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 ФЕВ 2018 № 07ИО-161128

На № _____ от _____

ООО «АДМ СИСТЕМЫ»

Большой Сампсониевский проспект,
д. 68, оф. 530,
г. Санкт-Петербург, 194100

sales@adm-systems.com

Заключение

Роскомнадзором в период с 15.01.2018 по 16.02.2018 проведено тестирование специализированного программного обеспечения «ADM Filter» (далее – СПО «ADM Filter»), 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 «АДМ СИСТЕМЫ».

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

Участие в тестировании приняло 11 операторов связи из 5 федеральных округов Российской Федерации, с различной численностью абонентов.

СПО «ADM Filter» может быть установлено на сети оператора по схеме «в разрыв», когда весь трафик оператора связи проходит через СПО «ADM Filter». Данная схема установки рекомендована производителем и была выбрана в качестве основной для проведения тестирования.

Тестирование СПО «ADM Filter» 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 «ADM Filter» на сетях 64% операторов связи не выявлены нарушения по Единому реестру и группе реестра «398-ФЗ».

На сетях 36% операторов связи, периодически выявлялись нарушения, в количестве не превышающем 0,03% по Единому реестру и не более 0,04% группы реестра «398-ФЗ».

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

3. В ходе тестирования СПО «ADM Filter» на сетях операторов связи фактов избыточной фильтрации, приводящей к ограничению доступа к ресурсам отсутствующим в выгрузке Единого Реестра – не выявлено.

4. Производитель предъявляет требования к составу и содержанию технических средств оператора связи в соответствии с приложением.

Вывод

Анализ результатов проведенного тестирования СПО «ADM Filter», разработанного ООО «АДМ СИСТЕМЫ», 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 0,03%, по группе реестра «398-ФЗ» не превышают 0,04%.

СПО «ADM Filter» может быть использовано 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 «ADM Filter», на 4 л.

Заместитель руководителя О.А. Иванов

1. Требования к инсталляции

СПО «ADM Filter» (далее - ADM S1) включается в сеть оператора на участке между BNG (BRAS) и внешним маршрутизатором, на котором опционально выполняется преобразование адресов NAT.

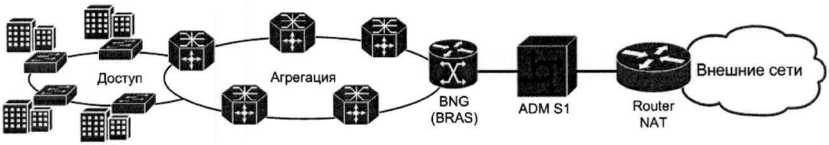

Рис. 1. ADM S1 в сети оператора ШПД

ADM S1 обрабатывает пакеты в прозрачном режиме (в разрыв). Система не идентифицируется в сети передачи данных ни на канальном, ни на сетевом уровнях, таким образом, конфигурация BNG и внешнего маршрутизатора не требует изменения.

Схема включения системы ADM S1 с оптическими интерфейсами 10GE представлена на рис. 2.

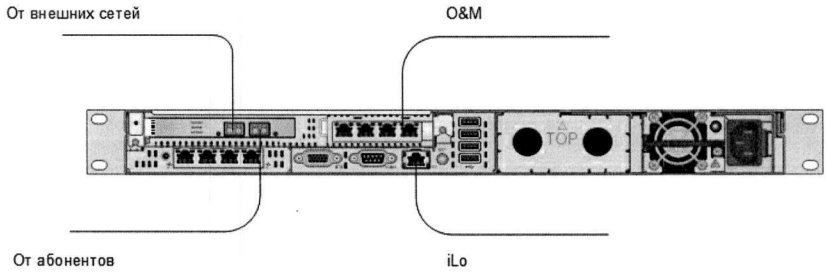

Рис. 2. Типовая схема подключения портов для 1 канала 10GE

2. Требования к оборудованию

Сервер с характеристиками 2xIntel Xeon E5 2699v4, 128 GB RAM, 2x1TB HDD RAID 1, сетевые интерфейсы 10GE с поддержкой технологии DPDK (контроллер Intel 82599 и новее) позволяет обработать 80 Гбит/с трафика в полнодуплексном режиме.

3. Общая информация

Система анализа трафика ADM S1 представляет собой полнофункциональную систему Deep Packet Inspection (DPI) и предназначена для мониторинга, анализа и управления трафиком оператора связи. В число задач, решаемых системой DPI, входят управление качеством обслуживания (QoS), построение статистических отчетов по структуре трафика с точки зрения протоколов и приложений, фильтрация трафика для оказания услуги Родительский контроль (Детский интернет) и соблюдения ФЗ РФ, а также предоставление дополнительных услуг с добавленной стоимостью.

Функциональные возможности:

Функция	Параметры
Управление политикой обслуживания (QoS)	▪ абонент ▪ принадлежность абонента к тарифному плану ▪ протокол ▪ приложение ▪ сервис (группа протоколов и приложений, а также их параметры в логических комбинациях) ▪ приоритет трафика ▪ принадлежность трафика абоненту-юридическому лицу ▪ принадлежность трафика абоненту-подразделению юридического лица ▪ интервал времени с возможностью разделения на будние и выходные дни
Управление политикой обслуживания включает в себя	▪ ограничение скорости ▪ управление приоритетом ▪ установку меток ToS/DSCP ▪ блокирование ▪ переадресацию запросов HTTP ▪ передачу трафика на внешние устройства по уровням L2, L3, L4 в режиме копирования и в режиме петли с возможностью добавления тегов VLAN и разделения нагрузки - блокирование URL по черным и белыми спискам, черным и белым спискам категорий
Классификация трафика	▪ более 2000 протоколов и приложений ▪ более 4000 параметров протоколов и приложений ▪ возможность применения правил на основе логических выражений ▪ корректная обработка заголовков второго и третьего уровней, таких как VLAN, MPLS, Q-in-Q
Идентификация абонентов	▪ получение IP-адреса абонента и его учетной записи через протокол RADIUS ▪ определение учетной записи абонента по статическому IP-адресу с возможностью задания одиночного IP-адреса, перечисления, диапазона, маски подсети и их комбинаций ▪ создание статических абонентов в массовом режиме через API и в одиночном режиме через WEB-интерфейс

	▪ графическое отображение привязки абонентов к географическим зонам ▪ управление не менее 10000 подразделений с единого сервера управления и с возможностью задания персональной политики по каждому из подразделений
Фильтрация трафика	▪ по черным спискам ▪ по белым спискам ▪ по черным спискам категорий ▪ по белым спискам категорий ▪ возможность формирования списков исключений ▪ фильтрация по IP-адресу или нескольким IP-адресам, заданным в виде одиночного адреса, перечисления, диапазона, подсети и произвольной их комбинации, hostname, а также URL ▪ блокирование ресурса, переадресация посредством 302 Moved или ответ 200OK с возвратом произвольного содержимого в качестве реакции на срабатывание фильтра ▪ фильтрация трафика https, http2, quic ▪ возможность проверки любого ресурса на блокирование/неблокирование с учетом абонента или подразделения, которое будет обращаться к данному ресурсу, через WEB-интерфейс
Отчеты и статистика	▪ IPDR по каждой TCP-сессии для протокола http ▪ IPDR по использованию протоколов и приложений ▪ Отчеты: --TOP-протоколов и приложений --TOP-доменов по переходам --TOP-доменов по трафику UL, DL и суммарному --TOP-абонентов --TOP-ресурсов (URL) --временная диаграмма по использованию протокола или приложения ▪ графическое отображение отчетов в виде круговой и столбиковой диаграмм, графика, таблиц. ▪ выгрузка данных любого отчета в формате xls ▪ Фильтрация результатов по -- произвольному временному интервалу -- абоненту -- группе абонентов -- подразделению -- домену

	-- уровню домена (первый, второй и третий уровни) --географической принадлежности клиента или клиентов, для которых строится отчет ▪ автоматические переходы между отчетами нажатием на пунктах таблицы, диаграммах ▪ возможность сохранения отчетов в шаблоны для дальнейшего повторного использования ▪ объединение ресурсов в категории по произвольному признаку с возможностью дальнейшего использования категории как инструмента фильтрации статистики
Регистрация действий пользователей с указанием	▪ даты и времени операции ▪ имени пользователя ▪ действия, выполненного пользователем ▪ результата действия, значение изменяемого параметра до и после внесения изменений
Управление правами пользователей	▪ управление доступом ко всем разделам WEB-интерфейса системы с возможностью разделения полномочий просмотра и полномочий изменения параметров ▪ управление доступом к подразделениям и юридическим лицам с возможностью указания данных подразделений как критериев при просмотре статистических отчетов
Дополнительно	▪ внешние интеллектуальные модули Bypass, отслеживающие состояние комплекса и отключающие подачу трафика на платформу в случае деградации обслуживания ▪ работа в архитектурах с асимметричным прохождением трафика без снижения качества классификации и с сохранением всех функциональных возможностей ▪ интеграция с системами мониторинга по протоколу SNMP с возможностью генерации трапов по авариям, включая аварии программного обеспечения и аппаратных компонент ▪ отведение трафика на внешние устройства последовательно через физические внешние порты или по L3 через единый внешний порт, подключенный к коммутатору ▪ обновление списков сигнатур не реже одного раза в месяц ▪ масштабирование с сохранением единого интерфейса управления и просмотра статистики на сети с географически разнесенными точками включения с произвольным количеством каналов и объемом трафика. Разовое обновление единой конфигурации на географически разнесенных точках обработки трафика
Интеграция с внешними системами	▪ RFC 2865, 2866, 5176 (RADIUS, RADIUS Accounting, RADIUS CoA) ▪ DHCP ▪ SNMP trap, (s)FTP, SSH ▪ CDR (IPDR): CSV, .xls ▪ SQL, HTTP Provisioning API ▪ Внешняя обработка трафика на T_Proxy