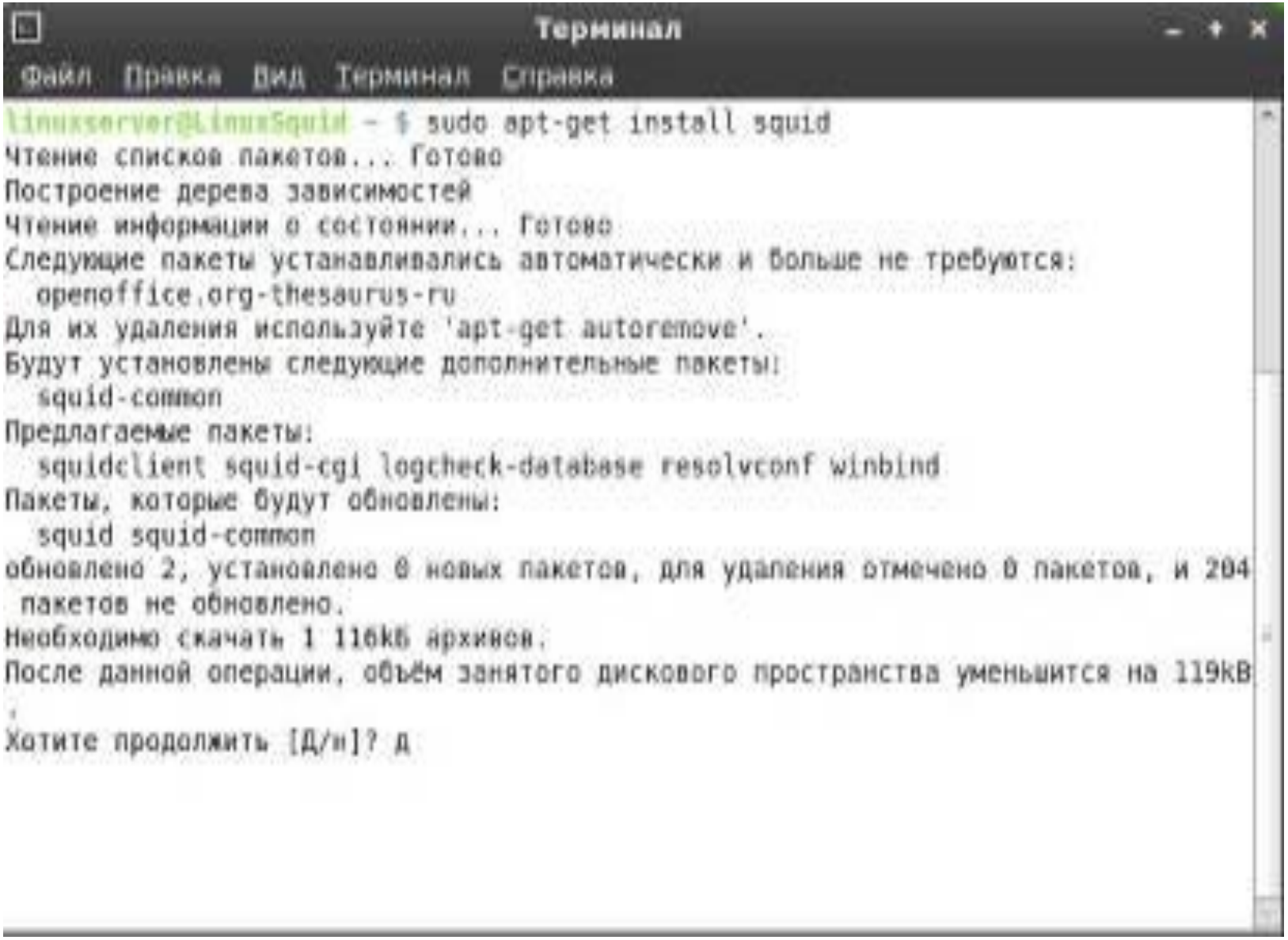
В ОС Linux прокси-сервер **Squid** входит в состав группы пакетов **Web Server**. Его также можно установить отдельно из пакета **Squid**.
После установки пакета **Squid** в системе будут присутствовать следующие конфигурационные и бинарные файлы, которые используются прокси-сервером **Squid**:
/etc/init.d/squid - init-скрипт запуска прокси-сервера Squid.
/etc/squid - каталог, в котором содержатся все конфигурационный файлы прокси-сервера **Squid.**
/etc/sysconfig/squid - файл, в котором содержатся опции запуска прокси-сервера Squid при помощи init-скрипта.
/usr/share/doc/squid - **<версия>** - каталог с документацией в формате HTML.
/usr/lib/squid/ - каталог, содержащий специальные программы (helpers) используемые прокси-сервером Squid для аутентификации пользователей.
/usr/sbin/squid - демон прокси-сервера Squid.
/usr/share/squid - каталог, содержащий шаблоны сообщений об ошибках.
/var/log/squid - каталог, в который выполняется журналирование системных событий прокси-сервера Squid.
/var/spool/squid - каталог, используемый для хранения кэшированных данных

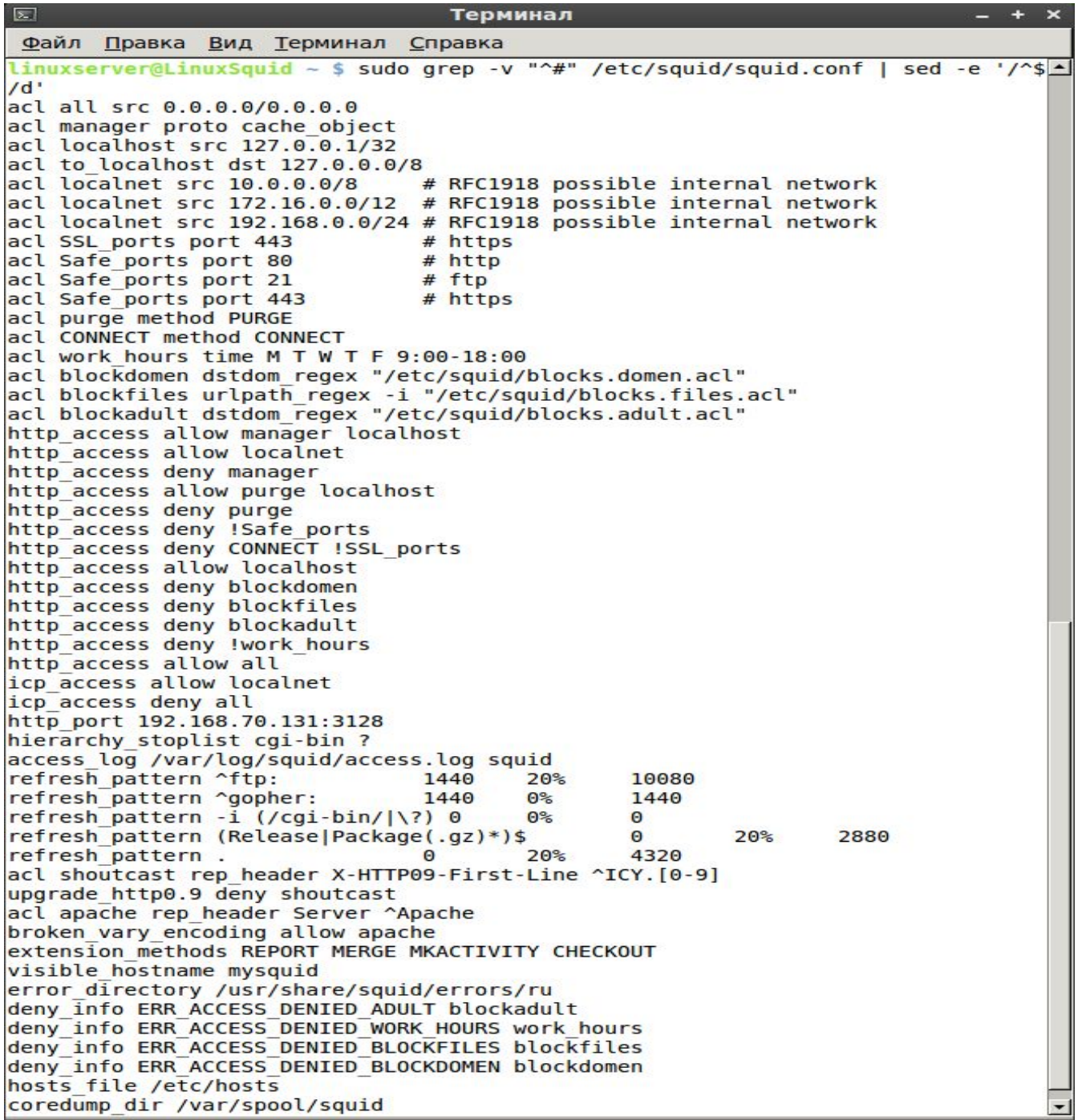
Общая последовательность действий для развертывания прокси-сервера **Squid** следующая:

1. Установить пакет squid и все его зависимости;
2. Настроить конфигурационный файл squid.conf;
3. Создать базу кэшированных данных;
4. Запустить демон **squid** и настроить его автозапуск.

Конфигурирование прокси-сервера Squid в основном сводится к настройке его конфигурационного файла **/etc/squid/squid.conf**, который содержит более 4000 строк, включая комментарии. На каждой не закомментированной строке указывается определенная директива, имеющая несколько параметров. Остановимся на некоторых из директив. Для того чтобы указать порт, который будет обрабатывать клиентские запросы, используется директива **http_port <номер_порта**, где необходимо указать номер порта выше 1024, поскольку демон squid запускается от не привилегированного пользователя. Директива **hierarchy_stoplist** определяет условия, при которых запросы будет направляться напрямую веб серверу, минуя кэш. Типовая директива **hierarchy_stoplist** имеет вид:

hierarchy_stoplist cgi-bin ?
acl query urlpath_regex cgi-bin \?
cache deny query .


Терминал
Файл Правка Вид Терминал Справка
linuxserver@LinuxSquid ~ $ sudo apt-get install squid
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Следующие пакеты устанавливались автоматически и больше не требуются:
openoffice.org-thesaurus-ru
Для их удаления используйте 'apt-get autoremove'.
Будут установлены следующие дополнительные пакеты:
squid-common
Предлагаемые пакеты:
squidclient squid-cgi logcheck-database resolvconf winbind
Пакеты, которые будут обновлены:
squid squid-common
обновлено 2, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 204
пакетов не обновлено.
Необходимо скачать 1 116kB архивов.
После данной операции, объём занятого дискового пространства уменьшится на 119kB
.
Хотите продолжить [Д/н]? д


Терминал
Файл Правка Вид Терминал Справка
linuxserver@LinuxSquid ~ $ sudo grep -v "^#" /etc/squid/squid.conf | sed -e '/^$/d'
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8
acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
acl localnet src 192.168.0.0/24 # RFC1918 possible internal network
acl SSL_ports port 443 # https
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl purge method PURGE
acl CONNECT method CONNECT
acl work_hours time M T W T F 9:00-18:00
acl blockdomen dstdom_regex "/etc/squid/blocks.domen.acl"
acl blockfiles urlpath_regex -i "/etc/squid/blocks.files.acl"
acl blockadult dstdom_regex "/etc/squid/blocks.adult.acl"
http_access allow manager localhost
http_access allow localnet
http_access deny manager
http_access allow purge localhost
http_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access deny blockdomen
http_access deny blockfiles
http_access deny blockadult
http_access deny !work_hours
http_access allow all
icp_access allow localnet
icp_access deny all
http_port 192.168.70.131:3128
hierarchy_stoplist cgi-bin ?
access_log /var/log/squid/access.log squid
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
refresh_pattern (Release|Package(.gz)*)$ 0 20% 2880
refresh_pattern . 0 20% 4320
acl shoutcast rep_header X-HTTP09-First-Line ^ICY.[0-9]
upgrade_http0.9 deny shoutcast
acl apache rep_header Server ^Apache
broken_vary_encoding allow apache
extension_methods REPORT MERGE MKACTIVITY CHECKOUT
visible_hostname mysquid
error_directory /usr/share/squid/errors/ru
deny_info ERR_ACCESS_DENIED_ADULT blockadult
deny_info ERR_ACCESS_DENIED_WORK_HOURS work_hours
deny_info ERR_ACCESS_DENIED_BLOCKFILES blockfiles
deny_info ERR_ACCESS_DENIED_BLOCKDOMEN blockdomen
hosts_file /etc/hosts
coredump_dir /var/spool/squid

Значения некоторых параметров конфигурации

Создание acl (Access Control List) с именем localhost для 127.0.0.1/32 ip-адресов:
acl localhost src 127.0.0.1/32
Создание acl (Access Control List) с именем to_localhost для 127.0.0.0/8 ip-адресов:
acl to_localhost dst 127.0.0.0/8
Указание сети, с которой можно присоединяться без авторизации:
acl localnet src 10.0.0.0/8
acl localnet src 172.16.0.0/12
acl localnet src 192.168.0.0/24
Описание портов:
acl SSL_ports port 443 – https порт
acl Safe_ports port 80 – http порт
acl Safe_ports port 21 – ftp порт
acl Safe_ports port 443 – https порт
Включение поддержки проброски соединения с помощью команды протокола CONNECT:
acl CONNECT method CONNECT
Описывает рабочее время с понедельника по пятницу:
acl work_hours time M T W T F 9:00-18:00
Описывает путь к файлу со списком доменов:
acl blockdomen dstdom_regex "/etc/squid/blocks.domen.acl" – в этом файде содержатся список доменов.
Описывает путь к файлу со списком файлов:
acl blockfiles urlpath_regex -i "/etc/squid/blocks.files.acl" – в этом файде содержатся данные о расширениях.
Описывает путь к файлу со списком значений адресса:
acl blockadult dstdom_regex "/etc/squid/blocks.adult.acl" – в этом файде содержатся регулярные выражения для интернет ресурсов.
Пропуск (allow) **или запрет** (deny) **для указанных портов**. Порядок http_acces важен, идет сверху вниз:
http_access allow manager localhost
http_access allow localnet
http_access deny manager

Разрешение или запрет доступа к ICP порту, основанное на заявленных списках доступа:
icp_access allow localnet
icp_access deny all
Адреса сокетов, на которых Squid будет ожидать запросы HTTP клиентов:
http_port 192.168.70.131:3128
В этих файлах размещаются журналы запросов клиентов. На каждый HTTP и ICP запрос отводится одна строка:
access_log /var/log/squid/access.log squid
Этот тэг определяет имя хоста(hostname), которое будет отображатся в сообщениях об ошибках, и т.д. в данном случае используется имя mysquid:
visible_hostname mysquid
Директория ошибок:
error_directory /usr/share/squid/errors/ru
Выводит ошибки для определенных ACL:
deny_info ERR_ACCESS_DENIED_ADULT blockadult
deny_info ERR_ACCESS_DENIED_WORK_HOURS work_hours
deny_info ERR_ACCESS_DENIED_BLOCKFILES blockfiles
deny_info ERR_ACCESS_DENIED_BLOCKDOMEN blockdomen
Расположение локальной базы данных связей IP адрес-имя узла:
hosts_file /etc/hosts
По умолчанию **Squid** оставляет файлы ядра в папке, из которой он был запущен:
coredump_dir /var/spool/squid
Формат **Squid.conf** стандартен для Unix, каждая запись состоит из строк вида: параметр значение.
Возможно использование переменных. Строки начинающиеся со знака решетки **(#)** являются комментариями. Для удобства настройки, все параметры разбиты по секциям. Такое разбиение чисто условно и можно прописывать свои параметры в любое место файла, лишь бы было понятно. Возможно подключение внешнего файла с настройками при помощи include. Единственное о чем следует помнить – установки применяются в порядке очередности. После установки в /usr/share/doc/Squid можно найти документацию и примеры конфигурационных файлов.

2.2 Запуск прокси-сервера Squid

Для запуска прокси-сервера Squid используется команда (Рис. 5):
$ sudo /etc/init.d/Squid start

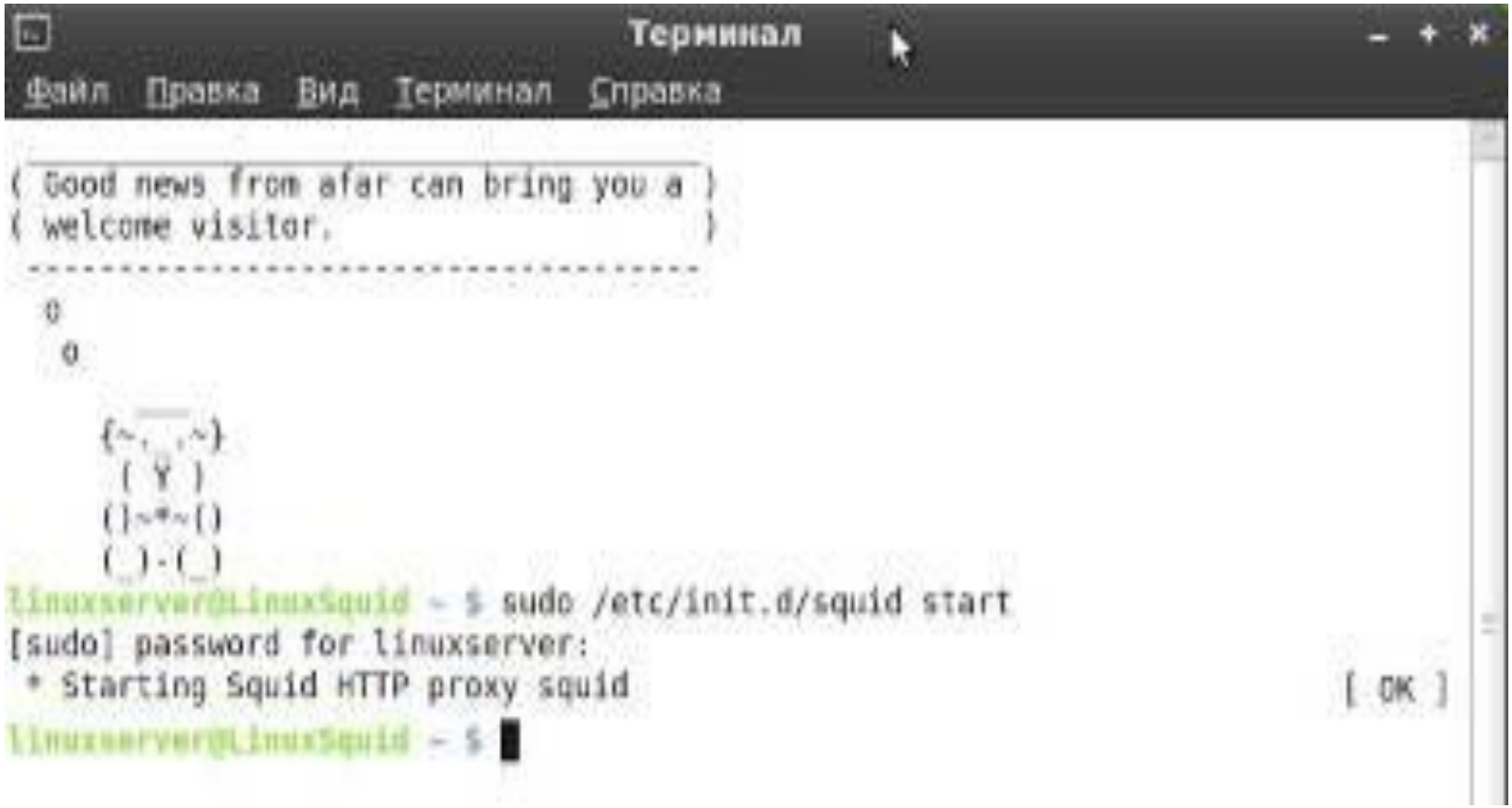
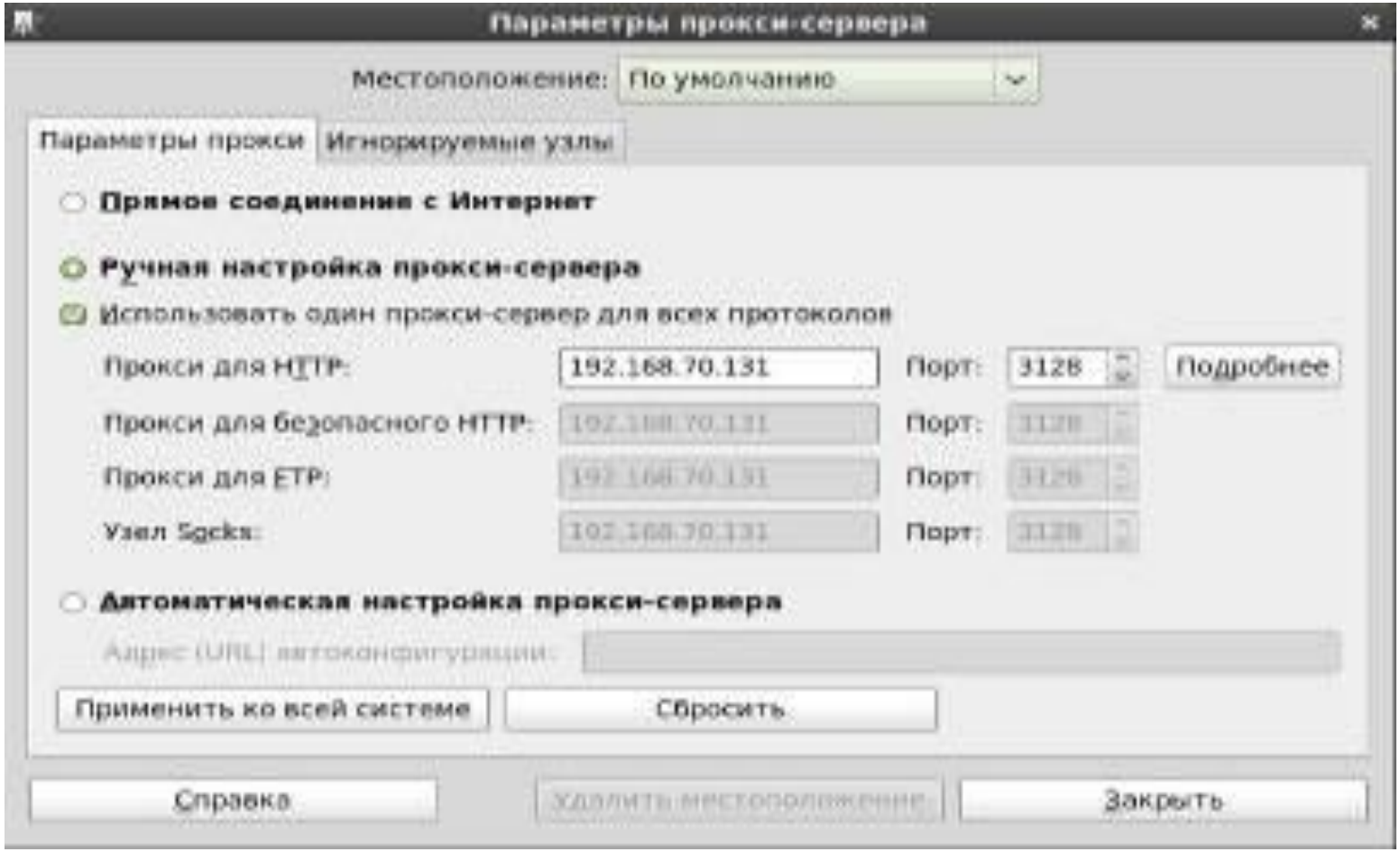


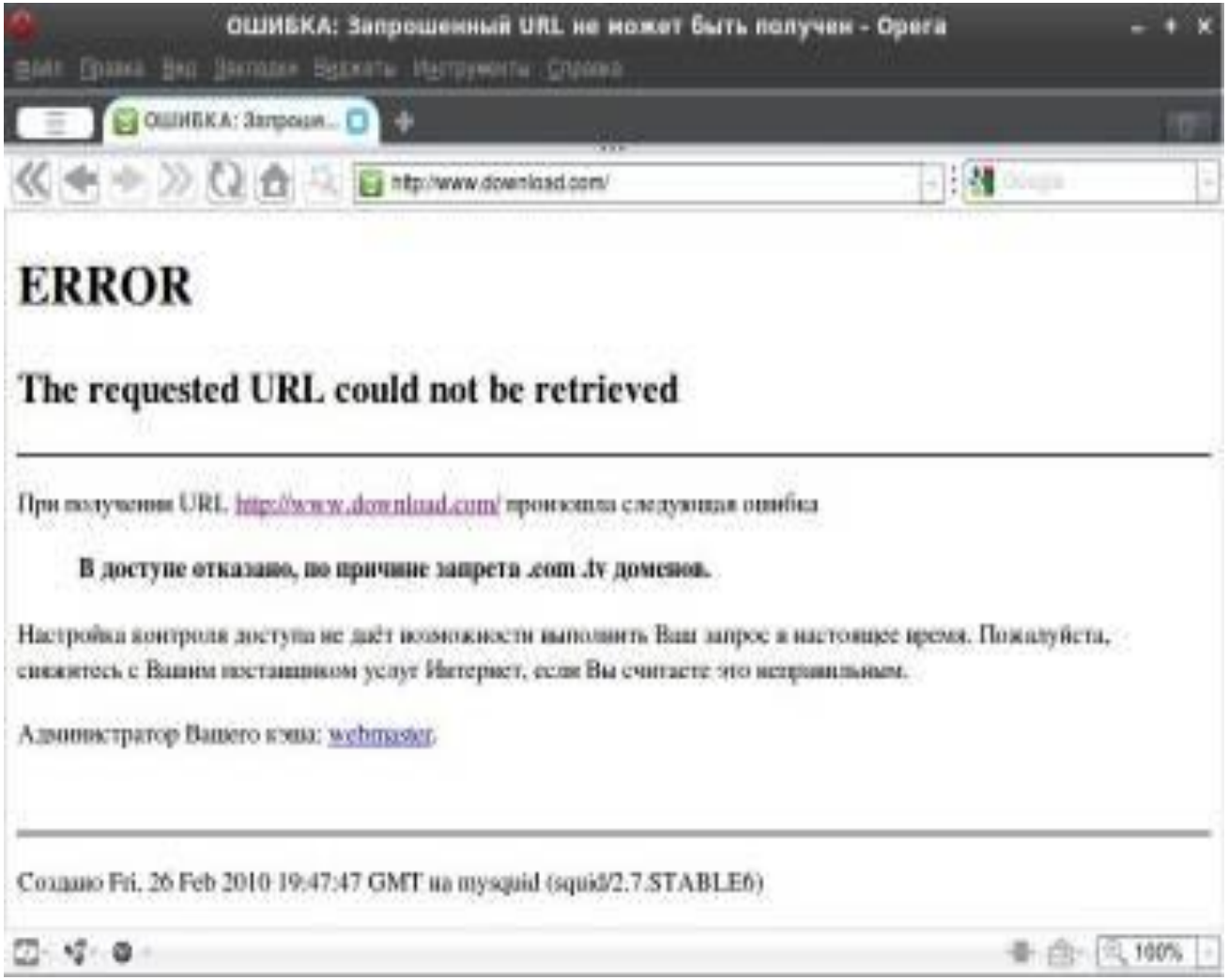
Рис. 5. Запуск Squid.

Так же нужно настроить клиентские машины для доступа в интернет через прокси-сервер Squid (Рис. 6).



Так же нужно настроить клиентские машины для доступа в интернет через прокси-сервер Squid (Рис. 6).

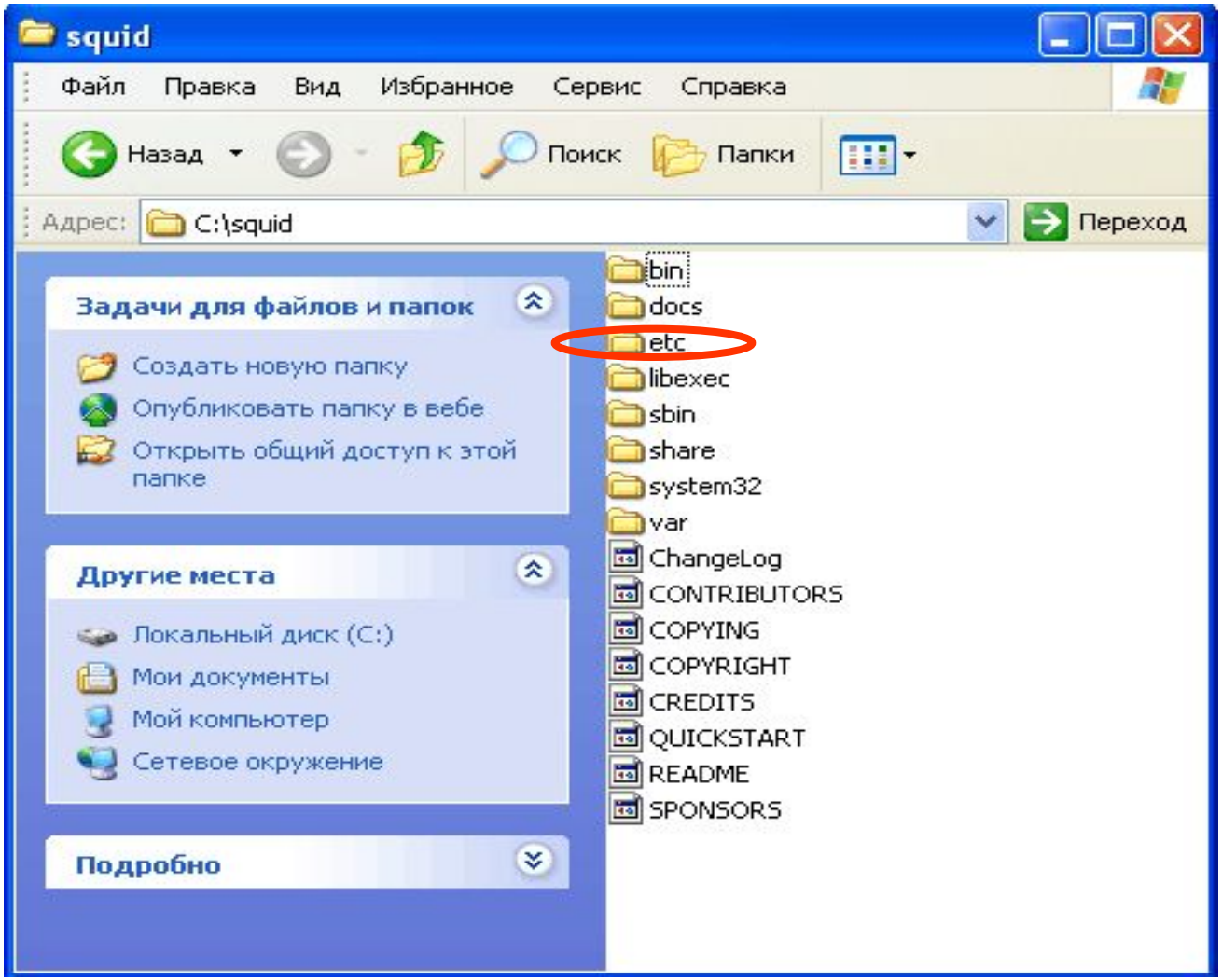
Теперь при попытке доступа к заблокированным ресурсам вместо них будут открываться надписи со сведениями причины блокировки:



Windows

Прокси сервер в **Windows** служит для раздачи интернета на другие компьютеры или для ускорения своего собственного интернета. Хотя «ускорение» будет довольно спорное, в пределах 10% и только для сайтов, на которые хоть раз, но заходили. Будем использовать **Squid**, как гибкое и стабильное решение, хотя и сложное в настройке для неподготовленного пользователя. Метод протестирован на Windows версий XP, 2003, 7.

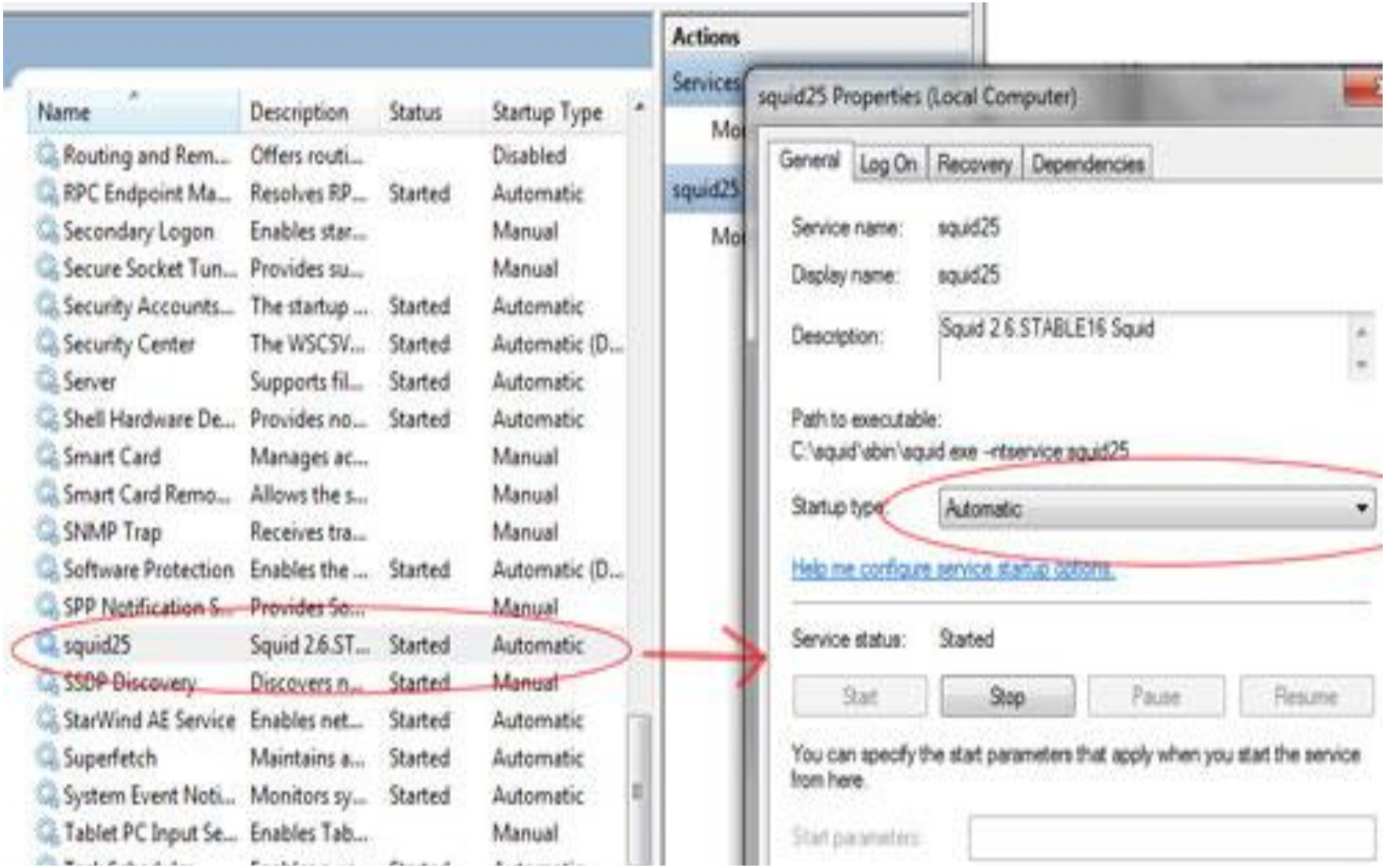
1. Качаем архив squid.rarsquid.rar squid-2.7.STABLE4-bin.zip (последняя стабильные версия)
2. Распаковываем в каталог c:\squid. Можно установить и в другой каталог, но придется поправить .bat файлы уже созданные в данной сборке для вашего удобства



Конфигурационные файлы Squid расположены в папке **etc.** Заходим туда и создаем собственные файлы конфигурации путем копирования оригинальных файлов конфигурации. Т.е. файл:
- **squid.conf.default** необходимо скопировать в файл **squid.conf**
- **cachemgr.conf.default** необходимо скопировать в файл **cachemgr.conf**
- **mime.conf.default** необходимо скопировать в файл mime.conf

3. Устанавливаем **Squid** как системную службу и создаем кэш, для этого запускаем файлы install_step1.bat и install_step2.bat

Все, у вас работает служба squid25, проверить ее можно в «Управлении» — правой кнопкой по «Мой компьютер» — «Управление» — «Службы» — «Squid25». Должна быть примерно такая картинка

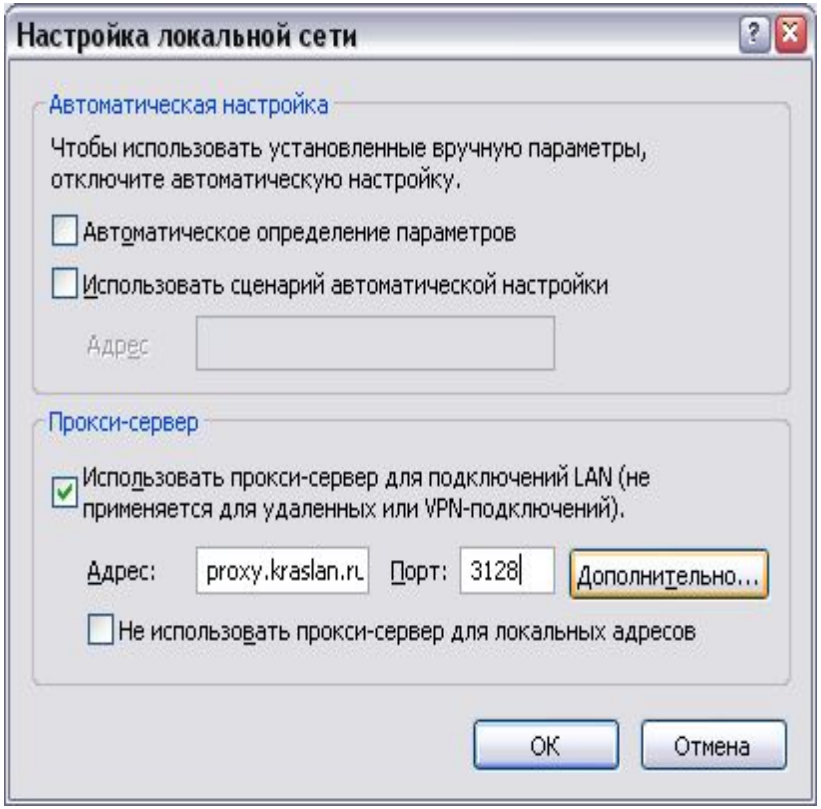


В конфигурационном файле, который находится в **C:\squid\etc\squid.conf** по умолчанию есть доступ только для локального компьютера. Если вы хотите дать доступ дополнительному устройству (ноутбуку, компьютеру, еще какому то пользователю в виде соседа), то нужно изменить файл примерно так: (в блокноте)
Начальная конфигурация
visible_hostname server // имя ПК
http_port 3128 // порт прокси
acl localhost src 192.168.0.1/255.255.255.255 // адреса которым мы разрешим доступ
acl Safe_ports port 80 110 25 //порты по которым мы можем обращаться в интернет, 80 - www, 25,110 - email
acl CONNECT method CONNECT
acl all src 0.0.0.0/0.0.0.0
http_access allow localhost // разрешаем доступ
http_access allow !Safe_ports // разрешаем порты
http_access deny CONNECT
http_access allow all
Изменим acl localhost src 127.0.0.1/255.255.255.255 на acl localhost src 192.168.0.0/255.255.255.0 для предоставления доступа сети 192.168.0.1 — 192.168.0.254 и запустим reconfsquid.bat для «применения» настроек.
UPD Обновил архив squid.rar — добавил логи кто что качал и две нужные папки, без них оказывается не стартовал сервис.

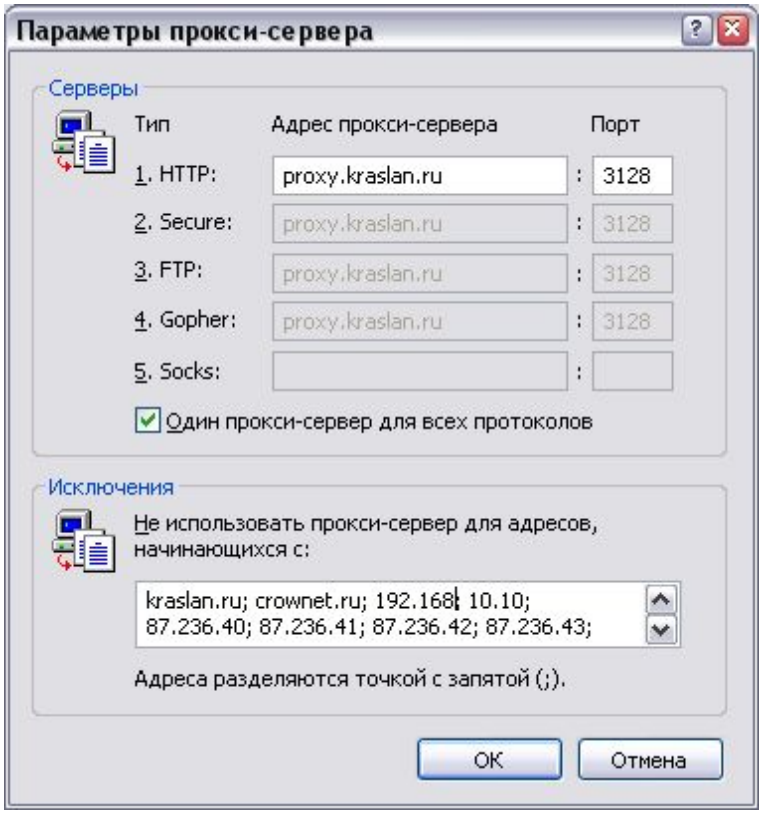
Настройка прокси-сервера для Internet Explorer

Зайдите в меню Сервис -> Свойства обозревателя. Выберите вкладку «Подключения», а затем нажмите кнопку «Настройка LAN...»

Установите галочку «Использовать прокси-сервер для подключений...».
В поле ввода «Адрес» введите «**192.168.0.1**», а в поле «Порт» — «**3128**»
Не забудьте включить «Не использовать прокси-сервер для локальных адресов».



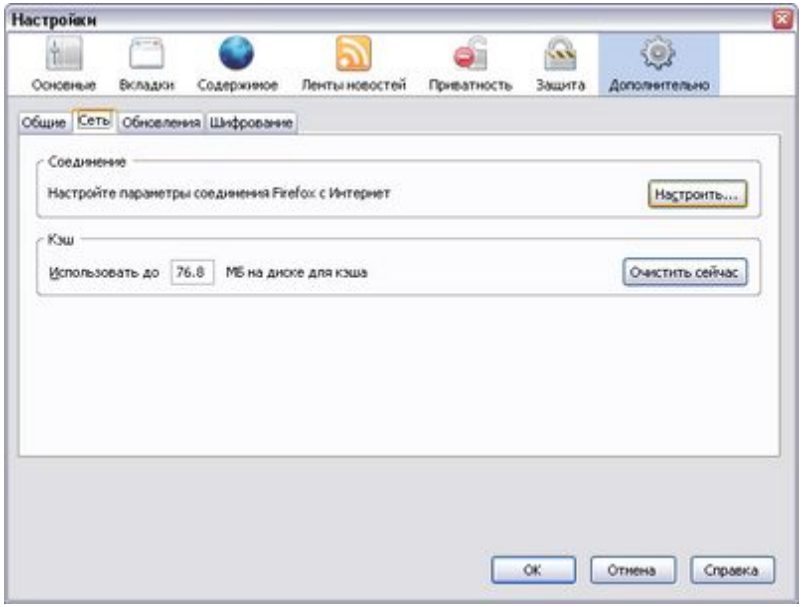
Установите галочку «Использовать прокси-сервер для подключений...».
В поле ввода «Адрес» введите «**192.168.0.1**», а в поле «Порт» — «**3128**»
Не забудьте включить «Не использовать прокси-сервер для локальных адресов».



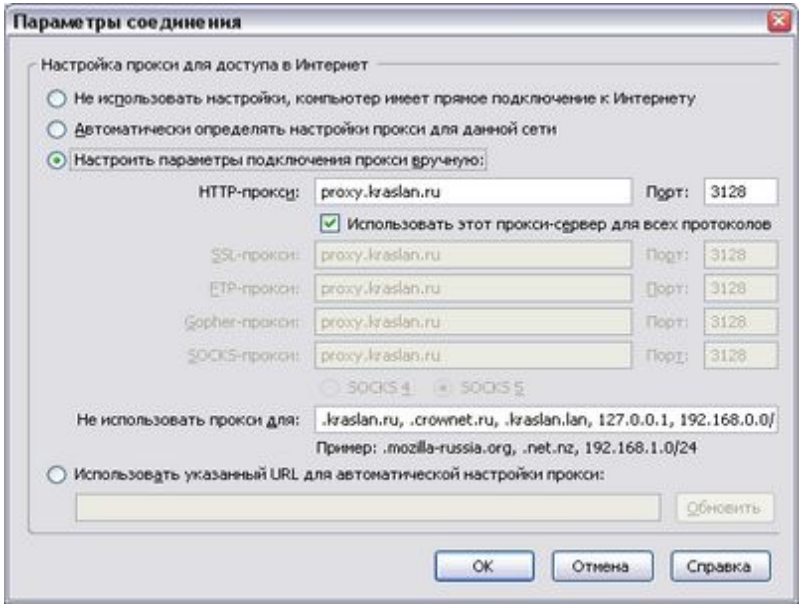
Теперь нажмите кнопку «Дополнительно».
В поле ввода «HTTP» введите «**192.168.0.1**», а в поле «Порт» — «**3128**».
Теперь поставьте галочку «Использовать один прокси-сервер для всех протоколов».

Настройка прокси-сервера для Mozilla FireFox 2

Зайдите в меню Инструменты -> Настройки. Затем перейдите на вкладку «Дополнительно».
Чуть ниже выберите вкладку «Сеть», в рамочке «Соединение» нажмите кнопку «Настроить».

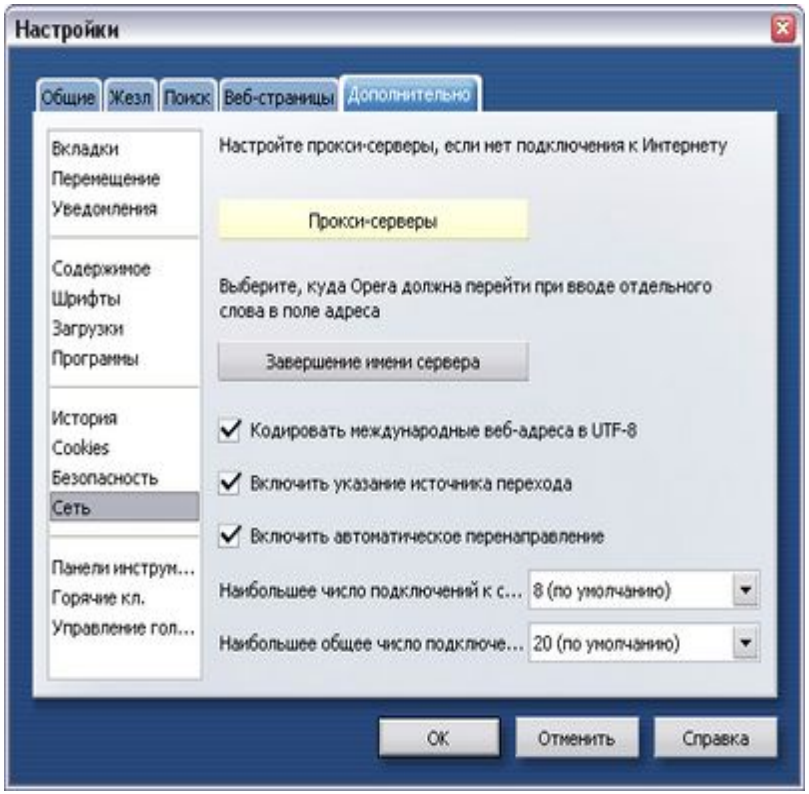


Установите галочку «Настроить параметры подключения вручную».
В поле ввода «HTTP - прокси» введите «**192.168.0.1**», а в поле «Порт» — «**3128**».
Затем установите галочку «Использовать этот прокси-сервер для всех протоколов».

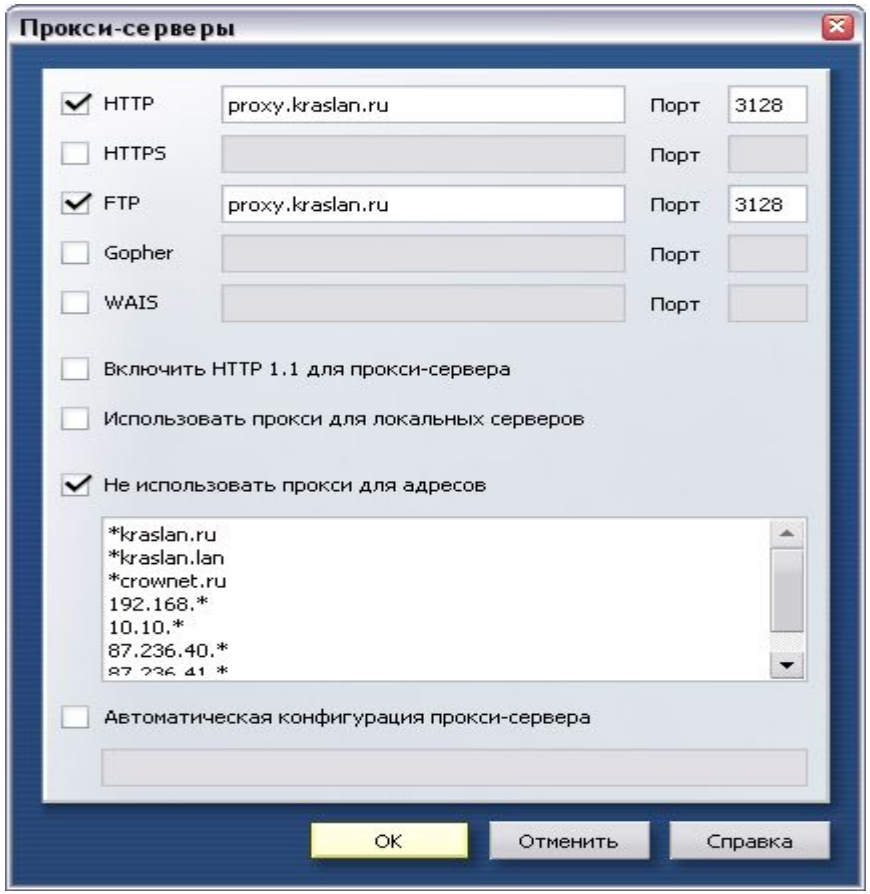


Настройка прокси-сервера для Opera

Зайдите в меню Инструменты -> Настройки.
Затем перейдите на вкладку «Дополнительно».
В списке слева выберите вкладку «Сеть».



Теперь нажмите кнопку «Прокси - серверы».
Поставьте галочки «HTTP» и «FTP», в полях ввода напротив них — введите «192.168.0.1 », а в полях «Порт» — «**3128**».



Список литературы

Бруй В. В., Карлов С. В. Б67 “LINUX-сервер: пошаговые инструкции инсталляции и настройки.” – М.: Изд-во СИП РИА, 2003. – 572 с. ISBN 5-89354-153-7

http://www.Squid-cache.org/- Домашняя страница проекта Squid

http://Squid.visolve.com/ - Руководство, советы по настройке

http://Squid.opennet.ru/ - FAQ, форум, ссылки на русскоязычные ресурсы, посвященные Squid

http://www.boq.pp.ru/ - Установка, настройка и использование

http://www.break-people.ru/ - Файл Squid.conf на русском, по секциям

Web страницы посвященные Squid.

Здесь информация по программе Squid http://squid.nlanr.net/Squid/Здесь информация по программе Squid http://squid.nlanr.net/Squid/,а здесь http://www.nlanr.net/Cache/дополнительная информация по кешированию вообще.