



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 23 НОЯ 2017 № 0410-103842

На № _____ от _____

ООО «СкайДНС»

Кулибина, д. 2, офис 502,
г. Екатеринбург, 620137

lubov@skydns.ru

Заключение

Роскомнадзором в период с 16.10.2017 по 13.11.2017 проведено тестирование специализированного программного обеспечения «SkyDNS Zapret ISP» (далее – СПО «SkyDNS Zapret ISP»), 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 «СкайДНС».

Целью тестирования СПО «SkyDNS Zapret ISP» являлось определение качества ограничения доступа к запрещенным ресурсам, внесенным в Единый реестр.

Участие в тестировании приняло 16 операторов связи из 7 федеральных округов Российской Федерации, с различной численностью абонентов.

СПО «SkyDNS Zapret ISP» может быть установлено на сети оператора по типовым схемам подключения рекомендуемыми производителем в соответствии с приложением. Тестирование СПО «SkyDNS Zapret ISP» на сетях операторов связи проводилось по 2 схемам:

1. По схеме с использованием динамической маршрутизации с внутренним и пограничным маршрутизатором, когда через СПО «SkyDNS Zapret ISP» проходит только исходящий трафик, который идет на сетевые адреса запрещенных ресурсов, при этом остальной трафик не меняет маршрут следования. Данная схема установки рекомендована

производителем и была выбрана в качестве основной для проведения тестирования.

2. По схеме «в разрыв», когда весь трафик оператора связи проходит через СПО «SkyDNS Zapret ISP». По данному типу подключения тестировался 1 оператор связи.

Тестирование СПО «SkyDNS Zapret ISP» 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 «SkyDNS Zapret ISP» на сетях 37% операторов связи не выявлены нарушения по Единому реестру и группе реестра «398-ФЗ».

На сетях 63% операторов связи, периодически выявлялись нарушения, в количестве не превышающем 0,22% по Единому реестру и не более 0,67% группы реестра «398-ФЗ».

2. На сетях 7 операторов связи в ходе тестирования систематически наблюдалась излишняя фильтрация, приводящая к ограничению доступа к ресурсам отсутствующим в выгрузке Единого Реестра. В том числе наблюдались случаи ограничения доступа к социально значимым ресурсам. За период тестирования указанная проблема была устранена у 6 операторов связи. У 1 оператора связи излишняя фильтрация наблюдалась в течение всего периода тестирования.

3. У ряда операторов связи возникали сложности на этапе установки и настройки СПО «SkyDNS Zapret ISP» по причине недостаточности информации в предоставляемой разработчиком документации.

4. Процедура развертывания и настройки СПО «SkyDNS Zapret ISP» на сети оператора связи, включая решение организационных и технических проблем, занимает от 1 до 3 недель.

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

Вывод

Анализ результатов проведенного тестирования СПО «SkyDNS Zapret ISP», разработанного ООО «СкайдНС», показывает что при установке по

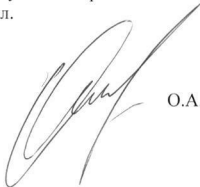
рекомендованной производителем схеме подключения и правильной настройке сети оператора связи количество выявленных нарушений по Единому реестру не превышают 0,22%, по группе реестра «398-ФЗ» не превышают 0,67%.

СПО «SkyDNS Zapret ISP» 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.

ООО «СкайдНС» рекомендуется оптимизировать СПО «SkyDNS Zapret ISP» с целью повышения качества ограничения доступа к ресурсам в сети «Интернет», включенным в Единый реестр, и распространение которых в Российской Федерации запрещено, а также с целью исключения случаев избыточной блокировки.

Приложение: Требования по составу и содержанию технических средств для СПО «SkyDNS Zapret ISP», на 6 л.

Заместитель руководителя



О.А. Иванов

Технические требования SkyDNS Zapret ISP.

1. Системные требования SkyDNS Zapret ISP

1.1. Минимальные требования к серверу

- ОС Debian 8 64-bit
- 8 GB RAM
- 1,6 GHz 4xCPU
- 100 GB свободного места на диске. (В основном под логи)

1.2. Показатели производительности

При тестировании на производительность рассматривался сценарий попадания в реестр URL с популярного сайта, и были получены такие результаты:

- Quad Core Xeon E5606 2,13 GHz
- 8 GB RAM
- обратный трафик в ответ на запросы на порт 80/tcp на IP-адреса запрещенных ресурсов: достигнутая пропускная способность – 1 Гбит/с
- загрузка CPU 50-70%
- load average 2

по субъективной оценке задержек в выдаче страницы блокировки или загрузке страниц с URL, содержащих в адресе тот же домен что и запрещенные ресурсы, не наблюдалось.

Требуемая мощность сервера зависит от потребляемой вашими пользователями ширины канала и популярности у них тех или иных ресурсов. Через систему фильтрации обычно проходит от 0,01% до 0,05% от используемой ширины канала. Для 10 Гбит/с используемой ширины канала подойдет однопроцессорный сервер начального уровня с одним или двумя (зависит от схемы внедрения) сетевыми

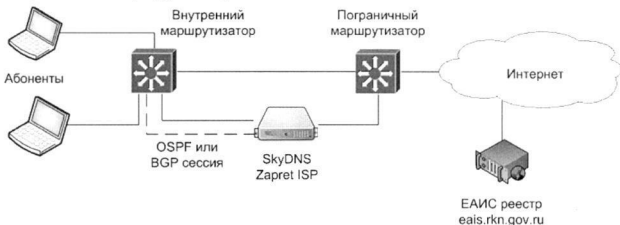
интерфейсами 1 Гбит/с с не сильно старым CPU Xeon с частотой больше 3 GHz. Количество ядер CPU от 8. Или сервер с аналогичным по производительности CPU AMD. Памяти примерно 12-16 Гбайт.

2. Схема работы SkyDNS Zapret ISP

SkyDNS Zapret ISP в автоматическом режиме скачивает реестр запрещенных ресурсов с eais.rkn.gov.ru. Так же SkyDNS Zapret ISP скачивает список URL, подготовленный SkyDNS, на основе списка экстремистских материалов Минюста. SkyDNS Zapret ISP постоянно в цикле разрешает домены запрещенных ресурсов в IP-адреса в асинхронном режиме. Затем SkyDNS Zapret ISP осуществляет перенаправление на систему фильтрации исходящего от абонентов трафика, который идет на IP-адреса запрещенных ресурсов. При этом остальной трафик не меняет маршрут следования. (см. Раздел 3 Схемы подключения SkyDNS Zapret ISP в сеть) Из перенаправленного исходящего трафика в систему фильтрации по URL перенаправляется трафик, который идет на порт 80/tcp. Трафик, который идет на порт 443/tcp на IP-адреса, в которые разрешились домены запрещенных ресурсов HTTPS, отклоняется. Остальной трафик пропускается без изменений. Ответы на пропущенный без изменений трафик идут через сеть напрямую к клиентам (осуществляется асимметричная маршрутизация). Перенаправленный на систему фильтрации по URL трафик (запросы на порт 80/tcp на IP-адреса запрещенных ресурсов) обрабатывается системой фильтрации по URL, которая работает в режиме прозрачного прокси-сервера. Разрешенные запросы пропускаются. На запросы к запрещенному URL, в ответ выдается страница блокировки. Также система фильтрации по URL выдает страницу блокировки при обращении к любому ресурсу по IP-адресу.

3. Схемы подключения SkyDNS Zapret ISP в сеть

3.1. Схема с использованием динамической маршрутизацией с внутренним и пограничным маршрутизатором



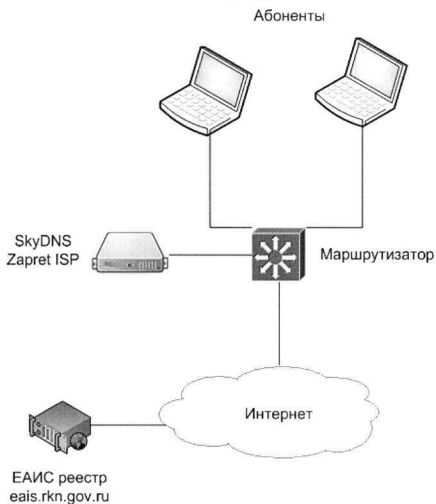
SkyDNS Zapret ISP использует eخابgr для установки и удаления маршрутов при использовании схемы с динамической маршрутизацией. Демон bgpd, входящий в Quagga получает маршруты от демона eخابgr по BGP. Оба запущены на loopback интерфейсе. Демон ospfd или bgpd, входящий в Quagga, устанавливает полученные маршруты во внутренний маршрутизатор. Внимание!!! Устанавливаемые SkyDNS Zapret ISP во внутренний маршрутизатор маршруты не должны попадать на пограничный маршрутизатор. Иначе фильтруемый трафик зациклится. Если пограничный маршрутизатор выполняет функции NAT, то убедитесь что для сервера фильтрации SkyDNS Zapret ISP на NAT отсутствует, например, ограничение на количество сессий или какие-либо другие ограничения, если такие ограничения используются в администрируемой сети. ерез систему фильтрации будет проходить трафик множества клиентов, поэтому к ней нельзя применять ограничения, которые применяются к одному клиенту.

3.2. Схема с использованием динамической маршрутизацией с одним маршрутизатором



При такой схеме можно настроить два VLAN. На vlan100 настроить OSPF или BGP, а через vlan200 настроить выход в интернет. На маршрутизаторе настроить PBR (Policy Based Routing), чтобы запросы из vlan200 не маршрутизировались во vlan100, а уходили в интернет.

3.3. Схема со статической маршрутизацией



В SkyDNS Zapret ISP есть возможность выгрузить список IP-адресов, в которые разрешаются домены запрещенных ресурсов. Для этого используется команда `zi-ctl routes` либо `zi-ctl routes --ipv6`. Вы можете написать свой скрипт загрузки маршрутов на роутер и добавить правило в `snop`. Примеры скриптов находятся в директории `/usr/share/skydns-zi/examples/`

3.4. Использование какой-либо другой схемы

Вы можете использовать какую-либо другую схему включения SkyDNS Zapret ISP в свою сеть. Целью является маршрутизация трафика к IP-адресам запрещенных ресурсов на сервер SkyDNS Zapret ISP. Имеется:

1. Quagga с маршрутами, получаемыми по BGP от `exabgp`. Вы можете настроить маршрутизацию между Quagga и вашим маршрутизатором по любому протоколу поддерживаемому Quagga.
2. Команда для получения списка IP-адресов `zi-ctl routes` и свой скрипт

3.5. Использование фильтрующего DNS сервера

Также для перенаправления запросов на систему фильтрации, дополнительно можно использовать фильтрующий DNS сервер. Такой подход гарантирует 100% перенаправление запросов, т.к нет необходимости зависеть от постоянно меняющихся IP адресов фильтруемых ресурсов. Вы можете отдавать адрес фильтрующего DNS по DHCP, либо указать его в качестве вышестоящего на имеющихся у вас DNS серверах, но нужно учитывать что пользователи могут легко изменить используемый DNS, поэтому полностью отказываться от ранее описанных схем нельзя. Для настройки следуйте инструкции Настройка фильтрующего DNS сервера

3.5.1 Настройка фильтрующего DNS сервера

Для начала обязательно нужно назначить серверу отдельный IP адрес, который будет использоваться в качестве адреса DNS сервера и адреса, куда будут перенаправляться запросы пользователей. Это также означает что данный адрес должен быть доступен из всех подсетей. При необходимости можно создать виртуальный интерфейс.

Добавить в конфиг файл /etc/skydns-zi/config.yml следующие строки:

```
dns-filter:
```

```
  address: <YOUR_DNS_ADDRESS>
```

```
  ttl: 60 # время на которое кешировать ответы (не обязательно)
```

Далее запустить команды

```
# создать необходимые ipset'ы
```

```
zi-ctl ipset-save
```

```
# добавить DNS сервер в автозапуск
```

```
systemctl enable skydns-unbound
```

```
# перезапустить сервис
```

```
service skydns-unbound restart
```

Проверить корректность работы сервиса, выполнив следующую команду:

```
# На сервере
```

```
dig @127.0.0.2 <SOME_BLOCKED_DOMAIN>
```

```
# На клиенте
```



```
dig @<YOUR_DNS_ADDRESS> <SOME_BLOCKED_DOMAIN>
```

В ответе должен присутствовать IP адрес, указанный в конфиге

3.6. Google Global Cache (GGC)

Если у вас установлена одна или несколько нод GGC, убедитесь, что IP-адрес, с которого SkyDNS Zapret ISP осуществляет запросы к серверам в интернет входит в адресное пространство, для которого настроено использование GGC.

4. Отказоустойчивость и масштабирование

При реализации схемы с динамической маршрутизацией в случае выхода из строя сервера SkyDNS Zapret ISP перенаправление исходящего трафика на систему фильтрации осуществляться не будет, таким образом, не пострадает основной сервис сети – предоставление доступа абонентам в сеть Интернет. Для масштабирования решения возможна установка в сеть дополнительного сервера SkyDNS Zapret ISP с установкой в OSPF маршрутов с той же стоимостью маршрута (Equal-cost multi-path routing - ECMP). В случае установки в сеть нескольких серверов SkyDNS Zapret ISP обеспечивается отказоустойчивость сервиса. В настоящее время единый центр управления серверами отсутствует, и управление дополнительным сервером осуществляется отдельно.

5. Требования к каналам по потере пакетов

Требования к каналам по потере пакетов отсутствуют. Не актуально для эффективной работы SkyDNS Zapret ISP.