**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

Долженко И.А.

Проверил:

Забаштанский А.К.

Севастополь

2021

**СОДЕРЖАНИЕ**

Прокси-сервер, или просто прокси – это сервер, выполняющий роль посредника между пользователем и целевым сервером. Сначала клиент подключается к прокси-серверу и запрашивает необходимый ресурс, расположенный на другом сервере. Например, почту или html-страницу. Затем прокси либо подключается к указанному серверу и получает у него ресурс, либо возвращает ресурс из собственного кэша.

Компании используют прокси для обеспечения безопасности, повышения производительности сети, доступа к «удаленным» ресурсам. Частные лица применяют прокси для анонимизации трафика или обхода ограничений доступа.

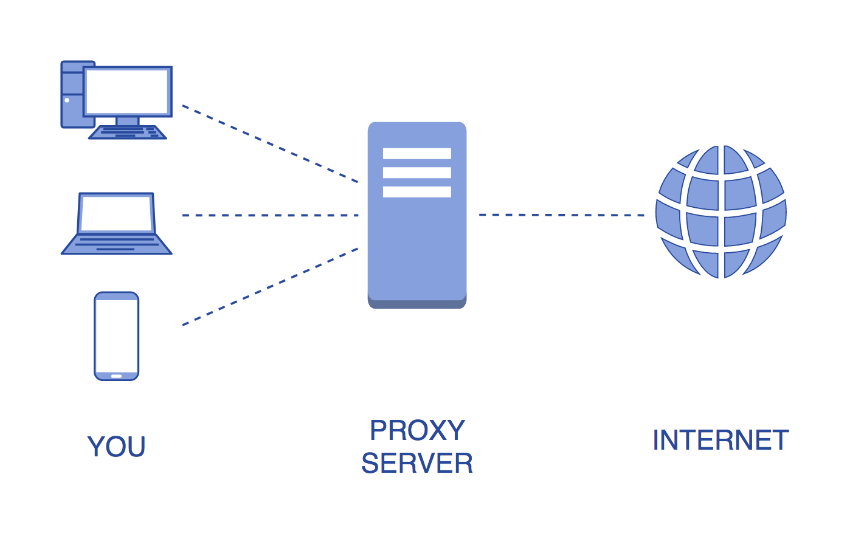


Рисунок 1 - Процесс работы с прокси

Когда речь заходит о прокси, обычно подразумевается прямой прокси-сервер. Представим, что мы делаем запрос, например, пытаемся перейти на GitHub – вводим URL, нажимаем Enter. Прокси не подключает нас к GitHub напрямую, а перехватывает соединение и обновляет содержание запроса, удаляя входящий IP и изменяя заголовок. В результате GitHub считает, что запрос пришел с другого компьютера, и отправляет нужные данные не нам, а прокси-серверу. Прокси принимает информацию GitHub, проверяет и отправляет данные нашему компьютеру.

**Как применяются прокси-серверы**

Распространенные варианты использования прокси:

* повышение безопасности сети с помощью шифрования запросов;
* предотвращение перехвата конфиденциальной информации;
* блокировка вредоносных сайтов и рекламы;
* кэширование сайтов для экономии трафика;
* контроль использования сетевого канала;
* блокировка доменов;
* мониторинг и регистрация веб-запросов;
* тестирование веб-ресурсов при заходе с различных IP.

**Какие бывают типы прокси-серверов**

В этом разделе определены существующие на рынке различные типы прокси, применяемые в обычных инфраструктурах.

Ключевыми типами прокси являются:

* пересылающие прокси (forward proxies);
* прозрачные прокси (transparent proxies);
* кеширующие прокси (caching proxies);
* прокси обеспечения безопасности (security proxies);
* обратные прокси (reverse proxies).

**Пересылающий прокси**

Пересылающий прокси 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).

С точки зрения безопасности простой прокси имеет целью обеспечение безопасности, состоящее в скрытии наименования (в терминах топологии внутренней сети) рабочей станции или процесса запрашивающего пользователя. Он может также применяться для скрытия некоторых других атрибутов сеанса пользователя.

Типичным примером этого типа являются корпоративные прокси, которые обслуживают внутренних пользователей посредством разрешения им доступа на внешние сайты для Web-браузинга или любого другого вида взаимодействия с Интернетом.

С точки зрения топологии (как в общем смысле, так и относительно ширины полосы пропускания) пересылающие прокси всегда относительно ограничены в терминах сетевой скорости по отношению к своим пользователям из-за более медленного WAN-соединения (соединения с глобальной сетью), которое обычно отделяет пересылающий прокси от реального контента в Интернете.

**Прозрачные прокси**

Прозрачные прокси являются прокси-серверами, которые "находятся здесь", но не осведомляют пользователей в прямой форме о том, что они здесь находятся. В пересылающих прокси обычно существуют LINUX/UNIX блоки, которые слушают весь трафик по определенному протоколу для определенного сегмента сети и перехватывают трафик, хотя пользовательский процесс в действительности не знает об их существовании. Фактически пользовательский процесс не общается с прокси, но общается с другим (конечным) сайтом, а прокси, в сущности, становится тем "человеком посередине", который "взламывает" соединение.

Прокси является непрозрачным, или объявленным, когда пользователи знают о том, что они общаются через прокси, потому что они обращаются (на языке прокси: HTTP) к прокси. Другими словами, если я объявил свой прокси как proxy.mydomain.com, то после этого мои процессы будут общаться с proxy.mydomain.com, запрашивая его об установлении контакта с конечным адресом назначения моих запросов.

Прозрачные прокси сами по себе не являются на самом деле типом прокси, скорее любой прокси является либо прозрачным, либо непрозрачным.

**Кэширующие прокси**

Кэширующие прокси, как указано в их названии, являются прокси-серверами, которые сконфигурированы на повторное использование кэшированных образов контента, когда это доступно и возможно. Когда кэшированная ранее часть контента недоступна, то производится ее выборка и использование в контенте, но также с попыткой ее кэширования.

Наиболее важным аспектом для кэширующих прокси является необходимость обеспечения того, что кэширующие прокси кэшируют только то, что на самом деле можно кэшировать. Динамический, регулярно изменяющийся контент не лучший выбор для кэширования, так как это может оказать воздействие на стабильность приложения, основанного на этом контенте. В случае HTTP-контента заголовки HTTP отображают возможность кэширования контента посредством указателей "cache".

**Прокси обеспечения безопасности**

В качестве высшего проявления необходимой для простых прокси функциональности прокси-серверы могут быть сконфигурированы для приведения в исполнение политик безопасности. Такие прокси 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 к конечным серверам с запросом, а конечный сервер должен быть сконфигурирован на оказание доверия предоставляемому прокси мандату.

**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. Прокси-сервер // Википедия. [Электронный ресурс]. URL: https://ru.wikipedia.org/?curid=75478&oldid=112403931 (дата обращения: 14.04.2021).

2. Обратный прокси // Википедия. [Электронный ресурс]. URL: https://ru.wikipedia.org/?curid=4690150&oldid=111306912 (дата обращения: 14.04.2021).

3. Веб-прокси // Википедия. [Электронный ресурс]. URL: https://ru.wikipedia.org/?curid=1597086&oldid=107916887 (дата обращения: 14.04.2021).

4. 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: 14.04.2021).