МИНИСТЕРСТВО СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО НАДЗОРУ В СФЕРЕ СВЯЗИ,
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И МАССОВЫХ КОММУНИКАЦИЙ
(РОСКОМНАДЗОР)**

ЗАМЕСТИТЕЛЬ РУКОВОДИТЕЛЯ

Китайгородский проезд, д. 7, стр. 2, Москва, 109074
тел. (495) 249-33-77; факс: (495) 587-44-68; www.rkn.gov.ru

от 19 ОКТ 2017 № 07ИО-97532

На № _____ от _____

ООО «ВАС Экспертс»

Литейный проспект, д. 26, Литер А,
офис 5-23, г. Санкт-Петербург,
191028

Заключение

Роскомнадзором в период с 13.09.2017 по 13.10.2017 проведено тестирование специализированного программного обеспечения «СКАТ DPI» (далее – СПО «СКАТ DPI»), предназначенного для получения, обработки и фильтрации трафика оператора связи с целью ограничения доступа к ресурсам, включенным в Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено (далее – Единый реестр), разработанного ООО «ВАС Экспертс».

Целью тестирования СПО «СКАТ DPI» являлось определение качества ограничения доступа к запрещенным ресурсам, внесенным в Единый реестр.

Участие в тестировании приняло 19 операторов связи из 6 федеральных округов Российской Федерации, с различной численностью абонентов.

СПО «СКАТ DPI» может быть установлено на сети оператора по 4 типовым схемам:

1. По схеме «в разрыв», когда весь трафик оператора связи проходит через СПО «СКАТ DPI». Данная схема установки рекомендована производителем и была выбрана в качестве основной для проведения тестирования.

2. По схеме ассиметрично «в разрыв», когда только исходящий трафик оператора связи проходит через СПО «СКАТ DPI». Данная схема

установки рекомендована производителем. По данному типу подключения тестировался один оператор связи.

3. По схеме «на зеркале», когда через СПО «СКАТ DPI» проходит копия трафика. При таком типе подключения существует сценарий, при котором ответ от сервера может быть получен быстрее, чем от СПО «СКАТ DPI», что приведет пропуску трафика без фильтрации. Данная схема не рекомендована производителем. По данному типу подключения тестировались три оператора связи.

4. По схеме «предфильтрации», когда СПО «СКАТ DPI» устанавливается в систему предварительной фильтрации трафика оператора связи. Данная схема установки не рекомендована производителем и по этой причине не тестировалась.

Тестирование СПО «СКАТ DPI» осуществлялось с использованием автоматизированной системы контроля за соблюдением операторами связи требований по ограничению доступа к сайтам в сети Интернет, содержащим информацию, распространение которой в РФ запрещено в соответствии с требованиями «149-ФЗ» (далее – АС «Ревизор»). АС «Ревизор» введена в промышленную эксплуатацию приказом ФГУП «РЧЦ ЦФО» от 29.12.2016 № 354 (сертификат соответствия № ОС-1СУ-0496, срок действия с 05.10.2016 до 05.10.2019).

Результаты тестирования

1. На основании данных АС «Ревизор», в процессе тестирования СПО «СКАТ DPI» на сетях 68% операторов связи не выявлены нарушения по Единому реестру и группе реестра «398-ФЗ».

На сетях 21% операторов связи, единично выявлялись нарушения, в количестве не превышающем 0,002% по Единому реестру и не более 0,03% группы реестра «398-ФЗ».

На сетях 11% операторов связи единично фиксировались нарушения в количестве не превышающем 0,03% по Единому реестру, из-за технических проблем на стороне операторов связи.

2. Процедура развертывания и настройки СПО «СКАТ DPI» на сети оператора связи, включая решение организационных и технических проблем, занимает от нескольких дней до 3 недель.

3. Производитель предъявляет требования к составу и содержанию технических средств оператора связи в соответствии с приложением, на которые устанавливается СПО «СКАТ DPI».

4. За период тестирования не выявлены нарушения на сетях операторов связи установивших СПО «СКАТ DPI» по схеме «на зеркале», которая не рекомендована производителем.

Вывод

Анализ результатов проведенного тестирования СПО «СКАТ DPI», разработанного ООО «ВАС Экспертс», показывает что при установке по рекомендованной производителем схеме подключения «в разрыв» и правильной настройке сети оператора связи количество выявленных нарушений по Единому реестру не превышают 0,002%, по группе реестра «398-ФЗ» не превышают 0,03%.

СПО «СКАТ DPI» может быть использован операторами связи в качестве средства ограничения доступа к информационным ресурсам в сети «Интернет», включенным в Единый реестр, и распространение которых в Российской Федерации запрещено.

Приложение: Требования по составу и содержанию технических средств для СПО «СКАТ DPI», на 8 л.

Заместитель руководителя О.А. Иванов

СКАТ
СИСТЕМА КОНТРОЛЯ
И АНАЛИЗА ТРАФИКА

191028, Санкт-Петербург,
Литейный пр. д. 26 Лит. А,
БЦ «Преображенский», офис 5-23
Телефон:+7 812 313 88 15
Эл. Почта:info@vasexperts.ru

Фильтрация по спискам РКН и Минюста

Всем операторам связи на территории РФ необходимо выполнять требования законов ФЗ-149, ФЗ-139, ФЗ-187, ФЗ-398, ФЗ-114. 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 целые 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.

Основные характеристики СКАТ

Характеристика	СКАТ-6	СКАТ-20	СКАТ-40	СКАТ-80	СКАТ-100
Пропускная способность	6 Гбит/с	20 Гбит/с	40 Гбит/с	80 Гбит/с	100 Гбит/с
Максимальное количество сессий	4 М	16 М	32 М	64 М	80 М
Максимальное количество новых сессий в секунду	100 К	250 К	350 К	400 К	500 К
К-во детектируемых протоколов	6000+				
Максимальное количество абонентов	400 К	2 М	4 М	8 М	10 М
Сетевые интерфейсы обработки трафика (без bypass)*	6x1GbE RJ-45	2x10GbE SFP+	4x10GbE SFP+	8x10GbE SFP+	10x10GbE SFP+
Максимальная задержка (Latency) не более	30 µc	30 µc	30 µc	30 µc	30 µc
Аппаратная платформа	1U, 19"	1U, 19"	1U, 19"	1U, 19"	1U, 19"

Устанавливая СКАТ DPI на свою сеть, оператор получает возможность использовать дополнительный функционал данного решения:

- Аналитика в режиме реального времени
- Управление полосой для абонентов и общей (QoS)
- Информирование абонентов, вставка рекламы
- CG-NAT
- Белые списки и Captive Portal
- Съемник для СОРМ-3 (538ПП)
- КЭШирование, ретрекер торрентов
- Защита от DDoS атак
- Предфильтр для СОРМ
- L2/L3 BRAS (PCRF, PCEF)

Для использования всех возможностей необходимо использовать схему установки «в разыв».

Лицензирование

Функциональность распределена между тремя лицензиями:

- **Entry** - фильтрация трафика по требованиям федерального законодательства
- **Base** - позволяет управлять трафиком в целом, т.е. управление полосой и приоритезацией канала, статистика и уведомления абонентов, маркетинговый кампании, предфильтр СОРМ, съемник для СОРМ-3
- **Complete** - управление абонентами, CG-NAT, белые списки, дополнительная функциональность

Система Контроля и Анализа Трафика - СКАТ-DPI комплектация	Entry	Base	Complete
Поддержка режима - Bypass	Да	Да	Да
Фильтрация по реестру запрещенных сайтов	Да	Да	Да
Сбор и анализ статистики по протоколам и направлениям	Нет	Да	Да
Разметка приоритета трафика в зависимости от протокола	Нет	Да	Да
Предфильтр СОРМ	Нет	Да	Да
Уведомление абонентов	Нет	Да	Да
Lawful interception	Нет	Да	Да
Распределение канала доступа между абонентами	Нет	Нет	Да
Блокировка и замена рекламы	Нет	Нет	Да
Белый список и Captive Portal	Нет	Нет	Да
Защита от DOS и DDOS атак	Нет	Нет	Да
CGNAT - Трансляция сетевых адресов	Нет	Нет	Да
Подписка на обновления 1 год	Да	Да	Да
Internet cache			
Internet cache - Кэш сервер	Лицензируется отдельно		
Резервирование			
Пассивный режим - резервный СКАТ устанавливается на альтернативный маршрут	25% от основной лицензии и ТП		
Активный режим - трафик разделяется между двумя платформами СКАТ	100% от основной лицензии и ТП		

Опция фильтрации

Характеристика	Описание
Загрузка реестра Роскомнадзора (ФЗ-139, ФЗ-187, ФЗ-398)	централизовано, облачный сервис
Возможность использования запроса подписанного своей ЭЦП	Да, размещается в облаке
Загрузка федерального списка экстремистских материалов Министерства Юстиции РФ (ФЗ-114)	централизовано, облачный сервис
Использование собственного списка оператора	Да
Поддержка централизованного собственного списка оператора для кластера серверов	Да
Поддержка схем подключения	в разрыв, асимметричная, зеркалирование
Возможность управления фильтрацией по определенным пользователям	Да
Блокировка трафика http/https	Да
Поддержка переадресации для http на информационную страницу	Да
Возможность сбора статистики по заблокированным страницам	Да
Возможность мониторинга загрузки списков и работы фильтрации	Да
Максимальный объём списка	до 4 млрд. URL

Блокировка HTTPS трафика

Работа с шифрованным трафиком СКАТ DPI осуществляет следующим образом:

- Проверяется наличие SNI, при совпадении осуществляется блокировка.
- Если SNI в списке нет, то проверяется Common Name сертификата SSL, при совпадении осуществляется блокировка.
- Если Common Name в списке нет, то проверяется IP+443 порт, при совпадении осуществляется блокировка.

Благодаря иерархической проверке СКАТ DPI осуществляет качественную блокировку и снижает количество ошибочно заблокированных ресурсов по сравнению с блокировкой только по IP+443 порт.

Для блокировки по CN и SNI требуется входящий и исходящий трафик.

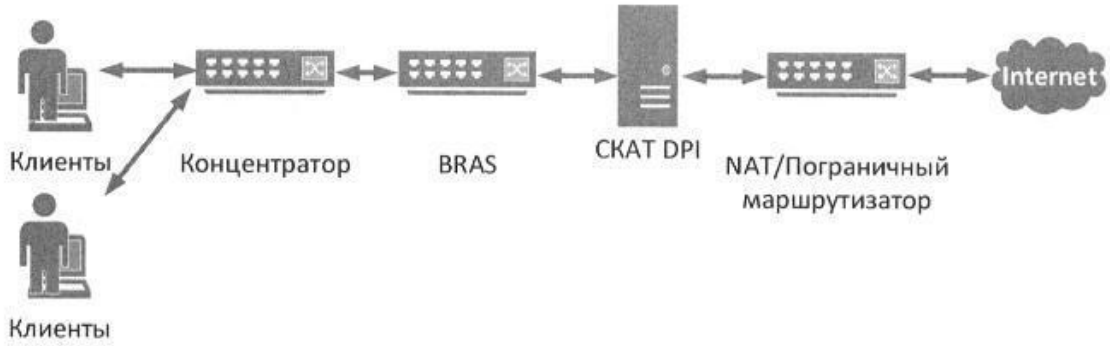
Минимальные технические требования к оборудованию

1. Один процессор с поддержкой инструкций SSE 4.2 начиная с Intel Nehalem (рекомендуется, но необязателен, Xeon серий E5/E3) с количеством ядер 4 и более, тактовой частотой 2.5 ГГц и выше
2. Для обработки трафика сетевые карты на чипсетах Intel 82575/82576/82580/82599/i350/i210 или x520 (чипсет 82599) с количеством портов 2, 4 и 6
3. Поддержка Bypass реализована для карт производства Silicom
4. Любой сетевой адаптер для управления устройством по SSH (обычно можно задействовать встроенный на основной карте)
5. DPI платформа запускается под управлением ОС CentOS 6.4 или 6.5 (CentOS x86_64)

Схемы подключения СКАТ DPI

Установка СКАТ DPI «в разрыв» - РЕКОМЕНДУЕМАЯ СХЕМА!

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.

Особенности:

- Минимально требуется 3 интерфейса на сервере. 1 (любой) для управления по SSH, 2 для трафика (! Обязательно DNA совместимые, см. поддерживаемые чипсеты выше)

Рекомендуется осуществлять резервирование СКАТ DPI для отказоустойчивости.

Установка СКАТ DPI ассиметрично «в разрыв» - РЕКОМЕНДУЕМАЯ СХЕМА!

Типовая схема в случаях, установки только на исходящий трафик. СКАТ подключается после граничного маршрутизатора в разрыв uplink.

Преимущества:

- Эффективная блокировка по спискам РКН.

Недостатки:

- Установка в разрыв предполагает использование bypass карт.
- Нет блокировки HTTPS по SNI

Особенности:

- Минимально требуется 3 интерфейса на сервере. 1 (любой) для управления по SSH, 2 для трафика (! Обязательно DNA совместимые, см. поддерживаемые чипсеты выше)

Установка на зеркалированный трафик – Не рекомендуемая схема!

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:

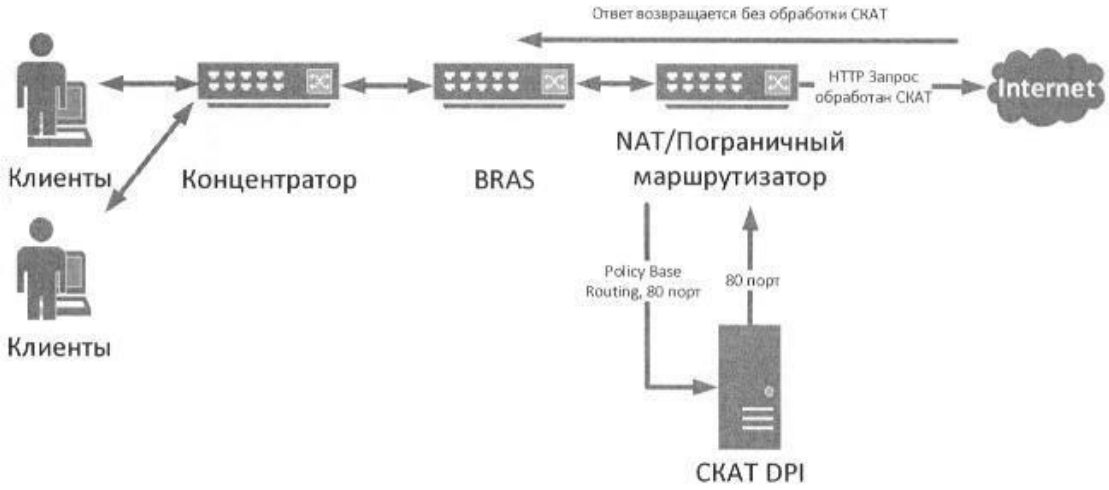
- Нет возможности использовать полный функционал СКАТ DPI

Особенности:

- Минимально требуется 3 интерфейса на сервере. 1 (любой) для управления по SSH, 1 для трафика и 1 для ответного линка (! Последние два обязательно DNA совместимые, см. поддерживаемые чипсеты выше)
- В случае зеркала вся емкость лицензии переходит на входящий трафик, т.е. лицензия СКАТ-6 позволяет подать на входящий интерфейс до 6Гбит/с.
- Для блокировки HTTPS по Common Name необходима передача на СКАТ входящего и исходящего трафика. в случае только исходящего трафика Блокировка HTTPS происходит по связке IP-порт.

Использование предфильтрации (BGP, Policy Based Routing - Не рекомендуемая схема!

Оператор направляет на СКАТ DPI только часть исходящего трафика 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.

Особенности:

- Оператор самостоятельно осуществляет перенаправление трафика (PBR, BGP). СКАТ не поддерживает притягивание трафика по BGP.
- Минимально требуется 3 интерфейса на сервере. 1 (любой) для управления по SSH, 2 для трафика (! Обязательно DNA совместимые, см. поддерживаемые чипсеты выше)
- Ответы о переадресации могут направляться как с IN, так и с OUT интерфейса.
- При конфигурировании указывается ассиметричные режим работы.
- Блокировка HTTPS происходит по связке IP-порт.

Техническая поддержка включает:

1. Регистрация обращений 24x7
2. Реакция на обращения в течение следующего рабочего дня (NBD - Next Business Day)*
3. Возможность обновления Программного Обеспечения СКАТ
4. Использование сервиса по автоматической загрузке списков с помощью ЭЦП провайдера

* - существует возможность приобрести расширенную поддержку: 8x5x8 (Время реакции 8 часов, в рабочее время) и 24x7x4 (Время реакции 4 часа)

Почему нас выбирают

Использование СКАТ для фильтрации трафика позволяет в полной мере и без лишних трудозатрат 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**.

Кто нас использует http://vasexperts.ru/otzyv.php

География установок СКАТ http://vasexperts.ru/about-company.php