Deep Packet Inspection (DPI)

ЧАСТЬ 1 - ТЕХНОЛОГИЯ DPI

Содержание

- О целях
- Определения и общие описания
- История развития оборудования с DPI
- Применение DPI систем
- Оборудование DPI
- Экономическая часть DPI
- Правовая часть DPI
- Источники

Введение

О целях данной презентации

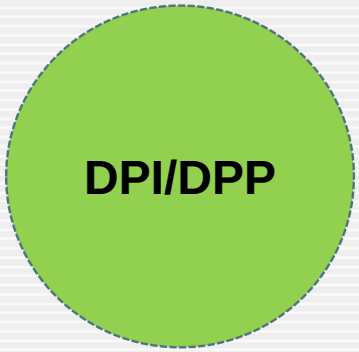
Получить представление о технологии DPI

- Что такое DPI
- Назначение DPI
- Возможности DPI
- Оборудование для DPI
- Примеры расчета DPI
- Правовые аспекты DPI

Дискуссия по теме DPI – обмен опытом, получение замечаний

Определение DPI и DPP

Deep Packet Inspection (сокр. DPI) — совокупное название технологии, позволяющей проводить накопление, анализ, классификацию, контроль и модификацию сетевых пакетов в зависимости от их содержимого в реальном времени.



Определение DPI и DPP

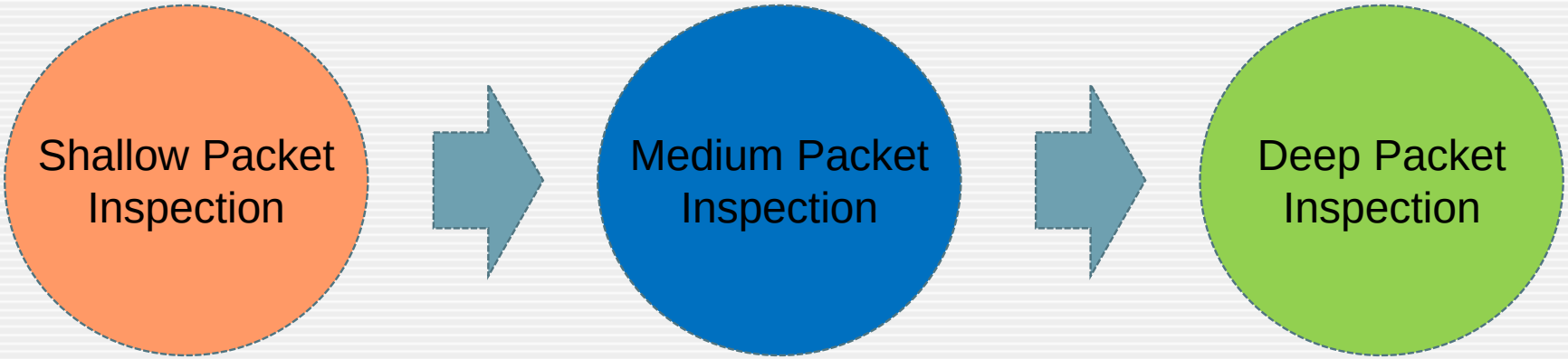
Иногда употребляют более узкий термин — DPP (Deep Packet Processing), который подразумевает такие действия над пакетами, как модификация, фильтрация или перенаправление.

Сегодня оба термина — DPI и DPP — часто используются как взаимозаменяемые.

История развития DPI

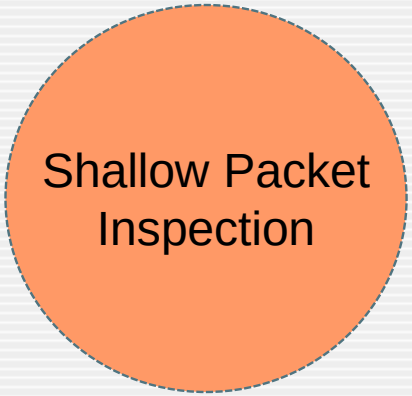
Модель развития DPI

Технологии инспекции трафика развивались последовательно, каждая последующая наследовала часть предыдущих механизмов и добавляла свои….



История развития DPI

Слабый анализ пакетов



Shallow Packet Inspection – технология анализа трафика, основывающаяся исключительно на заголовках пакета (не анализирует содержимое полезной нагрузки пакета).

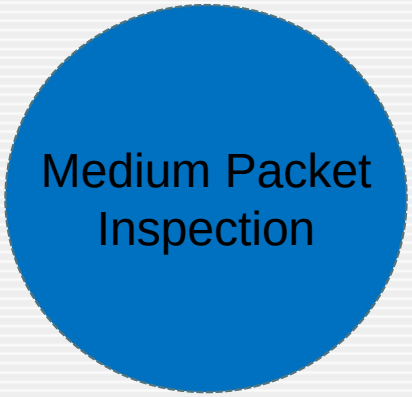
Это первая реализация технологии инспектирования трафика. Менее требовательна к ресурсам, чем MPI и DPI, за счёт чего, может обрабатывать гораздо большие объемы трафика с высокой точность определения.

Технология широко распространена, на её основе работает большинство брандмауэров операционных систем, маршрутизаторов (ACL) и т.д.

Примечание: не путать с технологией stateful packet inspection – технология проверки трафика на корректность.

История развития DPI

Средний анализ пакетов



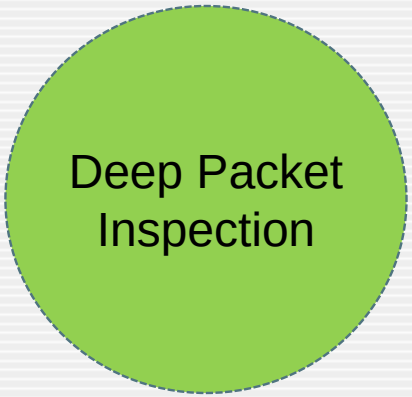
Medium Packet Inspection – технология анализа трафика, основывающаяся на инспектировании сессий и сеансов связи инициированных приложением, но устанавливаемых шлюзом-посредником. Как правило, название технологии MPI замещается обозначением «application proxy».

Частично анализирует содержимое пакетов по предопределенным правилам. Не используются сложные методы анализа (сигнатурный и т.д.)

Так же является одной из форм брандмауэра.

История развития DPI

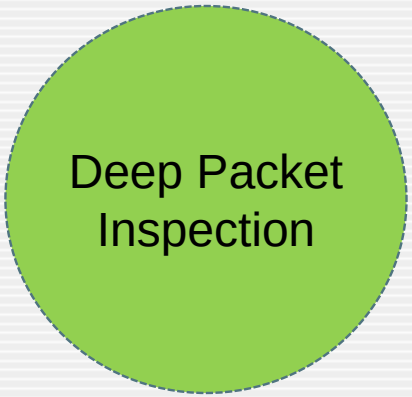
Глубокий анализ пакетов



Технология DPI возникла из-за необходимости анализировать, контролировать и управлять передаваемым трафиком. Технология DPI получила развитие, прежде всего, из-за стремительного роста вычислительных способностей чипов (процессоров), их быстродействия.

История развития DPI

Поколения DPI систем



В некоторых источниках встречается информация о поколении DPI систем управления трафиком. Отмечается два поколения таких устройств:

- Первое поколение: было приспособлено для решения более узких задач и имело только сигнатурный механизм анализа.
- Второе поколение: более универсальные и масштабируемые устройства с анализом имеющим эвристический и поведенческий механизмы, имеющие в своём составе инструменты классификации и управлениями политиками.

Иногда разделяют по поколениям исходя из производительности устройств:
1-ое поколение до 10Гибит/с, второе от 10 до 100 и третье поколение более 100.

История развития DPI

Историческая справка

- Первая DPI система управления трафиком появилась в России в 2004 году в компании Трансстелеком для использования во внутренней сети службой безопасности. Это была система компании Allot (модель не известна). Поставила систему компания RGRCom (Офф. Представитель Allot в России).
- С 2007 один из крупнейших интеграторов Inline Telecom Solutions начинает интегрировать DPI решения (в основном решения Cisco и Sandvine)
- К середине 2012 года DPI системы управления трафиком были внедрены у трех федеральных операторов:

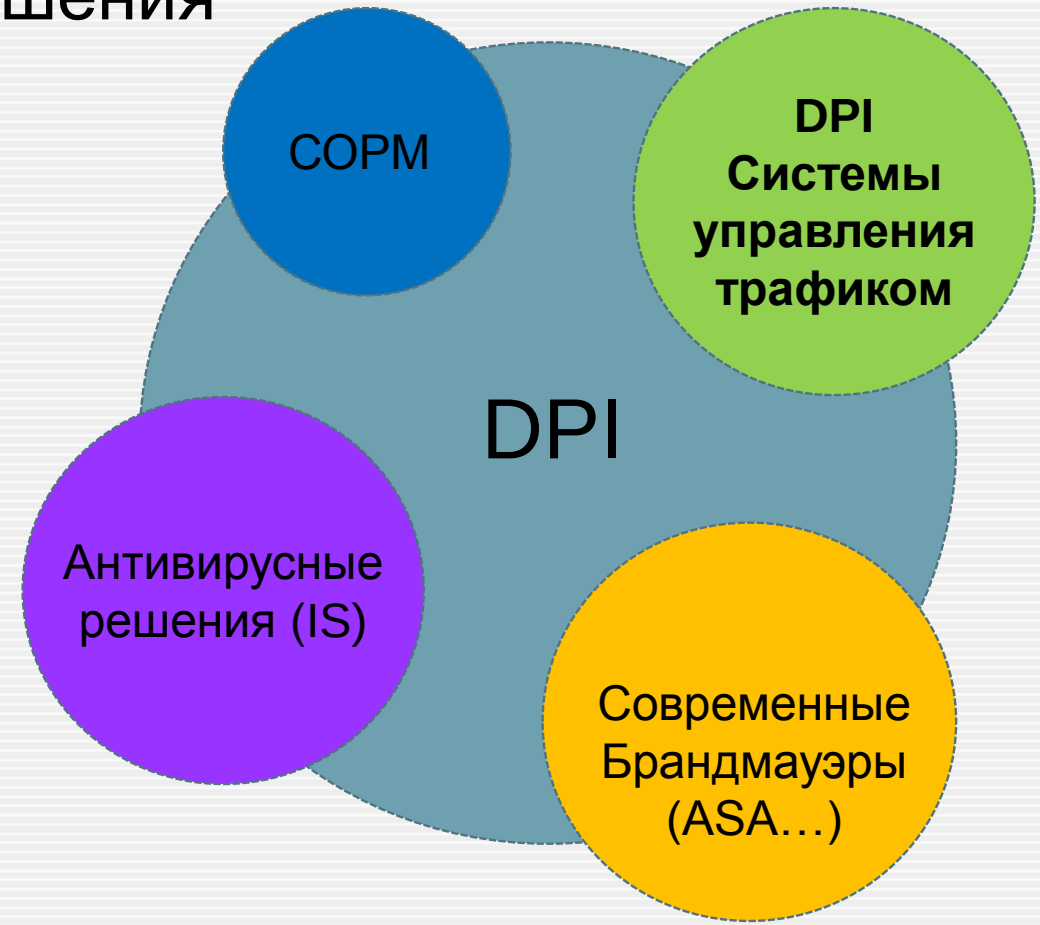
  Вымпелком – Procera

  МТС – Cisco

  Мегафон – Huawei
- 2012-2013 года, Ростелеком начинает внедрять различные DPI системы на Дальнем Востоке и Якутии.
- 2013 год, Появляется информация о том, что Ростелеком подпишет контракт с Allot на $1 млрд.
- 2013 год, разворачиваются дискуссии о интеграции СОРМ и операторских DPI системах…

Многоликий DPI

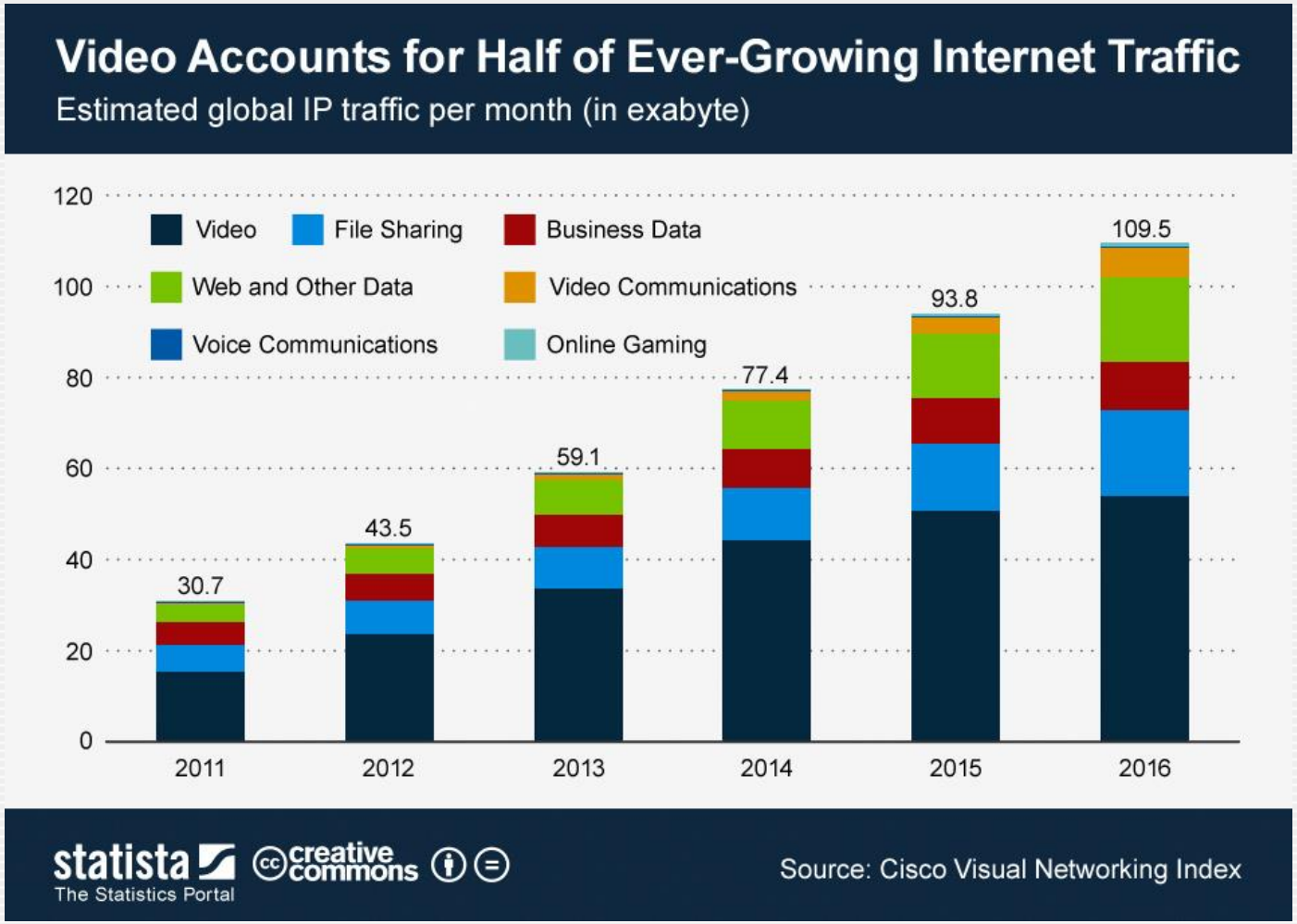
Современные решения использующие технологию DPI



Отличие DPI систем от брандмауэра

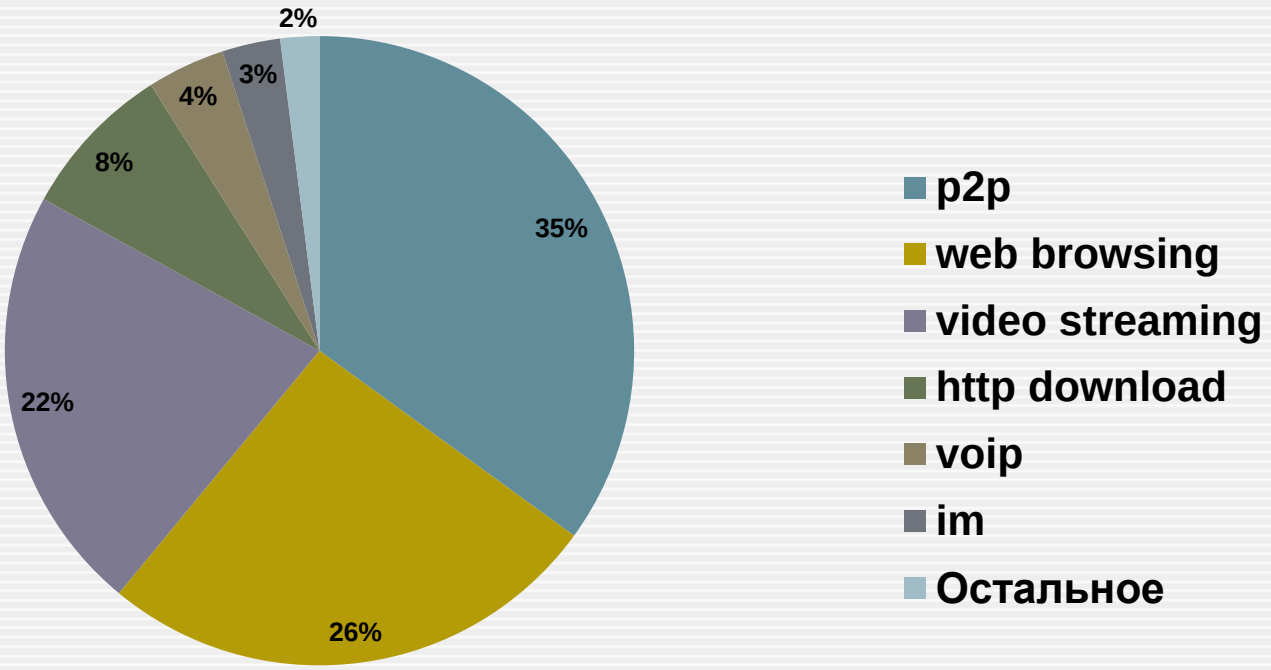
- DPI система анализирует не только заголовки пакетов, но и полное содержимое трафика на уровнях модели OSI со второго и выше.
- DPI система может принимать решение не только по содержимому пакетов, но и по косвенным признакам, присущим каким-то определённым сетевым программам и протоколам. Для этого может использоваться статистический анализ (например статистический анализ частоты встречи определённых символов, длины пакета и т.д.).
- DPI система в отличии от брандмауэра применяет различные модели действий над трафиком (классификация, ограничение полосы, приоритезация, маркировка, кэширование и т.д.)

Тренды Интернет трафика



Тренды Интернет трафика

Реальная статистика за неделю одного сегмента сети
ОАО «КБ «Искра» (ноябрь 2013)
(данные по распознанному трафику)



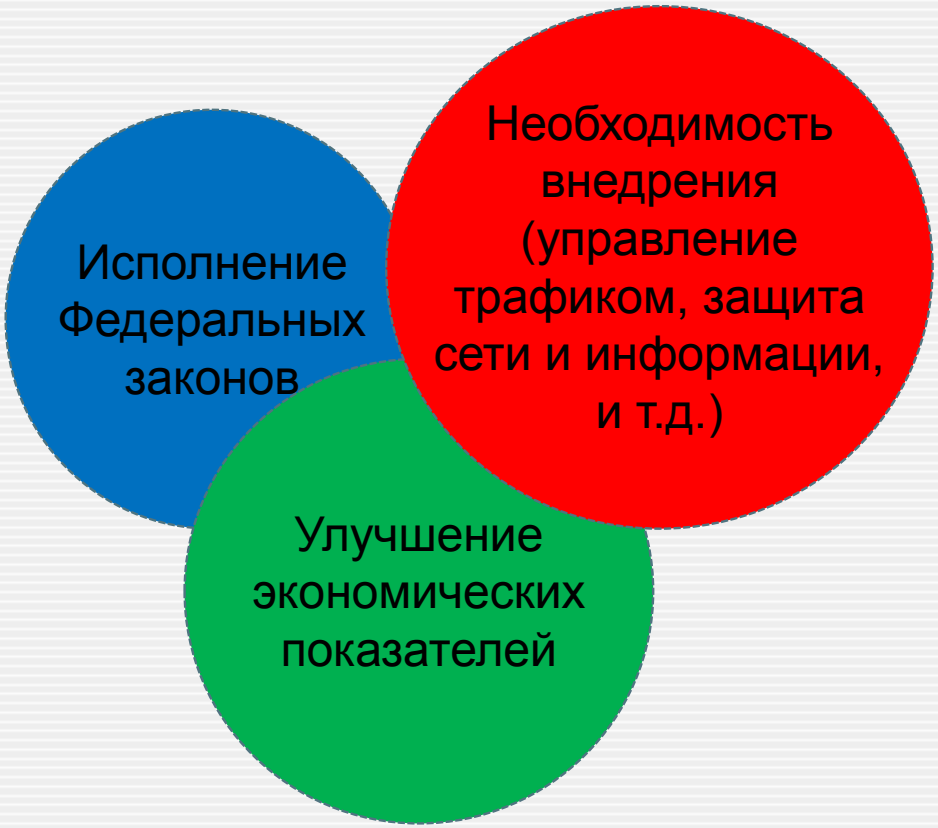
Тренды Интернет трафика

Выводы:

- По разным источникам ежегодный рост объемов трафика составляет около 25-35%
- Все типы трафика увеличивают объёмы
- Три основных типа трафика: P2P, онлайн видео и WEB браузинг
- Стремительно растёт доля онлайн видео, видео сервисы получают резкое развитие за счет онлайн кинотеатров (Netflix, VK, IVI и т.д.) и поддержки онлайн видео телевизорами и телевизионными приставками.
- Существенно увеличивается доля трафика видео-звонков и конференций

Внедрение DPI

Три основных причины внедрения DPI



Внедрение DPI

Основные направления применения DPI систем управления трафиком

Внедрение DPI

«Высокоскоростные» тарифные планы - 20, 30, 50 и 100 Мбит/с.
Только для HTTP трафика, за счёт ограничения скорости или изменения приоритета P2P приложений.

«Лёгкие тарифы» - тарифы без возможности просматривать онлайн видео, социальные сети и использовать P2P приложения - для пользователей/организаций не заинтересованных в доступе к развлекательным сервисам.

«Кнопка турбо» - дополнительный сервис позволяющий получить высокую скорость на определенный срок для всех или для избранных приложений/групп трафика.

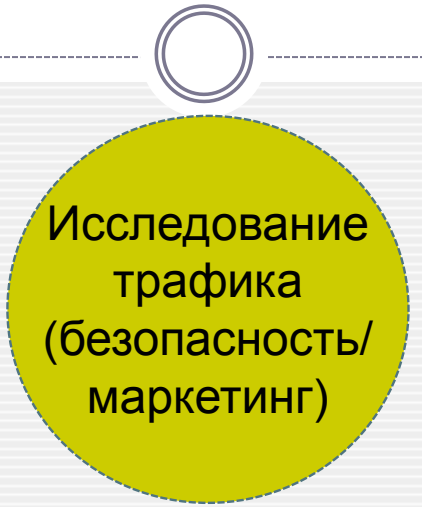
Внедрение DPI

Сейчас большинство операторов не блокируют конкурирующие сервисы VoIP, IPTV и теряют на этом как минимум сумму равную стоимости утилизации своих каналов связи. Таким образом, пропуская бесплатно ЁМКИЙ риал-тайм трафик внешних сервисов, оператор связи наносит себе экономический ущерб, из-за необходимости практически гарантированно на длительное время выделять необходимую полосу.

Оператор должен зарабатывать на своих сервисах!

DPI системы управления трафика позволяют не только ограничивать подобный трафик, но и управлять им помогая реализовать его как дополнительные сервисы.

Внедрение DPI



DPI системы управления трафиком широко применяются для решения вопросов безопасности. Большинство DPI решений позволяет бороться с вредоносным трафиком в сетях операторов. Так же существуют решения для обеспечения безопасности в корпоративных сетях компаний различного размера.

Исследование трафика в сети оператора позволяет техническим специалистам точно планировать строительство сети, своевременно решать вопросы связанные с её масштабированием.

Маркетологам исследование трафика позволяет выстраивать политику продаж, повышать эффективность тарифных планов и ,как следствие, планировать доходы и расходы.

Внедрение DPI

Маркировка цифрового контента позволяет устанавливать источники утечки и распространения не легальной цифровой продукции. С помощью DPI систем управления трафиком возможно отслеживание и блокирование источников того или иного контента в сети.

Сейчас технологии цифровой маркировки информации широко используется правообладателями и распространяющими компаниями. Судебные тяжбы стали частью бизнеса и приносят высокий доход правообладателям.

Внедрение DPI

В большинстве случает операторские DPI решения управления трафиком позволяют снизить нагрузку на сеть от 25 до 50%. Это возможно за счет управления, оптимизации и ограничения трафика P2P приложений и онлайн видео сервисов.

Так же оптимизировать ресурс каналов передачи данных возможно за счет борьбы с паразитным трафиком.

Внедрение DPI

Реклама как бизнес оператора связи

Рынок рекламы – огромный, и это можно увидеть двигаясь на работу, смотря телевизор, веб-сайты и т.д.

На сегодняшний день появилась компании, предлагающие развернуть системы целевой рекламы операторам связи.

Рекламный сервис iMarker предложил интернет-провайдерам еще один источник доходов. Операторам предлагается заработать на адресной интернет-рекламе, бесплатно установив фирменную систему анализа трафика iMarker. Система представляет из себя по сути DPI систему контроля и управления трафиком.

Внедрение DPI

Система сможет отслеживать любой незашифрованный трафик пользователей — от электронной переписки до личных сообщений в социальных сетях. iMarker будет собирать и анализировать данные о том, какие сайты посещает пользователь и сформирует его потребительский профиль.

Это позволит компании iMarker и её партнёрам производить таргетинг рекламы по интересам и, тем самым, повышать получаемую от продажи рекламы прибыль.

Сейчас одно домохозяйство приносит iMarker $0,1 в месяц, часть этих денег будут получать операторы.

Внедрение DPI

Развиваем тему рекламы у оператора…

Оператору, имеющему DPI систему, ничего не мешает настроить политики для развития самостоятельного бизнеса – целевой рекламы.

«Бесплатный Интернет» или интернет с ротацией рекламы – тарифный план предоставляемый абоненту на безвозмездной основе за счет периодического перенаправления (раз в час или раз в три часа…) на одну из страниц с рекламой…

Например:

Показ в обеденное время рекламы пиццерий, а в вечернее время рекламы такси и т.д.

Внедрение DPI

DPI системы управления трафиком с помощью инструментов анализа могут определять наличие вредоносных сигнатур в передаваемом трафике. После определения может быть выполнен ряд следующих действий:

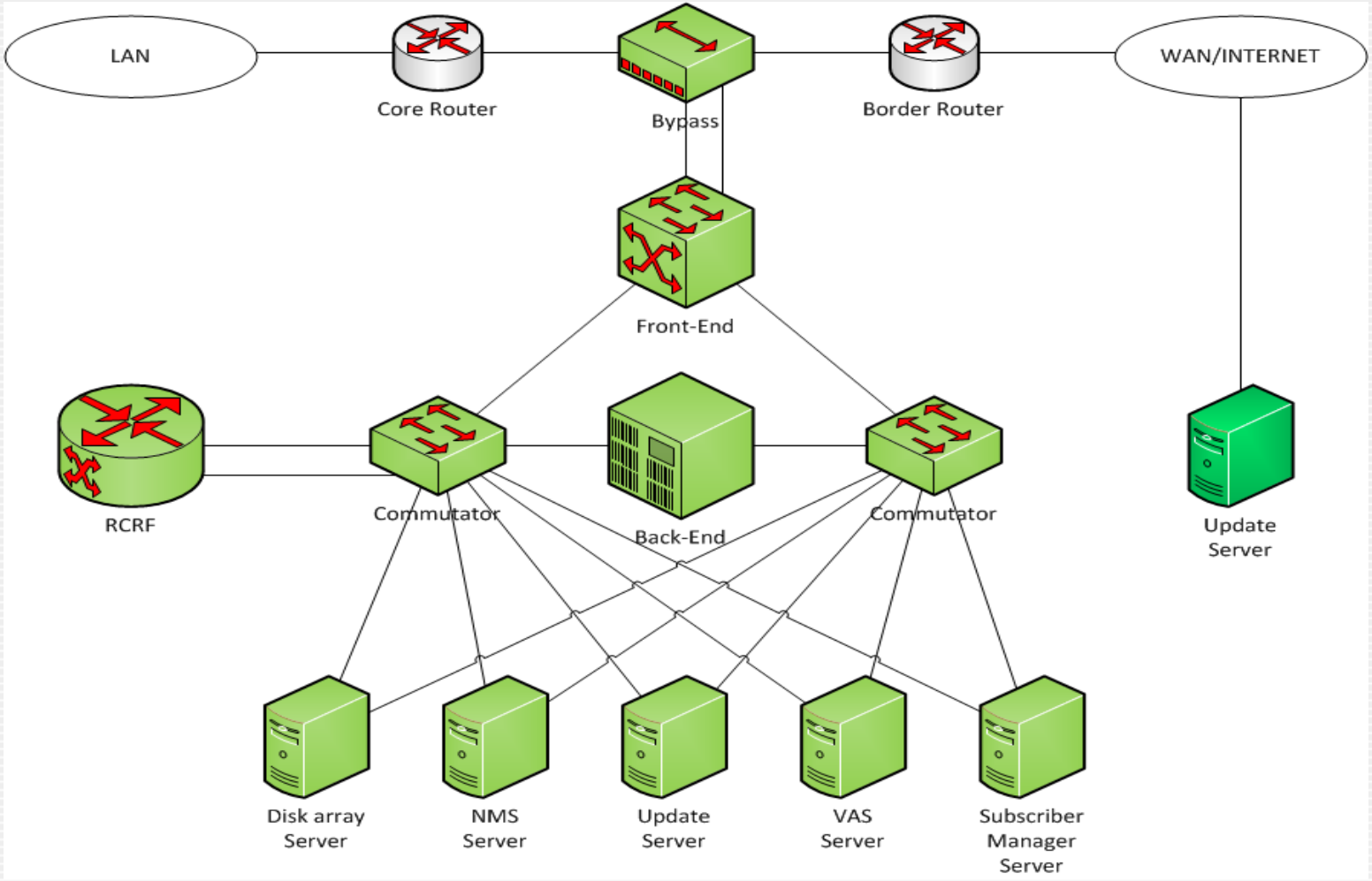
- Уведомление администратора системы для формирования политик
- Уведомление абонента/пользователя
- Ограничение вредоносного трафика путём удаления или его модификации

Внедрение DPI

Для кого?

DPI система, установленная у оператора связи, имеет прямое или косвенное влияние на всех участников единой сети передачи данных, так как оптимизированный/ освобожденный ресурс сети может быть распределён между другими типами абонентов.

Устройство DPI систем



Устройство DPI систем

Основные компоненты полноценной DPI системы управления трафиком

Bypass - высокопроизводительный коммутатор, основная задача которого пропускать трафик либо напрямую (без обработки), либо отправлять трафик на устройство обработки и анализа трафика - Front-End, Bypass постоянно следит за связью с Front-End компонентом и в случаи потери связи или получения сообщений от Front-End, о затруднениях обработки трафика, начинает пропускать трафик напрямую к пограничному маршрутизатору. Существуют различные типы Bypass интерфейсов: медные (не более 1 Гбит/с) и оптические (от 1 до 100 Гбит/с).

Поддерживается оптическое зеркалирование трафика «как есть» и соответственно возможен сбор статистики или подключение СОРМ.

Устройство DPI систем

Front-End – мозг DPI системы - центр обработки информации в соответствии с настроенными/имеющимися политиками. По сути это модульный центр обработки информации.

Существуют следующие модули:

- Вычислительные модули - это модули, построенные на многопроцессорной архитектуре, отвечающие за обработку информации. Именно эти модули выполняют функции инспекции всего проходящего трафика (инкапсуляция/де-инкапсуляция, анализ, классификация и т. д). Встречаются модули как с типовыми процессорами (x86), так и со специализированными процессорами, например ACIS. Обычно Front-End имеет два вычислительных модуля, основной и резервный (поддерживается горячее переключение).
- Линейные платы, отвечающие за приём-передачу трафика
- Коммутационные платы или платы-коммутаторы, отвечают за передачу данных между линейными платами и остальными компонентами DPI системы.
- Процессинговые платы, это платы отвечающие взаимодействие между компонентами системы, а так же за функции контроля (выполнение действий над трафиком).

Устройство DPI систем

Back-End – это высокопроизводительный кэш-сервер для оперативного использования баз сигнатур, различной статистики, политик и различных правил перенаправления трафика.

Основной задачей Back-End является моментальное предоставлении информации для Front-End компонента. Как правило, кэш-сервера имеют высокую степь резервирования своих компонентов, поддерживают горячую замену и умеют балансировать нагрузку (для работы в кластере).

Устройство DPI систем

PCRF-сервер (Policy and charging rules function) – один из основных компонентов DPI систем - сервер определения правил и политик.

Основная роль при получении от Front-End`а идентификатора пользователя/абонента, сообщить Front-End`у соответствующий номер политики.

(Далее Front-End запрашивает подробности соответствующей политики на Back-End’е).

В некоторых DPI системах роль PCRF компонента или часть функций выполняет Subscriber Manager сервер.

Устройство DPI систем

Disk array Server – Сервер дисковый массив предназначенный для хранения больших объемов информации (статистики, различных баз данных, иногда копий трафика). Как правило, взаимодействует только Back-End`дом с для актуализации кэш-фонда последнего.

NMS Server (Network Management Server) – Сервер управления системой.

Update Server – Сервер обновления. Основная задача получать обновления: системные обновления, обновления сигнатур и политик, моделей поведения и т.д. с сервера обновления производителя, через защищённое соединение.

Subscriber Manager – Сервер и/или программный компонент системы являющийся координационным центром DPI систем управления трафиком, реализует возможности персонализации и дифференцирования абонентских услуг (привязка к пользователю/устройству/сети).

Устройство DPI систем

VAS Server (Value Added Services Server) – Сервер дополнительных сервисов. Производители DPI систем управления трафиком интенсивно развивают VAS сервисы, из-за того, что это дает возможность использовать, как свои дополнительные сервисы, так и дополнительные сервисы других разработчиков/производителей, тем самым расширяя возможности своей системы.

VAS сервисами в DPI системах управления трафика являются:

- Предупреждение и/или блокировка пользователя при вирусной активности
- Услуга «Супер скорость на сутки» например для HTTP трафика
- Полноценный «Родительский контроль»
- Тарифы «Смотри онлайн» - тариф разрешающий смотреть онлайн видео в HD и т.д.

Модель OSI и DPI

Уровень	Модель OSI	Назначение	Объект управления	Возможность обработки Proxy	Возможность обработки Брандмауэр	Возможность обработки DPI
7	Прикладной	Доступ приложений к сетевым службам	Данные	Частично (application-level proxy)		Да
6	Представления	представление и кодирование данных	Данные	Частично (application-level proxy)		Да
5	Сеансовый	Управление сеансом связи	Данные	Да (application-level proxy)	Да (Stateful Packet Inspection)	Да
4	Транспортный	Соединение т-т, контроль передачи данных	Блоки	Да (application-level proxy)	Да	Да
3	Сетевой	Маршратизация, управление потоками данных	Пакеты	Да (transparent - level proxy)	Да (Stateless)	Да
2	Канальный	MAC- управление доступом к середе (коммутация), LLC - Контроль логической связи (формирование кардров)	Кадры		Да	Да
1	Физический	Физическая среда (битовые протоколы передачи данных)	Биты			

Типовая идентификация трафика

Используемые порты

Proxy – DNS имя

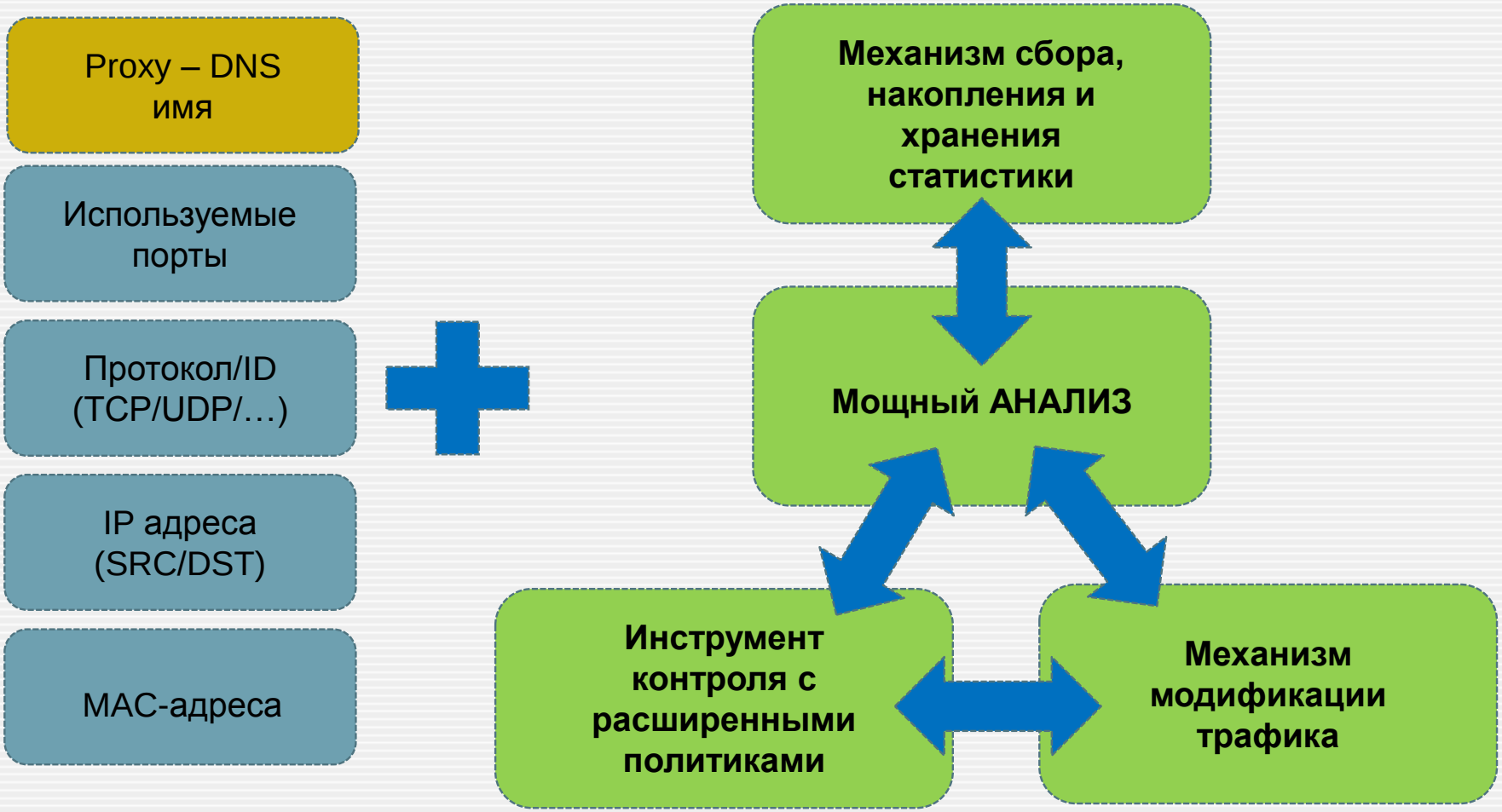
Протокол/ID (TCP/UDP/…)

IP адреса (SRC/DST)

MAC-адреса

Основные идентификаторы управления трафиком в коммутаторах, маршрутизаторах, брандмауэрах позволяющие настроить ACL или QoS

DPI средства управления трафиком



DPI средства управления трафиком

Механизм сбора, накопления и хранения статистики

Механизм сбора данных позволяет собирать, хранить и архивировать данные. Выдавать самую различную статистику, позволяющую оценить передаваемый трафик, панировать сеть и тарифные планы. Некоторые DPI системы заточены только под цели оценки и анализа трафика.

На некоторых DPI системах, для ускорения работы механизмов статистики существует многочасовой кэш всего трафика.

DPI средства управления трафиком

Инструмент контроля с расширенными политиками

Помимо стандартных инструментов контроля/управления трафиком – ACL и QoS, DPI системы управления трафиком имеют их расширенный функционал – политики. Политики основаны на динамическом изменении правил в зависимости от времени, объемов того или иного трафика, поведения трафика и т.д.

Политики контроля и обработки правил могут создаваться и изменяться как администратором системы, так и быть загруженными от производителя.

Возможно применение политик на географически разобщенный кластер устройств.

DPI средства управления трафиком

Механизм модификации трафика

Полноценные DPI системы имеют механизм изменения/модификации трафика.

Модификация трафика применяется как для защиты – например защита от спама (вырезается зараженное вложение) или сетевых червей, так и для дополнительных услуг – показ целевой рекламы, кнопка «Турбо» (ускорение некоторых типов трафика) и т.д.

DPI средства управления трафиком

Суммарное использование различных методов анализа позволяет значительно увеличить точность идентификации трафика

DPI
Анализ

Явно заданные правила

Сигнатуры

Эвристика

Анализ поведения

Классификация трафика

Идентификация трафика в DPI

Явно заданные правила

Явно заданные правила задаются администратором системы, полностью или частично из предоставленных наборов разработчика системы, путём активирования нужных правил.

Например, вы хотите заблокировать одну из страниц на Facebook.com. Для этого вам нужно выбрать протокол HTTP, выбрать/ввести домен Facebook.com, и ввести дополнительное условие user0165448123.

После проверки возможности блокировки, система заблокирует страницу указанного пользователя.

Идентификация трафика в DPI

Сигнатуры

Сигнатура — это набор байтов в пакете или файле, позволяющая установить приложение, протокол, вредоносный код и т.д. и/или классифицировать его.

Сигнатурный анализ – это анализ при котором система обнаружения производит поиск в анализируемой структуре и сравнивает его с известными ей случаями.

Сигнатуры подготавливаются и распространяются производителем оборудования и содержат набор самых разнообразных правил, на основе которых будет проводиться анализ. Файл сигнатур периодически обновляется и, в зависимости от производителя, либо автоматически скачивается оборудованием, либо обновляется вручную.

Идентификация трафика в DPI

Эвристика

Эвристический алгоритм — это алгоритм решения задачи, правильность которого для всех возможных случаев не доказана, но про который известно, что он даёт достаточно хорошее решение в большинстве случаев.

Эвристический анализ - это технология обнаружения по признакам (без гарантированной точности). Используется, когда невозможно определить трафик с помощью сигнатурного анализа, то есть с помощью поиска и сравнения по базе сигнатур.

Объектам, обнаруженным с помощью эвристического анализа, присваивается вероятность соответствия, к примеру - 85%.

Совместное использование с другими методами анализа позволяет увеличить точность общей идентификации трафика.

Идентификация трафика в DPI

Анализ поведения

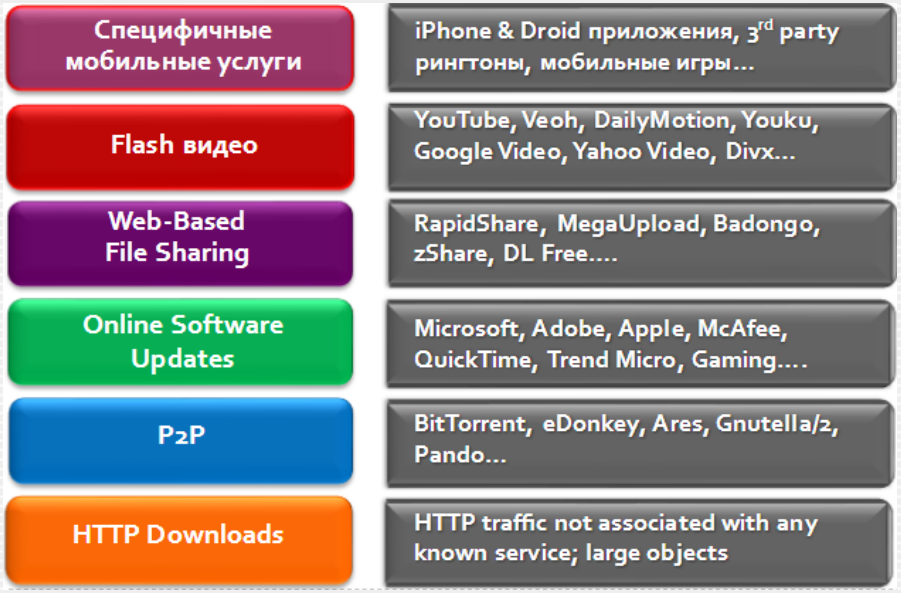
Анализ поведения трафика считается наиболее перспективны методом анализа в DPI системах управления трафиком, по следующим причинам:

- Возможность описать почти любую даже изменяющуюся модель поведения трафика
- Высокая скорость обработки по сравнению с эвристическим методом анализа
- Высокая точность идентификации трафика

Поведенческий алгоритм анализа очень похож на сигнатурный, но вместо базы сигнатур используется база с моделями поведения трафика. Базы с моделями трафика аналогично обновляются производителем оборудования.

Примеры: перебор портов, однотипный трафик с множества хостов, количество соединений + определенный размер пакета и т.д.

Идентификация трафика в DPI



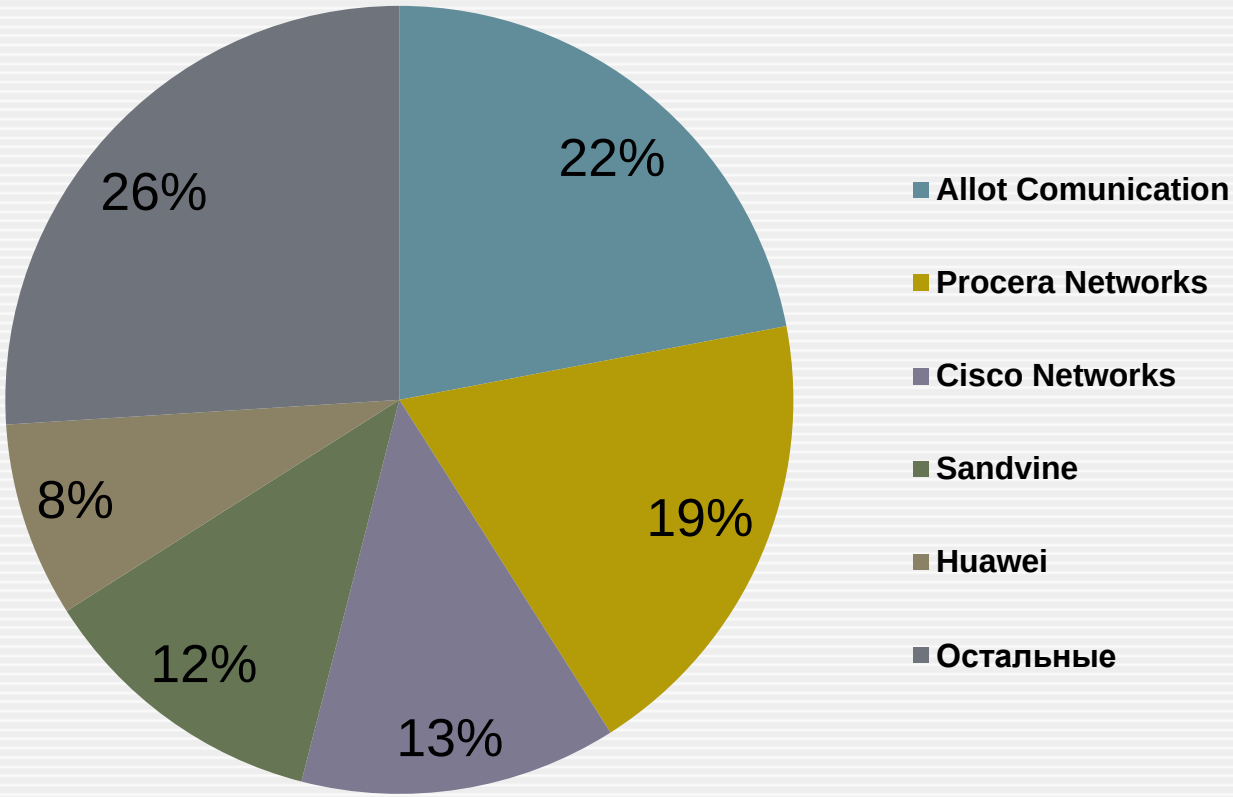
Большинство DPI систем управления трафиком поддерживают классификация трафика, для удобства выполнения операций по типам, приложениям или группам пользователей (Standard, Corporate, VIP, Dude is not from this planet и т.д.).

Все эти параметра настраиваются и гибко взаимодействуют с политиками.

Основные производители DPI систем

Диаграмма:

Основные производители DPI систем управления трафиком и их доли на рынке



DPI решения основных производителей

Производитель	Головной офис компании (Hi Support)	Наименовании линейки оборудования	Серии	Модельный ряд (актуальные модели)
Allot Comunication	Израиль	NetEnforcer, SG Sigma, SG Sigma E	AC, Sigma E	AC-500, AC-1400, AC-3000, AC-5000, AC-10000, Sigma E14, Sigma E6
Procera Networks	Канада	PacketLogic™	EDGE, ACCESS, CORE	EDGE - PL7810, ACCESS - PL8720, PL8820, PL8920, PL8960, CORE - PL10024, PL20000
Cisco Networks	США/Китай	SCE (Service Control Engine)	SCE 8000	SCE 8000
Sandvine	Канада	PTS (Policy Traffic Switch)	PTS 22000, PTS 24000	PTS 22050, PTS 22100, PTS 22600,PTS 22000 Cluster, PTS 24500, PTS 24700, PTS 24000 Cluster
Huawei	Китай	SIG (Service Inspection Gateway)	SIG9800	SIG9810, SIG9820

DPI и открытые системы

Краткий экскурс

С давних пор существовали надстройки для межсетевого экрана, такие как L7-filter и IPP2P. Они позволяли фильтровать определенный трафик, анализируя информацию, в том числе, и на прикладном уровне OSI. Эти механизмы легли в основу проекта OpenDPI, распространяемый по лицензии LGPLv3, построенного на коде коммерческого продукта PACE, который разрабатывался компанией Ipoque.

OpenDPI был модулем для iptables и умел фильтровать большое количество различных типов пакетов. Проект прекратил свое существование в 2011 году.

Далее появилась компания Ntop, которая стала использовать исходники OpenDPI, как основу для своих продуктов. Коммерческий продукт у Ntop называется nDPI. Умельцы, которые на основе исходников nDPI, создали модуль для iptables, таким образом, восстановив проект OpenDPI.

DPI и открытые системы

Проект IPP2P более не поддерживается и, в качестве замены, предлагает использовать именно OpenDPI. В отличие от IPP2P, основной целью которого является определение именно p2p трафика, OpenDPI поддерживает широкий набор различных протоколов (поддерживается идентификация 170 протоколов/приложений).

OpenDPI изначально спроектирован для очень низкого уровня ложных положительных срабатываний. В отличие от L7-filter не требует наложения патчей на iptables и ядро; работает в виде модуля ядра и библиотеки xtables. Так же определения протоколов представляют собой не список регулярных выражений, а модули на C, что повышает быстродействие.

Но на практике оказалось, что процесс создания рабочего модуля, требует огромного количества сил, нервов и напильников. Программа "из коробки" - очень сырая и требует большого количества изменений.

DPI и открытые системы

На основе открытых систем появилось огромное множество разнообразных продуктов

Из плюсов таких решений стоит отметить:

- Стоимость решений
- Узкая направленность решений (решения для определенных задач)
- Возможность использования имеющегося оборудования

Основными недостатками таких продуктов являются:

- Ограниченность производительности (2-5 Гбит/с)
- Низкая надежность
- Масштабируемость решений
- Отсутствие кластеризации и общих политик управления
- Своевременное обновление сигнатур и политик
- Поддержка

Обзор оборудования Allot Communication

Продукты Allot Communications

DART - Технология глубокого анализа трафика DART (Dynamic Actionable Recognition Technology) вобрала в себя большой экспертный опыт компании Allot Communications в области идентификации IP трафика и разработки политик управления трафиком для эффективного управления потреблением полосы пропускания и производительностью сервисов в мобильных и фиксированных сетях доступа. DART позволяет операторам оптимизировать, монетизировать и персонализировать предоставляемый ими сервис.

Обзор оборудования Allot Communication

Четыре уровня распознавания:

- Распознавание приложений: DART может идентифицировать и применять политики к большему числу приложений и протоколов, чем любое другое решение.
- Распознавание устройств: DART может различать используемые на сети устройства по их типу и производителю. Функционал распознавания устройств позволяет операторам определять факты использования тетеринга – использования мобильного устройства в качестве точки доступа для других устройств.
- Распознавание пользователей: DART также может определять пользователей, которые генерируют трафик. Например, оператор может определить, что определенный пользователь пользуется сервисом YouTube, со своего ноутбука, в то время, как другой пользователь совершает звонок с помощью Skype со своего мобильного телефона.
- Распознавание сетевой топологии: анализ сетевой топологии это четвертый уровень распознавания, предоставляемый DART решениям Allot.

Обзор оборудования Allot Communication

Безопасное обновление библиотеки сигнатур.

DART реализует безопасное обновление сигнатур, что позволяет не оказывая влияния на систему в целом непрерывно и точно распознавать приложения во время процесса обновления.

Масштабирование сетевой производительности

DART – это технология интегрированная в платформы NetEnforcer и SigmaE, которые масштабируются по производительности от 10Mbps до 160Gbps

Обзор оборудования Allot Communication

Высокопроизводительные платформы:

Платформы NetEnforcer – это специализированные устройства для мониторинга и управления трафиком в корпоративных сетях, облачных сетях и сетях провайдеров широкополосного доступа. Благодаря своей производительности от 10Mbps до 160Gbps эти устройства обеспечивают необходимую прозрачность трафика, управление политиками и перенаправление определенного типа трафика в сетях самых разных размеров. На всех устройствах NetEnforcer работает технология DART, которая распознает больше приложений, чем любое другое решение на рынке.

Обзор оборудования Allot Communication

Сервисный шлюз SG-Sigma E (Service Gateway Sigma E) – это модульное высокопроизводительное решение, которое позволяет обрабатывать трафик на скоростях до 160Gbps. Модульная архитектура Sigma E разработана на основе стандартов AdvancedTCA*, за счет чего достигается высокий уровень масштабируемости и возможность горячей замены модулей, что, в свою очередь, позволяет добиться высокой отказоустойчивости системы и надежности предоставляемого с ее помощью сервиса.

Сервисный шлюз Sigma E полностью интегрируется с другими решениями Allot, обеспечивая высокую производительность предоставления сервиса.

* - AdvancedTCA (Advanced Telecommunications Computing Architecture) — Усовершенствованная архитектура для телекоммуникационных вычислений представляет собой новое поколение стандартизованных телекоммуникационных вычислительных платформ - модульные решения с набором стандартных интерфейсов и технологий.

Обзор оборудования Allot Communication

Система централизованного мониторинга и управления NetXplorer (NMS):

Allot NetXplorer – это масштабируемая система управления сервисами и платформами Allot. Решение предоставляет контроль за состоянием сети, что позволяет операторам понять как используются ресурсы полосы пропускания приложениями и пользователями, для того, что бы разработать политики управления трафиком и привязать параметры сервисов и производительности к бизнес-целям и ожиданиям пользователей от предоставляемого сервиса.

Обзор оборудования Allot Communication

Инструменты для предоставления сервисов:

Постоянно пополняющийся портфель инструментов для предоставления новых услуг от компании Allot позволяет сократить расходы на инфраструктуру и сгенерировать прибыль от внедрения новых услуг.

Данный функционал встроен в решения NetEnforcer, а так же в сервисные платы платформы Sigma E.

- Allot VideoClass – интеллектуальная оптимизация передачи видео-контента
- Allot MediaSwift – кэширование данных и акселерация трафика
- Allot ServiceProtector – детектирование и блокирование аномального трафика
- Allot WebSafe – URL фильтрация
- Allot Proactive Analytics – многоуровневый анализ веб-трафика и поведения пользователей

Обзор оборудования Allot Communication

Платформа управления абонентским доступом:

Платформа SMP (Subscriber Management Platform) предоставляет операторам связи возможность создавать сервисы, ориентированные на конкретных пользователей и, при этом, контролировать общую утилизацию сети.

Платформа обладает функционалом, который позволяет получить аналитическую информацию о пользовательской активности, в том числе об используемых приложениях и устройствах с которых осуществляется доступ, а так же об объеме потребляемого трафика конкретным приложением определенного пользователя, и обеспечить тарификацию пользователей в режиме реального времени.

Инструментарий построения детализированных отчетов о пользовательской активности за краткосрочные и долгосрочные периоды времени позволяет операторам связи анализировать предпочтения и поведение своих пользователей, что в свою очередь делает возможным разрабатывать такие тарифные планы, которые удовлетворяют потребностям пользователей, но в то же время более эффективно используют ресурсы полосы пропускания.

Обзор оборудования Allot Communication

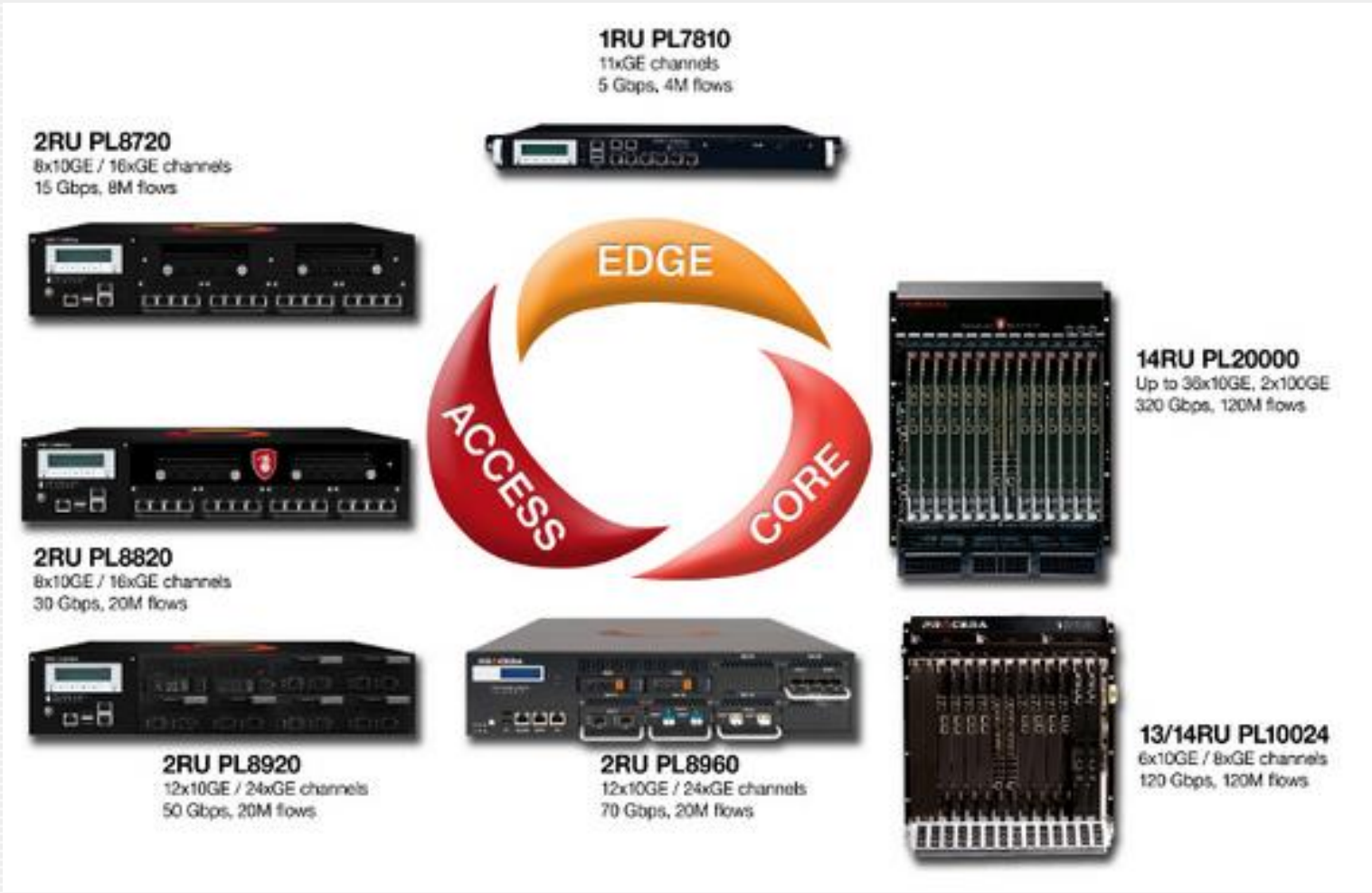
Обзор оборудования Allot Communication

		AC-502	AC-504
Capacity	Throughput	400 Mbps (200 Mbps full duplex)	
	Number of Connections/Flows	256,000 / 512,000	
	Number of Subscribers	20,000	
	Lines/Pipes/Virtual Channels	Up to 256 / 4096 / 32,768	
Interfaces and Connections	Management Interface	10/100/1000BASE-T	
	Network Interfaces (Internal / External)	2 x 10/100/1000BASE-T	4 x 10/100/1000BASE-T
	Cascading/Redundancy	2 x 10/100/1000BASE-T	4 x 10/100/1000BASE-T
	Console Port	Serial, RJ-45 Connector	
Examples of Application/Protocol Signatures Supported	P2P	Including BitTorrent, eDonkey, Ares, Gnutella, Thunder, Poco, Winny, eMule, Vuze	
	VoIP	Including Windows Live Messenger Voice, SIP, Skype, Yahoo Messenger Voice, GoogleTalk, Fring	
	Gaming	Including World of Warcraft, Final Fantasy, Guitar Hero, Second Life, QQ Games, Lineage, CounterStrike, Call of Duty , Apple Game Center	
	Instant Messaging/Chat	Including Windows Live Messenger, QQ, Yahoo Messenger, ICQ, WhatsApp	
	Web	Including HTTP Browsing, HTTPS , Mobile browsers , Facebook, Twitter	
	Streaming	Including YouTube, RTMP, QQ live, PPStream, DailyMotion, HTTP Streaming, HTTP Audio, NetFlix, Facebook Streaming	
Networking Standards	Traffic Encapsulation	Including L2TP, MPLS, PPPoE	
	IPv6	Ready	
Product Options	QoS Enforcement Levels	10, 45, 100 and 200 Mbps full duplex	
	Monitoring and Reporting	Real-time and Long-term	
	High Availability	Active Redundancy (1:1, 1+1)	
Management	NetXplorer Centralized Management	Yes	
	Allot Subscriber Management Platform (SMP)	Fully integrated with Allot SMP for subscriber-application control	
Full Integration with Network & Subscriber Services	Allot TierManager and QuotaManager	For subscriber service tiering and quota management solutions	
	Allot WebSafe	For URL filtering solutions	

Обзор оборудования Allot Communication

	SG-Sigma E14	SG-Sigma E6
Platform Configuration		
Chassis	14-slot, AdvancedTCA (ATCA)	6-slot AdvancedTCA (ATCA)
Maximum Available Slots	14	6
Core Controller (CC) Blade	2 to 10 (blade occupies 1 slot)	1 to 4 (blade occupies 1 slot)
Switch and Flow Balancer (SFB) Blade	2 to 4 (blade occupies 1 slot)	1 or 2 (blade occupies 1 slot)
Bypass (BP) Blade	1 to 2 blades (8 ports each), or external	1 blade (8 ports), or external
Service Blades	Up to 8 single-slot blades	Up to 3 single-slot blades
Capacity		
Throughput per Platform	Up to 160 Gbps	Up to 64 Gbps
Throughput per Cluster (cascading platforms)	1 Terabit/sec, using 8 devices	360 Gbps, using 8 devices
Number of Flows	Up to 100 Million (10 Million per CC)	Up to 40 Million (10 Million per CC)
Number of Subscribers / Active PDP Contexts	Up to 8,000,000	Up to 3,200,000
Connection Establishment Rate	150,000 per CC	150,000 per CC
Number of Lines / Pipes / Virtual Channels	Up to 256 / 1,000,000 / 2,000,000 (100,000 / 200,000 per CC)	Up to 256 / 400,000 / 800,000 (100,000 / 200,000 per CC)
Interface Types		
Ethernet Interfaces	Up to 24 x 10 Gigabit Ethernet SR/LR/ER	Up to 12 x 10 Gigabit Ethernet SR/LR/ER
Management	2 x 10/100/1000Base-T (1+1)	2 x 10/100/1000Base-T (1+1)
Console	Serial, RJ45 Connector	Serial, RJ45 Connector
Connectivity Configurations and Throughput Options		
Maximum Ports for Network Connectivity	16 x 10GE ports	8 x 10GE ports
Throughput	32 to160 Gbps (in increments of 16 Gbps)	16 to 64 Gbps (in increments of 16 Gbps)
Availability		
Hardware Bypass	1-2 independent passive optical bypass, each support up to 4 links/8 ports (external and internal options available)	Independent passive optical bypass (external and internal options available)
High Availability	1+1 system-level redundancy N+1 redundancy of Core Controller blades	1+1 system-level redundancy N+1 redundancy of Core Controller blades
Management	Active-Standby HA on management ports	Active-Standby HA on management ports
System	Full redundancy for system components: PSUs, fans, etc.	Full redundancy for system components, PSUs, fans, etc.

Обзор оборудования Procera Networks



PRE
PacketLogic™
Real-Time Enforcement

Specifications	PL7810	PL8720	PL8820
Connections/Flows	2,000,000/4,000,000	4,000,000/8,000,000	10,000,000/20,000,000
Connections Per Second	100,000	150,000	200,000
Throughput	5 Gbps[1]	15 Gbps[1]	30 Gbps[1]
Subscribers	100,000	500,000	2,000,000
Management Interfaces	2x10/100/1000	2x10/100/1000	2x10/100/1000
Number of Channels	11 x GE	8 x 10 GE, 16 x GE	8 x 10GE, 16 x GE
Physical Interfaces	10/100/1000 copper; Multi-Mode SX GE fiber; Single-Mode LX GE fiber	10/100/1000 copper; Multi-mode SX GE fiber; Single-mode LX GE fiber; Multi-mode SR 10GE fiber; Single-mode LR 10GE fiber	10/100/1000 copper; Multi-mode SX GE fiber; Single-mode LX GE fiber; Multi-mode SR 10GE fiber; Single-mode LR 10GE fiber
Serial Console Port	RJ-45	RJ-45	RJ-45
Redundancy	Bypass	Bypass	Bypass
Bandwidth Licensing	100 M, 500 M and 1Gbps increments	1 Gbps increments	1 Gbps increments
Network Intelligence	PacketLogic Intelligence Center	PacketLogic Intelligence Center	PacketLogic Intelligence Center
Subscriber Management	PacketLogic Subscriber Manager	PacketLogic Subscriber Manager	PacketLogic Subscriber Manager

Обзор оборудования Procera Networks

Specifications	PL8920	PL8960	PL20000
Connections/Flows	10,000,000/20,000,000	20,000,000/40,000,000	60,000,000/120,000,000
Connections Per Second	300,000	400,000	3,000,000
Throughput	50 Gbps[1]	70 Gbps[1]	320 Gbps
Subscribers	3,000,000	3,000,000	10,000,000
Management Interfaces	2x10/100/1000	2x10/100/1000Base-T	4x10GE, 4x10/100/1000Base-T
Number of Channels	24 x GE or 12 x 10GE	24 x GE or 12 x 10GE	Up to 36 x 10GE, 4 x 40GE
Physical Interfaces	10/100/1000 copper; Multi-Mode SX GE fiber; Single-Mode LX GE fiber; Multi-Mode SR 10GE fiber; Single-Mode LR 10GE fiber	10/100/1000 copper; Multi-Mode SX GE fiber; fiber; Single-Mode LR 10GE fiber	1000Base-T, 1000Base-SX, 1000Base-LX Multi-Mode SR 10GE, Single-Mode LR 10GE, Multi-Mode SR 40GE
Serial Console Port	RJ-45	RJ-45	RJ-45
Redundancy	Bypass	Bypass	Bypass, External Modules
Bandwidth Licensing	1 Gbps increments	1 Gbps increments	Per Flow Processing (FP) module
Network Intelligence	PacketLogic Intelligence Center	PacketLogic Intelligence Center	PacketLogic Intelligence Center
Subscriber Management	PacketLogic Subscriber Manager	PacketLogic Subscriber Manager	PacketLogic Subscriber Manager

Обзор оборудования Cisco Networks

	SCE1010	SCE2020	SCE8000	
Data plane interfaces	2x GE	4x GE	Modular 2x or 4x 10GE 8x or 16x GE	
DPI performance	2 Gbps	2.8 – 3.2 Gbps	15 Gbps	30 Gbps
Maximum Concurrent subscribers	40K – 200K	80K – 200K	250K – 1M	
Maximum open flows	1M – 400K		8M – 5M	16M – 10M
Insertion modes	Recv-only Inline MG-SCP	Recv-only Inline Cascade MG-SCP	Recv-only Inline Cascade MG-SCP	

Обзор оборудования Cisco Networks

Feature	Benefit
Traffic Handling	
Programmable Protocol Detection	• More than 600 protocols supported • Extensible to emerging protocols • Adaptive peer-to-peer (P2P) recognition • Asymmetric traffic classification support
Feature	**Benefit**
Differentiated Classes of Service (CoSs)	Support for: • Differentiated Services (DiffServ) • Type-of-service (ToS) byte
Capacity and Performance[1]	
Maximum Throughput	Up to 30 Gbps[2]
Number of Concurrent Subscribers	Up to 1,000,000
Simultaneous Unidirectional Flows	Up to 32,000,000
Maximum flow open rate	Up to 15 million flows per second[3]

Обзор оборудования Cisco Networks

Ordering Information

Table 3. Ordering Information for the Cisco SCE 8000 Service Control Engine

Product Name	Part Number
Cisco SCE 8000 Service Control Engine	SCE8000
Cisco SCE 8000 2 x 10GE interfaces bundle	SCE8000-2X10G-E
Cisco SCE 8000 4 x 10GE interfaces bundle	SCE8000-4X10G-E
Cisco SCE 8000 8 x GE interfaces bundle	SCE8000-8XGE-E
Cisco SCE 8000 16 x GE interfaces bundle	SCE8000-16XGE-E
Cisco SCE 8000 8 x GE & 1 x 10G interfaces bundle	SCE8000-8XGE-E-HA
Cisco SCE 8000 16 x GE & 2 x 10G interfaces bundle	SCE8000-16XGE-E-HA
Cisco Service Control Application View Only	SCA-BB-VO-R3
Cisco Service Control Application Capacity Control	SCA-BB-CC-R3
Cisco Service Control Application Tiered Control	SCA-BB-TC-8000-R3
Cisco Service Control Application Tiered Control	SCA-BB-TC-XXX-R3*

*XXX represents number of subscribers: 10,000, 50,000, 250,000, or 1 million

Обзор оборудования Cisco Networks

Продукт Cisco SCE не единственное DPI решения производителя для управления трафиком.

NBAR (*Network Based Application Recognition)* – механизм используемый в сетях передачи данных для распознавания потока данных (dataflow).

Требования:

Cisco ASR1000 Series (Cisco IOS XE Release), Cisco ISR-G2 (Cisco IOS T Train)

Обнаружение приложений маршрутизаторами Cisco ISR G2 и ASR 1000 осуществляется при помощи механизмов глубокой инспекции пакетов DPI (Deep Packet Inspection) и протокола NBAR2. NBAR2 является развитием и более новой версией протокола NBAR, который позволял классифицировать более 150 приложений, использующих статические порты.

Обзор оборудования Cisco Networks

Расширенные механизмы классификации NBAR2 с глубоким анализом потоков трафика (на уровнях L4-L7) позволяют идентифицировать более 1500 приложений, использующих как статические, так и динамические порты TCP/UDP с отслеживанием состояния. В отличие от NBAR версии 1, NBAR2 также поддерживает классификацию IPv6. Кроме этого, NBAR2 позволяет администраторам создавать собственные сигнатуры для приложений, которые не включены в стандартную библиотеку.

NBAR2 может применяться не только для обнаружения приложений и сбора статистики (количество пакетов, байт, bit rate и т.д.) по каждому идентифицированному приложению. Классифицировав приложения, можно применить политики QoS для них, например, ограничить полосу пропускания для трафика bittorrent или перемаркировать поля DSCP для youtube.

Обзор оборудования Cisco Networks

Политики QoS позволяют обеспечить контроль полосы пропускания для классифицированных приложений. При помощи технологии PfR (Performance Routing) также можно реализовать контроль маршрутов приложений с учётом информации о состоянии и метриках производительности каналов связи (потери пакетов, загрузка канала, задержки и jitter) в режиме реального времени.

PfR в интеграции с NBAR2 позволяют обеспечить адаптивный динамический выбор маршрутов для классифицированных приложений. Например, можно использовать один канал связи с низкой задержкой, jitter'ом и потерями пакетов для видеоприложений, а другой канал связи – для всего остального трафика.

Обзор оборудования Cisco Networks

Интеграция NBAR2 с технологией Flexible Netflow позволяет обеспечить IPv4/IPv6 мониторинг на уровнях L2-L7 для классифицированных приложений.

Таким образом, при помощи Flexible Netflow и NBAR2 можно понять, какие приложения работают в сети, какая полоса пропускания используется этими приложениями, определить направления потоков передачи данных, какие пользователи и IP-адреса являются наиболее “активными” с точки зрения потребления трафика.

Обзор оборудования Sandvine

	PTS 22000				PTS 24000		
	PTS 22050	PTS 22100	PTS 22600	Cluster	PTS 24500	PTS 24700	Cluster
Form Factor / Rack Space	2 RU	2 RU	2 RU	12 RU	4 RU	4 RU	24 RU
Max. Intersection Capacity	10 Gbps	10 Gbps	40 Gbps	240 Gbps	160 Gbps	160 Gbps	480 Gbps
Max. Inspection Throughput	4 Gbps	10 Gbps	40 Gbps	240 Gbps	80 Gbps	160 Gbps	480 Gbps
Max. New Flows per Second	50,000	100,000	200,000	1,200,000	1,500,000	2,000,000	9,000,000
Max. Concurrent Flows	2,000,000	4,000,000	16,000,000	96,000,000	50,000,000	72,000,000	270,000,000
10 GE Ports/RU	11	11	11	11	4	4	4
Max. Intersection/RU	5 Gbps	5 Gbps	20 Gbps	20 Gbps	40 Gbps	40 Gbps	20 Gbps
Max. Inspection/RU	2 Gbps	5 Gbps	20 Gbps	20 Gbps	20 Gbps	30 Gbps	20 Gbps
Max. New Flows Per Second/RU	25,000	50,000	100,000	100,000	375,000	500,000	375,000
Max. Concurrent Flows/RU	1,000,000	2,000,000	8,000,000	8,000,000	12,500,000	18,000,000	12,500,000

Обзор оборудования Sandvine

Standards-Compliance for Deployment Versatility and Predictability

Network Interface Standards	• Gigabit Ethernet • 10 Gigabit Ethernet • IEEE 802.1q and 802.1ad
Tunnel & Encapsulation Support	• GTP • GRE • L2TPv2 • MobileIP • VLAN • EoMPLS • MPLS • IPinIP • 6rd
Access Technologies	• DOCSIS • DSL • FTTx • WiMAX • 2G • 3G • 4G • LTE
IP Versions	• IPv4 • IPv6
Network Integration Support	• 3GPP TS 32.299 version 7.9 (Diameter Gy) • 3GPP TS 29.212 version 7.9 (Diameter Gx) • 3GPP TS 29.061 version 7.9 (3GPP RADIUS) • 3GPP TS 32.225 and 3GPP TS 32.299 (Rf) • BGPv4

RFC Support	• SNMPv2: RFC 1905, 2578, 3418 • SNMPv3: RFC 3411-3418 • RADIUS: RFC 2865, 2866, 2869 • Diameter: RFC 3588 • TACACS+: RFC 1492 • NTP: RFC 1305
Centralized Management	• Yes - refer to *Control Center: Management Simplified*
High Availability	• Yes - via clustering, unit redundancy and N:N+1 deployment redundancy
Regulatory Compliance	• Compliant with international standards for product safety and electromagnetic compatibility (EMC) • NEBS Level 3 Certified

Detailed specifications are available in *Policy Traffic Switch 22000: Datasheet* and *Policy Traffic Switch 24000: Datasheet*

Обзор оборудования Huawei

With the development of ALL IP network and arrival of the 3G/ LTE epoch, network services experience a significant change, and traditional telecom carriers are confronted with increasing challenges.

- **Weak service awareness:** weak awareness of applications and subscribers, causing the difficulties in business operation decision-making.
- **Poor network management:** insufficient capabilities over network management and control, causing continuous high expansion costs and poor subscriber experience.
- **Monotonous fee package:** fee package lack of personalization and differentiation, causing low attractiveness for high-value customers.
- **Shortage of value-added services:** lack of open cooperation and innovation on value-added services, causing the dilemma of operator's network channelization.

Based on the deep understanding of network development and carriers' service requirements, Huawei launches its SIG9800 series, which:

- Provides massive service processing capabilities and highly reliable service platforms by virtue of Huawei mature router platform.
- Provides powerful application and subscriber awareness capabilities, multi-dimensional service analysis, and assists in business operation decision-making.
- Provides multiple intelligent traffic management technologies to effectively optimize network traffic, simplify operations, and promote service quality.
- Provides differentiated services to realize "golden channel" for operation by means of diverse value-added services.
- Complies with 3GPP standards, and supplies an open service platform to construct an innovative commercial environment.

SIG9810

SIG9820

Обзор оборудования Huawei

Item		Specifications	
Model		SIG9810	SIG9820
Power consumption		< 2600 W	< 5000 W
Power	AC input (rated)	200 V AC to 240 V AC; 50/60 Hz	200 V AC to 240 V AC; 50/60 Hz
	AC input (maximum)	90 V to 275 V; 50/60 Hz	190 V AC to 264 V AC; 50/60 Hz
	DC input (rated)	-48 V DC	-48 V DC
	DC input (maximum)	-75 V to -38 V	-38 V to -72 V
Dimensions (W×D×H)		442mm×669mm×886mm (20 U)	442mm×669mm×1600mm (36 U)
SPU/LPU slot		8 slots per device	16 slots per device
LPUK interface		10 GE LAN/10 GE WAN/10G POS subcard	
		12×GE (optical) subcard	
		12×10/100/1000 Mbit/s (RJ-45 electrical) subcard	
Maximum processing capability		Fixed network: 50Gbps Wireless network: 40Gbps	Fixed network: 100Gbps Wireless network: 80Gbps
Maximum number of concurrent connections		Fixed network: 40M Wireless network: 32M	Fixed network: 80M Wireless network: 64M
Number of new connections per second		Fixed network: 2M Wireless network: 1.6M	Fixed network: 4M Wireless network: 3.2M
Latency		< 200 us	
Operating temperature		Long period: 0°C to 45°C Short period: -5°C to +55°C	Long period: 0°C to 45°C Short period: -5°C to +55°C
Ambient humidity		Long period: 5% to 85% Short period: 0% to 95%	Long period: 5% RH to 95% RH, non-condensing Short period: 0% RH to 95% RH, non-condensing

Обзор оборудования

Производитель	Количество обрабатываемых протокол/приложений	Сигнатурный анализ	Эвристический анализ	Поведенческий анализ	VAS
Allot Comunication	Более 1500	Да	Да	Да	Да
Procera Networks	Более 1500	Да	Да	Да	Да
Cisco Networks	Около 1500	Да	Да	Частично	Частично
Sandvine	Более 1000	Да	Да	Да	Да
Huawei	Около 1000	Да	Да	Частично	Да

Обзор оборудования

Различия в методах обработки ассиметричного трафика у разных производителей:

- Cisco довольствуется половинкой сессии и пытаются определить тип сетевого приложения, используя лишь эти данные. Очевидно, что при данной методике страдает точность детектирования приложений, особенно тех, для которых требуются поведенческие модели анализа. Также в такой реализации есть ряд ограничений, накладываемых на возможности управления таким трафиком, у каждого производителя они свои.

Обзор оборудования

- Sandvine для решения проблемы асимметричного трафика использует следующую модель — весь трафик, являющийся асимметричным, при помощи инкапсуляции в broadcast-фреймы пересылается на все устройства DPI, находящиеся в едином домене. В итоге данной пересылки устройства, видевшие до этого лишь одно направление в рамках сессии, увидят и второе, на основании чего можно будет осуществить полный комплекс мер по анализу и управлению трафиком. Недостаток данной схемы очевиден — при больших объёмах асимметричного трафика на сети предъявляются серьёзные требования к каналам связи, соединяющим устройства DPI на разных сайтах. В некоторых случаях, когда речь идёт об асимметрии порядков нескольких гигабит (или десятков гигабит) в секунду, данная методика неприменима в связи с высокими накладными расходами на организацию канала между сайтами.

Обзор оборудования

- Умнее всех поступают Procera и Allot. Идея похожа на реализацию Sandvine с тем отличием, что между сайтами пересылается не асимметричный трафик, а метаданные, явно характеризующие его.

За счёт подобной оптимизации требования к межсайтовым каналам связи заметно ниже, относительно реализации Sandvine.

Примечание: Метаданные - это данные содержащие описание первичных (истинных) данных (информация об информации) или описание контента.

DPI для корпоративного сектора

Специализированные DPI решений для корпоративного сектора

Пример: Российская компания «Трафика» и её DPI продукт «Monitorium»

Monitorium - это система для комплексной защиты данных предприятия от несанкционированных утечек и разглашения.

Задача системы: контроль входящего/исходящего трафика и автоматическое выявление нарушений пред настроенных правил/политик.

DPI для корпоративного сектора

Возможности:

Управление информационной безопасностью:

Контроль передачи через интернет конфиденциальных документов (целиком или любой части текста документа, в том числе и в заархивированном виде) через каналы: электронной почты, Интернет-ресурсы, передачи файлов по ftp.

- Предотвращение утечки конфиденциальной информации
- Выявление нарушителей
- Защита персональных данных

Управление информационно-вычислительной сетью:

- Контроль интернет активности сотрудников
- Ограничение доступа пользователей корпоративной сети к Интернет-ресурсам.

HR Управление:

- Мониторинг лояльности сотрудников (сайты о работе и т.д.)

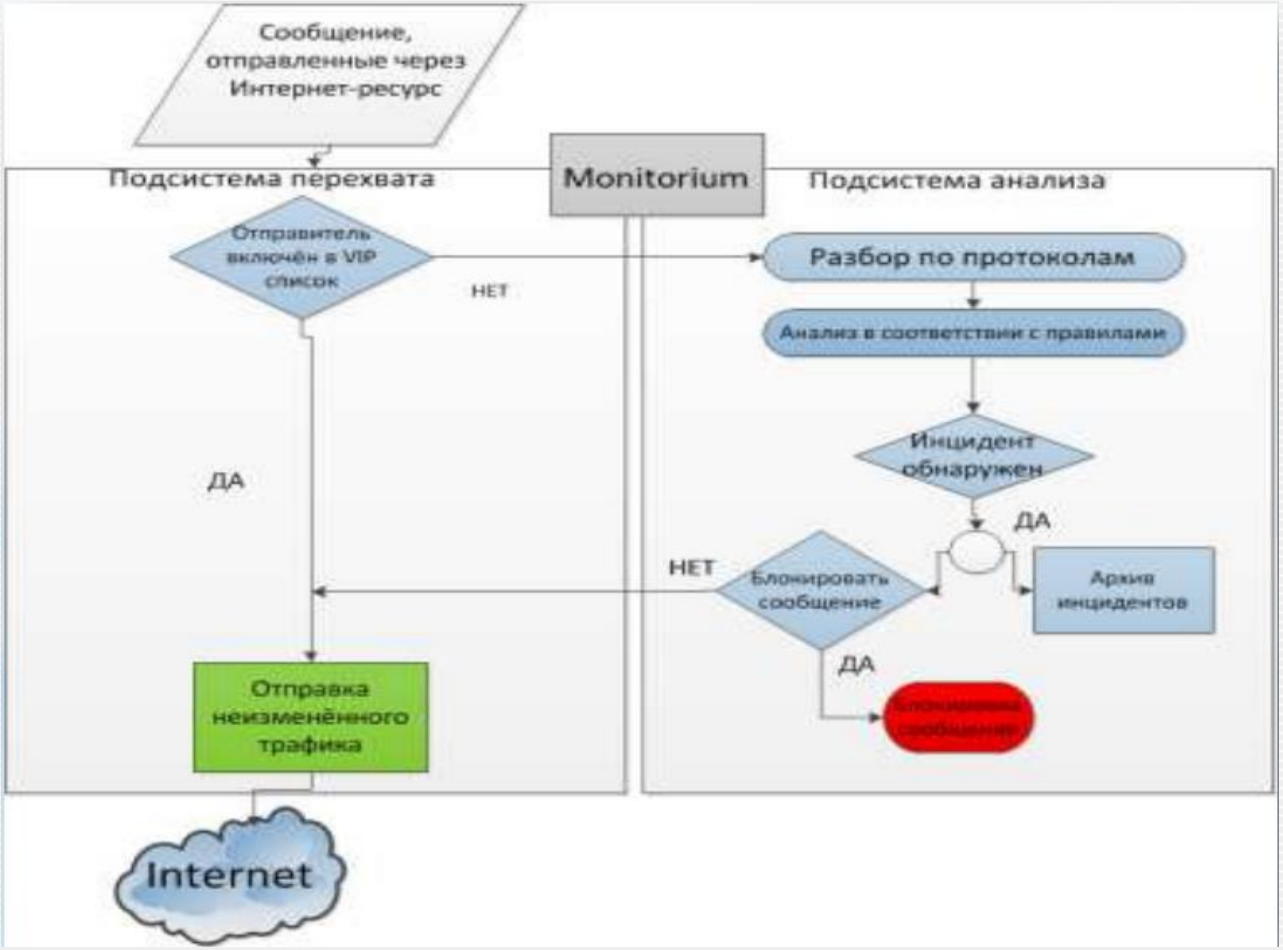
DPI для корпоративного сектора

Перехват и анализ трафика

Подсистема перехвата захватывает сетевые потоки данных и передает их на подсистему анализа.

Подсистема анализа разбирает сетевые пакеты по протоколам (HTTP, SMTP, IMAP, OSCAR (ICQ/AIM), XMPP(Jabber), Mail.Ru Агент, FTP), извлекает из разобранных пакетов текстовую информацию и проверяет ее на соответствие заданным в системе правилам.

DPI для корпоративного сектора



DPI для корпоративного сектора

Канал передачи сообщения	Протокол	Результат работы СИСТЕМЫ
Интернет-ресурсы (форумы, блоги)	HTTP POST	Сообщение не отсылается на интернет-ресурс. На экран выводится сообщение «Заблокировано Monitorium»
Интернет-ресурсы (поисковые ресурсы)	HTTP GET	Поиск не осуществляется. Страница не отображается
Электронная почта (в том числе веб-почта)	SMTP, IMAP	Письмо отправляется получателю без тела письма
Программы мгновенного обмена сообщениями	ICQ/AIM (OSCAR), XMPP(Jabber), Mail.Ru Агент	Сообщение не отправляется
Передача файлов по FTP	FTP	Передается пустой файл

Перехват и блокировка сообщений

Если в правилах не установлен режим блокировки, сообщение пропускается системой без изменений, копия сообщения сохраняется в архиве системы для дальнейшего ретроспективного анализа. Если отправляемое сообщение соответствует критериям, заданным в правилах, оно блокируется.

DPI для корпоративного сектора

Система является комплексным решением и имеет следующие инструменты управления:

Монитор
Отчеты
Редактор привил
Поиск
Настройки
Диагностика
Журнал

Из недостатков:

- Система масштабируется только увеличением числа комплексов
- Не имеет механизмов кластеризации, и как следствие отсутствие общей политики

Тестирование DPI систем

Французский национальный профсоюз звукозаписи SNEP (the Syndicat National de l'Édition Phonographique, an organization that represents the interests of the French music industry) совместно с компанией EANTC (The European Advanced Networking Test Center) провел тестирование DPI решений основных производителей.

- На тест были приглашены 28 компаний разрабатывающие DPI решения.
- Участие было бесплатно, все расходы оплатил SNEP
- Продолжительность тестирования составила 6 месяцев
- Для настройки оборудования допускалось использование инженеров от производителя оборудования
- Из 28-ми приглашенных согласились участвовать только 5 компании на условиях – не публикации результатов если им не понравится результат. В дальнейшем 3 из них воспользовались правом вето на публикацию результата.
- Только два производителя согласились с публикацией результатов. Это компании Arbor (Ellacoya) и ipoque GmbH.

Тестирование DPI систем

Заключение по тестированию:

- Оба устройства Abrob/Ellacoya E30 и Ipoque PRX-5G показали отличную производительность и очень хорошие возможности обнаружения и регулирования P2P трафика.
- Самые известные протоколы P2P были успешно обнаружены. У обоих производителей точность обнаружения составила более 90%. Ложные срабатывания не замечены.
- Наличие каждого из фильтрующих устройств не повлияло на производительность сети.
- Потеря пакетов не наблюдалось для двунаправленной скорости до 950 Мбит/с.
- Сетевая задержка всегда оставалась ниже 1 миллисекунды, и задержка не увеличивается, даже если устройства были испытаны со сложной смесью трафика.
- Abrob/Ellacoya и Ipoque способны фильтровать некоторые шифрованные протоколы P2P (BitTorrent и Filetopia).
- Тест DPI систем Abrob/Ellacoya и Ipoque и показал, что можно успешно ограничить трафик P2P на краю сети оператора.

Вывод:

Логично предположить что остальные компании, не согласившиеся на публикацию результатов, показали результаты хуже…

Экономическая часть DPI

За счет чего можно улучшить экономические показателей при внедрении DPI системы управления трафиком

Экономическая часть DPI

Используемые экономические термины и их определения

- CAPEX (англ. CAPital EXpenditure) - Капитальные расходы - капитал, который используется компаниями для приобретения или модернизации физических активов (жилой и промышленной недвижимости, оборудования, технологий).Нередко встречается и такое определение CAPEX — это инвестиционные затраты на покупку основных фондов/средств, а также затраты по обслуживанию кредитов на их приобретение.

- OPEX (англ., сокр. от operating expense) - Операционные затраты или операционные расходы - повседневные затраты компании для ведения бизнеса, производства продуктов и услуг.

Сумма операционных расходов OPEX и капитальных расходов CAPEX составляют расходы компании, которые не включаются в прямую себестоимость продуктов или услуг.

Экономическая часть DPI

Используемый экономические термины и их определения

- ARPU (англ. Average revenue per user) - средняя выручка на одного пользователя — показатель, используемый телекоммуникационными компаниями, в том числе интернет-провайдерами/IT-компаниями, предоставляющими онлайн-сервисы и означающий среднюю выручку (обычно за месяц) в расчёте на одного абонента. Является одним из показателей, характеризующих успешность бизнеса компании.

- Показатель ROI является отношением суммы прибыли или убытков к сумме инвестиций. Значением прибыли может быть процентный доход, прибыль/убытки по бухгалтерскому учёту, прибыль/убытки по управленческому учёту или чистая прибыль/убыток. Значением суммы инвестиций могут быть активы, капитал, сумма основного долга бизнеса и другие выраженные в деньгах инвестиции.

Экономическая часть DPI

Пример расчёта эффективности (ROI) внедрения DPI системы управления трафиком

Снижение требований к полосе пропускания магистрального канала при абонентской базе - 50000 абонентов.

Исходные данные:

Количество абонентов - 50000

Стоимость DPI решения - $80000

Предлагаемая эффективность DPI решения – 35%

Стоимость 1Гбит/с - $25000/месяц

Полоса пропускания на абонента – 64 Кбит/с

Коэффициент активности абонента – ½ (0,5)

Экономическая часть DPI

Пример расчёта эффективности (ROI) внедрения DPI системы управления трафиком

Пример расчета без DPI

(64 Кбит/с * 0,5) * 50000 = 1,6 Гбит/с

Пример расчета с DPI

1,6 Гбит/с * (1-0,35) = 1Гбит/с

Сокращение требований к магистральному каналу составляет - 600 Мбит/с

Экономическая часть DPI

Пример расчета эффективности (ROI) внедрения DPI системы управления трафиком

Расчет по сохранению OPEX (операционных расходов)

0,35 * 1,6 Гбит/с * 25000 = $14000 / месяц

Расчет окупаемости

$80000 / $14000 = 6 месяцев

Экономическая часть DPI

Пример расчёта внедрения DPI для новых услуг -
Организация «новой» услуги «Безлимитный безлимит»

Исходные данные:

Количество абонентов - 100000

Стоимость развёртывания – $4 на абонента

Процент абонентов - подписчиков на дополнительную услугу – 5%

Стоимость дополнительной услуги – $5,5 / месяц

Привлечение абонентов (миграция) – 2000

Ежемесячный платеж абонента - $24 /месяц

Экономическая часть DPI

Пример расчёта внедрения DPI для новых услуг -
Организация «новой» услуги «Безлимитный безлимит»

Пример расчета с учётом миграции

(100000 * $4) / ((0,05 * 100000 * $5,5) + (2000 * 24)) = 5,5

Срок окупаемости 5,5 месяца

Пример расчета без учёта миграции
(100000 * $4) / (0,05 * 100000 * $5,5) = 14,6

Срок окупаемости 14,6 месяца

Экономическая часть DPI

Пример расчёта внедрения DPI для новых услуг -
Организация «новой» услуги «Безлимитный безлимит»

5% - подписались на услугу 5000, еж. платеж $29,5
95% - еж. платеж $24

Дополнительная прибыль составила
(5000 * 29,5) – (5000 * 24) = $27500 / месяц
Суммарная прибыль
(5000 * 29,5) + (95000 * 24) = $2280000

ARPU
((5000 * 29,5) + (95000 * 24)) / 100000 = $24,3

Рост ARPU
((24,3*100)24)-100% = 1,3 %

Правовая часть DPI

Правомерность использования DPI систем в РФ

Упрощенная структура правовой системы РФ

Правовая часть DPI

Конституция РФ

Конституция Российской федерации – высший нормативный правовой акт РФ.

Глава 2. Права и свободы человека и гражданина

Статья 23

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.
2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Статья 24

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.
2. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 29

1. Каждому гарантируется свобода мысли и слова.
2. Не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства.
3. Никто не может быть принужден к выражению своих мнений и убеждений или отказу от них.
4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом.
5. Гарантируется свобода массовой информации. Цензура запрещается.

Правовая часть DPI

Федеральные законы

N 126-ФЗ
Глава 9. ЗАЩИТА ПРАВ ПОЛЬЗОВАТЕЛЕЙ УСЛУГАМИ СВЯЗИ
Статья 63. Тайна связи

1. На территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи.

Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами.

2. Операторы связи обязаны обеспечить соблюдение тайны связи.

3. Осмотр почтовых отправлений лицами, не являющимися уполномоченными работниками оператора связи, вскрытие почтовых отправлений, осмотр вложений, ознакомление с информацией и документальной корреспонденцией, передаваемыми по сетям электросвязи и сетям почтовой связи, осуществляются только на основании решения суда, за исключением случаев, установленных федеральными законами.

4. Сведения о передаваемых по сетям электросвязи и сетям почтовой связи сообщениях, о почтовых отправлениях и почтовых переводах денежных средств, а также сами эти сообщения, почтовые отправления и переводимые денежные средства могут выдаваться только отправителям и получателям или их уполномоченным представителям, если иное не предусмотрено федеральными законами.

Правовая часть DPI

Федеральные законы

Федеральный закон от 28.07.2012 N 139-ФЗ
"О внесении изменений в Федеральный закон
"О защите детей от информации, причиняющей вред их здоровью и развитию"
и отдельные законодательные акты Российской Федерации"

(Статьи 2 и 3 настоящего Федерального закона вступают в силу с 1 ноября 2012 года.)

Статья 2

Статью 46 Федерального закона от 7 июля 2003 года N 126-ФЗ "О связи" (Собрание законодательства Российской Федерации, 2003, N 28, ст. 2895; 2007, N 7, ст. 835; 2010, N 7, ст. 705; N 31, ст. 4190) дополнить пунктом 5 следующего содержания:

5. Оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", обязан осуществлять ограничение и возобновление доступа к информации, распространяемой посредством информационно-телекоммуникационной сети "Интернет", в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации"

Правовая часть DPI

Федеральные законы

Статья 3

10. В течение суток с момента включения в реестр сетевого адреса, позволяющего идентифицировать сайт в сети "Интернет", содержащий информацию, распространение которой в Российской Федерации запрещено, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", обязан ограничить доступ к такому сайту в сети "Интернет".

Примечание: Текст пункта 11 приведен в соответствие с публикацией в "Собрании законодательства РФ", 30.07.2012, N 31, ст. 4328 и на Официальном интернет-портале правовой информации http://www.pravo.gov.ru, 30.07.2012.

В "Российской газете", N 172, 30.07.2012 фрагмент текста пункта 11 после слов "...либо на основании вступившего в законную силу решения суда об отмене решения..." опубликован в следующей редакции:

"...уполномоченного Правительством Российской Федерации федерального органа исполнительной власти о включении в реестр доменного имени, указателя страницы сайта в сети "Интернет" или сетевого адреса, позволяющего идентифицировать сайт в сети "Интернет".

Правовая часть DPI

Федеральные законы

Статья 3

11. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, или привлеченный им в соответствии с частью 4 настоящей статьи оператор реестра исключает из реестра доменное имя, указатель страницы сайта в сети "Интернет" или сетевой адрес, позволяющий идентифицировать сайт в сети "Интернет", на основании обращения владельца сайта в сети "Интернет", провайдера хостинга или оператора связи, оказывающего услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", не позднее чем в течение трех дней со дня такого обращения после принятия мер по удалению информации, распространение которой в Российской Федерации запрещено, либо на основании вступившего в законную силу решения суда об отмене решения федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о включении в реестр доменного имени, указателя страницы сайта в сети "Интернет" или сетевого адреса, позволяющего идентифицировать сайт в сети "Интернет".

Правовая часть DPI

Отраслевые постановления и акты

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОСТАНОВЛЕНИЕ
от 10 сентября 2007 г. N 575
ОБ УТВЕРЖДЕНИИ ПРАВИЛ
ОКАЗАНИЯ ТЕЛЕМАТИЧЕСКИХ УСЛУГ СВЯЗИ
(в ред. Постановления Правительства РФ от 16.02.2008 N 93)
В действии с 1 января 2008 г.

26. Оператор связи обязан:

и) исключить возможность доступа к информационным системам, сетевые адреса или унифицированные указатели которых абонент сообщает оператору связи в предусмотренном договором виде.

27. Оператор связи вправе:

приостанавливать оказание телематических услуг связи абоненту и (или) пользователю в случае нарушения абонентом и (или) пользователем требований, предусмотренных договором, а также в случаях, установленных законодательством Российской Федерации;

осуществлять ограничение отдельных действий абонента и (или) пользователя, если такие действия создают угрозу для нормального функционирования сети связи.

Правовая часть DPI

Международные акты и соглашения

После обсуждения за закрытыми дверьми эксперты Международного союза электросвязи (МСЭ), в который входит и Россия, утвердили стандарт (рекомендации) Y.2770 на применение технологий Deep Packet Inspection.

Представители России и некоторых других стран предлагают сделать этот стандарт обязательным для интернет-провайдеров.

В текущей редакции документа, технические спецификации Y.2770 не предусматривают инспекции зашифрованного трафика, но предусматривают обязательную инспекцию незашифрованных фрагментов такого трафика.

Несмотря на то, что 6 декабря 2012 года на блоге МСЭ было опубликовано сообщение, что ситуация взята под контроль и утвержденный стандарт Y.2770 не разрешает доступ к личной информации пользователей, вероятность того, что DPI не будет применяться для обработки личной информации, исключить нельзя.

Нужно учитывать, что указанный стандарт теперь является официально разрешенным на территории стран-участниц МСЭ, что дает властям право использовать его.

Источники

Wiki
http://ru.wikipedia.org/wiki/Deep_packet_inspection

SPI /MPI
http://www.christopher-parsons.com

J’son & Partners Consulting
http://www.json.ru

Trafica
http://trafica.ru/monitorium

Федеральные законы
http://www.consultant.ru

Конституция РФ
http://www.constitution.ru/

МСЭ и DPI
http://habrahabr.ru/post/161409/
http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=7082
http://www.linux.org.ru/forum/talks/8565726
http://www.ixbt.com/news/hard/index.shtml?16/35/78

Источники

Описание оборудования

http://www.allot.com
http://www.netwell.ru/production/allot/allot_products.php
http://nag.ru:90/news/tag/4032/

https://www.sandvine.com

http://www.cisco.com

http://www.juniper.net

http://www.proceranetworks.com

http://www.huawei.com

Открытые системы и DPI
http://www.sysadmin.in.ua/info/index/21/35/50
http://ru.wikipedia.org/wiki/L7-filter
http://habrahabr.ru/post/108280/

Источники

Реклама как бизнес оператора связи
http://www.imarker.ru/
http://habrahabr.ru/post/190938/

Описание NBAR2
http://gblogs.cisco.com/ru/av%D1%81/#more-1466

Описание возможностей DPI систем
http://nag.ru/articles/article/22432/dpi.html

Расчёты внедрения DPI
http://www.ufts.ru/

Тестирование DPI систем
http://www.internetevolution.com

Идентификация трафика
http://spid.sourceforge.net/sncnw09-hjelmvik_john-CR.pdf
https://www.iis.se/docs/The_SPID_Algorithm_-_Statistical_Protocol_IDentification.pdf

Источники

Прочие производители DPI систем

http://www.it-grad.ru/uslugi/itaas/dpi/

http://mobak.ru/solutions/internet-provajderam.html

http://www.protei.ru/products/dpi/

http://qrator.net/solutions/tech.html

http://www.mfisoft.ru/products/information_security/ddos_perimetr/perimetr_f

http://www.qosmos.com/wp-content/uploads/2013/03/Qosmos_Intel_WhitePaper_Beyond-DPI_2012.pdf

http://www.arbornetworks.com/

http://www.ipoque.com/

Статистика по трафику
http://www.statista.com

История распространения DPI систем в России
http://m.forbes.ru/article.php?id=194198

И многие, многие другие…. Простите, если что-то забыл указать…

Конец

Спасибо за внимание!

Сергей Медведев

Красноярск
2014