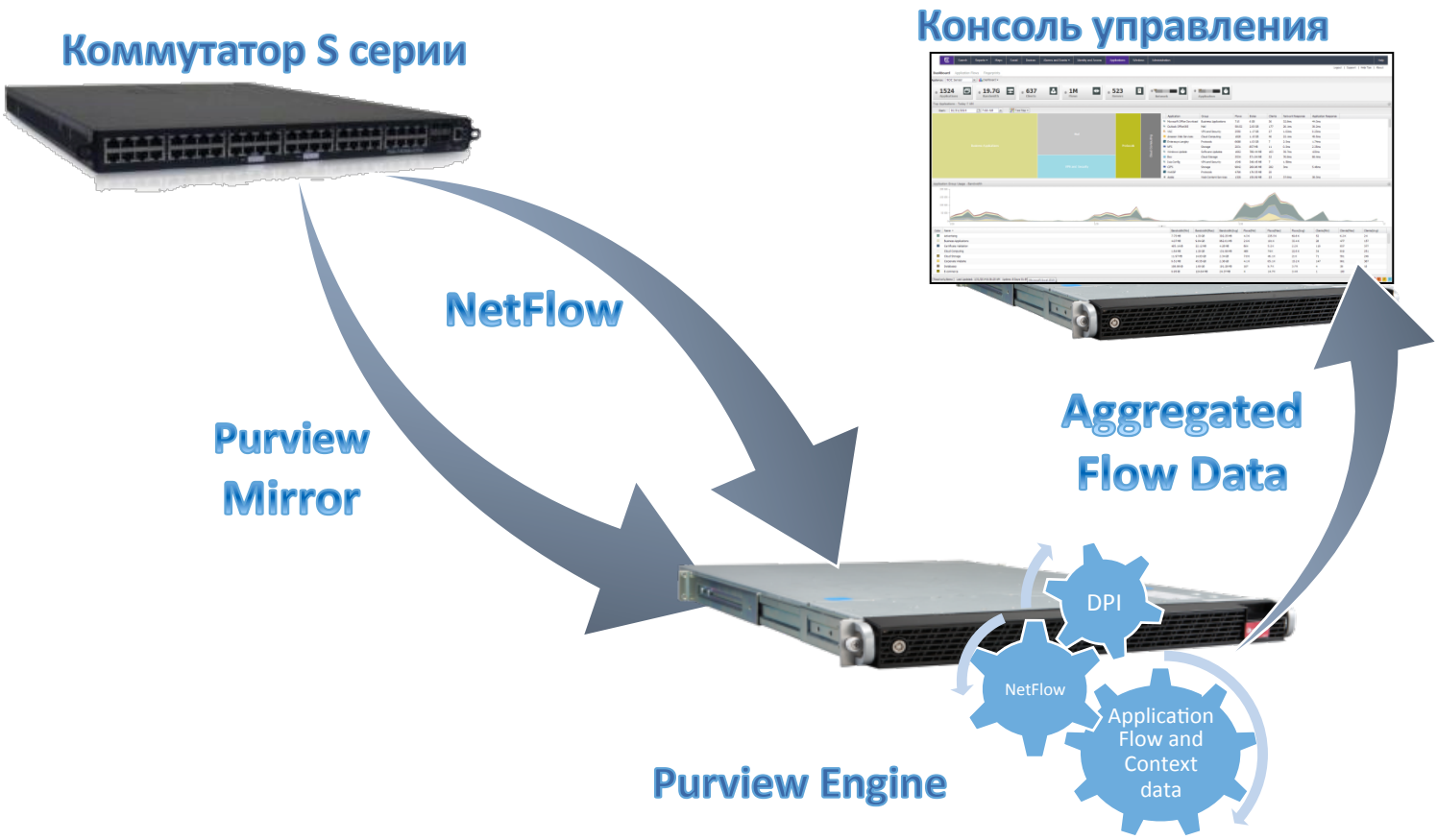
Система анализа потоков данных корпоративных сетей Extreme Networks PurView или как построить мост между вторым и седьмым уровнями модели OSI без тяжелых финансовых последствий

Необходимость глубокого анализа траффиков корпоративных сетей всегда «волновала умы» разработчиков сетевых инфраструктур, служб эксплуатации и поддержки и уж конечно же служб информационной безопасности. Информация о том какие именно приложения работают в сети до некоторых пор была доступна посредством анализа информации уровня 4 модели OSI (TCP/UDP порты и т.п.) Однако в связи с развитием облачных технологий, переселением приложений из корпоративной сети во внешний мир, появлением социальных сетей самого разного толка и калибра, такой подход совершенно утратил актуальность. По нынешним временам за TCP портом 80 могут скрываться сотни и тысячи разнообразных web приложений и отличить их друг от друга используя традиционный подход совершенно невозможно. Ситуация усугубляется тем, что абсолютное большинство устройств сетевой инфраструктуры (коммутаторов и маршрутизаторов) работают в логике packet by packet, т.е. каждый последующий пакет рассматривается вне какой-либо связи с предыдущим. При таком подходе выявить каким-то образом информационный поток того или иного приложения невозможно потому, что информация необходимая для идентификации приложения может быть сегментирована в нескольких пакетах и обретает смысл только после одновременного анализа последовательности пакетов. Таким образом мы приходим к тому, что для решения задачи идентификации приложений необходимо устройство способное следить за всеми соединениями сети через которые эти приложения работают, выделять из множества пакетов потоки этих приложений, реассемблировать их и анализировать полученную информацию.

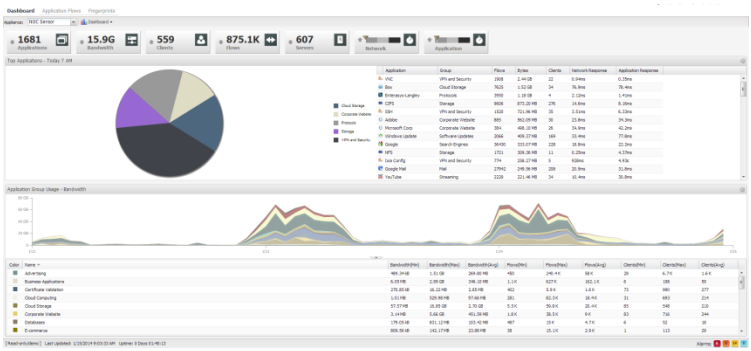
Такие, т.е. способные осуществлять Deep Packet Inspection вместе с с Application Identification устройства безусловно есть, прежде всего это межсетевые экраны, которые располагаются на границе сети и контролируют, кто, как и по какому поводу эту границу пересекает. Однако все без исключения межсетевые экраны представляют собой то, что по-русски называется программно-аппаратным комплексом, т.е. специализированное программное обеспечение работающее на универсальной аппаратной платформе. Универсальность аппаратной части всегда обусловливает невысокую производительность такого решения и дороговизну ее наращивания, масштабирование до десятков и сотен гигабит в секунду при таком подходе либо чрезвычайно дорого, либо невозможно.

На этом фоне система анализа и мониторинга сетевых приложений Purview компании Extreme Networks выглядит революционно. Самое существенное ее отличие от прочих решений подобного рода – это перенос значительной части функций на аппаратный уровень устройств сетевой инфраструктуры. Ядром системы служат высокопроизводительные коммутаторы S серии, построенные на базе специализированных микросхем (ASICs), на аппаратном уровне идентифицирующих потоки приложений. Коммутаторы S серии компании Extreme Networks работают не в логике packet by packet, а в логике flow based (на базе потоков), коммутатор идентифицирует поток, определяет куда и каким образом этот поток должен быть направлен, программирует соединение и все последующие пакеты этого потока направляются по соответствующему адресу. В отличие от классического дизайна, эти коммутаторы рассматривают каждый последующий пакет в связке с предыдущими. Происходит это без потери производительности, на проводных скоростях портов, независимо от форм фактора и портовой плотности коммутаторов. Система глубокого анализа пакетов и идентификации приложений Purview использует эту функциональность и выглядит следующим образом:

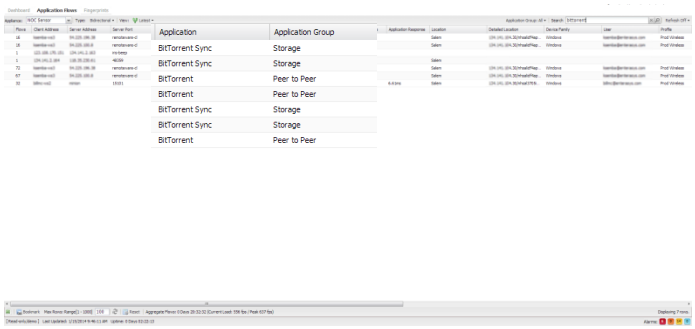


Коммутатор S серии выделив поток приложения осуществляет Purview Mirror, т.е. отсылает для анализа первые 15-30 пакетов этого потока, Purview Engine проделывает сигнатурный и эвристический анализ полученных с Purview Mirror пакетов, идентифицирует приложение сгенерировавшее этот поток, а затем результат анализа, вкупе с Netflow информацией по этому потоку, отправляется на консоль управления для визуализации и генерирования отчетов. Преимущества такого способа действия очевидны, самое главное состоит в том, что выделением потоков приложений занимаются специализированные микросхемы (ASICs) устройств сетевой инфраструктуры (коммутаторы S серии), в результате, в последующий анализ попадают не все пакеты, а только информативная часть каждого потока, что существенным образом снижает требования к мощности Purview Engine и снимает ограничения по масштабированию. Решение перестает быть граничным и становится распределенным, потому что все без исключения устройства сетевой инфраструктуры построенной на коммутаторах S серии занимаются выделением потоков приложений и могут быть сконфигурированы для отправления информативной части потока на Purview Engine для анализа.

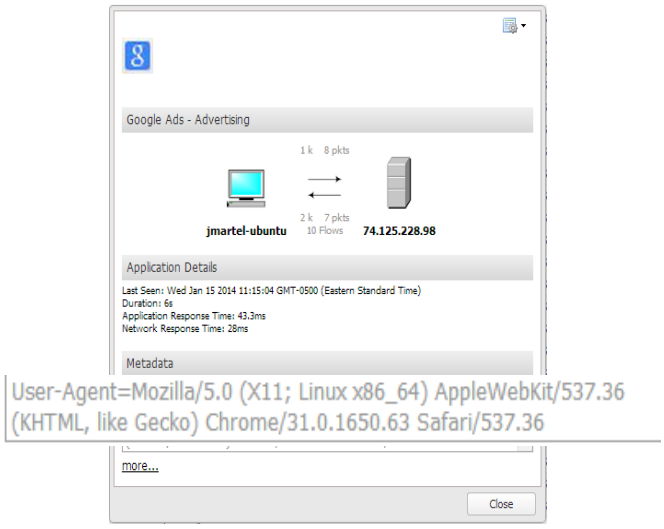
Отчеты и экранные представления Purview могут быть совершенно различными и приспосабливаться к нуждам каждой сети. Так, например, выглядит суммарная статистика по группам приложений и востребованной каждой группой полосе пропускания:



Система позволяет мгновенно идентифицировать пользователей имеющих нелегальные или уязвимые приложения:



Application	Application Group
BitTorrent Sync	Storage
BitTorrent Sync	Storage
BitTorrent	Peer to Peer
BitTorrent	Peer to Peer
BitTorrent Sync	Storage
BitTorrent Sync	Storage
BitTorrent	Peer to Peer



Purview позволяет измерить время отклика приложения и сравнить его с временем отклика сети, что дает бесценную исходную информацию для поиска неисправностей в сети, позволяет получить статистику Top N по приложением, пользователям этих приложений, сгенерированным ими потокам и использованной полосе пропускания.

База сигнатур, посредством которых производится идентификация приложений постоянно обновляется. На сегодняшний день она содержит более 13000 «отпечатков пальцев», по которым можно определить более 7000 приложений. Система позволяет пользователю как самостоятельно конструировать новые сигнатуры, так и модифицировать существующие для максимально точного детектирования новых или видоизмененных приложений. Использование Purview в комплексе с решением Identity Access Management позволяет детализировать отчетную информацию о пользователях, включая их имена, имена устройств, типы устройств, используемые операционные системы и веб браузеры, время и место подключения безотносительно к тому проводная или беспроводная инфраструктура была для этого использована. Столь исчерпывающий набор информации о пользователях и используемых ими приложениях открывает поистине уникальные возможности для решения задач оптимизации доставки этих приложений на любые, в том числе и мобильные устройства, поддержки работоспособности сетей, обеспечения надежности и информационной безопасности.