Многие администраторы сталкиваются с проблемой разумного использования времени и канала для выхода в сеть Интернет, задумываются о возможности экономии времени и денег, об ограничении скорости для отдельных видов файлов или личностей, в конце концов об экономии всего, что связано с теми или иными аспектами выхода в глобальную сеть. Я, с помощью этой статьи, попытаюсь наглядно и доходчиво объяснить о настройках самого распространенного прокси сервера - прокси сервера Squid. НАЧАЛЬНЫЕ НАСТРОЙКИ SQUID ДЛЯ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ Мы не будем вдаваться в процесс установки прокси сервера Squid, а перейдем сразу к его настройке. Самое элементарное, что нам после установки следует сделать, так это разрешить доступ пользователям нашей локальной сети. Для этого служат параметры http_port, http_access. Кроме этого, мы заведем acl (список контроля доступа) для нашей локальной сети. И так, http_port нам нужен постольку, поскольку наш прокси сервер Squid должен обслуживать только компьютеры нашей локальной сети и быть невидимым для внешнего мира, дабы исключить возможность "плохим людям" внешней сети воспользоваться нашим каналом или трафиком, а в случае, если будут обнаружены "дыры" в коде прокси сервера Squid, воспользоваться ими. Параметр http_access используется для разрешения или запрещения доступа к определенным ресурсам, определенным адресам либо с определенных адресов, к определенным сайтам, по определенным протоколам, портам и всему тому, что непосредственно указано с помощью Acl (списков контроля доступа). Таблица N 1. Некоторые подсети.

|Диапазон адресов |Полная форма |Краткая форма

192.168.0.1-192.168.0.254 192.168.0.0/255.255.255.0 192.168.0.0/24

192.168.20.1-192.168.20.254 192.168.20.0/255.255.255.0 192.168.20.0/24

192.168.0.1-192.168.254.254 192.168.20.0/255.255.0.0 192.168.20.0/16

10.0.0.1-10.254.254.254 10.0.0.0/255.0.0.0 10.0.0.0/8 Предположим, что у Вас сеть с адресами от 192.168.0.1 до 192.168.0.254, тогда добавим новый Acl (см. таблицу N1): acl LocalNet src 192.168.0.0/24 Предположим, что у Вас прокси сервер Squid расположен по адресу 192.168.0.200 на порту 3128, тогда пишем в файле конфигурации: http_port 192.168.0.200:3128 Следующим нашим действием будет запрет использования нашего прокси сервера, кроме как пользователями нашей локальной сети: http_access allow LocalNet http_access deny all В данном случае слово allow является разрешением, а слово deny запрещением, то есть мы разрешаем доступ к прокси серверу Squid с адресов нашей локальной сети и запрещаем доступ всем остальным. Будьте внимательны, указывая http_access, так как Squid использует их в порядке указания Вами. ИЗУЧАЕМ ACL (СПИСКИ КОНТРОЛЯ ДОСТУПА) Система управления доступом в прокси сервере Squid является очень

гибкой и обширной. Она состоит из элементов со значениями и списков доступа с указанием allow (разрешение) или deny (запрещение). Формат Acl следующий: acl имя элемент список Формат списка доступа: http_access указание имя_acl Мы рассмотрим некоторые элементы, которые позволяет использовать прокси сервер Squid, конечно же с примерами: * acl имя src список С помощью этого элемента (src) мы указываем IP-адрес источника, то есть клиента от которого пришел запрос к нашему прокси серверу. В следующем примере мы разрешим Васе Пупкину (Pupkin) и отделу программирования (Progs) доступ к нашему прокси серверу, а всем остальным запретим: acl Progs src 192.168.0.1-192.168.0.9 acl Pupkin src 192.168.0.10 http_access allow Progs http_access allow Pupkin http_access deny all * acl имя dst список Данный элемент (dst) указывает IP-адрес назначения, то есть IP-адрес того сервера, доступ к которому желает получить клиент прокси сервера. В следующем примере мы запретим Васе доступ к подсети 194.67.0.0/16 (к примеру, в ней находится тот же aport.ru): acl Net194 dst 194.67.0.0/16 http_access deny Pupkin Net194 * acl имя dstdomain список С помощью этого элемента (dstdomain) мы указываем домен, доступ к которому желает получить клиент прокси сервера. В следующем примере мы запретим Васе доступ к варезным сайтам nnm.ru и kpnemo.ru: acl SitesWarez dstdomain .nnm.ru .kpnemo.ru http_access deny Pupkin SitesWarez В случае, если будет необходимо указать домен источника, то используйте srcdomain. * acl имя [-i] srcdom_regex список * acl имя [-i] dstdom_regex список Данные элементы отличаются от srcdomain и dstdomain лишь тем, что в них используются регулярные выражения, которые в данной статье мы не рассматриваем, но пример всё-таки приведём: Acl SitesRegexSex dstdom_regex sex Acl SitesRegexComNet dstdom_regex .com$ .net$ http_access deny Pupkin SitesRegexSex http_access deny Pupkin SitesRegexComNet В данном примере мы запретили доступ Пупкину Василию на все домены, содержащие слово sex и на все домены в зонах .com и .net. Ключ -i призван игнорировать регистр символов в регулярных выражениях. * acl имя [-i] url_regex список С помощью этого элемента (url_regex) мы указываем шаблон регулярного выражения для URL. Пример указания файлов с расширением avi, начинающихся на слово sex: acl NoAviFromSex url_regex -i sex.*.avi$ В случае, если Вы желаете указать шаблон только для пути URL, то есть исключая протокол и имя хоста (домена), то используйте urlpath_regex. Пример для указания музыкальных файлов: acl media urlpath_regex -i .mp3$ .asf$ .wma$ * acl имя_acl port список Указание номера порта назначения, то есть порта, к которому желает подключится клиент нашего прокси сервера. Как пример, запретим всем использование программы Mirc через наш прокси сервер: Acl Mirc port 6667-6669 7770-7776 http_access deny all Mirc * acl имя_acl proto список Указание протокола передачи. Как пример, запретим вышеупомянутому Васе использование протокола FTP через наш прокси сервер: acl ftpproto proto ftp http_access deny Pupkin ftpproto * acl имя_acl method список Указание метода http запроса клиентом (GET, POST). Возьмем ситуацию, когда следует запретить Васе Пупкину просматривать его почту на сайте mail.ru, но при этом разрешить прогуливаться по сайту без запретов, то есть запретить Васе возможность войти в свой почтовый ящик через форму входа на сайте: acl SiteMailRu dstdomain .mail.ru acl methodpost method POST http_access deny Pupkin methodpost SiteMailRu

ОГРАНИЧЕНИЯ ПОЛЬЗОВАТЕЛЕЙ Достаточно часто в нашей стране возникает ситуация, что канала доступа в глобальную сеть Интернет на всех пользователей не хватает и возникает желание дать каждому по максимуму, но при этом не дать каналу "загнуться" из-за любителей позагружать файлы. Средства прокси-сервера Squid позволяют этого добится несколькими путями: - первый путь это оптимизация кеширования объектов; - второй - это ограничение по времени определенных пользователей, что не совсем корректно; - третий путь заключается в ограничении скорости для определенных типов файлов, пользователей и всего того, что определено нами через Acl. ОГРАНИЧЕНИЯ ПО ВРЕМЕНИ Ограничить пользователей по времени можно следующим образом: acl имя time дни чч:мм-ЧЧ:ММ Где день: M - Понедельник, T - Вторник, W - Среда, H - Четверг, F - Пятница, A - Суббота, S - Воскресенье. При этом чч:мм должно быть меньше чем ЧЧ:ММ, то есть можно указать с 00:00-23:59, но нельзя указать 20:00-09:00. Давайте запретим всё тому же Васе иметь доступ в сеть Интернет с 10 до 15 часов каждый день: acl TimePupkin time 10:00-15:00 http_access deny Pupkin TimePupkin Если хочется разрешить Васе пользоваться программой Mirc с 13 до 14 часов, то пишем: acl TimePupkin time 13:00-14:00 http_access allow Pupkin TimePupkin Mirc http_access deny Pupkin Mirc А что делать, если необходимо запретить или разрешить в определенные дни недели? Squid также позволяет это сделать, к примеру с 13 до 14 в понедельник и в воскресенье: acl TimePupkin time MS 13:00-14:00 Как видите, ничего сложного в этом нет. ОГРАНИЧЕНИЯ ПО СКОРОСТИ Регулировка скорости в прокси сервере Squid осуществляется с помощью пулов. Пул - это своего рода бочонок с пивом, в который пиво постоянно заливают до краёв, а клиенты наливают в свои стаканы или иные ёмкости для дальнейшего внутреннего потребления по мере надобности через свои персональные краны. Пулы регулируются с помощью трех параметров: delay_class, delay_parameters, delay_access. Количество пулов указывается с помощью параметра delay_pools. Пулы могут быть трёх классов: 1. Весь поток пива ограничен одним краном (на всю сеть). 2. Весь поток пива ограничен одним краном, но при этом кран делится на подкранчики (на каждый IP). 3. Весь поток пива ограничен одним краном, но кран делится на подкранчики (на подсети), которые также делятся на мини кранчики (на каждый IP). Форматы: delay_pools количество_объявленных_пулов delay_access номер_пула действие имя_acl действие может быть allow (разрешить) и deny (запретить). При этом, данный пул действует на тех, кому он разрешен и не действует на тех, кому он запрещен. В случае, если указано allow all, а затем deny Pupkin, то на Пупкина данный класс всё-равно подействует, т.к. IP-адрес Пупкина объявленный в acl Pupkin, входит в список адресов acl all. Имейте это ввиду. delay_class номер_пула класс_пула delay_parameters номер_пула параметры параметры отличаются в зависимости от класса пула: для первого класса: delay_parameters 1 байт_на_всю_сеть для второго класса: delay_parameters 1 на_всю_сеть на_клиента для третьего класса: delay_parameters 1 на_всю_сеть на_подсеть на_клиента Для примера, у нас канал на 128 Кбит (в среднем 15 Кбайт в секунду) и мы желаем Васе (Pupkin) дать всего 4 Кбайта/сек (на все про всё один маленький бокальчик), отделу программирования (Prog) дать всего 10 Кбайт/сек и на каждого всего по 5 Кб/сек (всего два бокальчика), всех остальных ограничить в 2 Кбайта/сек на каждого и 10 Кб/сек на всех, а файлы mp3

(media) ограничить в 3 Кбайта в секунду на всех (на всю бочку пива такой маленький кран). Тогда пишем: acl Prog src 192.168.0.1-192.168.0.9 acl Pupkin src 192.168.0.10 acl LocalNet src 192.168.0.0/255.255.255.0 acl media urlpath_regex -i .mp3$ .asf$ .wma$ delay_pools 4 # сначала ограничим mp3 delay_class 1 1 delay_parameters 1 3000/3000 delay_access 1 allow media delay_access 1 deny all # ограничим бедного Васю delay_class 2 1 delay_parameters 2 4000/4000 delay_access 2 allow Pupkin delay_access 2 deny all # ограничим отдел программирования delay_class 3 2 delay_parameters 3 10000/10000 5000/5000 delay_access 3 allow Prog delay_access 3 deny all # а теперь ограничим остальных (второй класс пула) delay_class 4 2 delay_parameters 4 10000/10000 2000/2000 delay_access 4 deny media delay_access 4 deny Pupkin delay_access 4 deny Prog delay_access 4 allow LocalNet delay_access 4 deny all Часто возникает вопрос, а как лучше всего использовать столь малый канал, чтобы он автоматически делился между всеми теми, кто в данный момент что-либо загружает? На этот вопрос имеется однозначный ответ - средствами прокси сервера Squid этого сделать не возможно, но всё-таки кое-что предпринять можно: delay_class 1 2 delay_parameters 1 -1/-1 5000/15000 delay_access 1 allow LocalNet delay_access 1 deny all Таким образом мы выделяем на всю нашу сеть и на подсети максимальный канал (-1 означает неограниченность), а каждому пользователю даем скорость максимум в 5 Кб/сек после того, как он скачает на максимальной скорости первые 15 Кбайт документа. Таким образом клиент не съест весь канал, но достаточно быстро получит первые 15 Кбайт. ОПТИМИЗИРУЕМ КЕШИРОВАНИЕ ОБЪЕКТОВ В SQUID ---------- Существует множество типов файлов, которые обновляются не достаточно часто, чтобы позволить прокси серверу реагировать на заголовки от вебсерверов о том, что данный объект не подлежит кешированию либо он был на удивление только что изменён. Это довольно частая ситуация. Для разрешения таких ситуаций призван параметр refresh_pattern в файле настроек прокси-сервера Squid, но полностью с формулами и т.п. мы его рассматривать не будем. Формат: refresh_pattern [-i] строка МИНВ процент МАКСВ параметры Данный параметр используется для того, чтобы определить возраст объекта (считайте файла) в кеше, следует ли его обновлять или нет. МИНВ (минимальное время) - время в минутах, когда объект, имеющийся в кеше считается свежим. МАКСВ (максимальное время) - максимальное время в минутах, когда объект считается свежим. Параметры - это один или несколько следующих параметров: - override-expire - игнорировать информацию об истечении свежести объекта и использовать МИНВ. - override-lastmod - игнорировать информацию о дате изменения файла и использовать МИНВ. - reload-into-ims - вместо запроса клиентского запроса "не кешировать документы" (no-cache) посылать запрос "Если изменен с" (If-Modified-Since) - ignore-reload - игнорировать запросы клиентов "не кешировать документы" (no-cache) или "перезагрузить документ" (reload). И так, мы подошли к самом главному. Ну, так какие же типы файлов реже всех обновляются? Как правило, это разнообразные музыкальные файлы и картинки. Установим свежесть объектов, для этого для картинок и музыкальных файлов укажем, скажем так для примера, целых 30 дней (43200 минут): refresh_pattern -i .gif$ 43200 100% 43200 override-lastmod override-expire refresh_pattern -i .png$ 43200 100% 43200 override-lastmod

override-expire refresh_pattern -i .jpg$ 43200 100% 43200 override-lastmod
override-expire refresh_pattern -i .jpeg$ 43200 100% 43200 override-lastmod
override-expire refresh_pattern -i .pdf$ 43200 100% 43200 override-lastmod
override-expire refresh_pattern -i .zip$ 43200 100% 43200 override-lastmod
override-expire refresh_pattern -i .tar$ 43200 100% 43200 override-lastmod
override-expire refresh_pattern -i .gz$ 43200 100% 43200 override-lastmod
override-expire refresh_pattern -i .tgz$ 43200 100% 43200 override-lastmod
override-expire refresh_pattern -i .exe$ 43200 100% 43200 override-lastmod
override-expire refresh_pattern -i .prz$ 43200 100% 43200 override-lastmod
override-expire refresh_pattern -i .ppt$ 43200 100% 43200 override-lastmod
override-expire refresh_pattern -i .inf$ 43200 100% 43200 override-lastmod
override-expire refresh_pattern -i .swf$ 43200 100% 43200 override-lastmod
override-expire refresh_pattern -i .mid$ 43200 100% 43200 override-lastmod
override-expire refresh_pattern -i .wav$ 43200 100% 43200 override-lastmod
override-expire refresh_pattern -i .mp3$ 43200 100% 43200 override-lastmod
override-expire Показанные Выше настройки лишь пример, для того, чтобы была понятна суть. Теперь можете проверить эффективность своего прокси сервера, она уж точно возрастет. ЗАКЛЮЧЕНИЕ Прокси сервер Squid не является одним лишь распространенным прокси сервером, существуют и другие. Но как показывает статистика, большинство используют именно этот прокси сервер, но при этом всё равно у многих начинающих возникают проблемы с настройкой. С помощью этой статьи я попытался хоть немного раскрыть для обширных масс некоторые функции прокси сервера Squid.

Забудкин Лев Мирославович, Россия, Тюменская область, Г. Нижневартовск, ведущий программист МУ "Библиотечная-информационная система" zabudkin@mail.ru http://zabudkin.com