DPI

Жил да был большой провайдер, пропускал пакеты, ограничивал понемногу трафик. Всем было счастье. Или почти всем. До тех пор, пока кто-то не сказал: "Нам мало средств контроля трафика". Так в уютной обжитой сети появился DPI. Эта молодая бестия со своим уставом лезет в самую глубину пакетов, куда не добраться простым файрволам.

Системы DPI (Deep Packet Inspection) приобретают всё большую и большую популярность, несмотря на их астрономическую стоимость. Сейчас почти у каждого большого вендора есть своё решение. У Cisco это Cisco SCE, у Huawei - SIG9800, у Juniper -VXA. Есть и менее известные компании, которые производят преимущественно оборудование DPI. Например, Allot или Inline Telecom с их Sandvine. Вроде бы, даже русские ребята засветились: Traffica.

Так чем же так занимательны эти комплексы, стоящие каких-то заоблачных денег? Ваш непокорный слуга посвятил несколько месяцев интеграции DPI и я имею, что сказать.

Какие у нас сейчас есть средства управления трафиком?

1. На основе MAC-адресов или VLAN’ов. Очень грубо.
2. По IP-адресам получателей или отправителей. Так сейчас зачастую и делают.
3. По портам TCP и UDP. Так тоже делают.
4. На прокси-серверах можно ограничить по доменному имени. Но вы представляете себе прокси-сервер для абонентов в сети провайдера?

На основе вышеуказанных параметров пакета можно строить ACL или настраивать QoS. Но, положа руку на клавиатуру, сможете вы ограничить доступ на один только блог в ЖЖ, не закрывая сам ЖЖ? А сможете вычленить трафик торрента из кучи остального?

То есть в руках у вас сейчас есть инструменты stateful файрвола, который максимум добирается до транспортного уровня (4 из 7). DPI позволяет врезаться в самую глубину пакета, анализируя данные на всех уровнях OSI с 1-го по 7-й. На то он и Deep. Даже туннели без шифрования (QinQ, GRE, MPLS и т.д.) ему по зубам.

Итак, что же он на самом деле может:

1. Собирать самую разнообразную статистику. Практически любой каприз маркетологов вы теперь преподнесёте им на блюдечке.
2. Фильтровать (вычленять) трафик по определённым критериям. Тут к очевидным IP-адрес+порт прибавляются доменные имена и протоколы. Например, сложновычисляемый трафик P2P или Skype определяется тут на ура.
3. Применять на абонентов всевозможные политики. Они могут быть, как статическими - вы сами выбираете кому, что и когда можно, и с какими приоритетами - так и динамическими - есть где-то один централизованный сервер, который отвечает на эти вопросы. К слову, абонентами могут быть не только обычные пользователи фиксированных сетей, но, также, к примеру, и беспроводных, со всеми присущими атрибутами (могут отслеживаться APN, номера телефонов, способ доступа - GERAN, UTRAN...)
4. Предотвращение атак. Речь идёт о сетевых атаках извне, таких как DoS, сканирование портов. Также детектируются некоторые атаки изнутри
5. Благодаря возможности зеркалирования и перенаправления трафика возможны всякие приятные штуки, вроде проверки почты на спам или трафика с вебсайтов на вирусы.

Каким образом шайтан-машина определяет атаки и принадлежность трафика тем или иным протоколам? Для этого у неё есть три пути:

1. Явно заданные правила. Например, вы сами решили вычленить трафик nag.ru и индикатором является фраза "nag.ru" в заголовке HTTP;
2. Сигнатуры. Они подготавливаются вендором и содержат набор самых разнообразных правил, на основе которых будет фильтроваться трафик. Вполне возможно, что этот файл будет подготовлен с учётом ваших пожеланий. Файл сигнатур периодически обновляется и, в зависимости от производителя, либо автоматически скачивается оборудованием, либо нужно сделать это вручную;
3. Анализ поведения. В этом пункте вся философия слова Deep в названии. Многие системы DPI позволяют на основе "странностей" в поведении трафика совершать действия - определить протокол или обнаружить и предотвратить атаку.

Самый простой пример: запустили вы сканер портов. Программа обращается к указанному адресу и перебирает все 65 535 портов протокола TCP, например. Ежу же понятно, что никакая здоровая программа не будет устанавливать такие дикие соединения - это колокольный звон для DPI, что в сети что-то неладно.

Мне довелось потрогать и даже покопаться с лихвой в командной строке SIG9810 - DPI решения Хуавэй. Поэтому про его интеграцию я и расскажу. Думаю, что принципы работы оборудования любого другого вендора отличаются незначительно.

Оборудование DPI ставится в разрыв, что весьма логично. То есть, очень грубо говоря, так:

Весь трафик, разумеется, проходит через систему, где на него и применяются политики и снимается вся статистика.

В плане железа DPI состоит из следующих компонентов:

1. Bypass;
2. Устройство Front-End;
3. Устройство Back-End;
4. PCRF-сервер (Policy and Charging Rules Function);
5. Коммутаторы для обеспечения связности между компонентами.

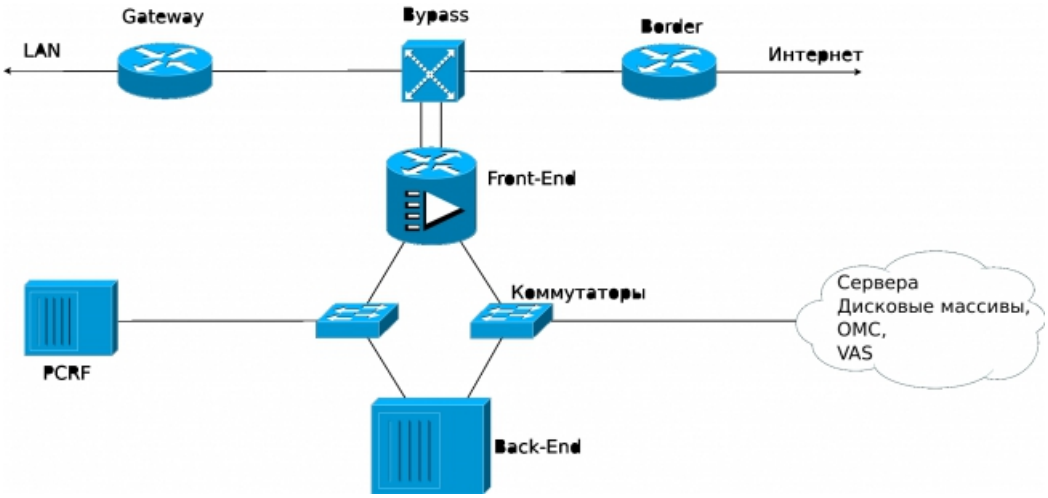
Опционально:

6. Серверы (мониторинг состояния системы, syslog);

7. Дисковые массивы (для хранения статистики и для серверов);

8. Устройства VAS (Value Added Services - проверка на спам и вирусы, родительский контроль).

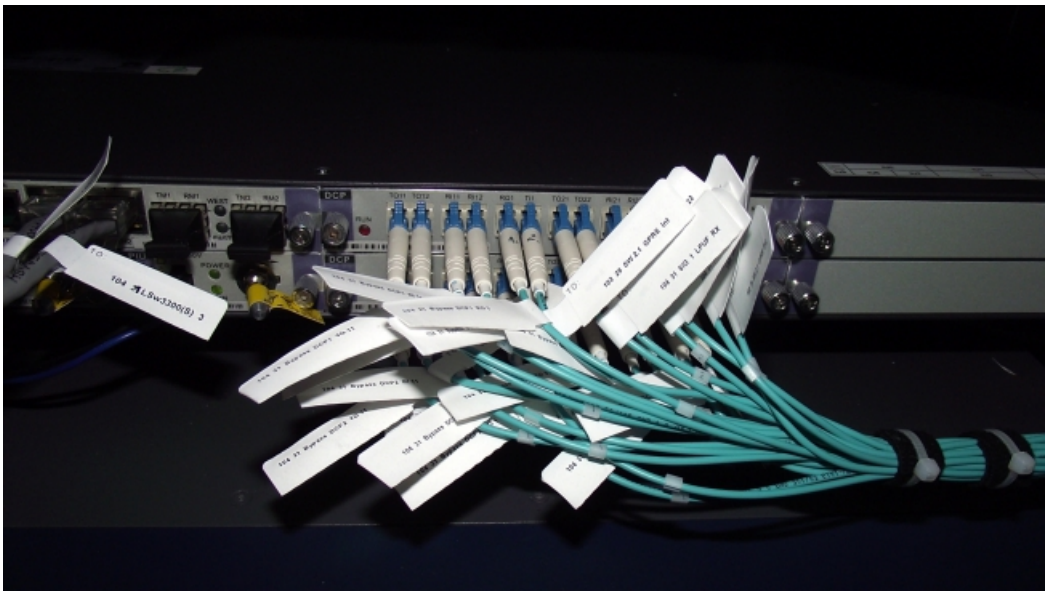
Типовая схема выгляди так:



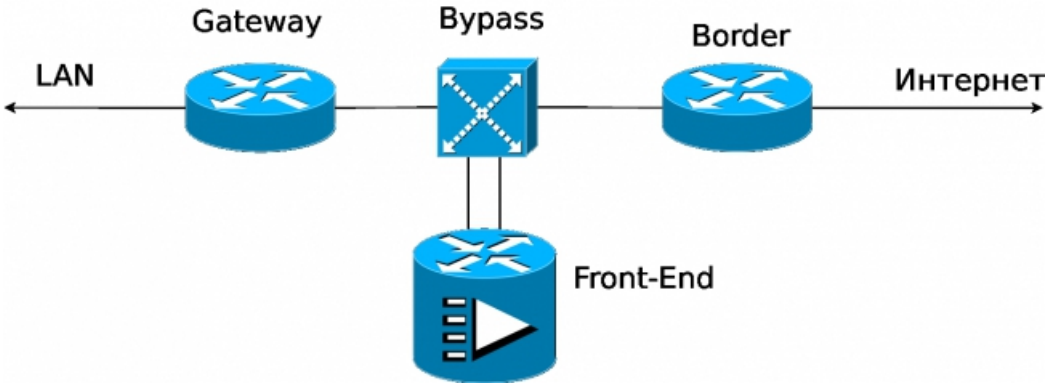
Всё это вместе занимает 2-3 стойки.Расскажу по порядку о каждом из них.

1) Bypass

Что происходит, когда в сеть вы добавляете ещё один элемент? А тем более стойку? Верно, появляется ещё одно слабое звено. Bypass призван хоть немного исправить это положение.

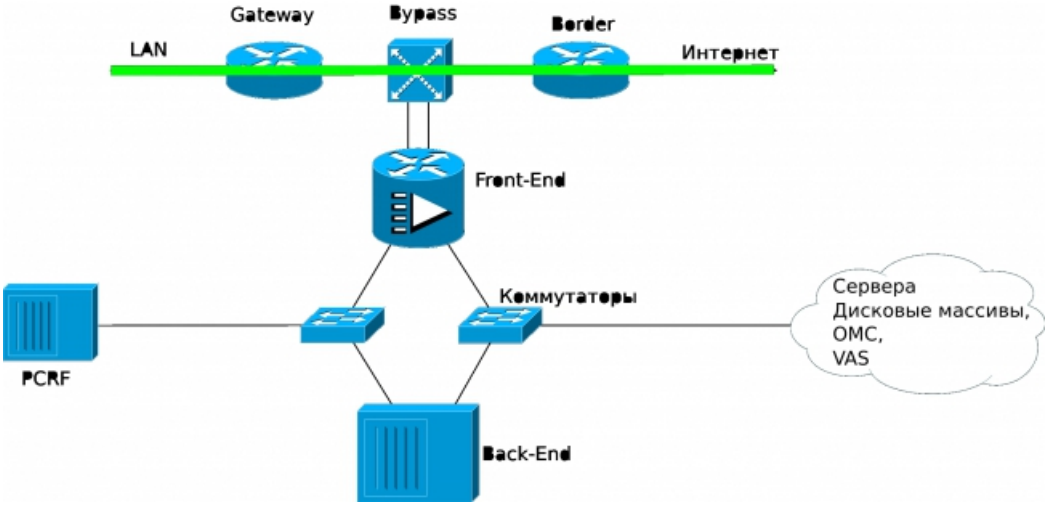


В сеть оно включается первым и уже к нему подключается Front-End.

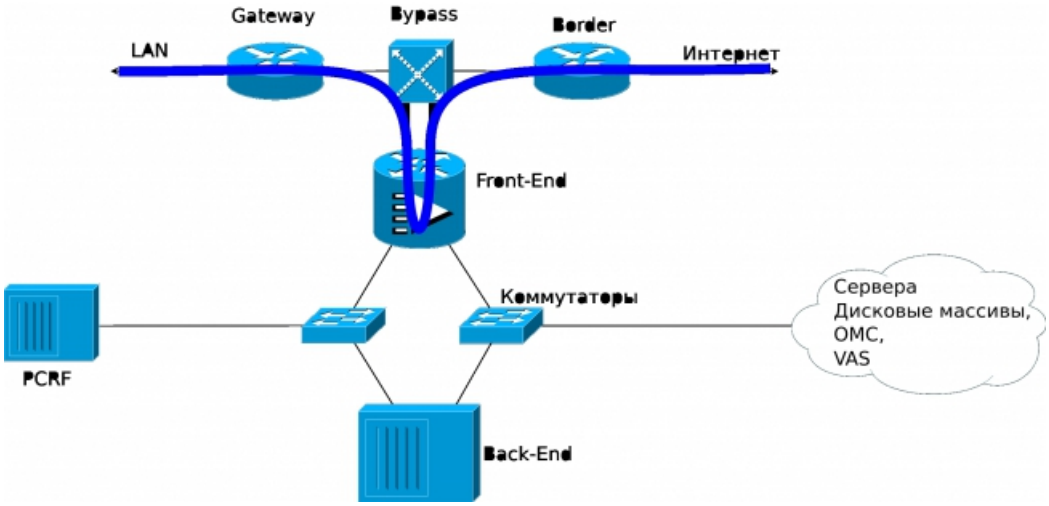


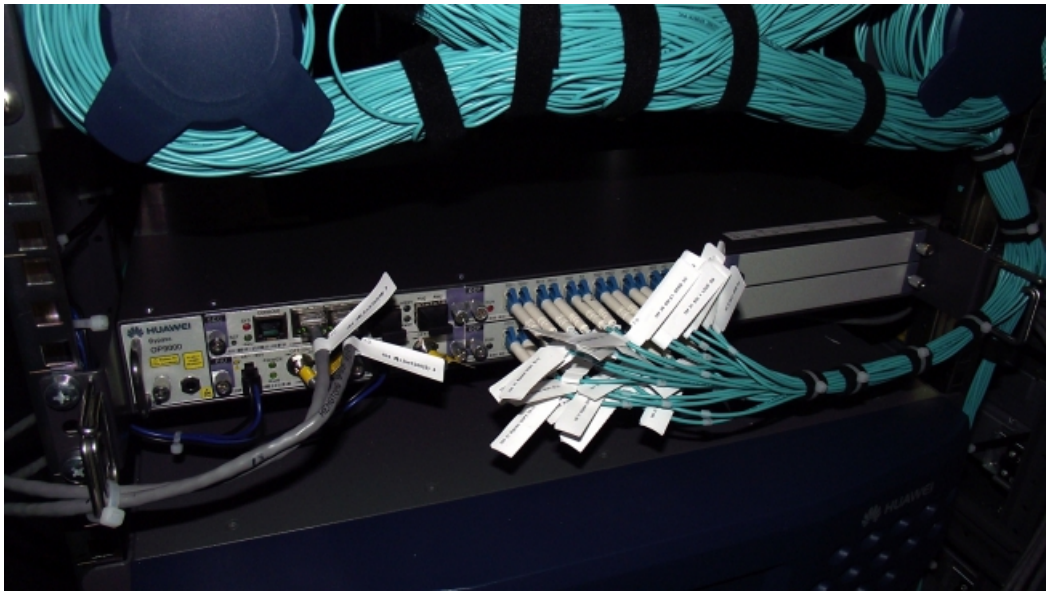
У него есть два режима работы:

1. Защитный. Трафик проходит напрямую и не заворачивается на Front-End



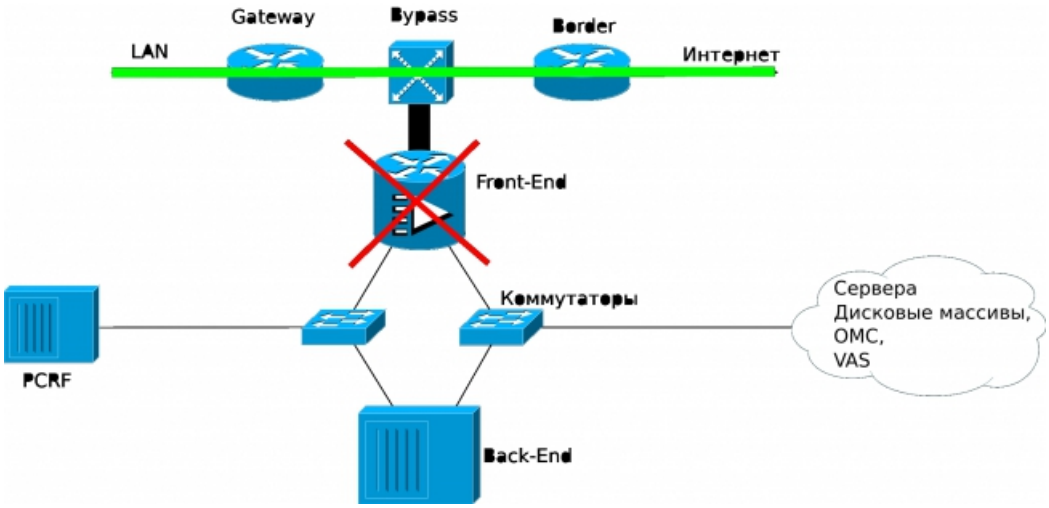
2. Рабочий. Трафик заворачивается на Front-End, но в случае чего переключается на прямой канал, как в первом случае.



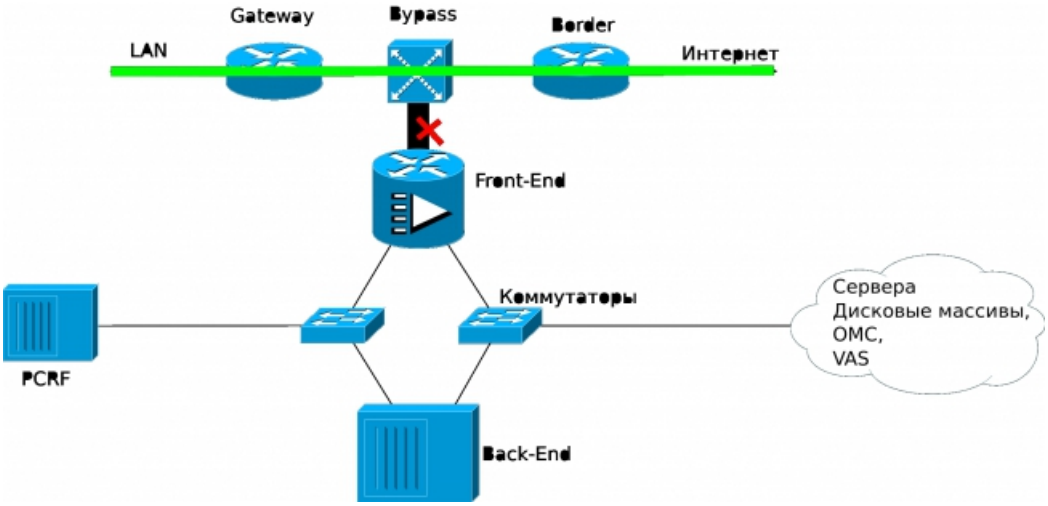


Bypass всеми силами будет пытаться удержать связь.

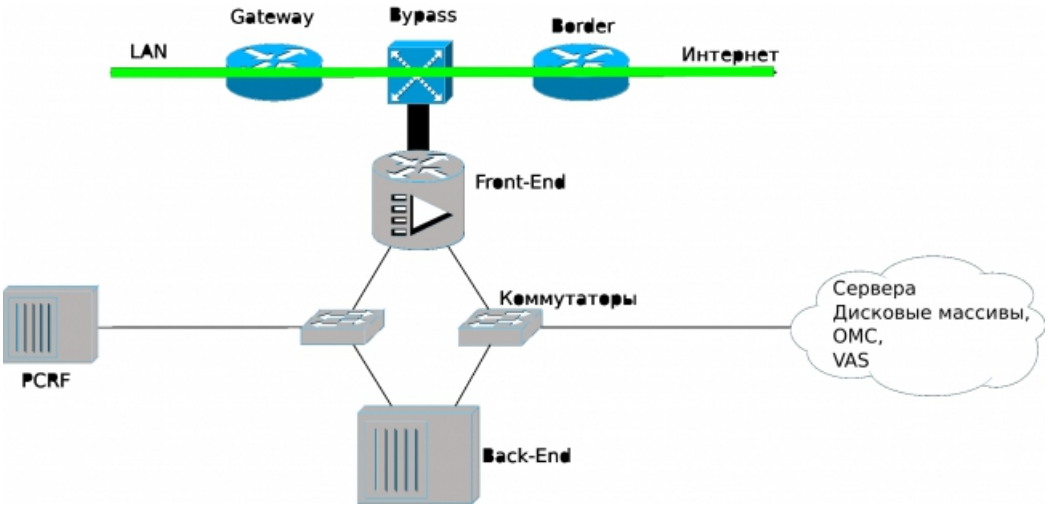
Ломается Front-End (сгорела плата) - трафик переключается на защитный канал.



Рвётся линк до Front-End’а (сгорел порт, повредился кабель) - трафик переключается на защитный канал.



Выключилось электричество - трафик переключается на защитный канал.



Bypass’ы бывают электрическими и оптическими. Электрические основаны на реле и применяются с медными проводами, то есть максимальная скорость, на канал 1 Гб/с.

Оптические сильно круче. Помимо того, что скорость на канал до 10 Гб/с, существует возможность зеркалирования трафика задаром - световому лучу не убудет. То есть в то время как трафик идёт по прямому каналу, его копия направляется на Front-End. Действия над трафиком никакие ещё совершать нельзя, но статистику уже собирать вполне можно.

D

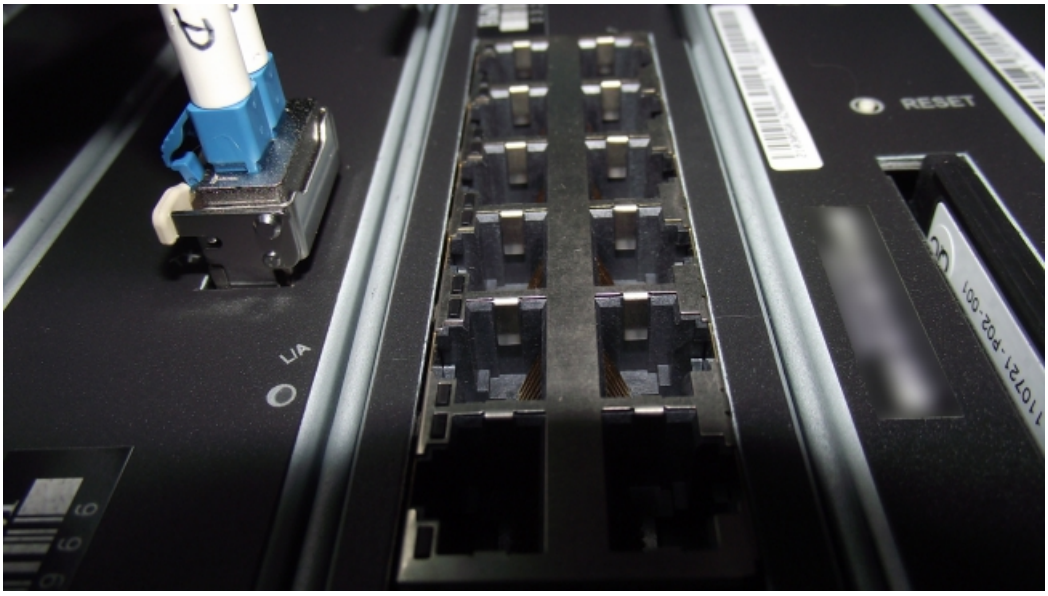
2) Front-End

Это адская молотилка. Через неё несутся гигабиты, именно в нём каждый пакет разбирается по байтикам, именно в нём трафик каждого абонента подвергается экзекуции в соответствии с политиками.

По сути это очень мощный модульный маршрутизатор.

В нём есть голова - платы управления самим устройством - их, как правило, две - мастер/слейв.

Есть линейные платы, отвечающие за приём-передачу трафика, то есть физический, канальный и немного сетевой уровни.



Есть фабрики коммутации, которые отвечают за передачу данных между платами.

И наконец, руки - процессинговые платы, которые и перелопачивают эти кучи, накладывают ограничения, собирают статистику и успевают при этом взаимодействовать с Back-End и с PCRF-сервером, запрашивая политики и передавая данные на них.

3) Back-End

Это огромный сарай, куда складируется всё подряд. Тут лежат подробности всех политик, вся собранная статистика, сигнатуры, правила зеркалирования и перенаправления, радиус-пакеты отправляются сюда и прочее-прочее. Что угодно в любой момент можно извлечь.

В плане железа у Хуавэй это блейд-сервер. Каждая плата дублируется. Некоторые из них на горячей замене, другие организуют балансировку нагрузки.

4) PCRF-сервер

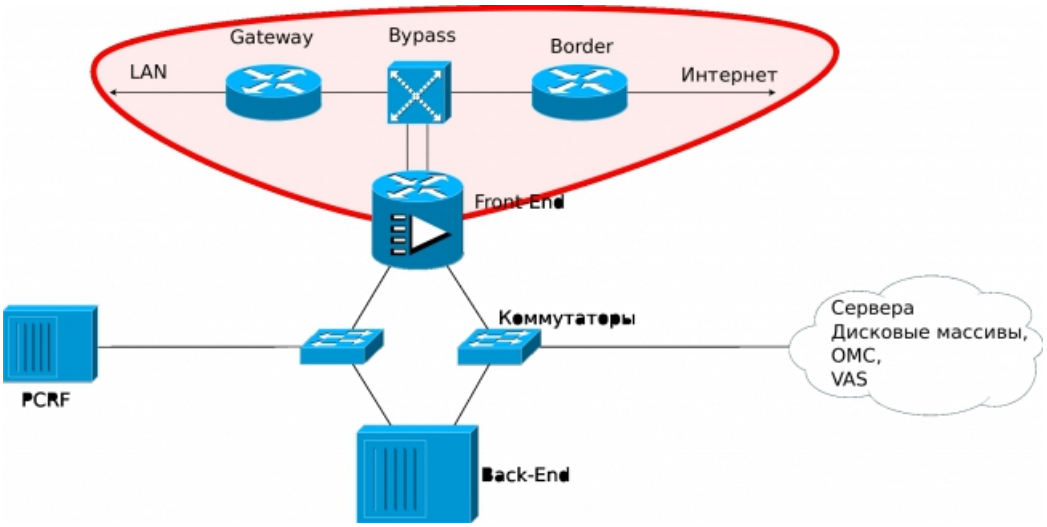
Очень грубо говоря, он хранит соответствия: пользователь - номер политики. Front-End отправляет ему идентификатор абонента, тот возвращает номер политики, Front-End запрашивает подробности соответствующей политики на Back-End’е.

Как правило, PCRF-сервер один на множество сайтов.

С точки зрения сети DPI можно разделить на три части:

1) супервысокоскоростная часть;

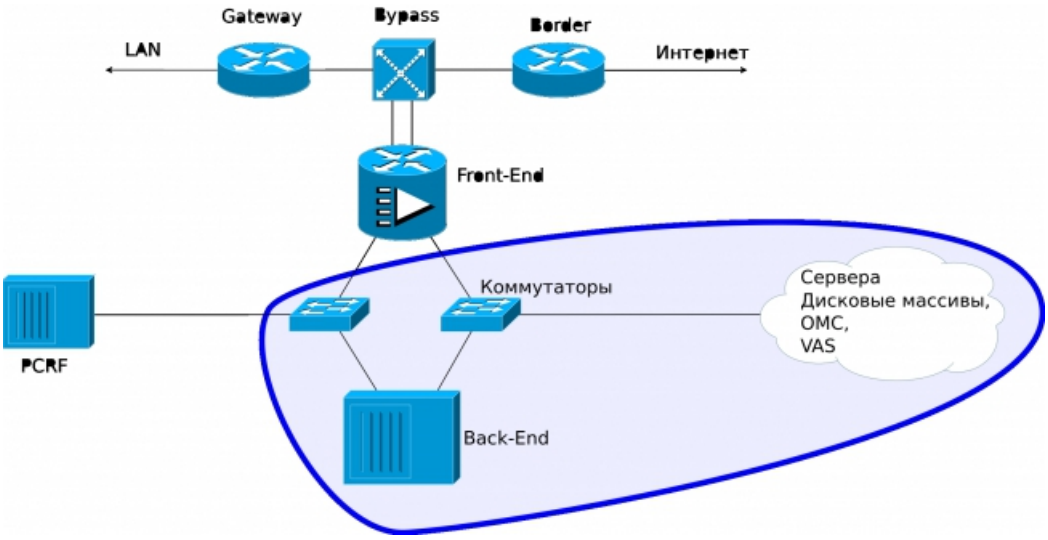
Трафик пользователей



Исчисляется Гигабитами в секунду

2) Сеть взаимодействия компонентов (FE, BE,сервера);

Тут трафик небольшой и гагибитного (даже сотки) с лихвой. По этой сети ходит только служебная информация.



3) управление и PCRF - стык с внешней (для DPI) сетью.

Это каналы в сеть OMC (operation and maintenance center) транзит до PCRF-сервера. Также только для служебных целей - доступ на оборудование и NMS (Network Management Server).

PCRF.png

[DPI]

На практике

Статистику можно собирать самую богатейшую. Приведу несколько примеров:

Общий трафик по городу с разделением по различным типам:

[DPI]

То же в виде пирога:

[DPI]

Какой хостинг видео преобладает:

[DPI]

Топ 10 сайтов по числу соединений:

[DPI]

Топ 10 сайтов по объёму трафика:

[DPI]

Трафик по каждому абоненту отдельно в категории WEB:

[DPI]

Самые активные пользователи:

[DPI]

А вот пример применения политик: всё делается на лету - и между командой и её эффектом проходит пара секунд.

На картинке показано действие политики, ограничивающей общий трафик до 700 кб/с, при этом приоритет на видео (зелёный), а для P2P (фиолетовый) гарантировано 200 кб/с.

[DPI]

А это пример использования просто приоритетов. Общее ограничение также на 700 кб/с, наивысший приоритет у видео (зелёный), на втором месте FTP (красный) и на последнем фиолетовый P2P

[DPI]

Политики тоже можно задавать очень гибко:

- ограничивать общую скорость трафика вплоть до блокировки;
- ограничивать скорость трафика по каждой категории (веб, видео, p2p, IM и так далее) отдельно вплоть до блокировки;
- выделять полосу для каждого типа трафика (например, не более мегабита/с, но 200 кб/с должно быть гарантировано);
- указывать приоритет для каждого типа.

И другие менее очевидные способы.

[DPI]

Я люблю всякие огромные махины, вроде КрАЗа, БелАЗа - чувствуется невообразимая мощь в урчании их двигателей и лёгкий трепет перед ними. Очень похожие ощущения от работы с DPI. Словами не передашь турбинного потока воздуха из кулеров, мигания десятков светодиодов в темноте машинного зала, тугого жгута оптических проводов, уходящих в загадочный Bypass и те, почти неограниченные, возможности, которые он предоставляет. Возможностям, которые делают вас не администратором сети, но хозяином.