50. Организация Интернет-шлюза. Трансляция адресов (NAT). Proxy – сервера. Принципы работы. Примеры реализаций и использования.

NAT:
http://ru.wikipedia.org/wiki/NAT

Сетевой шлюз (англ. gateway) — аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы (например, локальной и глобальной).

Описание Сетевой шлюз конвертирует протоколы одного типа физической среды в протоколы другой физической среды

(сети). Например, при соединении локального компьютера с сетью Интернет вы используете сетевой шлюз. Роутеры (маршрутизаторы) являются одним из примеров аппаратных сетевых шлюзов.

Сетевые шлюзы работают на всех известных операционных системах. Основная задача сетевого шлюза — конвертировать протокол между сетями. Роутер сам по себе принимает, проводит и отправляет пакеты только среди сетей, использующих одинаковые протоколы. Сетевой шлюз может с одной стороны принять пакет, сформатированный под один протокол и конвертировать в пакет другого протокола перед отправкой в другой сегмент сети. Сетевые шлюзы могут быть аппаратным решением, программным обеспечением или тем и другим вместе, но обычно это программное обеспечение, установленное на роутер или компьютер. Сетевой шлюз должен понимать все протоколы, используемые роутером. Обычно сетевые шлюзы работают медленнее, чем сетевые мосты, коммутаторы и обычные роутеры. Сетевой шлюз — это точка сети, которая служит выходом в другую сеть. В сети Интернет узлом или конечной точкой может быть или сетевой шлюз, или хост. Интернет-пользователи и компьютеры, которые доставляют веб-страницы пользователям — это хосты, а узлы между различными сетями — это сетевые шлюзы. Например, сервер, контролирующий трафик между локальной сетью компании и сетью Интернет — это сетевой шлюз.

В крупных сетях сервер, работающий как сетевой шлюз, обычно интегрирован с прокси-сервером и межсетевым экраном. Сетевой шлюз часто объединен с роутером, который управляет распределением и конвертацией пакетов в сети.

Интернет-шлюз — программный сетевой шлюз, распределяющий и контролирующий доступ в сеть Интернет среди клиентов локальной сети (пользователей).

Интернет-шлюз, как правило, это программное обеспечение, призванное организовать из локальной сети доступ к сети Интернет. Программа является рабочим инструментом системного администратора, позволяя ему контролировать трафик и действия сотрудников. Обычно Интернет-шлюз позволяет распределять доступ среди пользователей, вести учёт трафика, ограничивать доступ отдельным пользователям или группам пользователей к ресурсам в Интернет. Интернет-шлюз может содержать в себе прокси-сервер, межсетевой экран, почтовый сервер, шейпер, антивирус и другие сетевые утилиты. Интернет-шлюз может работать как на одном из компьютеров сети, так и на отдельном сервере. Шлюз устанавливается как программное обеспечение на машину с операционной системой (например, Kerio winroute firewall на Windows), либо на пустой компьютер с развертыванием встроенной операционной системы (такой, как Ideco ICS с встроенным linux).
Программные интернет-шлюзы:

- Microsoft ISA Server
- Kerio Winroute Firewall
- Traffic Inspector
- Usergate
- Ideco Internet Control Server
- TMeter
- UserGate

Интернет-шлюзы в виде ОС:

- LinuxWizard GET-Inet.biz
- Ideco ICS
- Kerio Control Software Appliance

NAT (от англ. **Network Address Translation** — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Также имеет названия IP Masquerading, Network Masquerading и Native Address Translation.

Преобразование адресов методом NAT может производиться почти любым маршрутизирующим устройством — маршрутизатором, сервером доступа, межсетевым экраном. Наиболее популярным является SNAT, суть механизма

которого состоит в замене адреса источника (англ. source) при прохождении пакета в одну сторону и обратной замене адреса назначения (англ. destination) в ответном пакете. Наряду с адресами источник/назначение могут также заменяться номера портов источника и назначения.

Помимо *source NAT* (предоставления пользователям локальной сети с внутренними адресами доступа к сети Интернет) часто применяется также *destination NAT*, когда обращения извне транслируются межсетевым экраном на компьютер пользователя в локальной сети, имеющий внутренний адрес и потому недоступный извне сети непосредственно (без NAT).

Существует 3 базовых концепции трансляции адресов: *статическая* (Static Network Address Translation), *динамическая* (Dynamic Address Translation), *маскарадная* (NAPT, NAT Overload, PAT).

Статический NAT — Отображение незарегистрированного IP адреса на зарегистрированный IP адрес на основании один к одному. Особенно полезно, когда устройство должно быть доступным снаружи сети.

Динамический NAT — Отображает незарегистрированный IP адрес на зарегистрированный адрес от группы зарегистрированных IP адресов. Динамический NAT также устанавливает непосредственное отображение между незарегистрированным и зарегистрированным адресом, но отображение может меняться в зависимости от зарегистрированного адреса, доступного в пуле адресов, во время коммуникации.

Перегруженный NAT (NAPT, NAT Overload, PAT, маскарадинг) — форма динамического NAT, который отображает несколько незарегистрированных адресов в единственный зарегистрированный IP адрес, используя различные порты. Известен также как PAT (Port Address Translation). При перегрузке, каждый компьютер в частной сети транслируется в тот же самый адрес, но с различным номером порта.
NAT выполняет три важных функции:

- Позволяет сэкономить IP-адреса (только в случае использования NAT в режиме PAT), транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних). По такому принципу построено большинство сетей в мире: на небольшой район домашней сети местного провайдера или на офис выделяется 1 публичный (внешний) IP-адрес, за которым работают и получают доступ интерфейсы с приватными (внутренними) IP-адресами.
- Позволяет предотвратить или ограничить обращение снаружи ко внутренним хостам, оставляя возможность обращения изнутри наружу. При инициации соединения изнутри сети создаётся трансляция. Ответные пакеты, поступающие снаружи, соответствуют созданной трансляции и поэтому пропускаются. Если для пакетов, поступающих снаружи, соответствующей трансляции не существует (а она может быть созданной при инициации соединения или статической), они не пропускаются.
- Позволяет скрыть определённые внутренние сервисы внутренних хостов/серверов. По сути, выполняется та же указанная выше трансляция на определённый порт, но возможно подменить внутренний порт официально зарегистрированной службы (например, 80-й порт TCP (HTTP-сервер) на внешний 54055-й). Тем самым, снаружи, на внешнем IP-адресе после трансляции адресов на сайт (или форум) для осведомлённых посетителей можно будет попасть по адресу http://example.org:54055, но на внутреннем сервере, находящимся за NAT, он будет работать на обычном 80-м порту. Повышение безопасности и скрытие «непубличных» ресурсов.

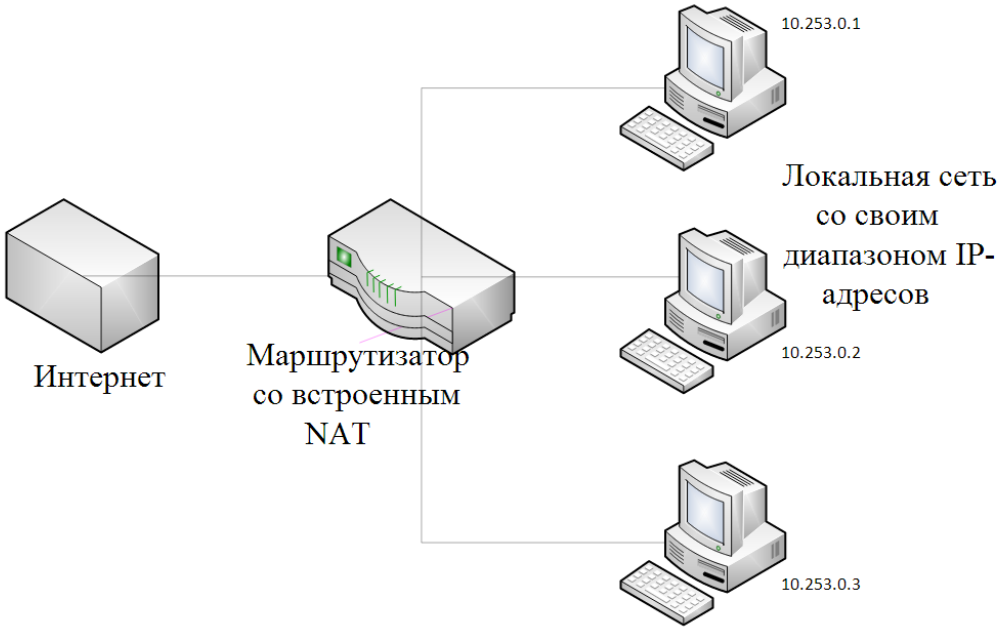
Недостатки:

- Не все протоколы могут «преодолеть» NAT. Некоторые не в состоянии работать, если на пути между взаимодействующими хостами есть трансляция адресов. Некоторые межсетевые экраны, осуществляющие трансляцию IP-адресов, могут исправить этот недостаток, соответствующим образом заменяя IP-адреса не только в заголовках IP, но и на более высоких уровнях (например, в командах протокола FTP). Из-за трансляции адресов «много в один» появляются дополнительные сложности с идентификацией пользователей и необходимость хранить полные логи трансляций.
- DoS со стороны узла, осуществляющего NAT — если NAT используется для подключения многих пользователей к одному и тому же сервису, это может вызвать иллюзию DoS-атаки на сервис (множество успешных и неуспешных попыток). Например, избыточное количество пользователей ICQ за NAT приводит к проблеме с подключением к серверу некоторых пользователей из-за превышения допустимой скорости подключений. Частичным решением проблемы является использование пула адресов (группы адресов), для которых осуществляется трансляция.
- В некоторых случаях, необходимость в дополнительной настройке (см. Трансляция порт-адрес) при работе с пиринговыми сетями и некоторыми другими программами, в которых необходимо не только инициировать исходящие соединения, но также принимать входящие. Однако, если NAT устройство и ПО, требующее дополнительной настройки, поддерживают технологию Universal Plug & Play, то в этом случае настройка произойдет полностью автоматически и прозрачно для пользователя.

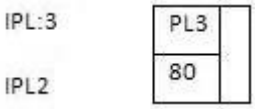
Техника NAT

Рассмотрим пример. Трансляция локальной сети с диапазоном адресов 172.17.14.0/24 в глобальную сеть будет осуществляться через один внешний IP-адрес (адрес маршрутизатора, выполняющего трансляцию).

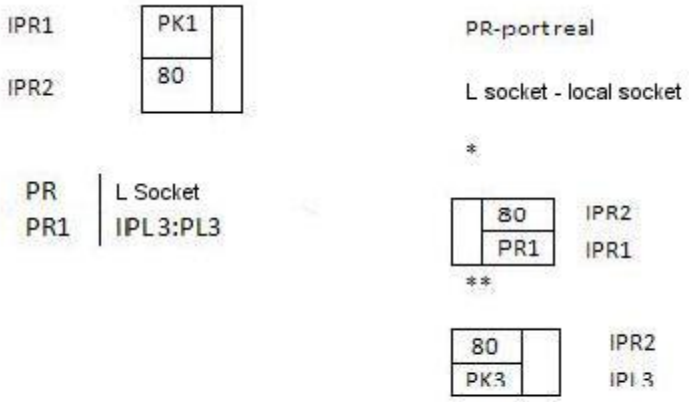
Для обеспечения доступа множества узлов во внешнюю IP сеть через единственный IP-адрес…



… на рабочих станциях указанный шлюз по умолчанию или gateway…

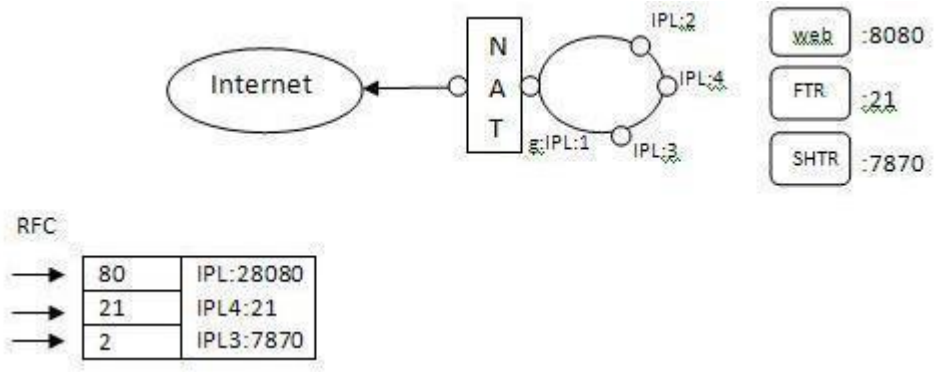


… преобразует служебные заголовки, формирует идентичный IP-пакет:



Если подменим Socket то знаем кому отвечать. а если подменим только IP, то не знаем кому

Публикация локальных ресурсов во внешней IP-сети



• Экономическая выгода вследствие приобретения единственного IP-подключения, а не IP-сети.

• Сокрытие от внешнего наблюдателя структуры внутренней IP-сети.

• Организация системы с распределенной нагрузкой.

• При общем доступе через NAT прозрачно открывается доступ к внутренней структуре с защитой без использования межсетевого экрана и т. п.

• Через NAT корректно работают многие сетевые протоколы. Конструктивные реализации (общий доступ — это и есть подключение NAT) есть аппаратная реализация NAT (интегрированы межсетевые экраны).

NAT Traversal (прохождение или автонастройка NAT) — это набор возможностей, позволяющих сетевым приложениям определять, что они находятся за устройством, обеспечивающим NAT, узнавать внешний IP-адрес этого устройства и выполнять сопоставление портов для пересылки пакетов из внешнего порта NAT на внутренний порт, используемый приложением; все это выполняется автоматически, пользователю нет необходимости вручную настраивать сопоставления портов или вносить изменения в какие-либо другие параметры. Однако существуют меры предосторожности в доверии к таким приложениям — они получают обширный контроль над устройством, появляются потенциальные уязвимости.

Прокси-сервер (от англ. proxy — «представитель, уполномоченный») — служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. 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. Также прокси-сервер позволяет защищать клиентский компьютер от некоторых сетевых атак и помогает сохранять анонимность клиента.

Чаще всего прокси-серверы применяются для следующих целей:

- Обеспечение доступа с компьютеров локальной сети в 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.
- 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.
- 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 запретить доступ к определённым веб-сайтам, ограничить 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.

Открытый прокси—прокси-сервер, к которому может получить доступ любой пользователь сети интернет.

Веб-прокси (англ. «web-based proxy») — это прокси-сервер и анонимайзер особого вида, представляющий собой веб-приложение (чаще всего PHP или Perl скрипт) установленное на веб-сервере, выступающее в роли посредника для загрузки контента различных веб-сайтов.
Веб-прокси могут быть использованы для:

- ускорения загрузки веб-сайтов;
- тестирования онлайн сервисов;
- обхода ограничений Администратора локальной сети на доступ к определенным адресам веб-сайтов;
- сокрытия реального IP-адреса и анонимного доступа к веб-сайтам;
- получения доступа к веб-сайтам закрытым для просмотра пользователей определенных стран.

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 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. Я полностью осведомлен о существовании прокси, о необходимости общаться с ним на "языке прокси" (HTTP), и о необходимости передать ему куда "идти" и откуда "принести" необходимый контент.

Вы можете иметь объявленные, непрозрачные прокси, которые автоматически объявлены, сконфигурированы или обнаружены. Вне зависимости от того как они были объявлены, эти прокси являются видимыми и известными для запрашивающего пользователя или процесса. Другими словами, неважно, как вы или ваш процесс узнали о существовании прокси, каковы причины того, что вы узнали о существовании прокси и о том, что вы общаетесь с прокси.

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

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

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

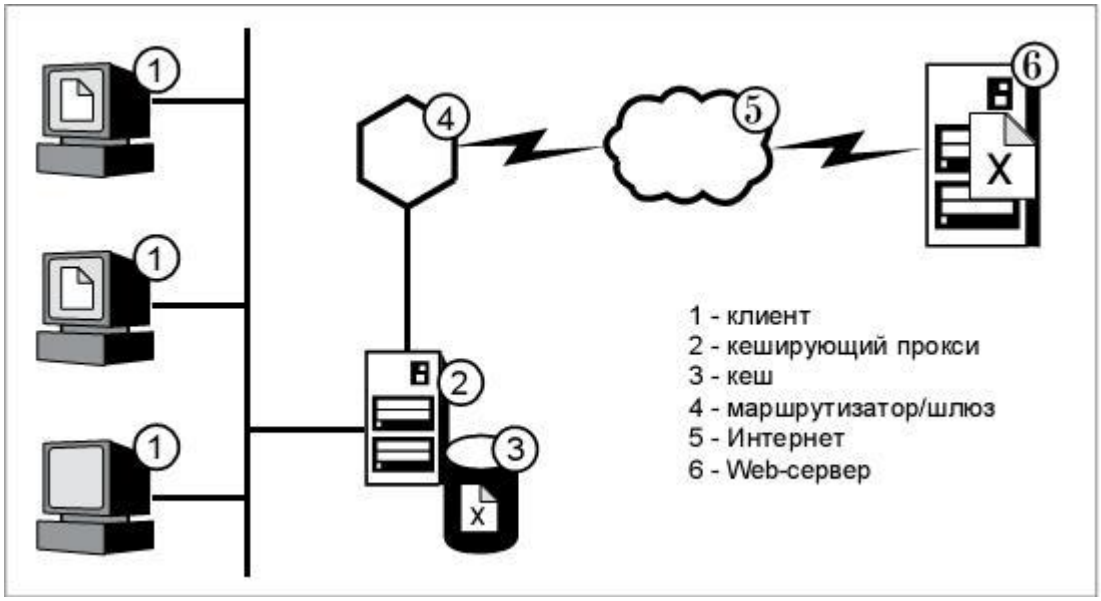


Рисунок - Кеширующий прокси, работающий как пересылающий прокси

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.

Обратные прокси

Разделение на зоны безопасности является ключевой концепцией при развертывании безопасной топологии. В этом контексте единственным, что позволяет делать обратный прокси, является обеспечение контролируемым и безопасным образом видимости находящегося позади прокси (как правило, во внутренней зоне) более чувствительного контента, без наличия реального необработанного контента, баз данных и т. д., показываемых во внешней зоне.

Обратные прокси имеют много общего кода с пересылающими прокси: фактически одни и те же продукты могут быть сконфигурированы одним или другим образом либо двумя сразу! Однако с функциональной и практической точки зрения в нашем случае мы рассматриваем обратные прокси как полностью другой инструмент.

Обратные прокси прозрачны, отчасти по определению. За обратным прокси пользователь вообще не знает о своем общении с прокси-сервером. Пользователь полагает, что общается с реальным предметом – сервером, на котором находится контент.

Пользователь не только будет думать о том, что он общается с сервером, на котором находится контент, но и может взаимодействовать и проходить аутентификацию на обратном прокси и быть субъектом по отношению к его политикам.

Обратные прокси обычно избраны и реализованы в целях обеспечения изоляции контента и зон. Однако, вы можете также добавить в обратные прокси функциональные возможности по кешированию для обеспечения производительности заодно с преимуществами обеспечения безопасности.

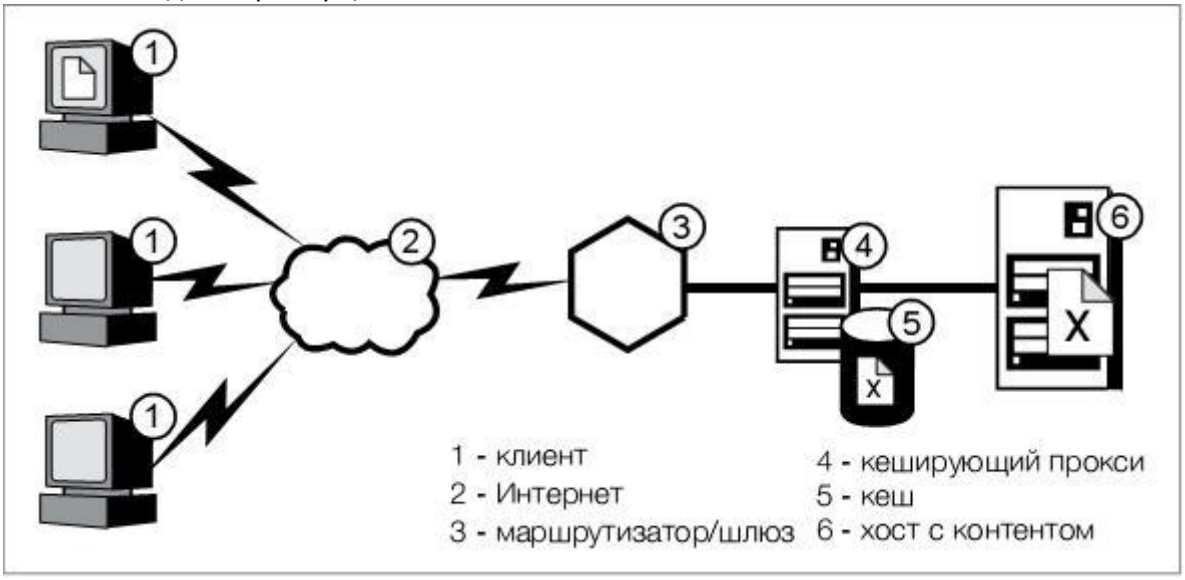


Рисунок - Типичный обратный прокси

Важным мотивом кеширования с помощью обратного прокси является разгрузка от подачи статического, кешируемого контента от конечных серверов приложений. Это позволит зачастую более дорогим конечным серверам приложений немного освободиться и сфокусировать свое внимание на пропускных способностях своих процессоров при выполнении более сложных динамических задач и задач, связанных с транзакциями.

Однако когда на обратном прокси разрешено кеширование, важным становится обеспечение его должной защиты. Весь контент, даже если он полностью статичен, продолжает нуждаться в защите. Вы же не хотите проснуться и обнаружить, что статическая и неконфиденциальная часть вашего Web-сайта была полностью уничтожена хакерами в кеше обратных прокси.

Серверы безопасности – обратные прокси *Reverse Proxies Secure Servers (RPSS)+ соединяют в одном блоке (или продукте) функции "чистых" обратных прокси и функции прокси обеспечения безопасности, которые были описаны ранее.

Зачастую такие продукты RPSS будут иметь в обратном прокси встраиваемый компонент, обрабатывающий запросы управления доступом и авторизации и объединенный с конечной системой управления доступом предприятия, которая фактически проверяет права пользователя или клиента на доступ и авторизацию.