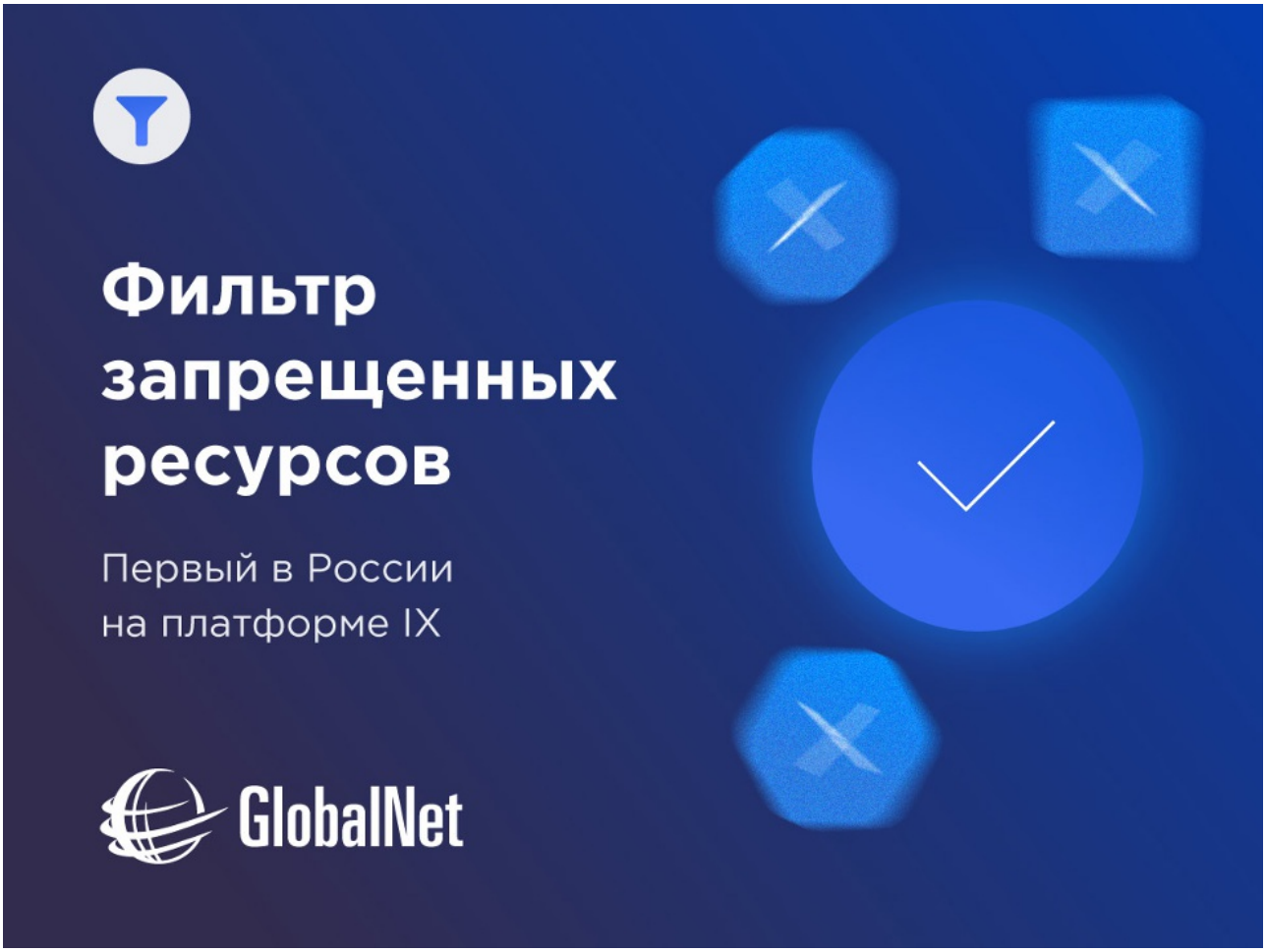
DATAIX/GlobalNet запустил первый в России фильтр по спискам РКН на платформе IX



Весной 2022 года команда DATAIX/GlobalNet столкнулась с ростом числа запросов по организации автоматической фильтрации трафика внутри сети. Такие обращения поступали одновременно с повышением внимания Роскомнадзора к соблюдению требований по запрету доступа к ряду ресурсов. Федеральная служба заметно усилила контроль за соблюдением текущего порядка блокировки, вводя в перечень нежелательных сайтов всё больше наименований. Так, операторы связи встали перед необходимостью решения вопроса фильтрации трафика внутри своей сети: самостоятельно устанавливать систему анализа и обработки трафика или обратиться с просьбой предоставления этой услуги к платформам, которые уже внедрили DPI.

Deep Packet Inspection или система анализа и обработки трафика — инструмент, который помогает заглянуть вглубь трафика и определить там всё: от IP-адресов до страниц в интернете, которые посещает устройство с доступом в сеть. Современные DPI используют для разнообразных целей: начиная с вычисления вредоносных пакетов данных заканчивая сбором статистики для маркетинговых исследований. Внедрить такую систему на сети отдельного интернет-провайдера — задача нетривиальная: необходимо выделить время, деньги и конкретных технических специалистов для подбора, настройки и развертывания подходящего решения. Кроме этого, при самостоятельном внедрении системы операторы нередко сталкиваются с временными лагами, когда из-за задержки фильтра при обработке информации пользователю удаётся либо открыть нежелательный сайт, либо зависнуть на открываемой странице на несколько секунд.

Альтернативным вариантом выступает получение аплинка, который бы самостоятельно фильтровал доступ к запрещенным сайтам при получении такого запроса от клиента. Так, распространенным решением среди интернет-провайдеров стало подключение к IP-Transit от другого оператора связи, который блокировал запросы клиентов к нежелательным ресурсам. Однако не всех клиентов этой услуги устроило увеличение задержек при получении пакетов данных, связанное со структурным устройством предоставления интернета нижестоящим операторам. Мы подошли к решению этой проблемы, развернув DPI-систему на платформе нашей распределенной пиринговой сети DATAIX.

Нам неизвестны другие прецеденты, когда кто-либо реализовывал похожее решение на платформе IX, поэтому сегодня мы можем говорить о том, что DATAIX — это первая точка обмена трафиком, на которой была внедрена автоматическая фильтрация при помощи системы DPI. Разработанное решение не создает дополнительных задержек свыше 1 микросекунды. Вместе с этим, структура IX

позволяет сохранить высокую связность сети и отсутствие L3-хопов. Это делает развернутую на нашей сети DATAIX систему DPI уникальным решением актуальной проблемы каждого оператора связи в России.

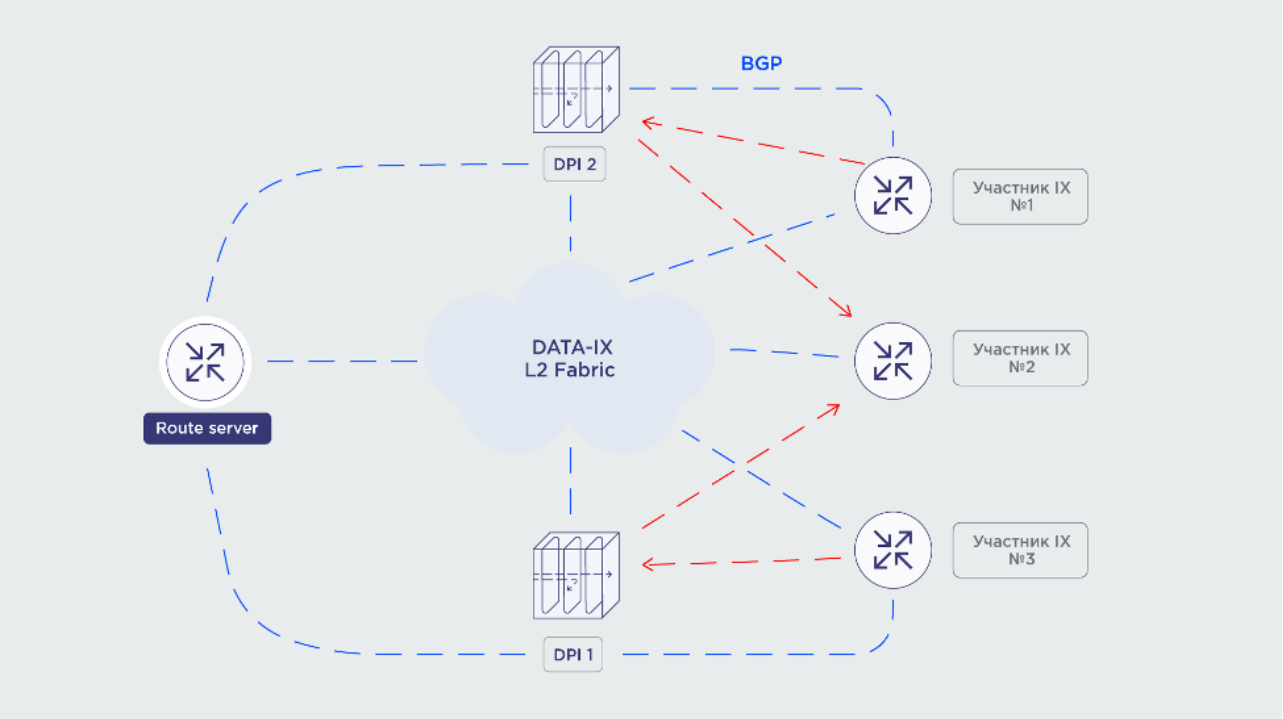


Схема фильтрации по спискам РКН в IX

Принципы работы современного DPI:

1. L2-канал остается прозрачным: клиент видит откуда приходит и куда уходит отфильтрованный трафик.

Площадки IX в первую очередь строятся на уровне L2, если говорить о сетевой структуре в терминах эталонной модели OSI. Отказ от принципа взаимного обмена трафика и создание дополнительных узлов приводят к нарушению такой структуры. В таком случае, мы имеем дело не с IX, а с IP-транзитом с неполной связностью. Кроме того, что появление дополнительных хопов в трассировке противоречит самой архитектуре IX, оно также увеличивает задержки и негативно влияет на общее восприятие качества сервиса. Необходимо сохранить главное преимущество сети обмена трафика, которое заключается в том, чтобы минимизировать количество промежуточных хопов и, как следствие, сократить задержки.

2. География минимально влияет на возможные задержки в географически распределенной пиринговой сети.

Высокая удаленность участников сети друг от друга накладывает определенные инфраструктурные ограничения, если IX не имеет значительного физического присутствия рядом с клиентом. Это становится заметнее при попытке внедрения системы предварительной обработки трафика, которая в таком случае может еще сильнее замедлить передачу данных. Наша сеть DATAIX позволяет устанавливать DPI географически максимально близко к клиенту, чтобы трафик не ходил для чистки в ЦОД, находящийся в нескольких тысячах километров, а, напротив, очищался максимально близко к клиенту.

3. Высокопроизводительный DPI позволяет быстро обработать большое количество трафика.

Заметное число участников нашей площадки являются операторами связи, которые регулярно передают большие объемы данных: 100, 200, 300 Гб/сек. Важно обрабатывать весь объем трафика максимально быстро и, соответственно, иметь наиболее производительную систему DPI, чтобы внутри сети никто не ощущал лишних задержек или прерывания интернет-соединения.

О технической стороне разработанного алгоритма для анализа трафика и всей системы DPI в целом можно судить по результатам нашей работы:

— Для конечного клиента фильтрация трафика происходит незаметно. Если пользователь не посещает запрещенные ресурсы, то DPI не коснется его трафика. Это значит, что задержек либо

не будет совсем, либо они будут совершенно незаметными. Клиент также не обнаружит и косвенных признаков при маршрутизации трафика (например, по пути не встретятся дополнительные хопы). А если пользователь попытается зайти на запрещенный ресурс, то получит предупреждение о запрете или же просто не сможет открыть ресурс без уведомления.

— Запас производительности разработанного инструмента анализа и обработки трафика на одном процессоре составляет 200 Гб/сек. Это заметный и конкурентный результат на рынке современных решений DPI-систем. При этом, мощности системы позволяют ей работать как в 1G, так и в 400G-портах. Стоит, тем не менее, помнить, что возможности производительности конкретного DPI-устройства зависят от хардварного аппаратного сервера.

Подключение к фильтрации трафика внутри нашей сети доступно для всех участников DATAIX. Для этого достаточно:

— поднять BGP-сессии до наших роут-серверов в DATAIX;

— поднять BGP-сессию до нашей системы фильтрации и повысить приоритет со своей стороны на этой BGP сессии;

— после этого система начинает самостоятельно анализировать получаемый трафик и блокировать запросы к запрещенным ресурсам.

DATAIX является первой и единственной точкой обмена трафика в России, которая внедрила DPI с фильтрацией трафика по правилам РКН на своей сети. Фильтр работает в портах любой пропускной способности, обрабатывая трафик на одном процессоре со скоростью 200 Гб/сек. Наши специалисты продолжают отслеживать работоспособность системы и помогать в настройке новым клиентам, которые хотят к ней подключиться. Широкая география присутствия и собственные DWDM-магистрали позволяют потенциальному участнику уже сегодня включиться в сеть и пользоваться преимуществами распределенной сети с минимальными задержками и бесперебойностью входящего и выходящего трафика.