Содержание:

1.Введение

Прокси-сервера в наше время являются очень полезным и удобным средством защиты личной информации, которыми с каждым днём пользуется всё большее количество людей.

Прокси-сервер (от англ. proxy — «представитель», «уполномоченный») — промежуточный сервер (комплекс программ) в компьютерных сетях, выполняющий роль посредника между пользователем и целевым сервером (при этом о посредничестве могут как знать, так и не знать обе стороны), позволяющий клиентам как выполнять косвенные запросы (принимая и передавая их через прокси-сервер) к другим сетевым службам, так и получать ответы. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, e-mail), 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. Прокси-сервер позволяет защищать компьютер клиента от некоторых сетевых атак и помогает сохранять анонимность клиента, но также может использоваться мошенниками, для скрытия адреса сайта, уличённого в мошенничестве, изменения содержимого целевого сайта (подмена), а также перехвата запросов самого пользователя.

2.Использование Proxy-серверов

Чаще всего прокси-серверы применяются для следующих целей:

-Обеспечение доступа компьютеров локальной сети к сети Интернет.

-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. С развитием динамического контента кэширование утратило актуальность.

-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 сетевого трафика клиента или внутреннего — компании, в которой установлен прокси-сервер.

-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). См. также NAT.

-Ограничение доступа из локальной сети к внешней: например, можно запрещать доступ к определённым веб-сайтам, ограничивать использование интернета каким-то локальным пользователям, устанавливать квоты на трафик или полосу пропускания, фильтровать рекламу и вирусы.

-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.

-Обход ограничений доступа. Прокси-серверы популярны среди пользователей стран, где доступ к некоторым ресурсам ограничен законодательно и фильтруется.

Прокси-сервер, к которому может получить доступ любой пользователь сети интернет, называется открытым.

3.Виды Proxy-серверов

Прозрачный прокси — схема связи, при которой трафик, или его часть, перенаправляется на прокси-сервер неявно (средствами маршрутизатора). При этом клиент может использовать все преимущества прокси-сервера без дополнительных настроек браузера (или другого приложения для работы с интернетом). Пример: route -p add 10.32.5.5 mask 255.255.255.255 10.32.1.14

Обратный прокси — прокси-сервер, который в отличие от прямого, ретранслирует запросы клиентов из внешней сети на один или несколько серверов, логически расположенных во внутренней сети. Часто используется для балансировки сетевой нагрузки между несколькими веб-серверами и повышения их безопасности, играя при этом роль межсетевого экрана на прикладном уровне.

Существуют различные виды прокси серверов, каждый из которых обладает своими преимуществами и особенностями. Несмотря на то, что их видов действительно очень много, основными и наиболее часто используемыми являются всего лишь несколько из них.

3.1. HTTP proxy

HTTP прокси - это самый распространенный вид прокси. Основное предназначение - организация работы браузеров и других программ, использующих TCP протокол. Стандартные порты 80, 8080, 3128.

Принцип работы: программа или браузер посылает запрос прокси-серверу на открытие определенного URL ресурса. Прокси-сервер получает данные с запрашиваемого ресурса и отдает эти данные вашему браузеру.

HTTP прокси позволяют:

-кешировать загруженные файлы (картинки, страницы) для увеличения скорости открытия веб-сайтов

-ограничивать доступ к определенным ресурсам (например, Youtube)

-фильтровать данные. Например, вместо баннеров с рекламой показывать прозрачные картинки, которые не будут нарушать дизайн сайта, но будут существенно экономить время загрузки страницы и трафик

-ограничивать скорость соединения

-вести логи, контролировать трафик по пользователям

HTTP прокси по анонимности делятся на следующие виды:

-прозрачные прокси заявляют о том, что используется прокси и передают реальный IP адрес пользователя в HTTP заголовках. Прозрачные прокси использовать опасно, так как они не обеспечивают анонимности

-анонимные прокси уведомляют, что используется прокси, но при этом не передают реальный IP адрес пользователя. Анонимные прокси не могут гарантировать настоящей анонимности, так как заявляют, что прокси используется

-элитные прокси не уведомляют, что используется прокси и не передают реальный IP адрес пользователя. Только элитные прокси можно использовать для полной анонимности

3.2. HTTPS proxy

HTTPS прокси - фактически это HTTP-прокси, буква "S" в данном случае означает "secure" (защищенный) с поддержкой защищенного SSL соединения. Эти прокси применяются, когда требуется передать секретную информацию (например, логины/пароли, номера пластиковых карт). Стандартные порты 80, 8080, 3128.

При использовании обычного HTTP прокси всю информацию, передаваемую через него, можно перехватить с помощью самого прокси или на более низком уровне.

Например, все Интернет-провайдеры перехватывают и логируют абсолютно всю вашу активность в сети Интернет. Эти логи хранятся провайдером и является обоснованным доказательством ваших действий в сети Интернет. Поэтому для безопасности личных данных применяется протокол HTTPS, при этом весь передаваемый трафик шифруется устойчивым к взлому алгоритмом.

Принцип работы: прокси-сервер соединяется с ресурсом и ваш трафик шифруется. При таком методе отсутствует возможность узнать, какая именно информация передается через прокси-сервер (это ограничивает применение прокси как фильтра). Также в процессе шифрации и дешифрации прокси участия не принимает. Этим занимается клиентская программа (браузер) и целевой сервер. Таким образом, HTTPS proxy занимается пассивной передачей зашифрованной информации и не производит никакой обработки передаваемой информации. Такой метод работы позволяет использовать HTTPS proxy для передачи практически любого TCP-протокола. То есть HTTPS прокси может использоваться и как POP3, SMTP, IMAP, NNTP прокси.

3.3. Socks

На сегодняшний день Socks прокси - самый прогрессивный протокол передачи информации. Иногда ошибочно называют Socs, Sox, Soks. Этот протокол разработан Дейвом Кобласом (Dave Koblas).

Протокол Socks разрабатывался для программ, которые не поддерживают использование прокси напрямую. Стандартные порты 1080, 1081.

Данный протокол пережил множество изменений и на данный момент используются две версии протокола:

-Socks 4 поддерживает только TCP соединения

-Socks 5 поддерживает TCP, UDP, авторизацию по логину и паролю и возможность удаленного DNS-запроса

Socks не занимается модерацией HTTP-заголовков. Socks-сервер будет передавать информацию через себя в чистом виде. Поэтому все Socks серверы являются анонимными.

Socks прокси не передает информацию о вашем IP адресе. Веб-сайт не сможет определить использование прокси. Соединение с веб-сайтом будет абсолютно прозрачным, также как если бы вы работали с ним напрямую. При этом веб-сайт будет видеть IP адрес прокси, а не ваш реальный IP адрес.

Socks поддерживает все протоколы, включая HTTP, HTTPS, FTP.

4.Принцип работы proxy-сервера

Любой запрос, который пользователь делает в Интернете через браузер своего компьютера, перехватывается прокси-сервером. Прокси-сервер считывает IP-адрес выходящего в сеть компьютера и перенаправляет его дальше по этапу, но используя уже свой IP-адрес, вместо полученного по внутренней сети. Получив в ответ из Интернета пакеты данных (допустим страницы сайта), прокси-сервер обрабатывает их и перенаправляет на IP-адрес пользователя, сделавшего данный запрос.
Если компьютер находится за пределами защищенной сети, то все запросы (страницы сайтов, файлы и т.д.) происходят от компьютера пользователя. Механизм применения частных адресов по внутренней сети и подключение сети Интернет через прокси-сервер с официальным IP-адресом именуют трансляцией Network Address Translation.

Внутренняя сеть, чаще всего, работает используя протокол TCP/IP, где любому компьютеру присвоен уникальный адрес. Эти внутренние IP-адреса, зачастую, могут помочь взломщикам проникнуть в закрытые для неавторизованного доступа зоны сети. Избежать этого можно используя прокси-сервера, в этом случае информация и запросы пользователей, которые передаются по протоколу TCP/IP, не будут выдавать действительные IP-адреса владельцев компьютера.

5.Технические подробности

Клиентский компьютер имеет настройку (конкретной программы или операционной системы), в соответствии с которой все сетевые соединения по некоторому протоколу совершаются не на IP-адрес сервера (ресурса), выделяемый из DNS-имени ресурса, или напрямую заданный, а на IP-адрес (и другой порт) прокси-сервера.

При необходимости обращения к любому ресурсу по этому протоколу, клиентский компьютер открывает сетевое соединение с прокси-сервером (на нужном порту) и совершает обычный запрос, как если бы он обращался непосредственно к ресурсу.

Распознав данные запроса, проверив его корректность и разрешения для клиентского компьютера, прокси-сервер, не разрывая соединения, сам открывает новое сетевое соединение непосредственно с ресурсом и делает тот же самый запрос. Получив данные (или сообщение об ошибке), прокси-сервер передаёт их клиентскому компьютеру.

Таким образом прокси-сервер является полнофункциональным сервером и клиентом для каждого поддерживаемого протокола и имеет полный контроль над всеми деталями реализации этого протокола, имеет возможность применения заданных администратором политик доступа на каждом этапе работы протокола.

Прокси-серверы являются самым популярным способом выхода в Интернет из локальных сетей предприятий и организаций. Этому способствуют следующие обстоятельства:

-Основной используемый в интернете протокол — HTTP, в стандарте которого описана поддержка работы через прокси;

-Поддержка прокси большинством браузеров и операционных систем;

-Контроль доступа и учёт трафика по пользователям;

-Фильтрация трафика (интеграция прокси с антивирусами);

-Прокси-сервер — может работать с минимальными правами на любой ОС с поддержкой сети (стека TCP/IP);

-Многие приложения, использующие собственные специализированные протоколы, могут использовать HTTP как альтернативный транспорт или SOCKS-прокси как универсальный прокси, подходящий для практически любого протокола;

-Отсутствие доступа в Интернет по другим (нестандартным) протоколам может повысить безопасность в корпоративной сети.

В настоящее время, несмотря на возрастание роли других сетевых протоколов, переход к тарификации услуг сети Интернет по скорости доступа, а также появлением дешёвых аппаратных маршрутизаторов с функцией NAT, прокси-серверы продолжают широко использоваться на предприятиях, так как NAT не может обеспечить достаточный уровень контроля над использованием Интернета (аутентификацию пользователей, фильтрацию контента).

6.Наиболее распространенные proxy-серверы

1)3proxy (BSD, многоплатформенный)

2)CoolProxy (проприетарный, Windows)

3)Eserv (shareware, Windows)

4)HandyCache (shareware, Windows) бесплатен для домашнего использования

5)Kerio Control (проприетарный, Windows, Linux)

6)Microsoft Forefront Threat Management Gateway, ранее Microsoft ISA Server (proprietary, Windows)

7)Blue Coat Proxy SG (аппаратный/виртуальный appliance)

8)nginx (веб-сервер, имеющий режим работы в качестве reverse proxy и часто для этого использующийся)

9)Squid (GPL, многоплатформенный)

10)Traffic Inspector (проприетарный, Windows)

11)UserGate (проприетарный, Windows)

12)Интернет Контроль Сервер (shareware, FreeBSD)

13)Tor (BSD, многоплатформенный)

14)Ideco ICS (проприетарный, Linux)

15)WinGate (проприетарный, Windows)

16)Cntlm (с авторизацией)

17)Apache (веб-сервер, имеющий дополнительные модули для реализации прямого и реверсного прокси)

7.Сравнение разных типов прокси

	HTTP	HTTPS	Socks
Кеширование страниц, быстрая загрузка	+	+	+
Поддержка https (SSL) соединения	-	+	+
Полностью анонимный протокол	-	-	+