Спасение утопающих - за счет водоема

Сайт реестра запрещённых сайтов попал в реестр запрещённых сайтов,
т.к. содержит запрещённую информацию о запрещённых сайтах.

Лирическое отступление вкл.

Прошлый год подарил миру как минимум один новый глобальный термин - им стала facebook-революция. Причем про это не просто говорили разные умные люди, все куда серьезнее, многие, не без основания считают, что социальные сети изменили государственный строй в Египте, Тунисе, Ливии... Лучше там сейчас жить людям или хуже, виновна Сеть в произошедшем, или это климат такой особенный в арабских странах, на самом деле совершенно не важно. Суть в другом - солидные государственные мужи начали воспринимать интернет не как игрушку тинейджеров, а... Слово "врага" в данном контексте будет смотреться слишком серьезно, так что пусть будет политкорректное - "конкурента традиционных СМИ".

А раз так - то и цензора внимания новому средству коммуникаций надо выделять соразмерно, на том же уровне, что телевидению, радио, и прессе. Повод искать долго не пришлось. Не секрет, что среди онлайнизированных граждан встречаются закономерный процент совсем не граждан психов, провокаторов, сумасшедших, и просто идиотов. Все как в обычной оффлайновой жизни, не лучше, но надеюсь и не хуже. Долгие годы они спокойно творили что-то свое, "выдающееся", или, наоборот, прикидывались вполне нормальными, но главное, никому при этом особо не мешали.

Для начала их пытались травить дустом "запрещать" как обычно, в административно-правовом или судебном порядке. Появлялись весьма оригинальные решения, "экстремистские" списки, кто-то что-то блокировал, или наоборот, отказывался это делать. Причем, такую насмешку над принципами работы интернет нельзя признать чисто Российским феноменом - на мой взгляд те же французы отличились на ниве интеретоборчества куда как более. Но общий эффект от правоохранительной суеты был явно на уровне теплового шума - сменить IP-адрес или доменное имя не великая проблема, а Google всегда подскажет, где искать "запрещенный" контент.

Очевидно скромные успехи в деле борьбы с "противозаконными" веб-весурсами побудили правительство на крайние меры. Нет, к счастью, до блокировки Google дело пока не дошло а ведь мог бы и полоснуть! (из анекдота про В.И. Ленина). Но пакет новых законов принят. По адресу zapret-info.gov.ru уже работает официальный список для запрещенных ресурсов. По процедурным вопросам на форуме есть специальный топик. Роскомнадзор делает робота-блокиратора, а добрые самаритяне простые пользователи в лучших традициях соцреализма успели за первую пару недель настучать 13 тысяч жалоб.

Впрочем, для "медианного" пользователя Сети история на этом, по сути, заканчивается. Государственные умы разработали какой-никакой механизм, приняли закон, определили способы контроля исполнения. Можно сказать, заботятся и любят, как родного. И на самом деле, пока работает вконтактик, ютуб, и твиттер - можно не волноваться. Фотографии пушистых кошечек, обнаженных девушек и пихаемого в автозак Удальцова более чем достаточны для подтверждения демократического курса ВКП(б) страны.

А вот для операторов связи начинается самое интересное. Хочешь, не хочешь - а закон надо соблюдать. И в нем никто не предусмотрел финансирование весьма непростой операции по фильтрации контента. Нет, Роскомнадзор не будет прямо писать - "провайдер обязан за свои деньги приобрести и установить...". Только от этого не легче - интересно, хоть одному провайдеру России удалось получить деньги за систему СОРМ? Нет? А в законе все основания для этого имеются...

Ну а коль скоро данный сайт в основном технический... То остается лишь посмотреть крышесносящую "рекламу" ринетовского тарифа "Чистый интернет", и... прикинуть, какие соответствующие возможности можно использовать для выживания в дивном новом мире.

Лирическое отступление выкл.

Первое, и самое очевидное - использование платных DNS-сервисов. Как ни странно, это не только "дешево и сердито", но и вполне реально. Примерами могут служить:
SkyDNS, GatewayWall, OpenDNS. А чтобы слегка потертые реальностью потребители анлимитного трафика не занимались противоправной чепухой через 8.8.8.8 "вражеские" DNS - их нужно заблокировать. Вот только сделать это надежно почти невозможно, уж больно много подобного в сети... Конечно, всегда остается вариант доказать товарищу майору Роскомнадзору, что, пока личные VPN не попали под расстрельную статью запрет, найдется возможность добраться до любого ресурса. Да и специальные сервисы - анонимайзеры никто не отменял. Но...

Если не баловаться плюшками думать о паллиативах, стоит посмотреть в сторону настоящего хардкора серьезного оборудования. Благо, в Cisco, Juniper, Checkpoint, Procera Networks и прочих компаниях давно разработали кучу сетевых экранов, вполне подходящих под нехитрые

отечественные требы.

На первый взгляд кажется, что оператору достаточно примененить ACL (access list) на оборудовании доступа пользователей (BRAS). Действительно, если поставить что-то специально придуманное, типа Ericsson SmartEdge с его технологией http-redirect, или аналог в виде Linux, а то и просто старенькую Cisco c3550, на них всех можно классифицировать трафик по информации второго уровня OSI (mac address) или третьего уровня (ip address), а потом и заблокировать хрупкие ростки свободы и порнографии требуемое.

Однако, в свете последних постановлений блокировка на уровне IP становится немодной, ну, в смысле так недолго оставить пользователя в чем-то действительно "уютненьком". Поэтому IP-фильтрация сгодится лишь для перенаправления трафика абонента на URL-фильтратор устройство сигнатурного анализа трафика, иначе говоря, DPI (Deep Packet Inspection). Говоря обычным языком - на анализ не только заголовков пакетов, протоколов, или портов, а на проверку любой части данных, как правило, по специально разработанному производителем оборудования набору сигнатур.

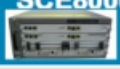
На подобных аппаратах нужно остановиться подробнее.

Классика жанра, Cisco SCE

Строго говоря, SCE - изначально разработка израильской компании P-Cube, которую "компания золотого моста" выкупила за 200 млн. USD в 2004 году. Вкратце напомним: SCE поддерживает все виды фильтрации трафика и позволяет производить сигнатурный анализ вплоть до 7 уровня модели OSI. Сигнатуры своевременно обновляются и выпускаются компанией в виде Protocol Pack'ов (1 раз в 2 месяца), что позволяет поддерживать сервис на необходимом уровне. Все отчеты выгружаются по технологии RDR с помощью специального ПО Cisco SCE Reporter (или конвертируются самописными конвертерами в Netflow v.5).

Важное свойство, на SCE можно не только блокировать трафик, но и "подрезать" его до нужной скорости. В свете рассматриваемой темы это не слишком важно, но для борьбы с торрентами реальной жизни такое свойство более чем полезно.

Линейка состоит всего из трех моделей.

Категория	SCE1000	SCE2000	SCE8000 
Интерфейсы	2-GBE (Fiber SX/LX)	4-GBE (Fiber SX/LX)	2-10G 4-10G (Fiber SX/LX/ZX)
Интерфейсы управления	2 x 10/100/1000 Eth	2 x 10/100/1000 Eth	2 x 10/100/1000 Eth
Макс. количество однонаправленных потоков приложений	2M	2M	16M (с увеличением до 32M)
Макс. количество абонентских контекстов	40,000	200,000	1,000,000
Включение в сеть	Out of Line Inline	Out of Line Inline Clustering	Out of Line Inline Clustering

По производительности получается следующая картина:

	Максимальное количество абонентов	Максимальное количество потоков
SCE1010 / SCE2020	40K	1M
	80K	850K
	120K	690K
	200K	370K
SCE8000	250K	8M
	500K	7M
	1M	5M

Но как видно из примера ниже, при превышении БД URL 4-5 тысяч записей, оборудование начинает плохо справляться со своей задачей.

System Cisco Service Control, SW version: Version 3.7.0 Build 222, HW version: SCE8000 2x10GBE
Status Operational, Total Traffic: 22994606
Subscribers Counters Active: 11730; Anonymous: 0; Introduced: 25133
Bandwidth (Kbps) 22994606
TenGigabitEthernet3/0/0 10963877
TenGigabitEthernet3/1/0 12030729
CPU Utilization (%) 81
Control Processor 17
Traffic Processor1 80
Traffic Processor2 64
Traffic Processor3 71
Traffic Processor4 64
Traffic Processor5 66
Traffic Processor6 81
Traffic Processor7 75
Traffic Processor8 71
Traffic Processor9 73
Traffic Processor10 68
Traffic Processor11 74
Traffic Processor12 73
Memory Utilization (%) 18
Total Active Flows 628565
Connections Per Second 17566

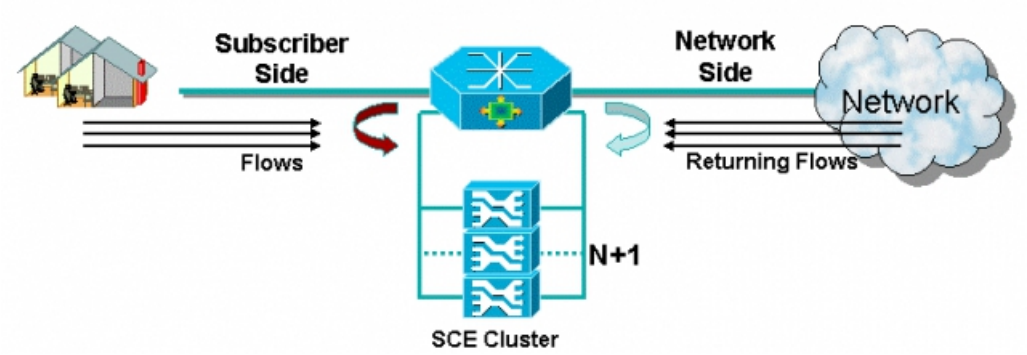
Кроме этого, стоит добавить небольшое how-to как быстро запустить cisco SCE в сеть, и темы форума, посвященные обсуждению Cisco SCE, самые интересные (раз, два, три). Что же касается непосредственно URL-фильтрации, через открытый API возможна интеграция с внешней базой URL-категоризации, например базами ЦАИР и Websense. Настройка достаточно тривиальна и сводится собственно к импорту списка URL. Все тонкости можно изучить здесь.

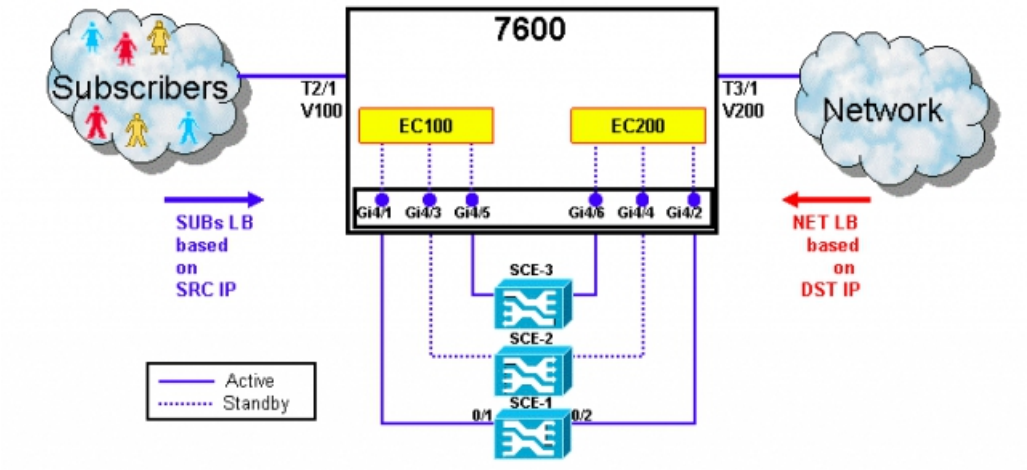
Следует обратить внимание, что файл для импорта имеет ограничение на количество URL:
Cisco SCE 8000 platform—100,000
Cisco SCE 2000 platform—100,000

Также доступен второй вариант - создание black-листа УРЛов прямо на SCE через SCA-BB console, при этом поддерживается до 500K строк URL.
Подробнее данный метод описан в небольшой how-to как настроить URL фильтрацию на Cisco SCE.

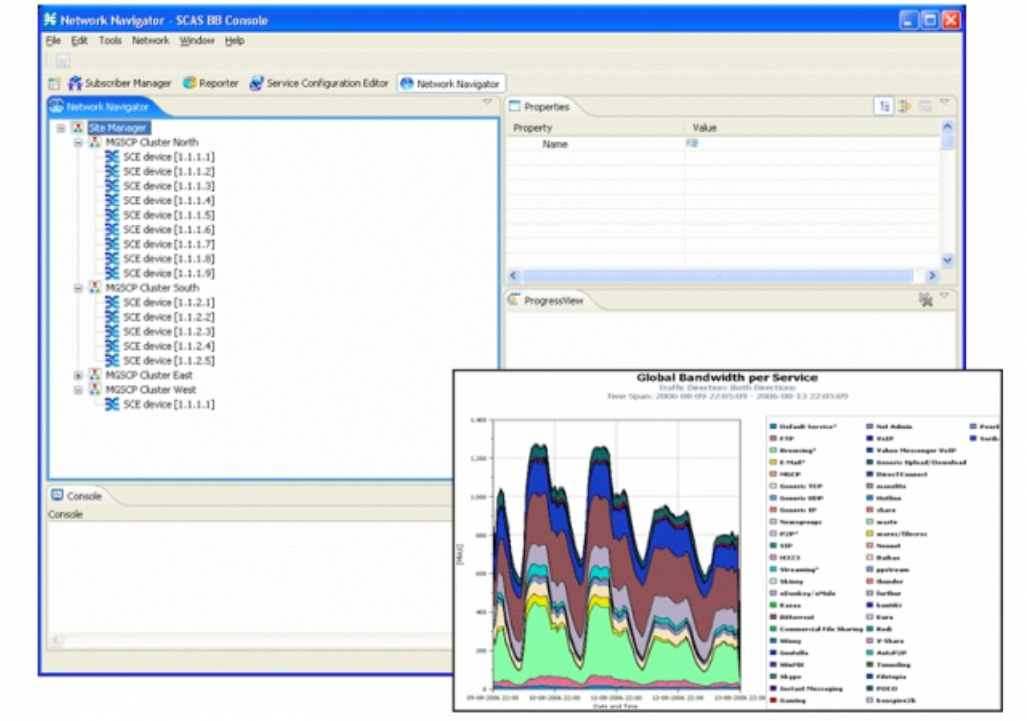
И самое интересное. Средняя цена на оборудование SCE2020 колеблется в районе 5000-6000 USD на б.у. рынке при стоимости по GPL $50 000 (без софта и лицензий). SCE1010 я бы вообще не рассматривал из-за очень малой производительности. Флагман SCE8000 стоит по GPL $110 000 за бандл в 2x10GE порта, но! При этом надо докупать еще обязательно XFP 10GB, софт... Так минимальная цена увеличивается до 128к баксов. Учитывая вполне реальный дисконт в 50% (хотя такой еще надо вырвать... обычно дают 42-46%), получаем 64к за коробку с 10Г каналом. На рынке б.у. можно купить подобный бандл примерно за 55k. Апгрейд мозгов SCM-E + пара SPA-1x10GE для увеличения производительности в два раза на б.у. рынке “выльется” во что-то порядка 38-40к баксов.

Каждый решает для себя сам - ставить стопку SCE2020 или одну SCE8000. При этом для первого варианта есть специалальный механизм - работа SCE в кластере (а не только PBR на роутере перед SCE):





При этом управлять и осуществлять мониторинг кластера можно через тот же SCA-BB



Как настроить MGSCP (или работу SCE в кластере) - можно посмотреть тут.

Новая волна, или Juniper SRX

Решение разработано на базе оборудования компании NetScreen. Поддерживает сигнатурный анализ трафика вплоть до 7 уровня модели OSI. Сигнатуры разрабатываются компанией NetScreen и обновляются через Сеть. Данное оборудование не позволяет ограничивать сетевой трафик до требуемого уровня, но позволяет осуществлять блокировку трафика в соответствии с требованиями. Поддерживает вывод результатов работы в графическом виде с помощью Network Security Manager.

SRX поддерживает четыре вида URL фильтрации:

В первом случае используется специальный лицензированный облачный сервис Juniper Network, который как понятно, требует дополнительных затрат на лицензии, пример тут, 0.6 Кб.
Во втором - используется специальный выделенный сервер, с установленным ПО от Websence, на котором содержится разбитая по спискам и категориям база данных URL. В процессе работы SRX перехватывает весь http/https трафик и направляет его на заданный сервер, который уже принимает решение блокировать, или логировать или разрешить. Пример здесь.
В третьем - используется встроенный механизм SurfControl позволяющий добавлять различные категории сайтов в конфигурацию, заранее заднные вендором, либо создавать свои категории со списками web url. Очередной кусочек кода.
Наконец, в четвертом варианте используются тривиальные черные и белые списки, которые настраиваются прямиком на оборудование. Смотреть тут.

Фактически для выполнения требований закона хватит самого простого - четвёртого варианта. Но почему бы не предложить родительский контроль или фильтрацию порно для образовательных учреждений? Раз уж деньги за железо заплачены...

Для обработки логов потребуется специальное ПО STRM - Security Threat Response Manager. Информация предоставляется по IP адресам источника/назначения, по категориям URL, по политикам применимым на данную URL и действиям проведенным этими политиками.

Линейка SRX на российском рынке представлена отдельными "коробками" SRX100/110, SRX210/220/240, SRX650 (с поддержкой 10-ти гигабитных портов) и большими стоечными системами SRX3000/5000 series.

[Спасение утопающих - за счет водоема]

[Спасение утопающих - за счет водоема]

Цены на оборудование SRX в "глобальном листе": самая младшая модель в линейке, SRX100/110, обойдется в $699-999 (в зависимости от размера памяти), SRX210/220/240 - 2199-3699, SRX650 - 16000-17200. Нужно помнить, что в настоящее время дисконты на Juniper примерно аналогичны “сисковским”, т.е. можно ориентироваться грубо на 50%.

Со старшими моделями история уже другая. Решение необходимо масштабировать по элементам - NPC карты + SPC карты + управляющие модуля и интерфейсные с ними. лучше обзавестись интегратором по-грамотнее и согласовать ТЗ на берегу, как пример:

[Спасение утопающих - за счет водоема][Спасение утопающих - за счет водоема]

Следует учитывать, серия SRX разрабатывалась как решение безопасности в корпоративных сетях, и на провайдерах по сути "не обкатано". Поэтому перед покупкой его на операторские нужды стоит обратить внимание на все параметры: полоса пропускания, mpps, количество абонентских сессий. Последнее в спецификациях приведено для работы в режиме L3 фильтрации, однако URL - фильтры работают вплоть до 7-го уровня модели OSI, так что может не дотянуть. В любом случае каждая web сессия для SRX уже будет "абонентской".

В первом примере SRX3600 в “полном фарше” для наших задач: резервирование RE, 2 NPC + 7 SPC + 4x10Ge, интерфейсов можно сделать и больше, но не за чем. В этой конфигурации производитель обещает: 6M сессий, 6Mpps, 15 Gbit FW IMIX трафика. Во втором примере наоборот - минималка. В таком варианте имеем: 0.5M сессий, 1Mpps, 2.5 Gbit FW IMIX трафика. Однако учитывая сказанное выше, цифру сразу следует делить пополам, а то и в три четыре раза.

Фенечка для BRAS, или Ericsson ASE.

По сути, это не отдельное устройство, а специальный модуль, устанавливаемый в шасси Smart Edge

от 600 модели и выше. Предназначен для функции DPI применительно для P2P трафика. Такое ограничение сделано в связи с тем, что оборудование Smart Edge используется как BRAS, и, по мнению Ericsson, работает в основном с данным видом трафика. Соответственно, основной функционал - выявление P2P трафика пользователей и осуществление ограничения или блокировки согласно заданным параметрам. Позволяет осуществлять фильтрацию по каждой абонентской сессии, что, в данном случае, является несомненным плюсом. Управляется и выдает отчеты с помощью специального ПО NetOp Policy Manager. Как устройство web фильтрации практически не применяется в связи с ограничением основного функционала карты.

Единственный верный режим эксплуатации - применять DPI к части абонентов. Например придумать экономный тариф без торренов как таковых, или же наоборот, чуть-чуть подрезать p2p наиболее злостным пирам.

Новичок из мира больших денег: Check Point Secure Gateway

Check Point 12600

Уверен, что данный бренд, специализирующийся на информационной безопасности, операторам России совершенно не знаком, но это не значит, что он плох. Банкиры (а именно они основной потребитель подобного оборудования) плохое использовать не будут. Тем более, линейка устройств сейчас идет совершенно новая, 2012 года.

Младшее устройство под номером 2205 имеет 6 портов 10/100/1000Base-T и производительность около 3 Гбит/секунду при выполнении правил фильтрации. Стоит - $3960. Моделька 4400 “потянет” по GPL $12 000, а наиболее производительная 12600 обойдется в $74 500. Надо понимать, дисконты тут сильно меньше, чем у Cisco или Jniper, хорошо если конечному пользователю удастся получить - 20%.

Провайдеры не банкиры, и понятно, что для них стоимость “железок” от Check Point едва ли будет симпатична. Однако, есть возможность ограничится только базовым функционалом URL фильтрации, которое можно реализовать как на базе программного обеспечения Open Server, так и подходящем Intel-based сервере. В зависимости от требований к производительности, стоимость софта составляет от $3 960 с ежегодной подпиской на облачный сервис URL фильтрации ($1500).

Сравнительная таблица аппаратных решений линейки 2012 года выложена в отдельном файле. Там есть над чем подумать.

Что касается управления, то к железкам "прилагается" Checkpoint mangement console, которая позволяет осуществлять настройку как одного так и сразу нескольких устройств, снимать статистику потребления трафика, по пользователям, видам трафика, и предоставлять ее пользователю в графическом виде. В общем, все как обычно.

Для того что бы настроить механизмы URL-фильтрации необходимо создать правила, в которых указать, какой ресурс и для каких пользователей необходимо блокировать, так же можно задать время работы правила, и дополнительные действия, например вывести уведомление о запрете данного ресурса в сети. Имеется очень удобная организация URL, которая позволяет как создавать собственные списки, так и использовать уже заранее готовую базу данных. Для примера, на пошаговую инструкцию по добавлению списка блокируемых сайтов из CSV файла можно посмотреть тут.

Надо сказать, что опыта применения решений Check Point в РФ по большому счету нет, вместе с тем показания к такому применеию имеются, всех желающих попробовать приглашаем к тестированию.

Краткие выводы

Попробуем прикинуть, во что обойдется условный "гигабит" фильтрации:

- Cisco SCE: 1G трафика с 1G портами (на базе б.у. SCE2020) будет стоить порядка 2500$. 1G трафика с 10G портами (на базе новой SCE8000) будет стоить порядка 6500$. В б.у. варианте дешевле на 20%, т.е. где-то в районе 5500$.
- Juniper SRX: 1G трафика поддержит только SRX650 и стоит будет 6400$, для больших решений сложно рассчитать это значение. Но цена врядли будет ниже, чем 6000$ за 1G.
- Unix based solution: вопрос остается открытым...

Однако, если считать, что счастье не в деньгах, то у Cisco есть свой достаточно интересный документ по сравнению устройств безопасности. Одна из глав посвящена как раз WEB фильтрации.

Disclaimer.

Редакция хорошо понимает, что все описанное можно сделать с помощью Iptables. Более того, это, никто не сомневается что файрвол на базе ОС Linux умеет вышивать крестиком и обметывать петли все описанное и даже чуть-чуть больше. Поэтому мы с удовольствием опубликуем статью, посвященную этой теме. И даже заплатим за нее авторский гонорар.
Тоже самое можно сказать про DPI от Allot, Huawei, Procera, Sandvine...
Так что "продолжение следует", если, разумеется, этот самый автор найдется.