Содержание:

Введение

Прокси-сервер 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.

Использование

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 законодательнои фильтруется.

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

Виды прокси сервера

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-серверамии повышения их безопасности, играя при этом роль межсетевого экрана на прикладном уровне.

Классификация прокси-серверов для целей анонимизации представлена в статье Веб-прокси.

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).

Наиболее популярные прокси серверы

- 3proxy (BSD, многоплатформенный)
- CoolProxy (проприетарный, Windows)
- Eserv (shareware, Windows)
- HandyCache (shareware, Windows) бесплатен для домашнего использования
- Kerio Control (проприетарный, Windows, Linux)
- Microsoft Forefront Threat Management Gateway, ранее Microsoft ISA Server (proprietary, Windows)
- Blue Coat Proxy SG (аппаратный/виртуальный appliance)
- nginx (веб-сервер, имеющий режим работы в качестве reverse proxy и часто для этого использующийся)
- Squid (GPL, многоплатформенный)
- Traffic Inspector (проприетарный, Windows)
- UserGate (проприетарный, Windows)
- Интернет Контроль Сервер (shareware, FreeBSD)
- Tor (BSD, многоплатформенный)
- Ideco ICS (проприетарный, Linux)
- WinGate (проприетарный, Windows)
- Cntlm (с авторизацией)
- Apache (веб-сервер, имеющий дополнительные модули для реализации прямого и реверсного прокси)

Проксификаторы

Проксификатор — это программа, перенаправляющая другие программы через прокси-серверы. Проксификаторы часто применяются для интернет-клиентов, которые не поддерживают прокси-серверы