**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**Реферат**

На тему: “Прокси-сервер”

Выполнил:

ст.гр. ИС/б-17-2

Черняев Н.Г.

Проверил:

Забаштанский А.К.

Севастополь

2021

**СОДЕРЖАНИЕ**

**Что такое прокси-сервер?**

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.

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.

**Еще немножко об IP-адресе**

Так как proxy-сервера отвечают за подмену IP, стоит немного пояснить, что он вообще делает и почему замена IP-адреса решает вышеописанные проблемы с доступом к сайтам и сервисам.

* IP-адрес говорит сайтам и веб-приложениям, где вы находитесь. Что ставит под угрозу конфиденциальность и безопасность.
* Его же используют, чтобы блокировать доступ к контенту. Зачастую на основе физического расположения.

Поэтому люди используют proxy и прячутся за посторонними адресами, чтобы избегать блокировок и не так сильно светиться в интернете. Но опять же есть исключения, когда proxy-сервер в открытую делится данными о пользователе с сайтом и используется только для ускорения передачи запросов.

**Типы прокси-серверов**

**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.

## Преимущества использования прокси-соединения

Главная причина, по которой пользователи пользуются прокси-серверами, заключается в том, чтобы скрыть свой IP-адрес. Некоторые сайты банят пользователей, проживающих в том или ином регионе. В таком случае единственной возможностью получить доступ к нужной информации – это прокси-соединение. Но это не единственная причина, по которой пользователи выбирают такую систему работы с информацией в интернете.

**Прокси-сервер может понадобиться:**

1. для защиты информации на своем компьютере от [сетевых атак](https://siteactiv.ru/terminy/ddos-ataki/);
2. для ограничения доступа сотрудников компании к сайтам развлекательного контента и социальным сетям;
3. для подключения к сети нескольких машин, если есть только один ip-адрес;
4. для экономии трафика;
5. для получение оперативного доступа к информации, что возможно благодаря созданию кэшированной копии.

Чаще всего прокси-соединением пользуется корпоративный сектор. Именно для него имеют значения такие преимущества, как:

* контроль доступа к интернету;
* учет и фильтрация трафика;
* безопасный обмен информацией;
* совместимость со всеми браузерами и операционными системами.

### Как получить прокси

Существуют версии аппаратного и программного обеспечения. Аппаратные решения располагаются между вашей сетью и интернетом, где они получают, отправляют и пересылают данные из интернета. Прокси-серверы программного обеспечения обычно размещаются провайдером или находятся в облаке. Вы устанавливаете приложение на свой компьютер, которое облегчает взаимодействие с прокси-сервером.

Зачастую прокси-сервер программного обеспечения можно получить за ежемесячную плату. Иногда они бесплатны. Бесплатные версии, как правило, предлагают пользователям меньше адресов и могут охватывать только несколько устройств, а платные прокси-серверы могут удовлетворить потребности бизнеса с большим количеством устройств.

### Как настроить сервер?

Чтобы начать работу с прокси-сервером, необходимо настроить его на компьютере, устройстве или в сети. Каждая операционная система имеет свои собственные процессы установки, поэтому проверьте действия, необходимые для вашего компьютера или сети.

Однако в большинстве случаев настройка подразумевает использование сценария автоматической конфигурации. Если вы хотите сделать это вручную, будут доступны опции для ввода IP-адреса и соответствующего порта.

### Как прокси-сервер защищает конфиденциальность и данные компьютера?

Прокси-сервер выполняет функцию межсетевого экрана и фильтра. Конечный пользователь или сетевой администратор могут выбрать прокси-сервер, предназначенный для защиты данных и конфиденциальности. В ходе этого исследования будут изучаться данные, поступающие в компьютер или сеть и выходящие из них. В нем также применяются правила, чтобы вам не пришлось раскрывать свой цифровой адрес миру. Хакеры или другие злоумышленники видят только IP-адрес прокси-сервера. Без вашего личного IP-адреса у людей в интернете не будет прямого доступа к вашим персональным данным, расписаниям, приложениям или файлам.

После этого веб-запросы отправляются в прокси-сервер, который затем получает то, что вам нужно, из интернета. Если сервер имеет функции шифрования, пароли и т. д., персональные данные получают дополнительный уровень защиты.

**ЗАКЛЮЧЕНИЕ**

Прокси-сервер — служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс, 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 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 и помогает сохранять анонимность клиента.

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.

**СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ**

1. Что такое прокси-сервер, зачем он нужен и как его настроить? // [Электронный ресурс]. URL: https://timeweb.com/ru/community/articles/chto-takoe-proksi-server-zachem-on-nuzhen-i-kak-ego-nastroit (дата обращения: 25.04.2021).

2. Прокси: что это такое и для чего он нужен - СайтАктив // [Электронный ресурс]. URL: https://siteactiv.ru/terminy/proksi (дата обращения: 25.04.2021).

3. Что такое прокси-сервер? // [Электронный ресурс]. URL: https://www.fortinet.com/ru/resources/cyberglossary/proxy-server (дата обращения: 25.04.2021).

4. Как работает прокси-соединение // [Электронный ресурс]. URL: https://wiki.rookee.ru/proxy (дата обращения: 25.04.2021).