Proxy-сервер Squid

Прокси-сервер — это
дополнительное звено между вами и интернетом. Некий посредник, который отделяет человека от посещаемого сайта. Создает условия, при которых сайт думает, что прокси — это и есть реальный человек. Только не вы.

Такие посредники довольно многофункциональны и используются в нескольких сценариях:

1. Для обеспечения конфиденциальности. Чтобы сайты не знали, кто именно их посещает.
2. Для повышения уровня безопасности при выходе в сеть. Базовые атаки будут направлены именно на прокси.
3. Еще он нужен, чтобы получать доступ к контенту, который существует только в определенной локации.
4. Чтобы ускорить доступ к некоторым ресурсам в интернете.
5. Ну и для того, чтобы получить доступ к заблокированным страницам. Сайтам, мессенджерам и так далее.

Все
 за счет того, что прокси подменяет IP-адрес, а трафик проходит через дополнительный сервер, на котором могут быть кэшированные данные или организованы дополнительные механизмы защиты данных.

Типы прокси-серверов

Косвенно
я уже упомянул о том, что proxy бывают разными. Зачастую тип сервера сопоставим с задачами, которые он выполняет. Но для начала мы обсудим именно базовую типизацию proxy, а потом более подробно поговорим о том, какие проблемы эти серверы решают.

Прозрачные

Такой
прокси-сервер не утаивает от посещаемого сайта никакой информации. Во-первых, он честно сообщит ему о том, что является прокси, а во-вторых, передаст сайту IP-адрес пользователя по ту сторону сервера. С подобным типом можно встретиться в публичных заведениях, школах.

Анонимные

Более
востребованный тип прокси. В отличие от первого, он тоже заявляет посещаемому ресурсу о своей proxy-сущности, но личные данные клиента не передает. То есть будет предоставлять обезличенную информацию для обеих

сторон. Правда, неизвестно, как поведет себя сайт, который на 100% знает, что общается с proxy.

Искажающие

Такие прокси тоже идентифицируют себя честно, но вместо реальных пользовательских данных передают подставные. В таком случае сайты подумают, что это вполне себе реальный человек, и будут вести себя соответствующе. Например, предоставлять контент, доступный только в конкретном регионе.

Приватные

Вариант для параноиков. Такие прокси регулярно меняют IP-адреса, постоянно выдают фальшивые данные и заметно сокращают шансы веб-ресурсов отследить трафик и как-то связать его с клиентом.

Другие подкатегории

Прокси-серверы отличаются друг от друга и технически. Существуют:

- HTTP-прокси. Самые распространенные. Используются для веб-браузинга. Но они небезопасные, поэтому лучше выбирать другие.
- HTTPS. То же самое, что и HTTP, только с шифрованием. Можно смело использовать для выхода на заблокированные сайты типа Pandora или Hulu.
- SOCKS. Вариация протокола, работающая с разными типами трафика. Более гибкая и безопасная.

Зачем нужен прокси-сервер?

На плечи proxy возлагают много задач. Сейчас подробно обсудим каждую.

Фильтрация доступных ресурсов

Распространенный сценарий использования в общественных сетях. С помощью такого сервера можно наблюдать за трафиком и при необходимости его «фильтровать». Это

как родительский контроль. Только масштабы иные. Подобный proxy запросто могут поднять в крупной компании, чтобы сотрудники не лезли в Твиттер, пока занимаются делами. Поэтому при входе в соцсеть может вылезти предупреждение с просьбой заняться работой. Ну или вместо этого начальник просто зафиксирует все время пребывания в Фейсбуке, а потом вычтет это из зарплаты. С детьми ситуация примерно такая же. Можно ограничить их свободу в сети на время выполнения домашнего задания, к примеру.

Ускорение работы интернета

На прокси-серверах могут храниться кэшированные копии сайтов. То есть при входе на определенный сайт вы получите данные именно с proxy. С большой долей вероятности, через прокси загрузятся они заметно быстрее. Так происходит, потому что загруженность популярного сайта, на который вы хотите зайти, пострадает меньше, если большое количество людей будет заходить на него через шлюз в виде прокси-сервера.

Сжатие данных

Тоже весьма практичный сценарий. Помогает заметно снизить количество затрачиваемого трафика. На некоторых прокси установлены инструменты, которые сжимают весь запрашиваемый контент перед тем, как перенаправить его к конечному пользователю. По такому принципу работает «Турбо-режим» в браузерах Opera и Яндекса. Сжатие происходит на прокси-сервере, только он загружает полную версию медиа-контента и берет на себя всю нагрузку. А клиент уже скачивает те же данные, только в облегченном виде. Поэтому люди с лимитированным трафиком от этого выигрывают.

Конфиденциальность

Если возникают беспокойства за частную жизнь, то можно настроить приватный или анонимный шлюз, который будет всячески скрывать информацию о компьютере, который сделал первоначальный запрос (уберет его IP-адрес как минимум). Ими пользуются как отдельные личности, уставшие от слежки

рекламистов, так и крупные корпорации, не желающие мириться со шпионажем со стороны конкурентов, например. Это, конечно, не панацея, но самые примитивные проблемы, связанные с конфиденциальностью, прокси решить может. А еще он не требует большого количества ресурсов и времени на реализацию.

Безопасность

Прокси может обезопасить не только частную жизнь, но и защитить от реальных угроз вроде вирусов. Можно настроить шлюз таким образом, чтобы он не принимал запросы с вредоносных ресурсов. И превратить получившийся прокси в своего рода массовый «антивирус», через который можно выпускать всех сотрудников компании, не переживая, что те нарвутся на какую-нибудь серьезную угрозу. Конечно, это не защитит пользователей на 100%, но зато даст небольшой прирост безопасности. А он тоже дорогого стоит. Поэтому proxy, используемые именно для защиты, не такая уж редкость.

Доступ к запрещенному контенту

Еще шлюз можно использовать, чтобы обойти региональные запреты. Это работает как с веб-страницами, так и с веб-приложениями. Можно смотреть заграничную библиотеку Netflix, слушать американский музыкальный сервис Pandora, смотреть что-то в Hulu и так далее. Можно заходить на сайты, которые блокируются конкретно в вашей стране. Или случайно заблокированные провайдером. Причем это могут быть совсем безобидные сайты. Я, например, долго не мог зайти на форум sevenstring.com. Ну и всем известная история с Телеграмом, который из недолгого забвения вытащили как раз таки proxy-серверы.

Сравнение прокси с VPN

VPN лучше как в плане безопасности, так и в плане удобства, но такая сеть чаще стоит приличных денег. Зачастую VPN сложнее в настройке и работают не так быстро. Сами посудите, вам обязательно нужен клиент для

работы с виртуальными сетями или как минимум разрешения для браузера. Через proxy же можно подключаться, не устанавливая на компьютер ничего.

Риски, которые несет с собой использование прокси

Да,
риски есть, причем серьезные. Придется потратить чуть больше времени на изучение proxy-серверов, прежде чем выбрать какой-то из них и начать использовать.

Например,
стоит взять во внимание тот факт, что бесплатные прокси зачастую не очень хорошо подходят для решения вопросов безопасности. Чтобы как-то зарабатывать, владельцы шлюзов ищут иные пути для этого. Они продают пользовательские данные. Помогают распространять таргетинговую рекламу. Но даже этих денег не хватает, чтобы обеспечить высокую безопасность и скорость работы сервера, поэтому бесплатные варианты бывают тормозными и небезопасными.

Также стоит понимать:
использование прокси-сервера равняется передаче личных данных третьему лицу. Обычно с ними знакомятся только провайдер связи и владельцы страниц, которые вы посещаете. Теперь появится еще одна сторона, у которой будет доступ ко всему вашему трафику. Не факт, что он будет шифроваться или храниться в безопасности. И неизвестно, на каких условиях proxy-сервер может взаимодействовать с государством.

Установка и настройка Squid

Squid является самым популярным кеширующим и пересылкой HTTP-прокси-сервером, использующим широкий спектр компаний для кэширования веб-страниц с веб-сервера для повышения скорости веб-сервера, сокращения времени отклика и сокращения использования пропускной способности сети.

Прежде чем мы начнем, вы должны знать, что у Squid-сервера нет требований, но объем использования ОЗУ может отличаться в зависимости от клиентов, просматривающих Интернет через прокси-сервер.

Пакет Squid доступен для установки из базового репозитория Ubuntu, но перед этим обязательно обновите свои пакеты, запустив:

```
sudo apt-get update
sudo apt-get upgrade
```

После того, как ваши пакеты обновлены, вы можете продолжить установку и запустить его и включить его при запуске системы, используя следующие команды:

```
sudo apt-get install squid
sudo systemctl start squid
sudo systemctl enable squid
```

В этот момент ваш веб-прокси Squid уже должен быть запущен, и вы можете проверить статус службы:

```
sudo systemctl status squid
```

Ниже приведены некоторые важные местоположения файлов squid, о которых вы должны знать:

- Файл конфигурации Squid: /etc/squid/squid.conf
- Журнал доступа Squid: /var/log/squid/access.log
- Журнал кэширования Squid: /var/log/squid/cache.log

Файл конфигурации по умолчанию содержит некоторые директивы конфигурации, которые необходимо настроить для изменения поведения Squid.

Теперь откройте этот файл для редактирования с помощью редактора nano и внесите изменения, как показано ниже

```
sudo nano /etc/squid/squid.conf
```

После внесения изменений, вы можете перезапустить прокси-сервер Squid с помощью команд:

```
sudo systemctl restart squid
```

> Убрать все комментарии из файла `cp /etc/squid/squid.conf /etc/squid/squid.conf.back`
> `cat /etc/squid/squid.conf.back | grep -v "^#" | grep -v "^$" > /etc/squid/squid.conf`

Настройка Squid как HTTP-прокси на Ubuntu

В этом разделе конфигурации squid мы объясним вам, как настроить squid как прокси-сервер HTTP, используя только IP-адрес клиента для аутентификации.

Добавить ACL Squid

Если вы хотите разрешить только один IP-адрес для доступа к Интернету через ваш новый прокси-сервер, вам нужно будет определить новый acl (список управления доступом) в файле конфигурации.

```
sudo nano /etc/squid/squid.conf
```

Правило acl, которое вы должны добавить:

```
acl localnet src XX.XX.XX.XX
```

Где XX.XX.XX.XX – IP-адрес клиентской машины.

Этот acl следует добавить в начале раздела ACL.

Всегда полезно определить комментарий рядом с ACL, который будет описывать, кто использует этот IP-адрес, например.

```
acl localnet src 192.168.0.0/24
```

Вам нужно будет перезапустить службу Squid, чтобы внести новые изменения.

```
sudo systemctl restart squid
```

Открыть порты в Squid Proxy

По умолчанию в конфигурации squid разрешены только определенные порты, если вы хотите добавить более – просто определить их в файле конфигурации, как показано ниже.

```
acl Safe_ports port XXX
```

Где XXX – номер порта, который вы хотите разрешить.

Опять же полезно определить комментарий рядом с acl, который будет описывать, какой порт будет использоваться.

Чтобы изменения вступили в силу, вам нужно снова запустить squid.

```
sudo systemctl restart squid
```

Аутентификация клиента прокси-сервера Squid

Чтобы пользователи могли аутентифицироваться перед использованием прокси-сервера, вам необходимо включить базовую проверку подлинности HTTP в файле конфигурации, но перед этим вам необходимо установить пакет apache2-utils, используя следующую команду.

```
sudo apt-get update
sudo apt-get upgrade
sudo apt install apache2-utils
```

Теперь создайте файл с именем passwd, который позже сохранит имя пользователя для аутентификации.

Squid работает с пользователем «proxy», поэтому файл должен принадлежать этому пользователю.

```
sudo touch /etc/squid/passwd
sudo chown proxy: /etc/squid/passwd
ls -l /etc/squid/passwd
```

Теперь мы создадим нового пользователя под названием «pylounge» и настроим его пароль.

```
sudo htpasswd /etc/squid/passwd pylounge
```

Теперь, чтобы включить базовую проверку подлинности HTTP, откройте файл конфигурации.

```
sudo nano /etc/squid/squid.conf
```

После ACL портов добавьте следующие строки:

```
auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/passwd
auth_param basic children 5
auth_param basic realm Squid Basic Authentication
auth_param basic credentialsttl 2 hours
acl auth_users proxy_auth REQUIRED
http_access allow auth_users
```

Сохраните файл и перезапустите squid, чтобы новые изменения вступили в силу:

```
sudo systemctl restart squid
```

Блокировать веб-сайты с Squid Proxy

Чтобы заблокировать доступ к нежелательным веб-сайтам, сначала создайте файл под названием «blacklisted_sites.acl», в котором будут храниться сайты, внесенные в черный список.

```
sudo nano /etc/squid/blacklisted_sites.acl
```

Теперь добавьте веб-сайты, которые вы хотите заблокировать, например.

```
.instagram.com
.youtube.com
.vk.com
```

Проходящая точка сообщает squid, чтобы заблокировать все ссылки на эти сайты, включая www.instagram, subsite.instagram.com и т. д.

Теперь откройте файл конфигурации Squid.

```
sudo nano /etc/squid/squid.conf
```

Сразу после вышеперечисленных ACL добавьте следующие две строки:

```
acl bad_urls dstdomain "/etc/squid/blacklisted_sites.acl"
http_access deny bad_urls
```

```
acl localnet src 192.168.0.0/24 # subnet of host

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
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*

auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/passwd
auth_param basic realm Squid Basic Authentication
acl auth_users proxy_auth REQUIRED

acl bad_urls dstdomain "/etc/squid/blacklisted_sites.acl"
```

```
http_access deny bad_urls
http_access allow auth_users

http_access allow localhost
http_access allow localnet
http_access deny all
http_port 192.168.0.95:3128 # ip squid host
#https_port 192.168.0.95:3128

http_port 3128
coredump_dir /var/spool/squid
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern \/Release(|\.gpg)$ 0 0% 0 refresh-ims
refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern . 0 20% 4320
```

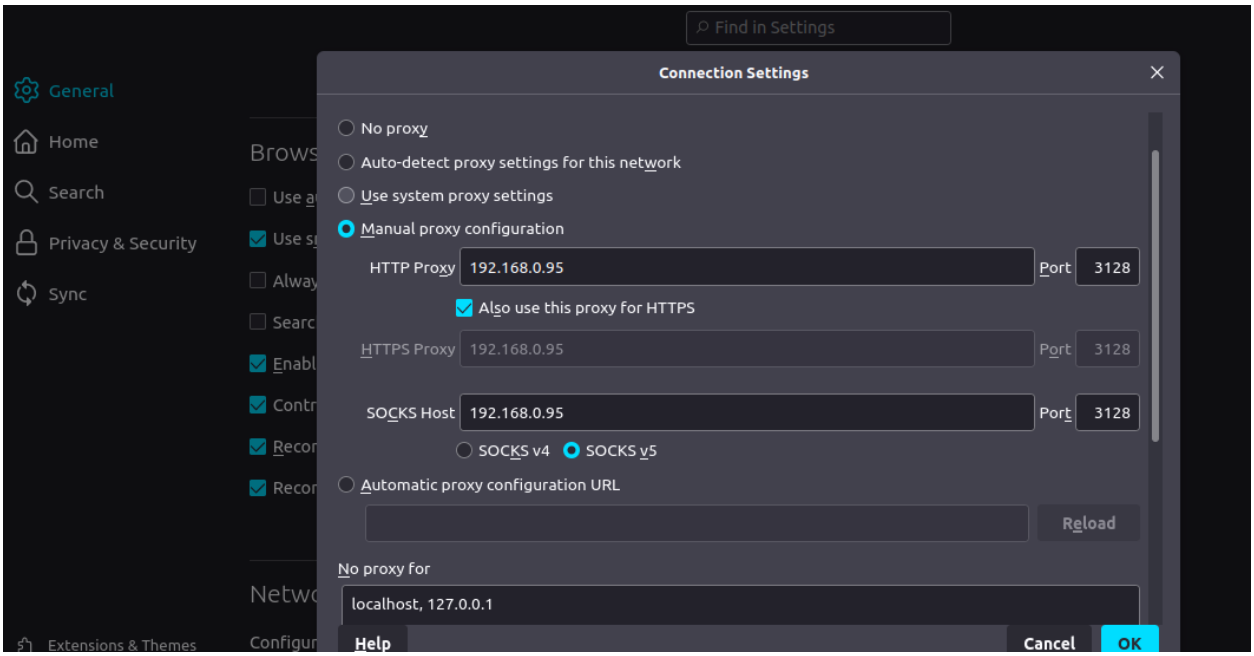
Теперь сохраните файл и перезапустите squid:

```
sudo systemctl restart squid
```

Настройка клиента для использования Squid Proxy

Теперь, чтобы проверить, работает ли ваш прокси-сервер или нет, вы можете открыть Firefox и перейти в **Edit -> Preferences -> Advanced -> Network -> Settings** и выбрать **«Manual proxy configuration**» и ввести IP-адрес и порт вашего прокси-сервера, который используется для всех соединений.

> Порт необходимо установить 3128 - стандартный порт squid.



После заполнения всех необходимых сведений о прокси-сервере вы сможете просматривать веб-страницы с помощью прокси-сервера Squid, вы можете сделать то же самое в любом другом браузере или программе.

Чтобы убедиться, что вы занимаетесь серфингом в Интернете с помощью прокси-сервера, вы можете посетить http://www.ipaddresslocation.org/, в правом верхнем углу вы должны увидеть тот же IP-адрес, что и IP-адрес вашего сервера.