

Shape-NAT-NetFlow на больших сетях. Часть 1.

Автор: Кирилл Малеванов, технический директор ООО "[Ниеншанц-Хоум](#)"

Статья опубликована в рамках конкурса "Формула связи"

На форуме все чаще и чаще поднимаются ветки о том, чем натить 1 гбит/с, чем шейпить 30 тыс пользователей, чем отфильтровать разные классы трафика, и особо острый вопрос - как получить netflow с хорошей точностью на потоках интернета от 1 гбит/с.

Раньше эти проблемы решались довольно просто, кто-то решал их на PC-серверах под FreeBSD/Linux/Mikrotik, кто-то на Cisco 7505/7204/7201 и т.п. Но на текущий день при потоках от 1 гбит/с и количестве пользователей около 10 тыс и выше это становится все сложнее.

По сути, можно разбить всю задачу на 3 части - shape, NAT, netflow. Понятно, что задачи эти можно решать как совместно, так и раздельно, главное, чтобы в правильном порядке (не пытаться снять netflow с уже сначенных пользователей, например).

Далее я бы хотел немного поговорить о терминологии. Под PC-серверами я буду подразумевать любой PC-сервер с любой установленной операционной системой. Это может быть Linux, может быть FreeBSD, Linux-клоны (Mikrotik, Vyatta), даже Windows. Но суть остается одна - это универсальная платформа, как правило, на базе x86, с одним или несколькими процессорами, как самосбор, так и брендовые серверы.

Софт-рутеры - это маршрутизаторы, построенные на базе универсальных CPU. Как правило, это все маршрутизаторы Cisco от 8xx до 72xx/73xx. Их всех отличает то, что весь маршрутизируемый трафик проходит через центральный процессор, в отличие от аппаратных платформ типа Cisco 6500/7600, Juniper M/MX. Помимо маршрутизаторов Cisco данной линейки сюда же входят маршрутизаторы типа Juniper J6350, Cisco ASR1000 (единственное отличие данной серии в том, что для маршрутизации трафика используется отдельный процессор), Ruijie NPE-50, линейка маршрутизаторов Huawei AR и другие.

Аппаратные платформы - это маршрутизаторы на базе специализированных процессоров, часто называемых ASIC. Их функционал достаточно жестко ограничен, количество сетевых трансляций, netflow entries, количество очередей для шейпинга, количество ACL, иногда количество интерфейсов и прочие технические параметры - заданы жестко в железе, и могут изменяться только путем апгрейда железа. Типичные представители аппаратных платформ - Cisco 6500/7600, Juniper M/MX. Так же для простоты я буду называть аппаратными платформами файрволы - начиная с Cisco ASA5520 и заканчивая линейкой ASA5580 (да, я знаю, что там внутри стоит PC-сервер - но на старших моделях стоит также и специальный чип для обработки трафика), Juniper Netscreen ISG1000/2000, Juniper NS5200/5400, Juniper SRX, Huawei Secpath, BRAS'ы от Juniper, Redback, Huawei, Cisco 10K.

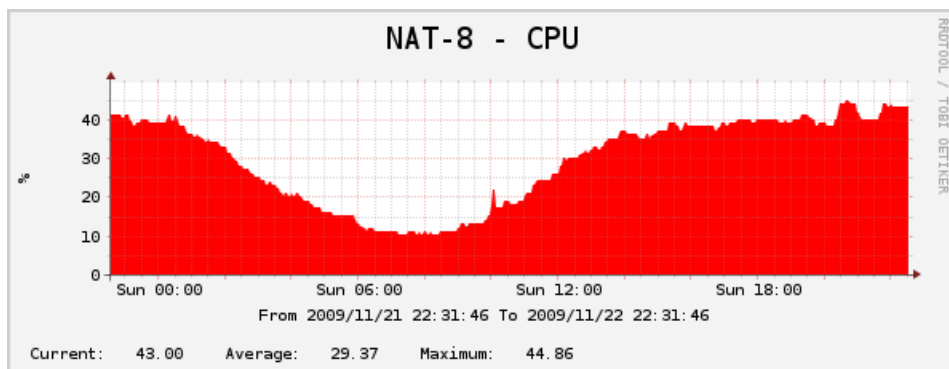
NAT

PC-серверы

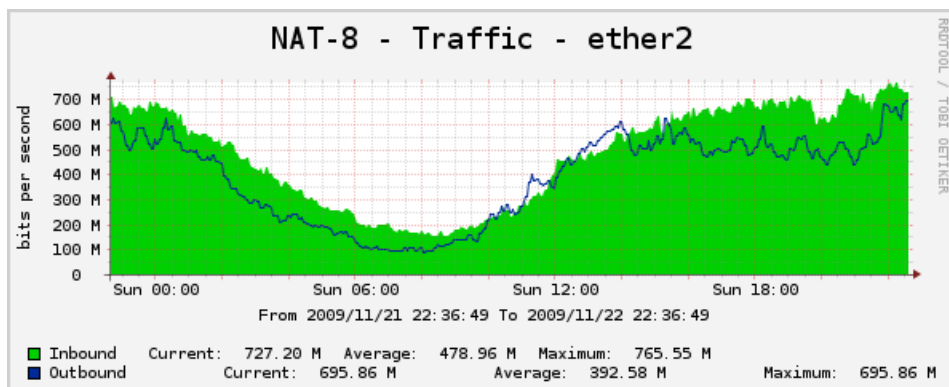
PC-сервер очень неплохо справляется с задачей NAT'a. На сегодняшний день, что FreeBSD, что Linux позволяют производить NAT в несколько потоков, используя все ядра и все процессоры системы. Однопроцессорный Quad-Core Xeon 2.66 с шиной 1.33ГГц (HP DL160) натит, не напрягаясь, около 600 Mbit/s FD при загрузке процессора в пиках до 40% при количестве пакетов до 100 kpps. Замена такого сервера на двухядерный Xeon 2.4 с шиной 800МГц (HP DL140) дает резкое падение производительности, 400 Mbit/s и максимум 80 kpps. Сразу оговорюсь, что rps и Mbit/s считаются на одном (внешнем или внутреннем интерфейсе) при примерно равном входящем и исходящем трафике, как по rps, так и по Mbit/s. Т.е. 600 Mbit/s 80 kpps - это 600/80 из интернета в локалку и 600/80 из локалки в интернет.

Если 100 kpps пересчитать по цисковской терминологии - как, скажем, "максимальная пропускная способность NPE-G2 - 2 mpps" - то получим 400 kpps (100 вход и 100 выход * 2 интерфейса). Использование PC-серверов радует еще и тем, что размер нат-таблицы сессий ограничен только количеством памяти, надо только помнить, что чем больше эта таблица - тем меньше будут показатели rps.

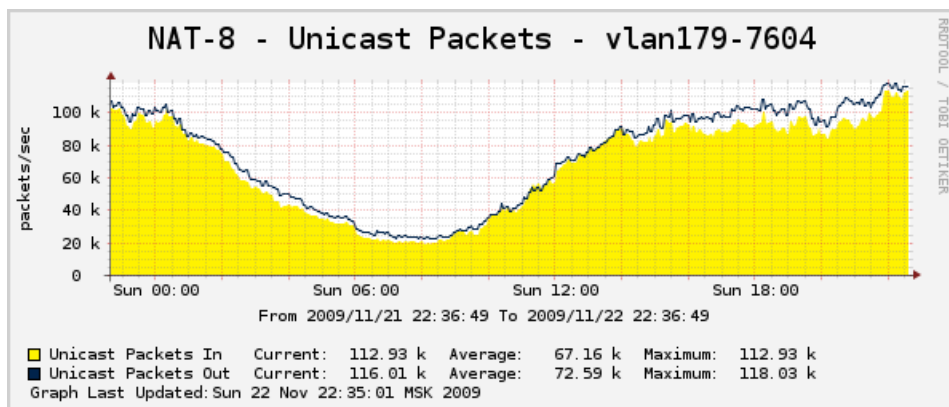
Вот показатели с сервера, который из сетевых задач выполняет только NAT. Загрузка CPU такого сервера редко превосходит 50%.



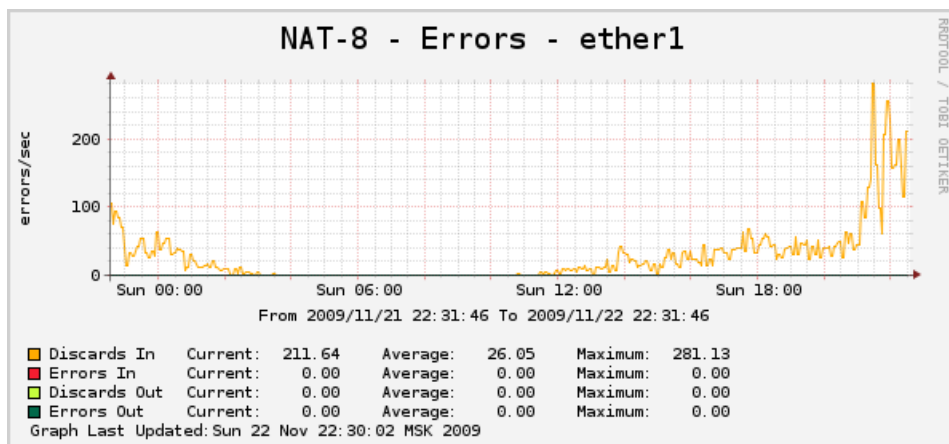
При этом сервер прогоняет через себя порядка 700 мбит трафика.



Немаловажный показатель для трафика – это количество пакетов в секунду:



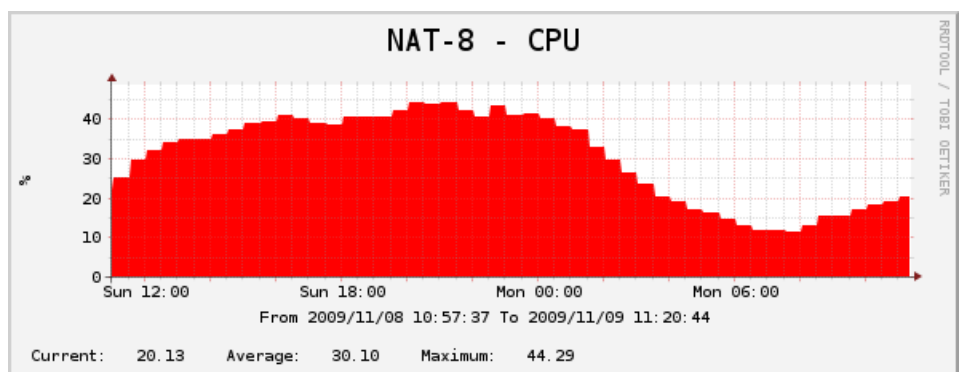
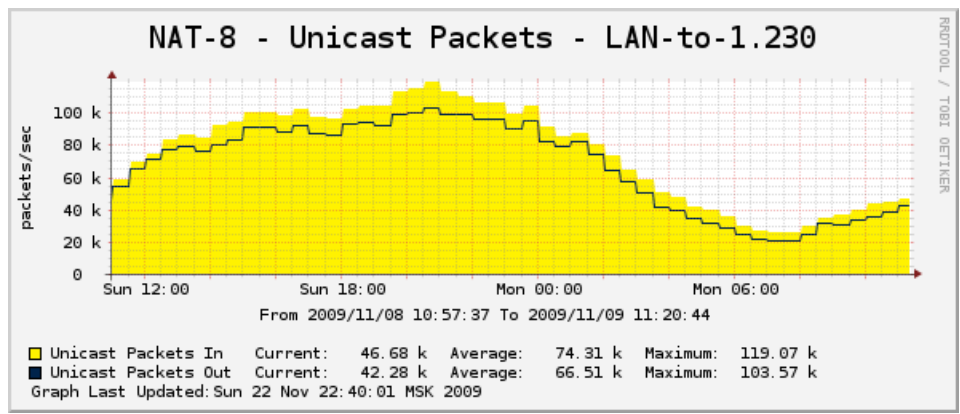
Как и описывалось ранее, сервер держит нагрузку до 100 kpps.



Ошибки на интерфейсе возникают в случае большого потока данных через сервер. Чем больше ошибок в секунду – тем хуже серверу. При превышении 400 ошибок/сек на интерфейсе пользователи уже замечают пакет-лосс и начинают жаловаться. Как видно, резкий рост количества ошибок на интерфейсе возникает при приближении количества пакетов в секунду к 100 тысячам. Это для данного сервера предельное значение, на котором может нормально происходить трансляция адресов.

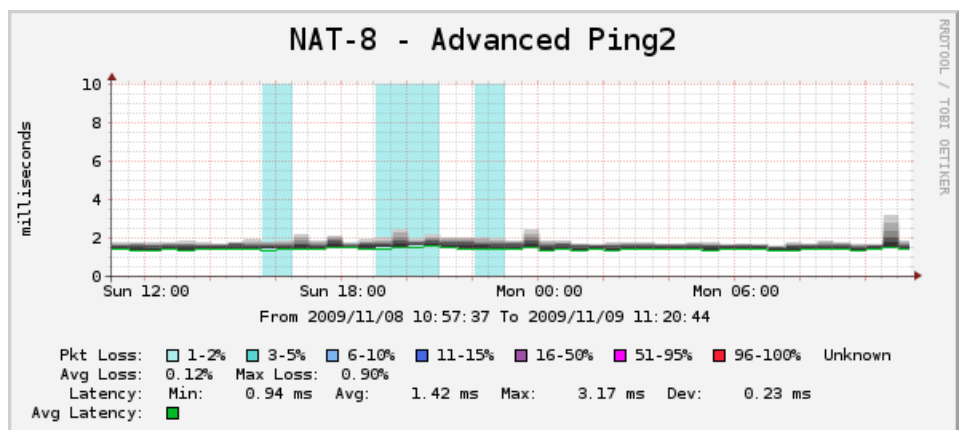
Если с этого сервера снять задачу трансляции адресов, то опыты показывают, что он в состоянии пропустить через себя до 3 Гбит/с трафика с количеством пакетов около 1.5 миллионов в секунду. Эти тесты можно найти, например, на сайте программного обеспечения Vyatta (www.vyatta.com).

Если превышать установленные параметры, то загрузка CPU может и не измениться, а вот ошибки на интерфейсе будут расти. В критических случаях повышения количества пакетов в секунду трафик через сервер будет не то, что расти, но даже и уменьшаться.



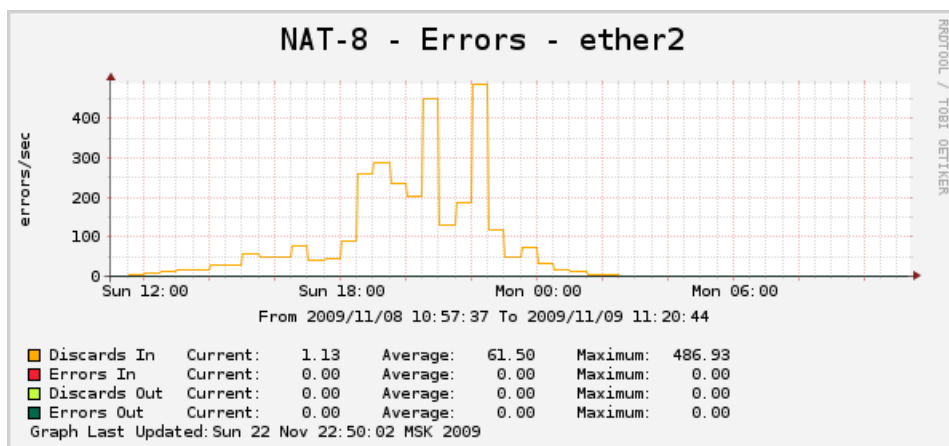
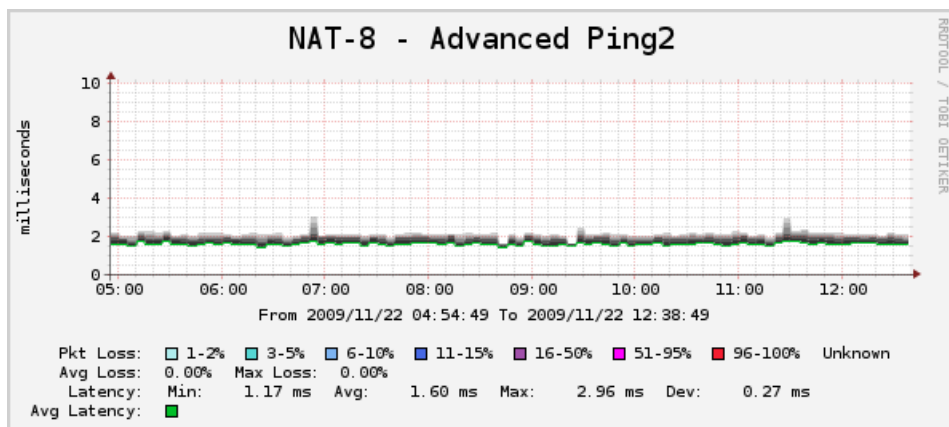
Как видим, на графике загрузки CPU определить то, что сервер уже вышел за границы допустимых объемов трафика, практически невозможно.

Очень хорошим показателем того, что необходимо добавить на трансляцию адресов еще один сервер, является график Advanced Ping:



При этом видно как просто увеличение задержки пакетов до сервера, так и процент потерь пакетов. В случае просто увеличения задержки – это звоночек в сторону «пора ставить еще один сервер», когда начинаются потери – «уже давно пора».

На 100 kpps сервер ведет себя при этом совершенно нормально, проблемы резко растут на 110 и, тем более, 120 kpps:



Софт-рутеры

Трансляция сетевых адресов на софт-рутерах на сегодняшний день в российском ШПД не так распространена, как на PC-серверах. Это довольно сильно связано с тем, что аналогичный по стоимости маршрутизатор не может пропустить и четверти того трафика, который пропускает через себя PC-сервер. И если маршрутизатор еще может как-то показывать приличные результаты на синтетических тестах (большие пакеты, малое количество сессий для трансляции), то в реальной ситуации количество сессий на маршрутизатор влияет очень и очень критично. Более того, маршрутизатор даже без трансляций сильно загружается просто при внесении в конфигурацию настроек для NAT и пропуска трафика, который транслировать не надо. Загрузка Cisco 7201 на терминеции 600 туннелей при трафике порядка 50 Мбит/сек (DOCSIS, PPPoE) только на реальных адресах составляет порядка 15%, при добавлении на внешний интерфейс строки ip nat outside, а на туннели - ip nat inside и задании NAT-пула - уже до 25%. Загрузка CPU Huawei AR46 (аналога Cisco 7204/NPE-G2) при трансляции около 300 мбит трафика составляет порядка 45%, что так же делает его неприменимым для задач «большого NAT'а». Так же в тесте побывал маршрутизатор Ruijie NPE-50, который заявляет производительность вдвое большую, чем Cisco NPE-G2. К сожалению, он не смог показать даже сравнимых результатов. Наиболее интересным софт-рутером для трансляции адресов в случае очень больших объемов трафика оказался маршрутизатор Cisco ASR1000. На тест была предоставлена конфигурация с ESP10, и через нее успешно было проведено около 800 мегабит/сек трафика на загрузке около 140 kpps. Загрузка маршрутизирующего процессора (40-ядерный QFP) составила 4 процента. Но - есть и определенные минусы, которые как напрямую связаны с ограничениями архитектуры ASR, так и с сыростью программного обеспечения (к чести Cisco, новый софт с исправлениями на ASR выходит очень часто, и работа с потребителями ведется очень плотно). Из архитектурных ограничений надо четко отдавать себе отчет в том, что ESP10 - это не 10 гигабит/сек трафика, а всего лишь 5 full-duplex, плюс понимать, что несмотря на наличие в SIP-карте четырех слотов под установку 10GE SPA, реально можно поставить только одну - больше не пропустит шина, и интерфейсы будут с переподпиской. В тестовой конфигурации не удалось пропустить через ASR1000 больше гигабита трафика, потому что 1GE порты на SPA не удалось нормально ввести в ether-channel (видимо, ограничения той версии ПО). Если поставить задачу «пропустить через ASR 10 гигабит/сек трафика, то конфигурация такого маршрутизатора выливается в:

- Шасси
- ESP20
- 2 x SIP
- 2xSPA 10GE

И, в конечном итоге, около \$80K GPL.

Huawei AR18 на синтетических тестах пропускает через себя до 80 мбит трафика. На реальной эксплуатации – при 5 тысячах трансляций он ощущает себя весьма нехорошо, и теряет пакеты.

Аппаратные фаерволы

Многие производители имеют в своей линейке продуктов так называемые «фаерволы». Сюда относятся и Cisco ASA, Juniper Netscreen, Huawei Secpath и другие. Так же, в принципе, в качестве аппаратной платформы для NAT можно рассмотреть Cisco 6500/7600 в стандартной набивке. И отдельно обязательно надо упомянуть модули для маршрутизаторов (Cisco FWSM, Cisco ACE, Juniper MS-100/200/500/DPC). Отдельно надо сказать, что использование этих фаерволов только для NAT в ШПД – это не рекомендованное производителем решение. Позиционирование данных фаерволов – это защита периметра сети, корпоративное использование, а не массовый ШПД.

На аппаратных платформах выплывают наружу такие ограничения, о которых при использовании PC-серверов или софт-рутеров думать не приходилось. Как правило, это связано с особенностями обработки определенных протоколов, где требуется разбор пакетов иногда и до 7го уровня модели OSI. Например, наиболее распространенной проблемой на аппаратных платформах является трансляция сетевых адресов для клиентов, которые используют PPTP VPN. Для обработки такого трафика в Linux/BSD/софт-рутерах есть специальные модули, которые обеспечивают корректность прохождения прямого и обратного трафика. Немало проблем в случае NAT может доставить SIP. Определенные нюансы есть на IRC-трафике, как ни странно – на Quake-трафике и ему подобным. Каждое такое решение требует определенных телодвижений, или со стороны производителя железа, или со стороны системного администратора – по выполнению обходных маневров для неподдерживаемого функционала.

Если спросить у Cisco, что они рекомендуют для NAT, то, как правило, один из ответов в последнее время был «Cisco ASA». Линейка ASA такова (www.cisco.com/go/asa):

Table 7. Characteristics of Cisco ASA 5500 Series Adaptive Security Appliances

Feature	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550
					
Users/Nodes	10, 50, or unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Firewall Throughput	Up to 150 Mbps	Up to 300 Mbps	Up to 450 Mbps	Up to 650 Mbps	Up to 1.2 Gbps
Maximum Firewall and IPS Throughput	• Up to 150 Mbps with AIP-SSC-5	• Up to 150 Mbps with AIP-SSM-10 • Up to 300 Mbps with AIP-SSM-20	• Up to 225 Mbps with AIP-SSM-10 • Up to 375 Mbps with AIP-SSM-20 • Up to 450 Mbps with AIP-SSM-40	• Up to 500 Mbps with AIP-SSM-20 • Up to 650 Mbps with AIP-SSM-40	Not available
3DES/AES VPN Throughput	Up to 100 Mbps	Up to 170 Mbps	Up to 225 Mbps	Up to 325 Mbps	Up to 425 Mbps
IPsec VPN Peers	10; 25*	250	750	5000	5000
SSL VPN Peers* Included/Maximum	2/25	2/250	2/750	2/2500	2/5000
Concurrent Connections	10,000; 25,000*	50,000; 130,000*	280,000	400,000	650,000
New Connections/Second	4000	9000	12,000	25,000	36,000

При выборе подходящей модели необходимо обращать внимание на максимальную производительность, на количество сессий и на максимальную скорость появления новых сессий. Последний параметр позволит вам жить спокойнее в случае вирусных атак в сети или на сеть. ASA, по сравнению с другими фаерволами, можно рекомендовать и по такому параметру, как количество корректно обрабатываемого трафика – здесь есть функционал для PPTP, SIP и других протоколов.

На тестовом стенде побывала Cisco ASA5520. При заявленной производительности 450 мегабит/сек (half-duplex, естественно) она показала 150 мегабит/сек full-duplex при загрузке CPU 60%. Т.е. как решение для NAT она весьма неплоха, но есть один нюанс – ее стоимость. При такой стоимости \$/Mbit рассматривать эту линейку очень тяжело.

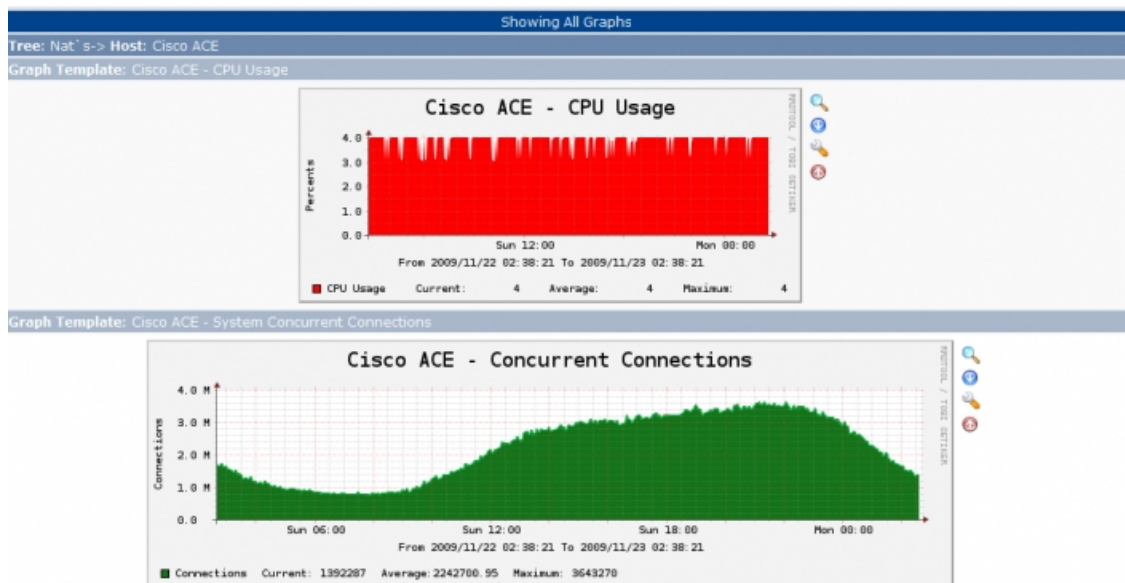
Сотовый оператор производил синтетическое тестирование Cisco ASA5580-20 (заявленная пропускная способность до 10 гигабит/сек) на сгенерированном трафике, 60% которого составлял битторрент. Получены результаты около 600 kpps, 1Gbit/s, загрузка процессора около 80%. В перерасчете на kpps – неплохой результат, на реальном трафике это будет около 3.5 гигабит/сек.

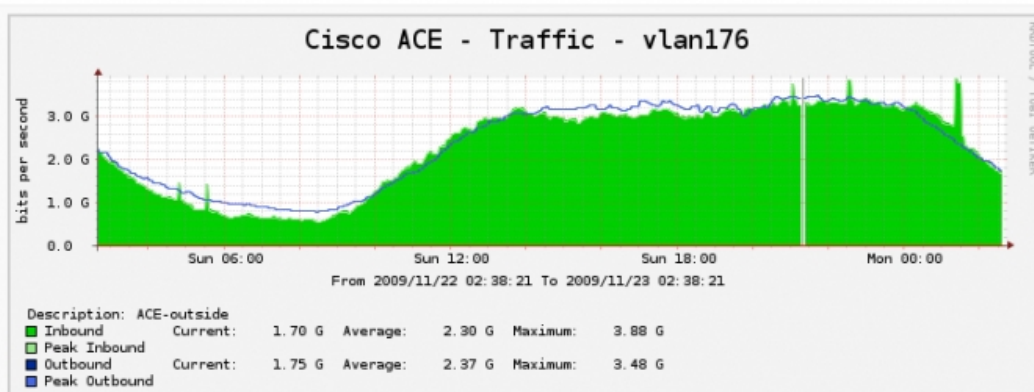
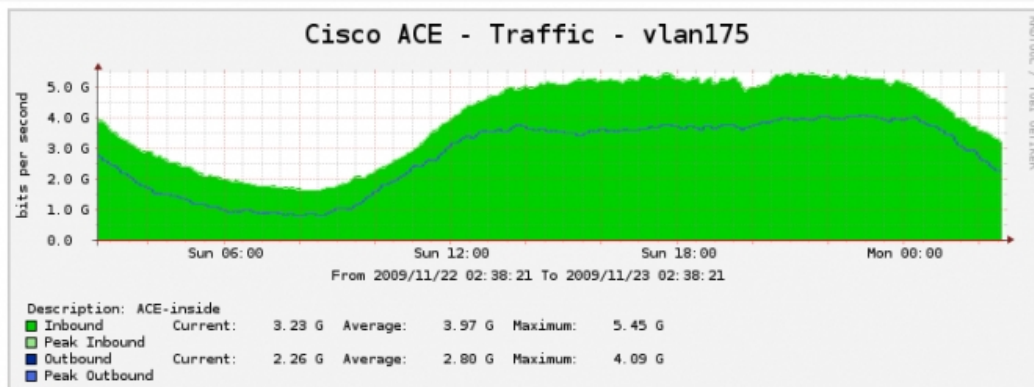
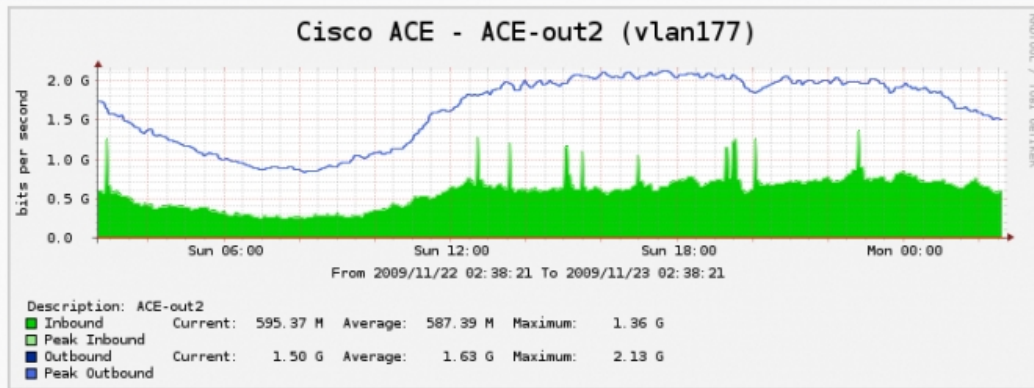
Huawei Secpath 1000F не смог в тестовой эксплуатации показать результата выше 400 мегабит/сек, и эта линейка в дальнейшем не рассматривалась.

Juniper ISG2000 так же был одним из потенциальных кандидатов на покупку. При заявленной производительности 2 гигабита/сек он казался весьма конкурентно-способным, даже несмотря на высокую цену. Но – опять же, при тестировании на реальном трафике результат с трудом дошел до 500 мегабит/сек, были выполнены рекомендованные производителем действия по отключению функционала обнаружения атак, обновлено программное обеспечение – но желаемых результатов он не достиг. Сюрпризом явилось то, что он не имеет встроенного функционала для корректной обработки специфического трафика (PPTP VPN, например). Путем изучения сайта производителя был найден пример конфигурации, в котором PPTP трафик выпускается через NAT в интернет без использования PAT (port address translation) – в дальнейшем подобное решение использовалось и для других аппаратных платформ.

В качестве NAT-маршрутизатора была также произведена попытка использования Cisco 6500/SUP32. Задача в данном случае ставилась не по выводу пользователей в интернет, а по трансляции адресов 1-в-1 «сеть в сеть», для доступа к пиринговой площадке ШПД-операторов в Москве, где у нас были проблемы с пересечением адресаций. До 300 мегабит/сек трафик Cisco показывала отличные результаты, после – наступил предел количества NAT-сессий на данной платформе, и загрузка CPU тут же взлетела до 100%. На этом эксперимент прекратили, после попыток ограничения времени жизни сессий. На Cisco 7609/SUP720 при 4 тысячах пользователей, пытающихся получить доступ к сети /24 (опять же, проблемы с пересечением адресаций) с локальными игровыми серверами, файловыми, DC++ хабом и прочими внутрисетевыми ресурсами – получен примерно такой же результат.

На сегодняшний день используется и работает модуль Cisco ACE. Решение, которое казалось наименее функциональным и меньше всего рассчитанным на проблемы ШПД, явилось наиболее производительным и оптимальным по параметрам цена/производительность. Наиболее «говорящим» в данном случае будет снимок с системы мониторинга:





Лимиты производительности модуля таковы:

- трафик - 16 гбит/сек half duplex
- 8 000 000 одновременных соединений

Сейчас через модуль пропущено около 35-40 тысяч пользователей, еще не вся сеть, но он осилит и больше.

При использовании модуля стоит обратить внимание на тему «NAT на ACE» на форуме, там рассмотрены многие нюансы его настройки и ограничения получившейся схемы. Но с точки зрения получения одного устройства, которое пропускает через себя действительно много трафика - это, на мой взгляд, оптимальное решение.

Shaping

1. PC-сервер

Для шейпинга на PC-серверах есть определенные ограничения. Во-первых, это ограничение по rps. Любой PC-сервер загнется, если на него придет поток в 750-900 kpps от пользователей, а такое вполне может быть в случае вирусной активности внутри сети и наличия ботнета, который выполняет команду "ддосить хост А". Во-вторых, насколько показали тесты, шейпинг на FreeBSD/Linux производится в один поток - а это значит, что об обработке шейпинга на всех ядрах всех процессоров можно забыть. Возможно, что второе ограничение снимается установкой яндексовских драйверов для сетевых карт.

Но на практике - шейпинг на PC-серверах требует очень и очень серьезной настройки системы. В

случае использования rscq-очередей по адресным спискам в Linux на входе приходится маркировать (mangle) пакеты, а это достаточно процессороемкая операция. В случае PC-сервера, выполняющего NAT и шейпинг, до 70% времени уходит на шейпинг, остальные 30% загрузки - нат. Реальные показатели шейпинга (только шейпинга, без NAT) на PC-серверах – около 800 мбит при rps около 100-120 тысяч пакетов в секунду. Дальше начинаются потери пакетов. Стоит также отметить одну особенность шейпинга на серверах под управлением FreeBSD. Как известно, параметры шейпинга и точность нарезки канала очень сильно зависят от параметра ядра HZ. Этот параметр задает количество срабатываний внутреннего таймера прерываний в секунду, как правило, он ставится в значение 1000. При необходимости шейпинга трафика на больших количествах очередей и при высокой загрузке сетевой системы по количеству пакетов в секунду, значение этого параметра надо увеличивать, в противном случае пакеты будут пролетать по трубе быстрее, чем шейпер будет успевать их обрабатывать в случае превышения полосы пропускания на клиента. Так, при настройках по умолчанию, на торрент-трафике есть шансы выдать клиенту не 5 мбит/сек, а все 25. В случае шейпинга на ОС Mikrotik данная особенность обнаружена не была.

2. Софт-рутеры

В качестве платформ для массового шейпинга клиентов софт-рутеры часто используются в случаях использования на сети туннельных методов авторизации и доступа в интернет. Это может быть PPPoE, PPTP или L2TP, редко когда это vlan-per-customer. Но, как правило, ограничение скорости применяется целиком к интерфейсу, который смотрит только на одного клиента. Не очень сильно развит вариант ограничения скоростей на разделяемых между пользователями интерфейсами в случае ISG, но его тоже не стоит выбрасывать из вида. На софт-рутерах часто используется даже не шейпинг, как мы привыкли использовать на PC-серверах, а рейт-лимитинг или полисинг. Это несколько отличающиеся технологии ограничения скорости для пользователей. При использовании ограничения скорости на интерфейсе очень часто ограничение накладывается на весь интерфейс, а не на определенные классы трафика. Более того, не каждый маршрутизатор умеет определять классы трафика на интерфейсе и применять к нему заданные политики. Если при использовании FreeBSD провайдеры могли управлять шейпингом клиентов достаточно свободно, то при использовании туннелей такая гибкость в управлении скоростью зачастую бывает не очень доступна. Из туннельных применений (PPTP или PPPoE) наиболее широкое распространение в российском ШПД, на мой взгляд, получили маршрутизаторы Cisco 7200 и 7301. Стойку и целый датацентр даже Cisco 7301/7204 использовала Корбина для терминирования PPTP. Количественные показатели по трафику, полученные на данных представителях, таковы: до 400 мбит трафика, до 2000 туннелей. Больше – уже тяжело. При использовании ASR1002/ESP10 удавалось получить до 15 000 туннелей на пользователей и несколько гигабит трафика (информация с форума nag.ru). Cisco 7140 терминировала до 600 клиентов по PPTP, трафик при этом был порядка 80 Мбит/сек.

В случае с софт-рутерами других производителей ситуация обстоит примерно так же, ни на каком железе, кроме совсем новых вариантов, не снять большую производительность на задачах шейпинга. Среди софт-рутеров новых линеек как раз посмотреть на то, что они могут, будет очень даже интересно. Но, насколько я понимаю, кроме Cisco и Juniper, новых линеек маршрутизаторов из производителей практически никто и не анонсировал. При этом я бы не стал сравнивать Juniper MX 3D с маленькими рутерами Cisco – типа 28xx, 38xx, и даже с 72xx. А тестов и реального использования Cisco ISR G2 пока не наблюдается, линейка только недавно анонсирована. Но – если надо много шейпить на туннелях – то Cisco ASR на текущий день является очень достойным выбором. В случае же не туннельных применений шейпинга клиентов на софт-рутерах и без использования ISG-функционала – то конфигурация устройства становится весьма нетривиальной, это порождает громадные полиси-мапы на интерфейсах, много списков ACL и другие вещи, которые в итоге ручной просмотр и изменение конфигурации маршрутизатора делают практически нереальными. Выходом в подобной ситуации является или ISG, на котором Cisco 7200/7301 показывают почти такие же результаты, как и в случае с терминированием туннелей, или использование специального синтаксиса для массовой классификации пользователей и ограничения их скорости – UBRL в терминологии Cisco. Но UBRL как функционал на софт-рутерах недоступен на текущий день. При использовании rate-limit для удовлетворения пользователей достаточно часто надо выставлять параметры ограничения скорости на несколько процентов больше, чем требуемая скорость – это снижает загрузку технической поддержки жалобами пользователей на то, что «в зоопарке тиграм недокладывают мяса», особенно это ощущается при коротких тестах скорости, когда передается 1-10 мегабайт данных, а не ощутимо большой кусок, который бы показал вменяемую скорость на тесте. Так же при rate-limit надо обращать внимание на то, что правильность выдачи полосы с точки зрения пользователя будет сильно зависеть от вида трафика. Если tcp-трафик сможет согласовать параметры передачи под формат канала, то udp-трафик таких механизмов не имеет.

3. Аппаратные платформы

При использовании аппаратных платформ для задач массового ограничения скоростей клиентам наибольшее распространение получили следующие варианты работы:

- UBRL на Cisco 6500/7600 SUP32/SUP720/RSP720

- BRAS/ISG функционал

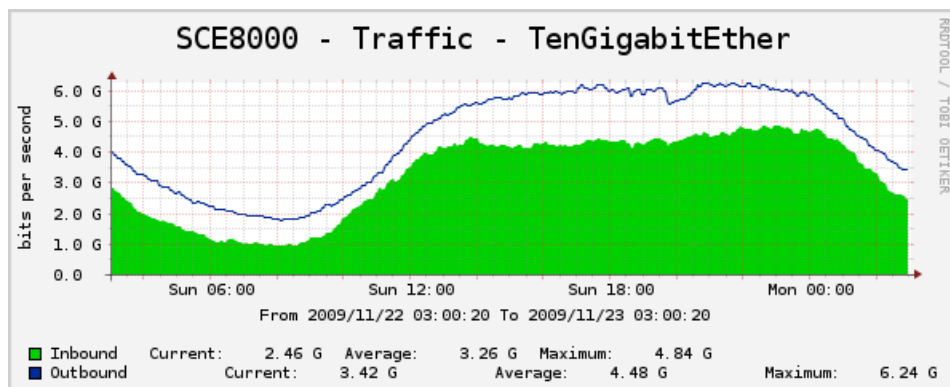
Использование UBRL на Cisco 6500/7600 накладывает ограничения на количество очередей, которые мы можем использовать на одном устройстве, и то, что мы можем использовать только rate-limit. Также к серьезным недостаткам данного решения стоит отнести то, что изменение больших access-list'ов на Cisco 6500/7600, даже при удалении/добавлении всего одной записи, может привести к 100% загрузке CPU. Также используемые внутри алгоритмы оптимизации ACL не позволяют использовать ресурсы ACL TCAM на 100%. Документация по настройке на сайте находится по адресу http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_white_paper0900aecd803e5017.html, там же есть и ограничения по использованию в зависимости от типа управляющего модуля.

Table 2. Supervisor Engine 720 NetFlow Capacities

Supervisor	PFC Type	Total Capacity	Effective Capacity	Hash Efficiency
Supervisor Engine 720	PFC3a	128 K	64 K	50%
Supervisor Engine 720-3B	PFC3B	128 K	115 K	90%
Supervisor Engine 720-3BXL	PFC3BXL	256 K	230 K	90%

Использование UBRL на этих устройствах приводит еще и к невозможности совместного использования этого функционала с netflow, что может так же явиться одним из факторов при принятии решения.

В случае использования BRAS/ISG функционала рекомендуется применение других аппаратных линейных карт, со встроенными очередями. В случае с Cisco это будет ES20+ и подобные, в случае с Juniper – то использование маршрутизаторов E-серии или, в случае с MX-серией, DPCE-R-Q-карт. Есть альтернативный вариант ограничения полосы пропускания в зависимости от трафика. Это решения Cisco SCE. Решение представляет собой «шейпящий мост». Производительность для модели 2020 составляет 3.6 гигабит/сек half duplex, SCE8000 – 15 гигабит half duplex на один модуль DPI и до 30 гигабит/сек на коробку в случае двух модулей. Устройство позволяет вести базу данных пользователей, тарифы с разделением трафика по приложениям, адресам, портам, времени доступа, количества скачанного трафика за последний час/день. Бандл Cisco SCE8000 стоит 110K по GPL, и способен обработать до 50 тысяч пользователей в реальной жизни (далее просто трафика больше производительности одного модуля DPI. Если у вас тарифы 1-2-3Мегабит, а не 10-20-30, то и по количеству пользователей соответственно).



Конкурентами Cisco SCE с похожим функционалом являются решения компаний Arbor/Allacoya, Huawei (совместно с Symantec), Iproque.

Часть вторая