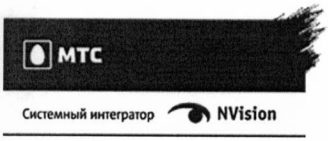
Приложение



Требования по составу и содержанию технических средств для СПО «Барьер» (СОД «Барьер»)

Москва 2017

Акционерное общество «Энвижн Груп»
ул. Новослободская, д. 29 строение 2, Москва, Россия, 127055. Тел. +7 (495) 641-12-12, факс +7 (495) 641-12-11, www.nvg.ru

Оглавление

1. Термины и сокращения

Термин/сокращение	Описание
URL	Адрес Интернет-сайта состоящий из доменного имени и символов, определенных владельцем сайта в сети Интернет
Абонент	Физическое или юридическое лицо, которому Заказчик предоставляет услуги доступа к Интернет
Абонентский трафик	Трафик, направленный от абонента на ресурс
Авторизация	Предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий
Аутентификация	Процедура проверки подлинности, например: проверка подлинности пользователя путём сравнения введённого им пароля с паролем в базе данных пользователей
Веб-трафик	Трафик, передаваемый по протоколу http
ЕАИС Реестр	Единая автоматизированная информационная система «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»
ИС	Информационная система. В контексте ТЗ: под ИС МТС подразумеваются системы, используемые в ОАО МТС, которые имеют возможность передавать информацию о ресурсах в СОД
Ресурс	Сайт целиком, либо отдельные страницы сайта. – Запрещенный ресурс – ресурс, доступ к которому запрещен Системой. – Разрешенный ресурс – ресурс, доступ к которому не запрещен Системой. – Вирусный ресурс – ресурс с подозрением на вирусы. – Сомнительный ресурс – ресурс, IP адрес которого совпадает с IP-адресом запрещенного или вирусного ресурса, хотя доступ к этому ресурсу может и не быть запрещен
РКН	Роскомнадзор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

РФ	Российская Федерация
Страница редиректа	URL, на который выполняется перенаправление абонента в момент блокировки доступа к ресурсу
Трафик	Объём информации, передаваемой через компьютерную сеть за определенный период времени
СОД	Система ограничения доступа
ПО	Программное обеспечение (как разрабатываемое в рамках текущего проекта, так и стороннее)
Модуль управления	Центральный модуль, обеспечивающий взаимодействие с оператором Системы, управление жизненным циклом ресурсов (от получения до блокировки), резолвинг IP адресов из DNS, провижининг ресурсов на сетевом оборудовании.
Модуль фильтрации	Модуль распределенной системы ограничения доступа, выполняющий непосредственную обработку трафика на сети оператора.
Модуль мониторинга	Модуль распределенной системы контроля качества фильтрации.

2. Назначение решения

Система ограничения доступа «Барьер» (далее - СОД «Барьер», Система) предназначена для обеспечения выполнения требований федерального законодательства РФ в области ограничения и запрещения распространения определенной информации посредством информационно-телекоммуникационных сетей.

СОД «Барьер» является программно-аппаратным решением.

Основной задачей СОД «Барьер» является ограничение доступа абонентов фиксированной и подвижной связи к интернет-сайтам, содержащим информацию, распространение которой в Российской Федерации запрещено в соответствии с требованиями федерального законодательства РФ. Дополнительно, система позволяет фильтровать доступ к вирусным ресурсам, информация о которых может быть получена из других внутренних систем оператора связи.

3. Список операторов связи, у которых внедрено решение

Публичное Акционерное общество «Мобильные ТелеСистемы» (ПАО «МТС»)

ИНН 7740000076

Дата установки – 12.03.2013 г.

Место установки – г. Москва

Модули мониторинга платформы мониторинга развернуты в городах: Москва, Ижевск, Сахалин, Петропавск-Камчатский

4. Типы поддерживаемых (обслуживаемых) ресурсов

При функционировании система работает со следующими типами ресурсов:

Разрешённые ресурсы: ресурсы, не содержащие информацию, распространение которой запрещено на территории РФ. Система не участвует в процессе обмена трафиком с данными ресурсами.

Запрещённые ресурсы: ресурсы, содержащие информацию, распространение которой запрещено на территории РФ.

Сомнительные ресурсы: разрешенные ресурсы, которые делят один IP-адрес с запрещёнными.

Вирусные ресурсы: ресурсы, доступ к которым возможен, но пользователь должен быть дополнительно оповещен об опасности.

5. Функциональные возможности решения

Система обеспечивает выполнение следующих задач:

- Предотвращение доступа пользователей сети к запрещенным ресурсам;
- Возможность направления нужного трафика на платформу фильтрации;
- Перенаправление на страницу «заглушку» или страницу подтверждения с последующим доступом на запрашиваемый ресурс;
- Возможность работы, как в разрыв, так и на копии трафика;
- Автоматическая актуализация перечня запрещенных ресурсов из Единого реестра доменных имен и сетевых адресов, запрещённых к распространению;
- Предоставление интерфейса для ручного управления блокируемыми ресурсами;
- Сбор статистики и формирование отчетов о работе системы;
- Логирование действий пользователей в системе.

6. Схема обмена трафиком между абонентами и ресурсами

На рисунке ниже приведена схема, описывающая прохождения абонентского трафика в процессе обмена информацией между абонентами и ресурсами.

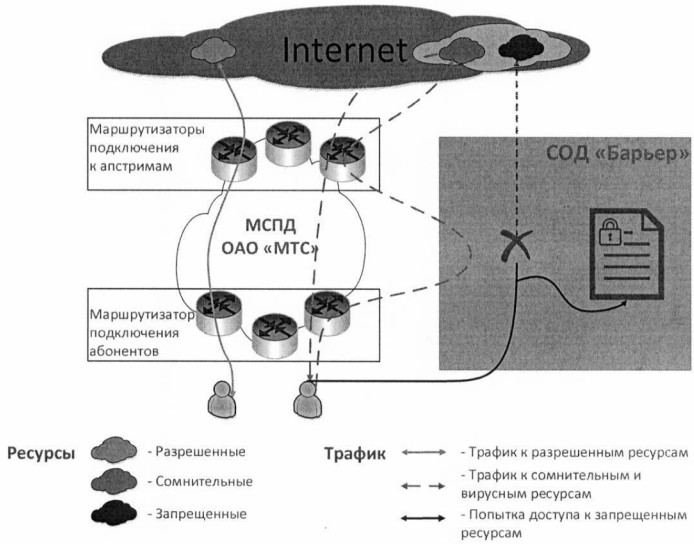


Рис. 1. Логическая схема передачи и обработки абонентского трафика с участием СОД «Барьер»

В зависимости от типа ресурса обработка выполняется следующим образом:

- Доступ к разрешенным ресурсам предоставляется в полном объеме. Система не участвует в процессе обмена трафиком с данными ресурсами;
- При попытке доступа к ресурсам, которые делят один IP-адрес с запрещенными (сомнительные), выполняется проверка, что ресурс является разрешенным после чего система допускает абонента к нему;
- При попытке доступа к вирусным ресурсам, система предупреждает пользователя об опасности, и после его согласия пропускает трафик к ресурсу на определенный период.

Требования к программно-техническому комплексу для внедрения решения

Компонент	Минимальные характеристики
АРМ администратора	– 2Gb RAM; – 2Ghz CPU; – минимальное разрешение экрана 1280x1024. Операционная система: – Windows 7, 8, 10 и выше. Прикладное ПО: – WEB-браузер Browser Internet Explorer версии 11 и выше или аналоги (Mozilla Firefox, Google Chrome и т. д.). Доступы: – Учетная запись «суперадминистратора» системы (для WEBинтерфейса). – Сетевой доступ к серверам системы. – Учетные записи с правами администратора на серверах системы (модули управления, мониторинга и фильтрации).
Сервера платформы управления	CPU: 6 x Xeon E5-2640 6C 2.5 GHz; RAM, 128 Gb; HDD, Gb 64 (ОС)+ 64 (прикладное ПО) + 2048 (только для БД)+512(архивные лог-файлы); OS: OS Linux (RHEL 7 или Oracle Linux 7); БД (устанавливается только на одном из серверов): Oracle Database 12g
Сервера платформы мониторинга	CPU: не менее 1GHz; RAM: не менее 1Gb; HDD: не менее 10Gb; OS: Ubuntu
Сервера платформы фильтрации	До 1Gb/s: X86 совместимый сервер, Intel Xeon E5-2640 6 core 12 thread, Адаптер: 4 порта 1Gb любой поддерживаемый ОС Ubuntu Linux 14, Mem: 60Gb До 10Gb/s: X86 совместимый сервер, Intel Xeon X5650 2 socket 12 core 24 thread, Адаптер: 1 порт 1Gb любой поддерживаемый ОС Ubuntu Linux 14 2 потра 10Gb SFP+ (чипсет 82599), Mem: 60Gb

7. Масштабируемость решения

Увеличение производительности системы достигается следующими решениями:

- Увеличение производительности модуля управления выполняется путем вертикального масштабирования: увеличением характеристик серверов модуля.
- Увеличение производительности модуля фильтрации осуществляется либо увеличением характеристик серверов, либо их количества с установкой балансировщика.

8. Типовые схемы внедрения решения

Схема внедрения решения «В разрыв»

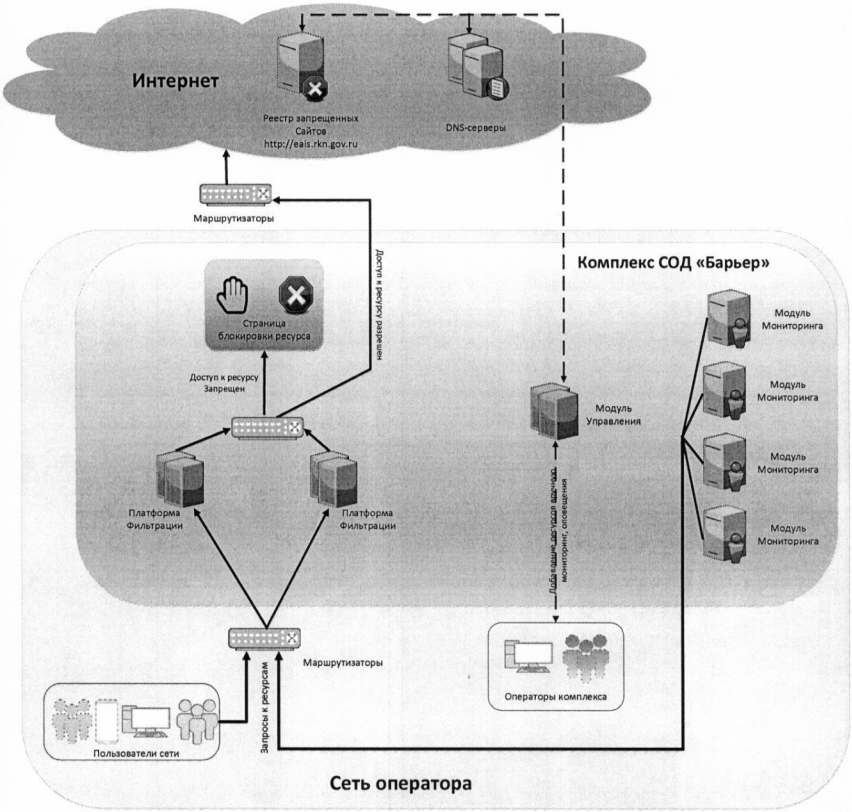
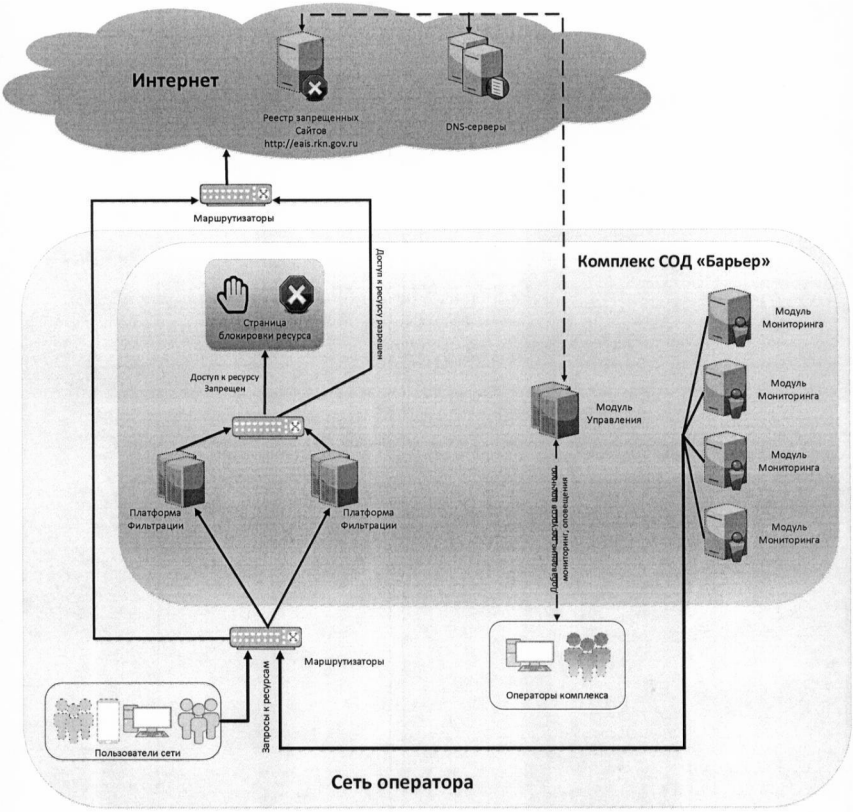


Схема внедрения решения «На зеркале»



9. Требования к пропускной способности канала

В зависимости от версии 1Gb/s или 10 Gb/s

10. Требования к каналам (по потере пакетов)

Система не предъявляет специфичных требований к потерям пакетов на сети оператора.

11. Другие обязательные требования

Доступ с платформы управления на платформу фильтрации по порту 22.

Доступ с платформы управления к ресурсам РКН.

Доступ с платформы управления к одному или нескольким DNS серверам.