

Министерство образования и науки Российской Федерации
Федеральное государственное
бюджетное образовательное учреждение высшего профессионального
образования «Российский экономический университет им. Г.В. Плеханова»
Московский приборостроительный техникум

ЛАБОРАТОРНАЯ РАБОТА.

«SQUID»

Выполнил: Кочарян Эрик Робертович
студент группы КС – 3 – 17

Москва, 2020 г

Ход работы.

1) Установка Squid.

```
root@ErikKocharuan:/home/erik# apt-get -y install squid
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  libcap3 squid-common squid-langpack
Предлагаемые пакеты:
  squidclient squid-cgi squid-purge resolvconf ufw winbindd
НОВЫЕ пакеты, которые будут установлены:
  libcap3 squid squid-common squid-langpack
обновлено 0, установлено 4 новых пакетов, для удаления отмечено 0 пакетов, и 25 пакетов не обновлено
.
Необходимо скачать 2 761 кБ архивов.
После данной операции, объём занятого дискового пространства возрастёт на 10,4 МБ.
0% [Обработка]
```

Рис.1-Установка.

2)Проверяем статус сервера.

```
root@ErikKocharuan:/home/erik# systemctl status squid
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; generated; vendor preset: enabled)
   Active: active (running) since Thu 2020-04-09 11:20:51 MSK; 1min 46s ago
     Docs: man:systemd-sysv-generator(8)
  Main PID: 1470 (squid)
    CGroup: /system.slice/squid.service
            └─1468 /usr/sbin/squid -YC -f /etc/squid/squid.conf
              └─1470 (squid-1) -YC -f /etc/squid/squid.conf
                └─1471 (logfile-daemon) /var/log/squid/access.log
                  └─1472 (pinger)

апр 09 11:20:51 ErikKocharuan systemd[1]: Starting LSB: Squid HTTP Proxy version 3.x...
апр 09 11:20:51 ErikKocharuan squid[1468]: Squid Parent: will start 1 kids
апр 09 11:20:51 ErikKocharuan squid[1427]: Starting Squid HTTP Proxy: squid.
апр 09 11:20:51 ErikKocharuan systemd[1]: squid.service: PID file /var/run/squid.pid not readable (yet?) after start: No such file or directory
апр 09 11:20:51 ErikKocharuan squid[1468]: Squid Parent: (squid-1) process 1470 started
апр 09 11:20:51 ErikKocharuan systemd[1]: squid.service: Supervising process 1470 which is not our child. We'll most likely not notice when it exits.
апр 09 11:20:51 ErikKocharuan systemd[1]: Started LSB: Squid HTTP Proxy version 3.x.
апр 09 11:20:51 ErikKocharuan systemd[1]: squid.service: Supervising process 1470 which is not our child. We'll most likely not notice when it exits.
```

Рис.2-Статус.

Важные файлы Squid располагаются в следующих директориях:

Файл конфигурации: /etc/squid/squid.conf

Журнал доступа: /var/log/squid/access.log

Журнал кэша: /var/log/squid/cache.log

3)Конфиг сервера.

```
GNU nano 2.7.4                               Файл: /etc/squid/squid.conf

# WELCOME TO SQUID 3.5.23
# -----
#
# This is the documentation for the Squid configuration file.
# This documentation can also be found online at:
#   http://www.squid-cache.org/Doc/config/
#
# You may wish to look at the Squid home page and wiki for the
# FAQ and other documentation:
#   http://www.squid-cache.org/
#   http://wiki.squid-cache.org/SquidFaq
#   http://wiki.squid-cache.org/ConfigExamples
```

Рис.3-Конфиг.

4) `http_port` порт HTTP-прокси сервера, по умолчанию 3128. Для безопасности рекомендуется сменить его на другой.

```
# Squid normally listens to port 3128
http_port 2020
```

Рис.4-Смена порта.

`visible_hostname` Параметр используется для определения имени узла сервера Squid. Можно задать любое имя.

Также можно указать параметр `intercept` (или `transparent` для старых версий), например, `http_port 3128 intercept`. В этом случае ваш сервер будет работать как прозрачный прокси (без необходимости настраивать его использование на стороне клиента).

Для последующего понимания работы прокси, нужно понять следующие параметры

`http_access` - Данный параметр регулирует доступ к HTTP-прокси серверу. С помощью него можно разрешить или запретить доступ через сервер как к определенным ресурсам в интернете, так и определенным группам пользователей.

В данный момент любой доступ запрещен (`deny all`). Чтобы начать использование сервера, нужно изменить ее, например, на `http_access allow all` (разрешить любой доступ). Параметр `all` можно заменить на имя списка доступа, которые мы рассмотрим чуть ниже.

```
# And finally deny all other access to this proxy
http_access allow all
```

Рис.5-Смена параметра доступа.

`acl`(access control list) — В этом параметре указываются ресурсы в интернете, порты, `ip` адреса пользователей, локальные сети. В общем это список к которому будут применяться различные правила. Таких списков может быть неограниченное количество.

После внесения изменений нужно перезапустить Squid следующей командой а также проверяем статус для проверки на ошибки:

```
root@ErikKocharuan:/home/erik# systemctl restart squid
root@ErikKocharuan:/home/erik# systemctl status squid
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; generated; vendor preset: enabled)
   Active: active (running) since Thu 2020-04-09 11:34:17 MSK; 1min 24s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 1594 ExecStop=/etc/init.d/squid stop (code=exited, status=0/SUCCESS)
  Process: 1624 ExecStart=/etc/init.d/squid start (code=exited, status=0/SUCCESS)
 Main PID: 1664 (squid)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/squid.service
           └─1662 /usr/sbin/squid -YC -f /etc/squid/squid.conf
             └─1664 (squid-1) -YC -f /etc/squid/squid.conf
               └─1665 (logfile-daemon) /var/log/squid/access.log
                 └─1666 (pinger)
```

Рис.6-Перезагрузка.

Настройка Squid как HTTP-прокси.

1)Добавляем в конфиг acl клиента

```
#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 192.168.0.0/16  # RFC1918 possible internal network
#acl localnet src fc00::/7       # RFC 4193 local private network range
#acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines

#acl client src 192.168.1.17/24 #client virtual
```

Рис.1-Добавление списка клиента.

2)Перезагружаем.

```
root@ErikKocharuan:/home/erik# systemctl restart squid
root@ErikKocharuan:/home/erik# systemctl status squid
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; generated; vendor preset: enabled)
   Active: active (running) since Thu 2020-04-09 11:34:17 MSK; 1min 24s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 1594 ExecStop=/etc/init.d/squid stop (code=exited, status=0/SUCCESS)
  Process: 1624 ExecStart=/etc/init.d/squid start (code=exited, status=0/SUCCESS)
 Main PID: 1664 (squid)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/squid.service
           └─1662 /usr/sbin/squid -YC -f /etc/squid/squid.conf
             └─1664 (squid-1) -YC -f /etc/squid/squid.conf
               └─1665 (logfile-daemon) /var/log/squid/access.log
                 └─1666 (pinger)
```

Рис.2-Перезагрузка.

Работа прокси в прозрачном режиме.

1)Прозрачный режим предполагает автоматическую работу

прокси-сервера без необходимости в явном виде указывать его на клиентских машинах. В общем случае клиент может вообще не знать, что работает через прокси. Это может быть полезным для обеспечения анонимности, ограничения доступа к некоторым сайтам и даже экономии сетевого трафика, так как прокси-сервер может сжимать данные.

Помимо уже рассмотренной выше опции `intercept` в параметре `http_port` файла конфигурации, для обеспечения правильной работы прозрачного прокси требуется соответствующим образом настроить маршрутизатор. Чтобы все входящие и исходящие запросы на порт 80 перенаправлялись на порт, используемый прокси-сервером.

В случае использования `iptables` нужно добавить следующие правила (в рассматриваемом примере `eth1` — внутренний интерфейс, `eth0` — внешний, `SQUID_IP` — IP-адрес прокси-сервера):

```
root@ErikKocharuan:/home/erik# iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to 192.168.1.15:2020
root@ErikKocharuan:/home/erik# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 2020
root@ErikKocharuan:/home/erik#
```

Рис.1-Правила.

Аутентификация клиента.

1)Создадим файл passwd для хранения имени пользователя для аутентификации. Скви́д работает как пользователь squid, поэтому он должен быть владельцем файла. Создадим нового пользователя erik и установим ему пароль 123.

```
root@ErikKocharuan:/home/erik# touch /etc/squid/passwd$ sudo chown squid:squid /etc/squid/passwd
root@ErikKocharuan:/home/erik# sudo htpasswd /etc/squid/passwd erik
bash: sudo: команда не найдена
root@ErikKocharuan:/home/erik# htpasswd /etc/squid/passwd erik
New password:
Re-type new password:
Adding password for user erik
root@ErikKocharuan:/home/erik#
```

Рис.1-Создание файла и пользователя.

2)Для задания базовой HTTP-аутентификации откроем файл конфигурации Скви́д в текстовом редакторе. И пропишем следующие директивы после ACL портов.

```
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

auth_param basic program /usr/lib64/squid/basic_ncsa_auth
/etc/squid/passwdauth_param basic children 5auth_param basic
realm Squid Basic Authenticationauth_param basic
credentialsttl 2 hoursacl auth_users proxy_auth
REQUIREDhttp_access allow auth_users
```

Рис.2-Директивы.

Настройка параметров кэширования.

1)Одна из важных функций прокси-сервера — кэширование веб-страниц для разгрузки веб-сервера и ускорения доступа. Скви́д поддерживает два типа кэша, в оперативной памяти и на жёстком диске.

Кэш в оперативной памяти настраивается следующими параметрами:

cache_mem 1024 MB — выделенный для кэширования объем памяти

maximum_object_size_in_memory 512 KB — максимальный размер объекта в кэше. Параметры кэша на жёстком диске задаются следующей директивой:

```
#Default:
# No disk cache. Store cache objects only in memory.
#

# Uncomment and adjust the following to add a disk cache directory.
#cache_dir ufs /var/spool/squid 100 16 256

cache_dir ufs /var/squid_cache 2048 32 512
```

Рис.1-Кеш.

Аналогично кэшу в памяти при помощи следующего параметра указывается максимальный размер объекта в кэше на диске:

```
#Default:
# maximum_object_size 8MB
```

Рис.1-Макс кеш элемент.

Ограничение скорости.

1) Squid может ограничивать скорость доступа к сети. Хотя в современных условиях эта функция может показаться избыточной, она часто может оказаться полезной, например, для ограничения использования пропускной способности канала какими-либо автоматизированными задачами.

Для реализации ограничения скорости Сквида использует механизм пулов задержки (delay pools). Пулы задержки можно условно представить в виде ёмкости, которая “заполняется” данными, и после этого “выпускает” их только с определенной скоростью. Количество пулов задаётся в файле конфигурации следующим образом:

Каждый пул имеет номер (от 1 до заданного количества), а также класс. Классы реализуют многоступенчатую структуру ограничения:

1 класс — общее ограничение

2 класс — общее ограничение и ограничения для подсетей

3 класс — общее ограничение, ограничения для подсетей и ограничения для отдельных IP-адресов

Классы пулов задаются директивой `delay_class`, в качестве аргументов которой передаются номер пула и класс.

```
#configuration details:
#Default:
# delay_pools 2delay_class 1 1delay_class 2 2
```

Рис.1-Количество пулов.

2) Параметры пулов задаются директивой `delay_parameters` и описывают максимальный объем пула и ограничение на каждый уровень (в байтах) в зависимости от класса. Например, параметры для пула 1 класса с номером 1:

```
# For example, if delay pool number 1 is a class 2 delay pool as in the
# above example, and is being used to strictly limit each host to 64Kbit/sec
# (plus overheads), with no overall limit, the line is:
#
#      delay_parameters 1 64000/256000
#
# Note that 8 x 8K Byte/sec -> 64K bit/sec.
#
# Note that the word 'none' is used to represent no limit.
#
```

Рис.2-Параметры.

Будут означать, что после получения первых 256 Кб запроса на максимальной скорости скорость будет ограничена 64 Кб/с, то есть 512 Кбит/с.

Для 2 класса и выше аналогичным образом задаются ограничения для подсети, отдельного адреса и т.д., например следующая директива ограничивает общую скорость до 8 Мбит/с, а скорость для подсети после первых 256 Кб запроса — до 512 Кбит/с.

```
(if the network is not being limited due to overuse) but slow down
large downloads more significantly:
```

```
delay_parameters 2 512000/512000 64000/256000
```

```
Note that 8 x 32K Byte/sec -> 256K bit/sec.
           8 x 8K Byte/sec -> 64K bit/sec.
           8 x 600 Byte/sec -> 4800 bit/sec.
```

Рис.3-Параметры.

Блокировка веб-сайтов.

1)Для блокировки доступа к нежелательным веб-сайтам сначала создайте файл с “черным списком”:

```
root@ErikKocharuan:/home/erik# touch /etc/squid/blacklisted_sites.acl
root@ErikKocharuan:/home/erik#
```

Рис.4-Черный список.

Теперь в этот файл нужно добавить сайты, к которым требуется заблокировать доступ. Например заблокируем доступа к одноклассникам и вконтакте:

```
erik@192.168.1.15:22 - Bitvise xterm - erik@ErikKocharuan: ~
```

```
GNU nano 2.7.4
```

```
Файл: /etc/squid/blacklisted_sites.acl
```

```
.vk.com.ok.ru
```

Рис.5-Сайты.

2)Далее нужно открыть файл конфигурации .И добавить список контроля доступа по доменным именам, указанным в файле, а также правило, запрещающее доступ для этого списка:

```
# Deny requests to certain unsafe ports
acl bad_urls dstdomain "/etc/squid/blacklisted_sites.acl http_access deny bad_urls
http_access deny !Safe_ports
```

Рис.6-Правило.

3)Перезагружаем.

```
root@ErikKocharuan:/home/erik# systemctl restart squid
root@ErikKocharuan:/home/erik# systemctl status squid
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; generated; vendor preset: enabled)
   Active: active (running) since Thu 2020-04-09 11:34:17 MSK; 1min 24s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 1594 ExecStop=/etc/init.d/squid stop (code=exited, status=0/SUCCESS)
  Process: 1624 ExecStart=/etc/init.d/squid start (code=exited, status=0/SUCCESS)
 Main PID: 1664 (squid)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/squid.service
           └─1662 /usr/sbin/squid -YC -f /etc/squid/squid.conf
             └─1664 (squid-1) -YC -f /etc/squid/squid.conf
               └─1665 (logfile-daemon) /var/log/squid/access.log
                 └─1666 (pinger)
```

Рис.7-Перезагрузка.

Теперь при попытке получить доступ к сайтам из списка, пользователь получит предупреждени.