Установка и настройка Squid на Ubuntu

Обновлено: 11.11.2021 Опубликовано: 30.07.2020

Используемые термины: Squid, Ubuntu.

Данную инструкцию можно также применять для установки SQUID на Debian. В качестве клиентов могут использоваться Windows, Linux, Mac OS и любые браузеры.

Установка и базовая настройка

Устанавливаем прокси-сервер следующей командой:

```
apt-get install squid
```

Открываем на редактирование конфигурационный файл:

```
vi /etc/squid/squid.conf
```

Если сеть клиентских компьютеров отличается от стандартной (192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8), необходимо ее добавить в acl, например:

```
#  TAG: acl
...
acl localnet src 217.66.157.0/24
```

или через файл:

```
#  TAG: acl
...
acl localnet src "/etc/squid/acl_localnet"
```

** кавычки обязательны*
*** после необходимо создать файл **/etc/squid/acl_localnet** и с каждой строчки перечислить разрешенные IP-адреса.*

С точки зрения безопасности, лучше закомментировать все подсети, которые не используются в нашей локальной сети, например:

```
#  TAG: acl
...
#acl localnet src 0.0.0.1-0.255.255.255
#acl localnet src 10.0.0.0/8
#acl localnet src 100.64.0.0/10
#acl localnet src 169.254.0.0/16
#acl localnet src 172.16.0.0/12
acl localnet src 192.168.0.0/16
#acl localnet src fc00::/7
#acl localnet src fe80::/10
```

** в данном примере мы оставили только подсеть **192.168.0.0/16**.*

Разрешаем доступ для локальных сетей, которые заданы опцией **acl localnet**:

```
#  TAG: http_access
...
http_access allow localnet
```

** данную опцию нужно либо раскомментировать, либо вставить выше опции **http_access deny all**.*

Настраиваем директорию для кэша:

```
#  TAG: cache_dir
...
cache_dir ufs /var/spool/squid 4096 32 256
```

** где **ufs** — файловая система (ufs для SQUID является самой подходящей); **/var/spool/squid** — директория хранения кэша; **4096** — объем пространства в мегабайтах, которое будет выделено под кэш; **32** — количество каталогов первого уровня, которое будет*

создано для размещение кэша; ***256*** *— количество каталогов второго уровня, которое будет создано для размещение кэша.*

Останавливаем squid:

```
systemctl stop squid
```

Создаем структуру папок под кэш следующей командой:

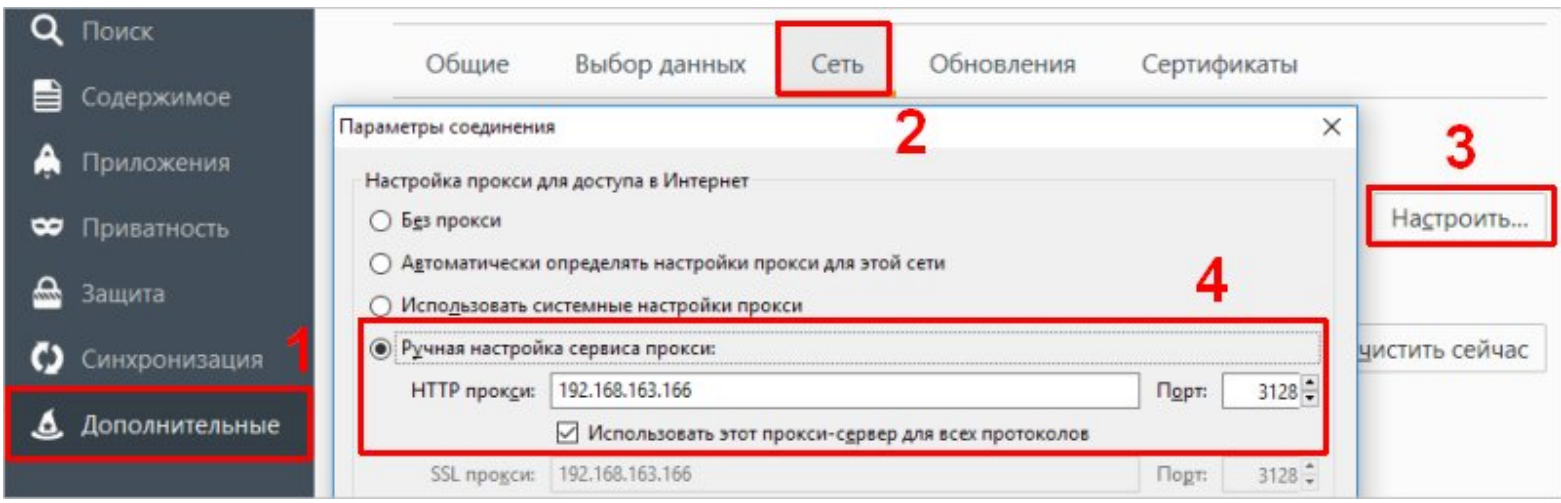
```
squid -z
```

Запускаем squid и разрешаем его автозапуск:

```
systemctl enable squid --now
```

Проверка

Заходим в настройки браузера и настраиваем использование прокси-сервера. Например, в Mozilla Firefox настройки нужно выставить такими:



** где* ***192.168.163.166*** *— IP-адрес моего прокси-сервера.*

Теперь открываем сайт 2ip.ru. После его загрузки мы увидим внешний IP-адрес — он должен соответствовать той сети, от которой работает настроенный SQUID.

Прозрачный прокси

Прозрачный прокси позволяет автоматически использовать прокси-сервер, не настраивая при этом браузер компьютера. Пользователи могут даже не знать, что трафик идет через squid.

Открываем конфигурационный файл:

```
vi /etc/squid/squid.conf
```

Находим строчку:

```
#  TAG: http_port
...
http_port 3128
```

И приводим ее к следующему виду:

```
#  TAG: http_port
...
http_port 3129
http_port 127.0.0.1:3128 intercept
```

** порт **3128** будет для прозрачного проксирования.*
*Порт **3129** должен быть указан в качестве прокси.*

И перезапускаем конфигурацию squid:

```
squid -k reconfigure
```

Для работы прозрачного проксирования. необходимо, чтобы шлюз перекидывал запросы по нужным портам на наш прокси. Это выполняется разными способами в зависмости от реализации шлюза.

Для примера, если нашим шлюзом будет наш сервер со squid, то нужно выполнить команды:

```
iptables -t nat -A OUTPUT -o lo -p tcp -m
tcp --dport 80 -j REDIRECT --to-ports 3128

iptables -t nat -A PREROUTING -i eth0 -p tcp
-m tcp --dport 80 -j REDIRECT --to-ports
3128

iptables -t nat -A OUTPUT -o lo -p tcp -m
tcp --dport 443 -j REDIRECT --to-ports 3128

iptables -t nat -A PREROUTING -i eth0 -p tcp
-m tcp --dport 443 -j REDIRECT --to-ports
3128
```

Авторизация по логину и паролю

Открываем конфигурационный файл:

```
vi /etc/squid/squid.conf
```

Вставляем следующее:

```
#  TAG: auth_param
...
auth_param basic program
/usr/lib/squid/basic_ncsa_auth
/etc/squid/auth_users
auth_param basic children 25
auth_param basic realm SQUID PROXY
auth_param basic credentialsttl 3 hours
```

** где **/usr/lib/squid/basic_ncsa_auth** — расположение ncsa_auth (в зависимости от системы может находиться в другом каталоге); **/etc/squid/auth_users** — файл с логинами и паролями; **children 25** разрешает 25 одновременных подключений; **SQUID PROXY** — произвольная фраза для приветствия; **credentialsttl 3 hours** будет держать сессию 3 часа, после потребуется повторный ввод логина и пароля.*

Создаем acl для пользователей, которые прошли регистрацию. Сделаем регистрацию обязательной:

```
#  TAG: acl
...
acl auth_users proxy_auth REQUIRED
```

Находим опцию:

```
http_access deny !Safe_ports
```

И после нее добавляем:

```
http_access allow auth_users
```

Устанавливаем утилиту apache2-utils:

```
apt-get install apache2-utils
```

Создаем файл с пользователями и создаем первую пару логина и пароля:

```
htpasswd -c /etc/squid/auth_users user1
```

Создаем второго пользователя:

```
htpasswd /etc/squid/auth_users user2
```

И перечитываем конфигурацию squid:

```
squid -k reconfigure
```

Слушаем на определенном интерфейсе

По умолчанию, squid будет слушать запросы на всех сетевых интерфейсах, которые доступны серверу. Чтобы указать конкретный, добавляем его IP к http_port:

```
vi /etc/squid/squid.conf
```

```
#  TAG: http_port
...
http_port 192.168.1.15:3128
```

** в данном примере squid будет слушать на адресе **192.168.1.15**.*

И перечитываем конфигурацию squid:

```
squid -k reconfigure
```

Исходящий сетевой интерфейс

На нашем сервере может быть несколько внешний IP-адресов. По умолчанию, все исходящие запросы будут работать через интерфейс со шлюзом по умолчанию. Чтобы иметь возможность работы со squid через разные интерфейсы в настройку вносим:

```
vi /etc/squid/squid.conf
```

```
acl 217_66_157_33 localip 217.66.157.33
tcp_outgoing_address 217.66.157.33
217_66_157_33
```

```
acl 217_66_157_34 localip 217.66.157.34
tcp_outgoing_address 217.66.157.34
217_66_157_34
```

** в данном примере, при подключении к прокси через IP **217.66.157.33**, исходящие пакеты будут от IP **217.66.157.33**; аналогично для IP **217.66.157.34**.*

Перечитываем конфигурацию squid:

```
squid -k reconfigure
```

Настройка цепочки прокси-серверов

Мы можем передать запрос на другой прокси-сервер. Для этого открываем конфигурационный файл:

```
vi /etc/squid/squid.conf
```

Настраиваем передачу запроса на другой прокси сервер:

```
#  TAG: cache_peer
...
cache_peer 10.11.12.13 parent
3128 3128 proxy-only
```

** в данном примере мы передадим запрос на сервер 10.11.12.13. Синтаксис для cache_peer — cache_peer <hostname> <type> <http-port> <icp-port> [options]:*

- ***hostname —** другой сервер, на который мы будем передавать запрос.*
- ***type —** тип «родства» другого сервера. Могут быть варианты:*
  - *parent*
  - *sibling*
  - *multicast*
- ***http-port —** номер порта, на котором партнер принимает HTTP-запросы.*
- ***icp-port —** порт для запроса кэша.*
- ***options —** дополнительный опции.*

** более подробное описание можно найти в самом конфигурационном файле SQUID.*

Если на прокси, к которому мы подключаемся, необходима авторизация, добавляем опцию login:

```
cache_peer 10.11.12.13 parent
3128 3128 proxy-only
login=loginname:password
```

Запрещаем использование нашего прокси-сервера напрямую (не через cache_peer):

```
#  TAG: never_direct
...
never_direct allow all
```

Перечитываем конфигурацию squid:

```
squid -k reconfigure
```

Ubuntu # Безопасность # Интернет # Серверы # Сети

Была ли полезна вам эта инструкция?

Да Нет

Обсудить (телеграм-чат)

Дмитрий Моск — IT-специалист.
Настройка серверов, услуги DevOps.

Нужна бесплатная консультация?

Написать в телеграм-чат

Инструкции

Установка и настройка кластера Kubernetes на Linux Ubuntu

Как настроить почту для корпоративной среды на Ubuntu Server

Установка, настройка и использование системы по сбору логов Grafana Loki на Linux

Как установить и настроить связку Asterisk + FreePBX на Rocky 8

Как установить и настроить прокси-сервер Squid на Ubuntu Server

Как настроить почту для корпоративной среды на CentOS 8

Установка и настройка Remote Desktop Gateway на Windows Server

Другие инструкции

Все статьи

Задать вопрос по электронной почте:

Ваш вопрос

Контактная эл. почта

Запросить инструкцию