Отфильтрованные (update)

Как бы ни относиться к идее фильтрации российского сегмента всемирной сети, как говорится Dura lex sed lex. Если поставлена задача фильтровать - значит нужно фильтровать. Следовательно, необходимо найти техническое решение поставленной задачи. В данной статье будет описание того, как это делается и описание существующих систем фильтрации в сравнительных характеристиках с целью найти оптимальное решение.

Небольшое дополнение к статье:

Автор статьи получил массу обратной связи к данной статье. Прежде всего, письма касались того, что перечислены не все продукты, которые выполняют функцию фильтрации в соответствии со 139-ФЗ. Да, это так. В статье не упомянуты:

- Компания РусПромСофт из Нижнего Новгорода с продуктом "Барьер 139-ФЗ"
- Компания EntenSys (Новосибирск) с решением UserGate Web Filter

Думается, что на просторах одной седьмой части суши имеется еще некоторое число компаний и решений, которые в данный обзор не попали по причине малой образованности автора. Но на то и нужен интернет, и сайт Nag.ru, чтобы собрать как можно больше нужной и полезной информации и докопаться до истины.

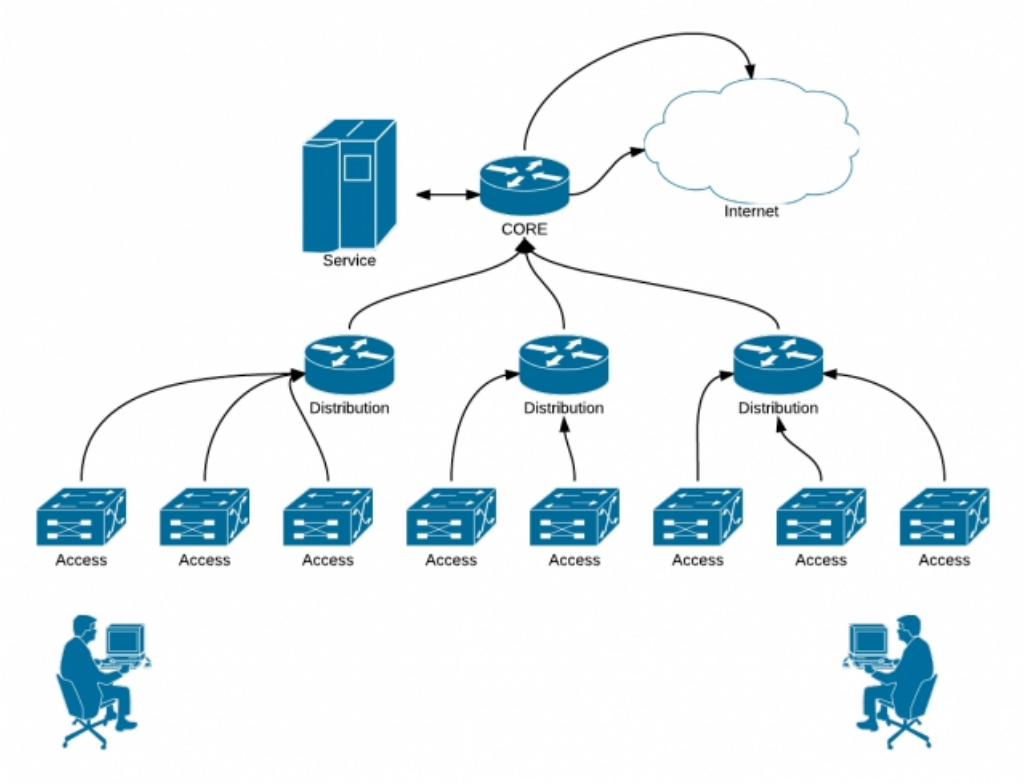
Второй вопрос был связан с некоторыми неточностями допущенных в статье. В основном они касались того, что тот или иной продукт был "описан не правильно" и поступали просьбы исправить "неточности". К сожалению, уже поздно. Статья была проиндексированна поисковиками и скопирована на многие другие ресурсы. Мы не в силах это исправить. Но за факты приведенные в статье автор готов поручиться - если на официальном сайте в описании продукта не было описания той или иной функции, то автор не должен нести за это ответственности - нужно просто внимательнее относиться к таким публикациям. Кроме того, в статье несколько раз упоминалось, что это субъективный обзор, отражающий мнение автора и только. Статья не руководство к немедленной покупке и не гид по системам фильтрации. Это просто статья, где собраны и описаны факты из открытых источников информации и официальных ресурсов.

Автору этой статьи разработчики могут написать по электронной почте klimarev[at]gmail[dot]com. И даже настоятельно рекомендуется это сделать, ибо готовится вторая часть материала, но уже не как обзорная, но с протестированными продуктами, таблицами и объективными рейтингами.

Начнем с описания задачи по принципу "как это работает" от печки. Некоторым описание может показаться несколько упрощенным и недостойным траты времени - что же. Можно пропустить часть текста и сразу перейти в конец статьи с описанием существующих на рынке систем. Причем, поддавшись модному тренду импортозамещения программного обеспечения, обозревать мы будем исключительно системы российского производства.

Как это работает

Для того чтобы понять суть™ фильтрации, приведем принципиально-техническую схему типичного Интернет-провайдера:



Очень поверхностно эту схему можно описать так:

Юзеры, сидящие в позе мыслителя за своими терминалами, подключены физическим кабелем к коммутаторам, обычно установленным в подъезде дома. Коммутаторы доступа (Access) объединяются в ветки на маршрутизаторы (или управляемые коммутаторы) в уровень, который называется "агрегация" (distribution). И уже все каналы от агрегации стекаются в уровню, который называется "ядро" (Core).

Чуточку подробнее про "ядро". Это такой хороший мощный маршрутизатор (или кластер их), способный перемалывать весь трафик от пользователей и отправлять запросы/ответы в "большой интернет". Рядом нарисован сервер, где пользователям могут оказываться всяческие услуги - дополнительные или основные. Например, учет времени и денег пользователя - это сервис "биллинг". При этом решение пускать или не пускать конкретного пользователя дальше в сеть принимается именно на уровне ядра в service и исполняется центральным маршрутизатором "Core".

Еще один момент, который нам понадобится в дальнейшем - обратите внимание, что от маршрутизатора "Core" к облаку "интернет" отходит два отростка. Это магистрали в большой интернет. Обычно у нормального провайдера таких магистралей минимум две. Бывает и больше. Смысл в том, чтобы зарезервировать магистральный доступ от всевозможных неприятностей, связанных с пьяными экскаваторщиками, отключением электроэнергии и прочими действиями лиц интеллектуального большинства и/или стихий.

В общем и целом, мне в три абзаца удалось рассказать, как устроен провайдер. Теперь перейдем к теме повествования. А именно, поразмышляем, где в этой схеме нам установить то самое хитрое устройство, которое будет непущать и запрещать пользователям осуществить доступ к неправоверной информации.

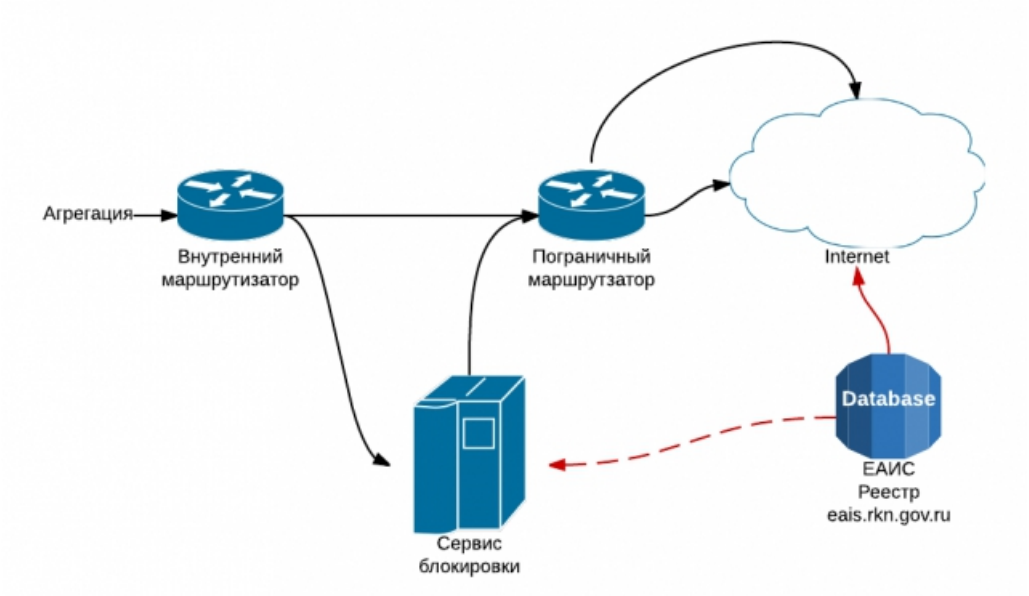
Вполне логично было бы, в соответствии с целями закона, который, напомню, называется «*О внесении изменений в Федеральный закон „"О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет*», установит фильтры на компьютерах пользователей. Ибо далеко не все пользователи являются детьми, а защищать взрослого как ребенка несколько неоптимально (я долго подбирал тут слово и остановился на эдаком политкорректном слове). Но очевидно, что у регулятора несколько другой взгляд на окружающий мир и этот вариант был отвергнут. Хотя услуга "детский интернет" предлагается пользователям добрых полтора десятка лет, а также была сформирована целая экосистема средств защиты детей от неподобающей информации из "дикого интернета".

Следующим логичным местом установки фильтра является магистральный оператор связи. Таких операторов значительно меньше в общей массе, я оцениваю количество таковых в ≈500 штук живых организаций на всю страну, а магистральных примерно с десяток. Но тут у регулятора не оказалось метрики дифференциации - лицензии у всех одинаковые, что у магистральных/оптовых, что у

розничных районных провайдеров. Кто же их будет делить - этому нужна система фильтрации, а этому не нужна.

Очевидно, что мозг у регулятора кипел не на шутку, и в итоге был выпущен нормативно-правовой акт, обязывающий фильтровать контент всем операторам, имеющим лицензии на оказание услуг доступа в интернет - и большим, и малым. Причем, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее - Роскомнадзор или РКН) очень ответственно отнеслась к возложенной на них государственной обязанности. Реестр пополняется ежедневно, а выгрузку реестра контролируют по каждому в отдельности оператору с помощью нехитрой информационной системы.

Итак, техническое решение по фильтрации трафика от неугодного контента выглядит следующим образом:



На уровне Core у провайдера должно стоять два маршрутизатора: один занимается внутренними делами (например, собирает трафик с уровня агрегации в один поток), другой внешними относительно провайдера - разруливает этот трафик по магистралам. Еще раз - это очень упрощенная схема предназначена для образовательных целей и общего понимания. Понятно, что в реальной реализации схема будет сильно отличаться в зависимости от оператора, его величины, географии обслуживания и прочих факторов объективно существующей реальности.

Сервис блокировки размещается физически на тех самых серверах, которые были приведены в общей схеме, а информацию о запрещенных ресурсах этот сервис получает из интернет в виде специального XML-файла, который скачивается с сервера РКН через интернет. Чтобы получить этот файл, оператор должен быть зарегистрирован в ЕАИС "Реестр", а доступ к нему осуществляется через электронно-цифровую подпись.

Далее начинается интересное. Дело в том, что фильтровать трафик можно тремя способами: по IP-адресу (простой способ), DNS-фильтрация и конкретному адресу (url), введенному пользователем в адресной строке браузера. В конечном итоге все сводится к IP-адресам, но в первом случае достаточно внести IP-адреса в таблицу маршрутизации "внутреннего маршрутизатора" и все "айпишники", не допущенные "министерством правды" к просмотру в демократической стране, будут полностью недоступны. Включая ресурсы, которые имели неосторожность разместиться на том же сервере, что и запрещенный сайт.

Статистика "случайно заблокированных" ресурсов выглядит так:



Более подробно смотрите на сайте РуБлэкЛист

Второй способ фильтрации - по доменным именам. Он чуточку сложнее, но столь же несовершенен. Этот способ базируется на одном из главнейших протоколов современного Интернета - DNS. Его суть сводится к тому, что запрет осуществляется (устанавливается - лучше) на доменное имя, которое резолвится (разрешается) в тот же самый IP-адрес - нужно просто запретить нехорошим сайтам превращать http-запрос в конкретный IP-адрес и/или подставлять вместо него специальную заглушку. Недостаток тот же - если на некоем неправильном ресурсе имеется одна нехорошая страница, которую нельзя смотреть, то запрещается сайт целиком. Например, весь ЖЖ или Вконтакт из-за одного наркоманского поста. Самое простое (и БЕСПЛАТНОЕ) решение по блокировке данным способом есть у Яндекса - http://dns.yandex.ru. Причем, оно несколько более совершенное, ибо блокирует не только (и не столько) реестр, сколько действительно делает Сеть безопаснее для пользователя. Я бы рекомендовал частным пользователям пользоваться этим сервисом (хотя некоторые меня сейчас в комментариях подвергнут обструкции).

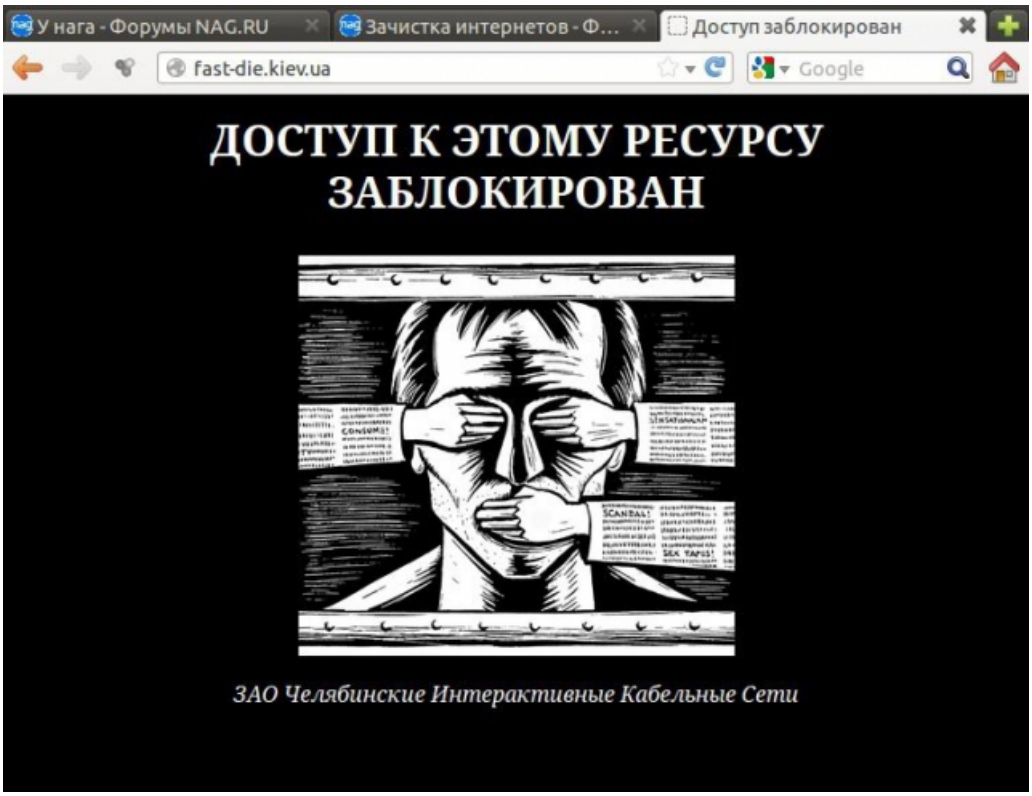
Наиболее совершенный (если этот термин применим к цензуре) из существующих способов блокировки - запрет на конкретный интернет-адрес url. То есть, если на некоем сайте http://bad-site.com существует страничка с нехорошим содержанием, то заблокируется только эта самая страничка, а остальные материалы сайта будут доступны.

И здесь имеется технологическая проблема в проверке на разрешенность каждого введенного пользователем адреса. А это не самая тривиальная задача, ибо слушать нужно весь трафик и сравнивать его с "черным списком". И пусть алгоритм незамысловат, но если представить себе количество ежесекундно вводимых (клик по ссылке - url ушел в запрос) пользователями адресов, то вычислительные возможности сервиса блокировки потребуются нехилые. А это а) деньги, требуемые на покупку оборудования плюс программное обеспечение и б) скорость отклика на каждый клик пользователя будет хоть и чуточку, но ниже.

Техническое решение проблемы, разумеется, нашлось. Почти все системы фильтрации у провайдеров работают теперь следующим образом:

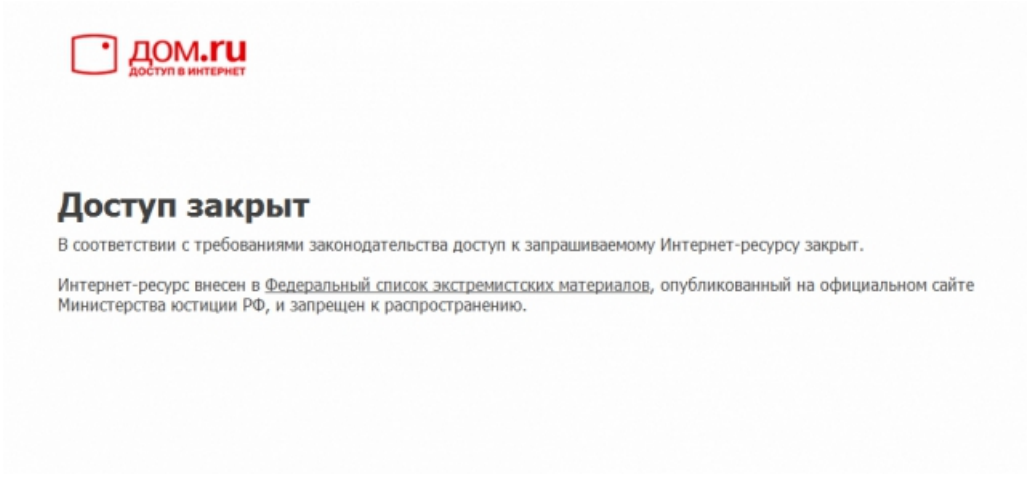
1. На внутренний маршрутизатор подается специально подготовленная сервисом блокировки таблица IP-маршрутизации, которая содержит все IP-адреса занесенные в реестр, включая и те, которые должны фильтроваться по url, и те, которые блокируются жестко по IP.
2. Если пользователь вводит хороший годный адрес, который ни в каком виде не присутствует в реестре, то такой трафик с адреса проходит прямиком на пограничный (border) маршрутизатор без участия реестра.
3. Ежели адрес входит в пул подозрительных, то трафик заворачивается на сервис фильтрации, где происходит его дальнейшая обработка.
4. … которая заключается в том, что http-запрос сравнивается с табличкой запрещенного и обрабатывается в соответствии с алгоритмом, заложенным разработчиком - не включенные в реестр ссылки пропускаются дальше на border, а вместо крамолы демонстрируется экран "HALT!"

Вот такой, например:



Кстати, реквестирую больше скриншотов в мою коллекцию экранов блокировки. БОЛЬШЕ!

И, кстати, я лично нахожу, что такие экраны должны быть более креативными и интересными. Ну, право слово, видеть вот такое скучно и не полезно:



Гораздо приятнее увидеть что-то более информативное на таких экранах. Например, ссылку "как обойти блокировку", описанную Артемом Козлюком, или цитату из ст. 29 Конституции Российской Федерации, или описание того, как борются с противоправным контентом в других странах, или веселый ролик из Ютюба. В общем, чтоб пользователю было, если не полезно, то хотя бы познавательно. Описание вреда наркотиков со ссылкой на блог Ройзмана, например.

Но чуточку отвлеклись...

Итак, нехитрая схема блокировки не всего трафика, а выборочно, по таблице маршрутизации позволяет весьма нехило экономить на вычресурсах и сделать систему чуточку надежнее - в случае выхода из строя сервиса блокировки, трафик просто потечет прямо (схема называется "байпас"), пока доблестные инженеры героически восстанавливают работоспособность системы.

Экономия составляет вполне себе ощутимые цифры - по сведениям, предоставленных непосредственными разработчиками и эксплуатантами системы, на гигабитный общий трафик, трафик по сервису составляет единицы мегабит. То есть, это сотые доли процента, что позволяет обходиться малой кровью и не тратить сотни денег на системы DPI. Посему, в данном обзоре будут представлены только и исключительно системы фильтрации, а не системы анализа трафика. Впрочем, вопросы сообществу я задам в самом конце, а мы продолжим.

Кто есть кто

Рынок фильтрации контента по ФЗ-139 на сегодня представлен четырьмя игроками:

- SkyDNS (Екатеринбург)
- Carbon Soft (Москва)
- МФИ Софт с решением "Периметр-Ф" (Нижний Новгород)
- СКАТ "Система контроля и анализа трафика" от VAS Expert (Санкт-Петербург)

Возможно, кого-то пропустил / не заметил - прошу производителей соответствующих решений отписаться в комментариях, я обязательно исправлюсь в последующем и включу вас в "лист наблюдения". Но это относится только к российским разработчикам, ибо политика партии такова.

Кстати, первый и последний (в списке, а не вообще!) разработчики представлены в Shop.Nag.Ru и купить эти решения вы сможете легко через менеджеров Нага - страничка SkyDNS и страничка СКАТ соответственно. Велкам!

Почти все решения выполнены по "классической схеме", описанной выше. То есть сначала производится предфильтрация на внутреннем маршрутизаторе, а весь некошерный поток обрабатывается "в чистую" уже на сервере, установленном в стойку.

Однако существуют попытки создать так называемый "облачный сервис", что на мой субъективный взгляд является маркетинговой уловкой, ибо объем трафика у боле-менее крупного интернет-прова достаточно велик, чтобы прокачивать весь массив данных через сервера "в облаке" - это просто бессмысленно, сначала собрать весь трафик в один поток, отправить его куда-то далеко, обработать менее промилле от его общего объема, и загнать в "паблик-интернет". Возможно, это имеет смысл для небольших организаций, но в этом случае, очевидно, будут расти задержки и джиттер. Кроме того, появляется еще одна точка отказа, на которую клиент не сможет повлиять, несмотря на всяческие заверения поставщика услуги и подписанные жесткие SLA. Впрочем, облачная схема может быть более чем интересна, повторюсь, корпоративным клиентам, у которых отсутствует в достаточной мере квалифицированный персонал, способный внедрить и эксплуатировать системы фильтрации in house, но насущная необходимость в этом есть. Те же школы и образовательные учреждения, например.

В данной статье нет рекомендаций и результатов теста класса "лучше/хуже". Это просто описание существующих решений. Если публике будут интересны результаты именно тестов - маякните в комментариях. А мы постараемся связаться со всеми заинтересованными сторонами и организовать такое тестирование с методиками и метриками.

Кроме того, данный обзор базируется исключительно на открытой и доступной в Сети информации. Никакого “инсайда” и/или непроверенной информации здесь вы не найдете.

SkyDNS

Екатеринбургский разработчик SkyDNS начал заниматься фильтрацией задолго до того, как это стало мейнстримом - компания разрабатывает системы безопасности и контент-фильтры для госучреждений с 2009 года. С выходом упомянутого закона вышли на рынок систем для интернет-провайдеров, что весьма логично и правильно - если имеется наработанный опыт и отлаженные решения, то использовать их является эффективной стратегией.

В портфеле решений SkyDNS имеется линейка продуктов всего спектра от "для частных лиц" до операторских решений. Особняком стоит решение для фильтрации в учебных заведениях, где степень параноических настроений сильно зависит от политизированности руководства в управлении образования и упоротости региональной прокуратуры.

Собственно решение для контент-фильтрации в интернет-провайдере рассчитано на среднего и малого оператора - разработчик на своем сайте утверждает, что могут фильтровать потоки "до 80 Gbps". Очевидно, что смогут сделать и больше, но это уже проектные работы, за которые парни с удовольствием возьмутся, но за другие деньги.

СКФ работает по описанной выше схеме:

Софт с оригинальным названием "SkyDNS Zapret ISP" скачивает реестр запрещенных ресурсов с eais.rkn.gov.ru (ЭЦП, разумеется, присутствует) и разрешает домены из реестра в IP-адреса. Далее, таблица полученных адресов в виде OSPF-маршрутов выгружается на подключенный внутренний маршрутизатор, и полученные IP-адреса перенаправляются на систему фильтрации с указанием себя в качестве next-hop. Остальной трафик не меняет маршрут следования.

Выбор OSPF-маршрутизации связан с тем, что большинство провайдеров используют для маршрутизации во внутренней сети именно этот протокол. При необходимости возможно использование протокола BGP.

Весь трафик, который был определен как "необходимо фильтровать", попадает в систему фильтрации, но по URL фильтруется только трафик, который идет на порт 80/tcp. Остальной трафик можно либо пропускать без изменений, либо выборочно уничтожать или перенаправлять. Ответы на пропущенный без изменений трафик идут через сеть напрямую к клиентам (асимметричная маршрутизация).

Перенаправленный на систему фильтрации по URL трафик (запросы на порт 80/tcp на IP-адреса запрещенных ресурсов) обрабатывается системой фильтрации по URL, которая работает в режиме прозрачного прокси-сервера. Разрешенные запросы пропускаются. На запросы, попадающие под регулярное выражение, сформированное из запрещенного URL, выдается страница блокировки. В случае попытки пользователем обойти систему фильтрации путем перестановки местами параметров в URL, такой URL попадет под регулярное выражение и пользователю будет выдана страница блокировки.Достаточно просто.

Собственно система поставляется в виде установочного образа для установки на "пустую" машину, включая виртуальную. Система, установленная на тестовую машину Quad Core Xeon E5606, 2,13 GHz с 2 Гб RAM при загрузке CPU в 50-70% обеспечивала поток в 1Gbps. Но понятно, что это был тест синтетический, а в реальности пропускная способность будет ограничена не столько мощностью сервера, сколько коммуникационной подсистемой OSFP-маршрутизатора. И еще раз напомню, что соотношение по количеству запросов между хорошим/плохим трафиком находится в пропорции примерно 10 000 к 1. Так что, возможно, столь "мощной машины" может и не потребоваться (тэг #irony становится довольно актуальным).

В открытых источниках указывается, что стоимость системы составляет 60 тысяч рублей. Но это, насколько я понимаю, стоимость исключительно софта. При внедрении определенно будут затраты на дополнительное оборудование, интеграцию, тестирование и ввод в эксплуатацию. Но мы себе поставим галочку, что сумма примерно такая, и не зависит от объема прокачиваемого трафика.

Помимо просто фильтрации трафика и последующей выдачи пользователю специальной странички "не влезай", SkyDNS предлагает еще ряд возможностей, которые возможно заинтересуют (мне очень интересно - заинтересуют ли?) провайдера:

- "детский интернет" как дополнительная опция в тарифном плане;
- "корпоративный фильтр" с фильтрацией запрещенных именно в данной организации сайтов;
- упомянутая выше опция "школьный интернет" с повышенным градусом паранойи и/или вообще с белыми списками;
- фильтрация контента на Wi-Fi хот-спотах.

Все эти опции могут стать дополнительным фактором повышения ARPU там, где на это есть спрос. Обязательно к использованию в госучреждениях и офисах "Единой России". Тем паче, благодаря легкой интеграции со всеми достаточно популярными системами биллинга, возможно все, при наличии достаточно хороших продавцов в корпоративном секторе.

Carbon Soft

Компания Carbon Soft тоже не новичок в телеком-бизнесе - как указано на ее страницах, более 8 лет ее команда разрабатывает программное обеспечение для бизнеса и операторов связи.

Их решение для фильтрации называется Carbon Reductor и построено по совершенно аналогичной описанной выше схеме. Каких-то дополнительных фич, отличных от уже описанных, я тоже не обнаружил, за исключением, пожалуй, нативной интеграции с биллингом указанной компании Carbon Billing. Вот как описывают свое решение сами разрабы:

На сервер фильтрации устанавливается дистрибутив CentOS 6, на нём настраивается доступ в интернет, устанавливается RPM-пакет Carbon Reductor. На коммутаторе, ведущем к фронт-роутеру настраивается дублирование трафика на порт сервера Carbon Reductor. Carbon Reductor анализирует этот трафик и на обращения к запрещённым сайтам формирует HTTP-пакет (или tcp-reset, если модуль редиректа отключен), отправляющийся к пользователю от имени запрашиваемого ресурса и перенаправляет пользователя на страницу с уведомлением о том, что данный сайт заблокирован.

Отличительным зато является способ ценообразования, которое парни попытались сделать гибче в зависимости от заказчика. Я не буду приводить полностью информацию с сайта - просто скажу, что у

Carbon продает услугу помесячно, давая возможность заказчику выбрать устраивающий их план и уровень обслуживания. Цены начинаются буквально с тысячи рублей в месяц для решения класса минимум-миниморум, до полумиллиона рублей за систему, поддерживающую сто тысяч юзеров с полным пакетом технической поддержки.

МФИ Софт Периметр-Ф

Один из крупнейших разработчиков программных решений для телекомов в России, компания "МФИ Софт" из Нижнего Новгорода так же не осталась в стороне от внезапно появившегося рынка контент-фильтров.

Решение называется "Периметр-Ф2, схема - классика. Очевидно, решение возникло на базе предыдущих разработок линейки анти-DoS продуктов "Периметр", а "Ф" - это "фильтр". Думается, что "Ф" - это система с урезанным функционалом и добавленной функцией выгрузки реестра с сайта РКН.

Описанные преимущества системы банальны, а информации о стоимости системы на сайте я не обнаружил. Посему прибег к методу "инсайдерской информации" и выяснил, что один "федеральный оператор" получил компред на сумму в примерно один миллион рублей за фильтрацию канала 1-10 гигабит.

Но преимущества у данной компании все же имеются. Это опыт взаимодействия с бюрократией в крупных компаниях.

CKAT VAS Expert

Компания из Санкт-Петербурга "VAS Expert" представлена линейкой продуктов CKAT (Система Контроля и Анализа Трафика) и это единственное решение, построенное не по классике.

CKAT по сути является DPI системой и купить ее можно как в виде софт-бокса, так и в виде готового решения - специализированного сервера с уже предустановленной системой.

Разброс цен довольно значителен - от 40 тысяч рублей за CKAT-6 (цифра - лицензионная ширина канала) до почти миллиона за CKAT-40, с сервером Fujitsu PRIMERGY RX200S8 в комплекте.

Трудно утверждать, чем решение на базе DPI более лучше, чем "классика", но одно сказать можно уверенно - это другая архитектура с другим философским взглядом на решение проблемы фильтрации.

Система DPI подразумевает "прочесывание" всего трафика с заранее определенным реагированием на тип и адреса пакетов. Разумеется, что одним из "6000+ прикладных протоколов, которые при необходимости пополняется новыми", может быть и быть и банальный http/80, на который налагается правило проверки адреса из реестра и его переадресация на страничку "no way".

Цена вполне сопоставима с вышеперечисленными системами, и поэтому CKAT вошел в данный список, хотя, очевидно, что DPI может много больше, чем просто фильтровать.

Но хочу заметить, что философия DPI несколько отличается от основополагающего этического принципа, на котором базируется Интернет в широком понимании - "сетевого нейтралитета", при этом производители решений до сих пор так и не смогли сформулировать целей и задач сей группы решений, которые бы не основывались на дуализме "защиты потребителя от потребителя". Я с удовольствием выслушаю все аргументы в пользу DPI, но пока не нашел ни одного аргумента в пользу этой технологии. Даже для использования в качестве фильтра по действующему законодательству, лично мне эта технология кажется избыточной, хотя теоретически DPI должна фильтровать трафик заметно лучше, чем "классика", которую легко обойти анонимайзерами, VPN и прочими нехитрыми уловками, например, перестановкой аргументов в GET-запросах.

Подводя итоги

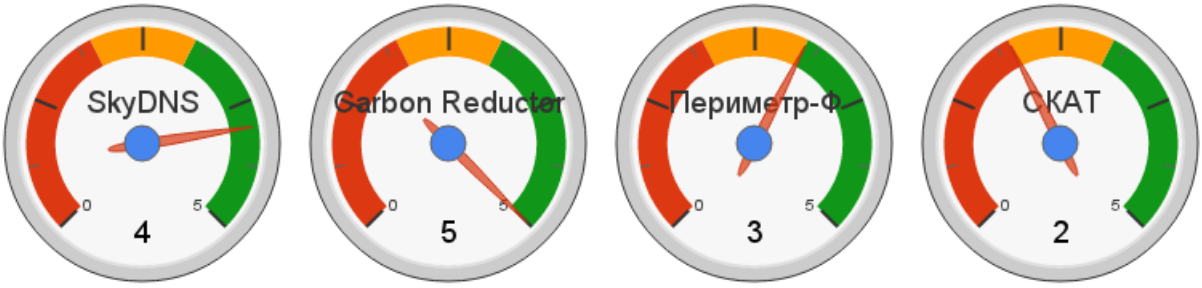
Для подведения итогов "кто на свете всех умнее2 принято приводить сравнительные таблицы. Я поначалу тоже хотел сделать нечто подобное, но отказался по следующим причинам: во-первых, это никакой не тест и у меня нет на руках объективных цифр и полного набора характеристик. Во-вторых, для объективной оценки нужно просто подержать в руках продукты, попытаться понять их логику и, если хотите, философию. Например, не хочу обидеть парней из VAS Expert - возможно, у них весьма приличный продукт, но я субъективно настроен против систем DPI. Возможно, у МФИ Софт имеется продукт класса "установил и забыл", что перекроет все недостатки закрытой компании. Возможно, коммерческо-маркетинговые новации в ценообразовании Carbon Soft имеют логическое обоснование и технические предпосылки. А мои личные предпочтения SkyDNS объясняются простым

фактом личного знакомства с земляками.

Посему, сводной таблицы не будет - для этого нужно более тщательно проанализировать состав и функционал. Но некоторые характеристики я все же объединю в модные инфографические приборы и выставлю субъективные оценки по следующим параметрам со странным для сравнительных таблиц недифференцированными значениями - 0/1:

1. Возможность загрузки реестра с сайта РКН по ЭЦП:
   - SkyDNS - 1
   - Carbon Soft - 1
   - Периметр-Ф - 1
   - СКАТ - 0 (не указано на сайте, хотя может я невнимательно читал)
2. Возможность дополнения списков региональными блокировками
   - SkyDNS - 1
   - Carbon Soft - 1
   - Периметр-Ф - 0 (нет информации)
   - СКАТ - 0 (нет информации)
3. Схема реализации решения на оборудовании провайдера
   - SkyDNS - 1
   - Carbon Soft - 1
   - Периметр-Ф - 1
   - СКАТ - 0 (за DPI и специальный сервер)
4. Допуслуги по фильтрации отдельных клиентов и интеграция с биллингами, белые списки etc
   - SkyDNS - 1
   - Carbon Soft - 1
   - Периметр-Ф - 0
   - СКАТ - 0 (не указано на сайте, хотя может я невнимательно читал)
5. Схема мониторинга сервиса с алармами администрации (по материалам сайта)
   - SkyDNS - 0
   - Carbon Soft - 1
   - Периметр-Ф - 0
   - СКАТ - 0

Итого, получилась вот такая картинка:



Остальные параметры системы, такие как "производительность" (включая булл шит вида "Самый быстрый фильтр"), "отказоустойчивость" (странно было бы прочитать на рекламной странице, что решение ломается два раза в день) и "масштабируемость2 обсуждать имеет смысл только после конкретных тестов, которые возможно будут, если участники соревнования в явной форме изъявят свое желание публично или приватно.

Из главных же, на мой взгляд, действительно полезных функций, которые стоило бы перечислить: интерфейс администратора, легкость внедрения, гибкость управления, количество предустановленных политик, на оффсайтах не упомянул никто.

Всем мир, и не ходите по запрещенным ссылкам!

Традиционная смешная гифка, олицетворяющая победу здравого смысла над разумом, в конце статьи выглядит так:

[Отфильтрованные (update)]