ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ»

ФИЛИАЛ РГГУ В Г. ВОСКРЕСЕНСКЕ

Факультет управления

**ПРОКСИ-СЕРВЕР**

Контрольная работа по системе интернет

Студента 3 курса группы ДГМУ-3/5

Научный руководитель:

Воскресенск 2010

#### Оглавление

#### Глава 1. Определение прокси……………………………………………….3

#### Глава 2. Процесс сетевого посредничества…………………….…………..4

#### Глава 3. Типы прокси………………………………………………………..5

#### 3.1 Пересылающие прокси…………………………………………....5

#### 3.2 Прозрачные прокси……………………………………………….6

#### 3.3 Кэширующие прокси……………………………………………...7

#### 3.4 Прокси обеспечения безопасности……………………………….8

#### 3.5 Обратные прокси………………………………………………….9

#### 3.6 Обратные прокси и прозрачность………………………………10

#### 3.7 Обратные прокси с кэшем……………………………………….10

#### Заключение………………………………………………………………….12

#### Список источников и литературы ………………………............................14

#### 

#### Глава 1. Определение прокси

*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.

Прокси-сервер (известный также как шлюз приложений) представляет собой приложение, которое выступает для трафика в качестве посредника между доверенной сетью и недоверенной сетью. Это не снимает необходимости применения брандмауэра для управления трафиком на IP-уровне, чтобы не предусматривать наличие брандмауэра прикладного уровня.

Вы можете представить себе посредника как доверенное лицо или посла, которым предписано находиться где-то, где не может непосредственно находиться их клиент (или предпочитает не находиться) по причинам неудобства или безопасности. Послы обычно знают местный язык и обычаи, могут привести несовершенный запрос клиента в форму, допустимую в местном масштабе другой зоны, и, конечно, могут перевести обратно полученный ответ. В компьютерных понятиях такой "посол" может получать https-запросы по порту 443 и преобразовывать их в http-запросы по порту 80.

Прокси в более повседневных, практических компьютерных терминах являются процессами, запущенными на компьютерах, которым, как правило, предоставлен доступ (в брандмауэре) к более чем одной зоне. Именно эта способность делает их полезными. В типичном случае прокси просто будет работать от имени своего пользователя на месте перекрытия зон (в образе приложения), выполняя и получая нечто из зоны, с которой при других обстоятельствах запрещено устанавливать контакт или запрашивать что-либо со стороны отдельных процессов и пользователей из другой зоны.

С другой стороны, на прокси можно посмотреть с точки зрения "человека посередине". Как мы видели в предыдущих лекциях, одной из фундаментальных концепций всеобщей безопасности (не только в криптографии) является концепция атаки со стороны "(плохого) человека посередине", которая заключается в перехвате и ретрансляции передаваемой между двумя сторонами информации третьей, незваной, "плохой" стороной.

Прокси могут восприниматься как "хорошие" приемники (слушатели) информации или как "люди посередине". Это значит, что они перехватывают информацию, ретранслируют ее далее, но с некоторой предопределенной и полезной для сетевой инфраструктуры целью.

#### Глава 2. Процесс сетевого посредничества

Как правило, компьютерный прокси является базовым серверным процессом. Этот серверный процесс является слушателем, который "слушает" определенный порт (говорят также – связан с ним – bind), ожидая запросов по определенному протоколу. Когда установлено соединение с клиентом и получен правильный запрос, он "повторит" этот запрос другому серверу от имени клиента, как определено в его правилах для этого типа запросов. Когда от сервера получен ответ, прокси передает этот ответ назад пользователю или процессу клиента, которые ранее осуществили запрос, применяя все необходимые преобразования.

Если смотреть на вещи упрощенно, прокси на самом деле существуют во множестве различных продуктов. К примеру, большинство технологий порталов, которые сегодня легкодоступны, запрашивают контент от лица пользователя и компонуют его в отдельный "вид портала". Другим примером прокси являются "транзитные пересылки" Notes, которые существовали в Lotus Notes определенное количество лет и разрешали удаленный доступ в среды Notes на протяжении всех ранних лет развития Интернета. Тем не менее далее в этом разделе мы сосредоточим внимание на прокси в виде отдельных продуктов, так как наиболее часто используемым сегодня передовым опытом является применение отдельных прокси-сервисов.

##### Глава 3. Типы прокси

В этом разделе определены существующие на рынке различные типы прокси, применяемые в обычных инфраструктурах. Как было установлено ранее, зачастую предоставленное для прокси оборудование будет на самом деле выполнять или поддерживать множество типов прокси-сервисов. К примеру, прокси-сервер может предоставлять возможности кэширования и аутентификации в дополнение к основной функции обеспечения сетевого посредничества для приложений. Однако мы будем трактовать эти ключевые возможности прокси как отдельные типы прокси для облегчения дальнейшего рассмотрения.

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).

###### 3.1 Пересылающие 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.

###### 

###### 3.2 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. 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.

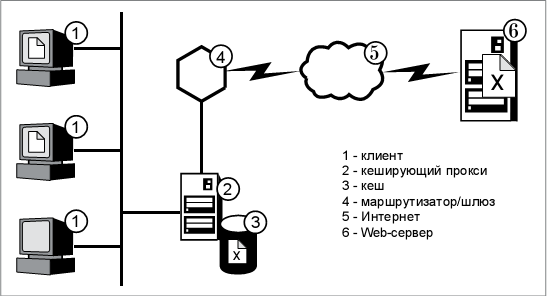
Прозрачные прокси сами по себе не являются на самом деле типом прокси, скорее любой прокси является либо прозрачным, либо объявленным по проекту.

###### 3.3 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".

В большинстве случаев пересылающие прокси конфигурируются также для работы в качестве кэширующих прокси. Это явление используется настолько часто, что компания IBM включила это в название компонента своего Edge Server: IBM Caching Proxy. На рис. 1 отображен типичный пересылающий и кэширующий прокси-сервер.



**Рис. 1** Кэширующий прокси, работающий как пересылающий прокси

###### 3.4 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.

Существует много различных продуктов и предложений, а также множество топологий на выбор, но с точки зрения выполнения прокси-функций безопасность является дополнительной функцией, которую может выполнять прокси.

В большинстве случаев функциональные возможности по обеспечению безопасности могут быть добавлены стандартному прокси в виде дополнительного программного модуля [plug-in (плагин)] (к примеру, IBM Tivoli WebSeal Plug-In для IBM WebSphere Edge Server). Существуют также и отдельные продукты, такие, как IBM Tivoli Access Manager for e-Business, которые служат только в качестве прокси обеспечения безопасности.

###### 3.5 Обратные прокси

Ранее в этой лекции мы установили, что 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.

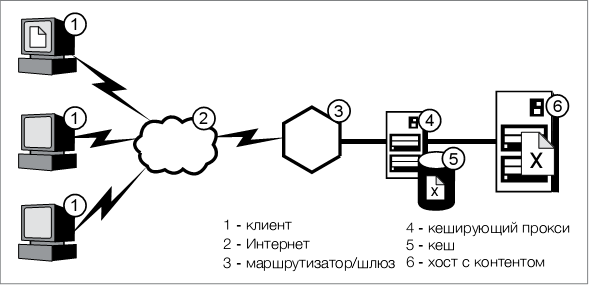
###### 3.6 Обратные прокси и прозрачность

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.

###### 3.7 Обратные прокси с кэшем

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



**Рис. 1** Типичный обратный прокси

Обратите внимание, что при этом виде сценария выигрыш в производительности за счёт кэширования относится к производительности сети, так как обычно обратный прокси расположен близко к конечному серверу. Важным мотивом кэширования с помощью обратного прокси является разгрузка от подачи статического, кэшируемого 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 кэширование, 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 кэше обратных прокси.

**ЗАКЛЮЧЕНИЕ**

*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:

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 ИСТОЧНИКОВ И ЛИТЕРАТУРЫ**

1) Макарова Информатика. Учебник для ВУЗов М.: Дрофа 2000

2) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы /В.Г. Олифер, Н.А. Олифер. - СПб.: Питер, 2002.- 672 с.: ил.

3) С. Симонович, Г. Евсеев, А. Алексеев. Специальная информатика. Учебное пособие. М.: «АЕ-ПРЕСС

4) [INTUIT.ru: Курс: Руководство по безопасности в Lotus Notes : Лекция № 5: Прокси-серверы](http://www.intuit.ru/department/security/seclotus/5/)