



191028, Санкт-Петербург,
Литейный пр. д. 26 Лит. А,
БЦ «Преображенский», офис 5-23
Телефон:
Эл. Почта:

СКАТ – СИСТЕМА КОНТРОЛЯ И АНАЛИЗА ТРАФИКА

Фильтрация по спискам РКН и Минюста

Всем операторам связи на территории РФ с 2012г необходимо выполнять требования закона ФЗ 139. Закон требует от провайдеров следить за федеральными реестрами запрещенных веб-ресурсов и своевременно их блокировать. Для того, чтобы осуществлять такую фильтрацию достаточно оперативно, необходимо решить две задачи:

1. Проверка реестров и загрузка новых записей;
2. Фильтрация трафика, который поступает с любого из запрещенных веб-сайтов. Здесь есть нюанс – фильтрация должна быть максимально гибкой, чтобы по IP не заблокировать заодно группу не попадающих в списки сайтов.

Среди возможных решений можно выделить следующие:

- Ручная загрузка файла реестра на регулярной основе, импорт в местную систему управления трафиком. Фильтрация осуществляется по IP адресу;
- Ручная загрузка файла реестра на регулярной основе, импорт в местную систему управления трафиком. Фильтрация осуществляется по URL адресу;
- Автоматическая загрузка реестра, импорт в систему управления трафиком. Фильтрация осуществляется по URL адресу.

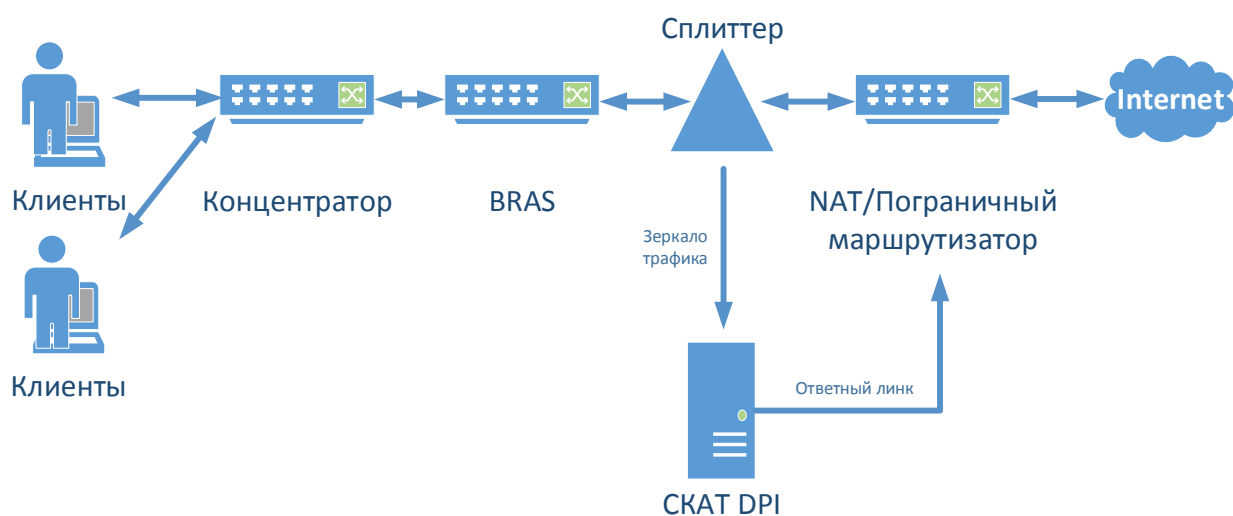
Два первых способа несут в себе лишнюю нагрузку на персонал за счет ручных операций. По этой же причине в подобных конфигурациях велик процент ошибок. К тому же, фильтрация по IP адресу не достаточно гибка в применении: при смене адреса запрещенный сайт может продолжать работать, может быть случайно заблокирован целый веб-сегмент из-за использования общего внешнего IP. Получается, что наиболее эффективным решением будет фильтрация по URL адресу с использованием DPI-технологий. DPI позволяет разбирать все проходящие через него сетевые пакеты, определять их принадлежность и заголовки.

Для решения задачи по наиболее эффективному и автоматизированному варианту компания **VAS Experts** предлагает воспользоваться продуктом **СКАТ DPI**. Это платформа глубокого анализа трафика, предназначенная для инспекции и классификации пакетов с последующей обработкой по потребностям компании. В системе доступна функция фильтрации трафика в соответствии с законами ФЗ-139, ФЗ-187, ФЗ-398. Загрузка списков Роскомнадзора и Министерства Юстиции происходит автоматически. Для большей гибкости возможно и ведение собственных черных списков.

Для фильтрации трафика СКАТ можно подключить тремя способами.

Установка на зеркалированный трафик

Схема с зеркалированием трафика через SPAN порты или оптические сплиттеры.



Преимущества:

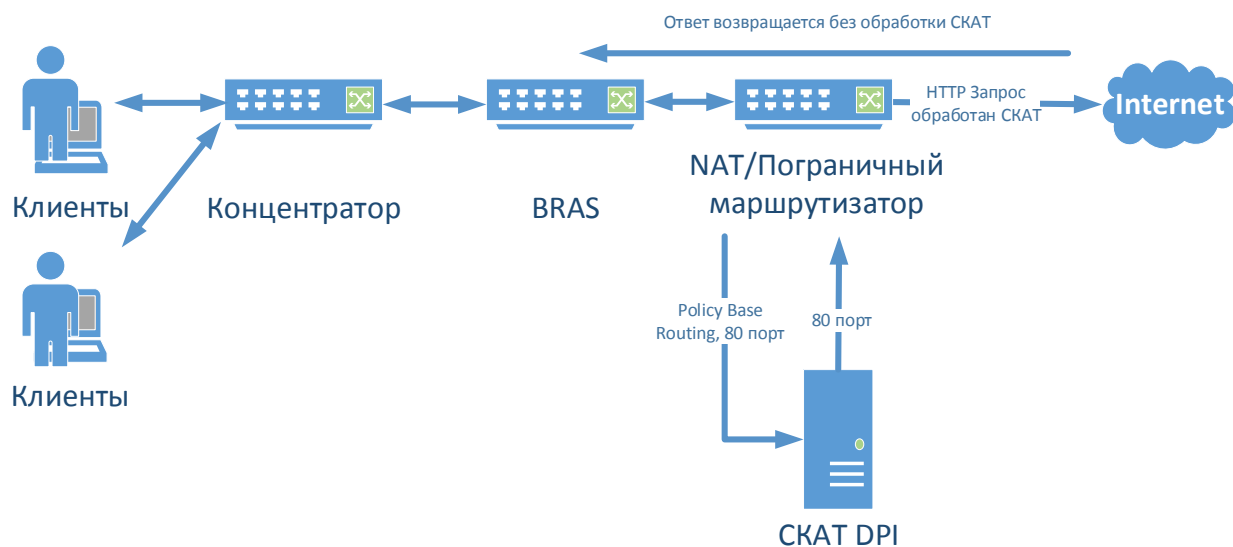
- Не требуются bypass карты;
- Минимальные изменения в сети;
- Возможность снятия аналитики с трафика и использование СКАТ в связке с КЭШ сервером.

Недостатки:

- Нет возможности использовать полный функционал СКАТ DPI

Установка только на web трафик с помощью настройки Policy Based Routing

Асимметричная схема обработки трафика на основе policy based routing применима только для фильтрации.



Преимущества:

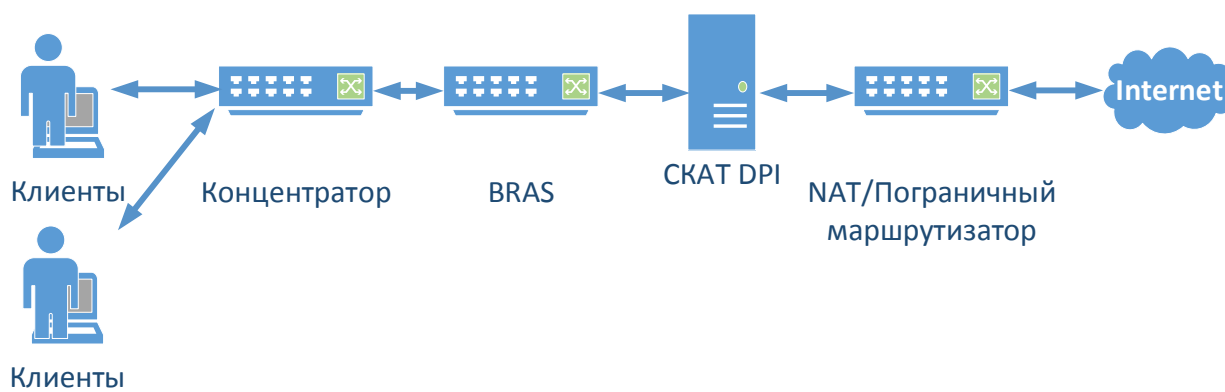
- Не требуются bypass карты;
- Минимальные изменения в сети;
- Снижение требований по производительности, т.к. web трафик занимает небольшую часть от общего трафика.

Недостатки:

- Нет возможности использовать полный функционал СКАТ DPI в том числе аналитики.

Установка СКАТ DPI «в разрыв»

Типовая схема в случаях, когда от системы требуется только фильтрация трафика. СКАТ подключается после граничного маршрутизатора в разрыв uplink.



Преимущества:

- Пропуск полного трафика через DPI, что дает возможность использовать полную функциональность (шейпинг, уведомления, кэширование).

Недостатки:

- Установка в разрыв предполагает использование bypass карт.

Использование СКАТ для фильтрации трафика позволяет в полной мере и без лишних затрат соблюсти требования законодательства. Это программное решение, которое не зависит от конкретного поставщика серверного оборудования и может гибко подстраиваться под требования бизнеса. В отличие от конкурирующих решений, СКАТ DPI обеспечивает высокую производительность по привлекательной цене.

К дополнительным преимуществам продукта можно отнести:

- Лучший % фильтрации по мнению РКН;
- Открытие дополнительных возможностей DPI с помощью повышения уровня лицензии;
- Большой объем списков (до 4млрд записей), минимальная задержка.
- Для полноценной работы функции фильтра достаточно версии **Entry**.