Документация, 19.08.2019

http://www.zapretservice.ru/

Введение
Программный комплекс ZapretService предназначен для взаимодействия с интернет-порталом http://vigruzki.rkn.gov.ru/, чтобы обеспечить помощь в web-фильтрации по реестру запрещенных сайтов, требуемую федеральными законами 139-ФЗ, 149-ФЗ и 187-ФЗ действующего российского законодательства. Данный программный комплекс состоит из дистрибутива операционной системы Debian GNU/Linux и специального ПО, которые устанавливаются на отдельный «железный» сервер или виртуальную среду.

В качестве виртуальной среды рекомендуем использовать VMWare (vSphere Hypervisor). Так же есть возможность использование и других гипервизоров, т.к. среди наших клиентов успешно применяют VirtualBox, QEMU и Proxmox.

Важно! Обращаем Ваше внимание, что последние являются OpenSource и используются на «промышленных» серверах в компаниях реже, что не гарантирует их отказоустойчивость, как VMWare.

Требования к конфигурации сервера
Минимальная:
- Процессор: количество логических ядер – 2, линейка Intel Core I
- Оперативная память: 4 Гб ОЗУ
- Жесткий диск: 10 Гб, 7200rpm
- Сетевая карта: 1x1 Гбит/с (с применением технологии vlan)

Пропускная способность при данной конфигурации: < 5 Kpps *

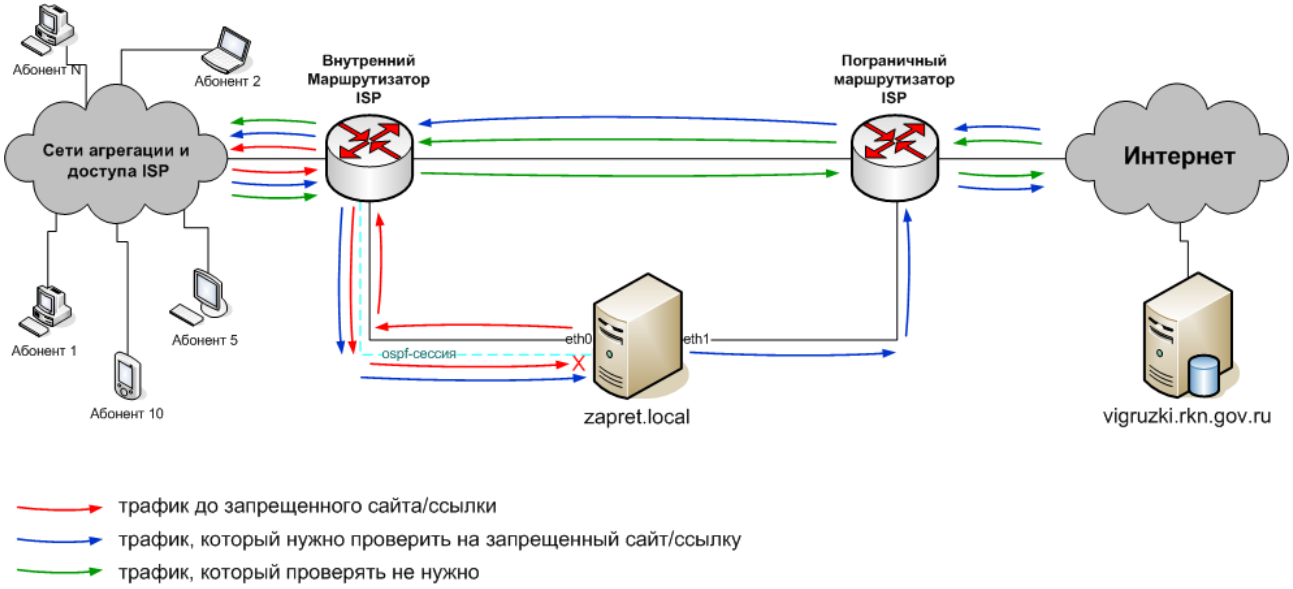
Рекомендуемая:
- Процессор: количество логических ядер – 8, линейка Xeon
- Оперативная память: 8 Гб ОЗУ
- Жесткий диск: 10 Гб, 7200rpm или SSD
- Сетевая карта: 2x1 Гбит/с (по одной на вход и выход)

Пропускная способность при данной конфигурации: > 10 Kpps *

* Данные были получены при тестировании программного комплекса в «лабораторных условиях». В реальных условиях эти данные могут отличаться. Для получения более высокой пропускной способности, возможно, потребуется подбор центрального процессора или специальных сетевых карт.

Важно! Объем оперативной памяти на сервере не должен превышать размера жесткого диска, иначе автоматическая установка программного комплекса ZapretService не сможет правильно рассчитать размер swap-раздела.

Схемы использования
Стандартная схема внедрения программного комплекса ZapretService подразумевает использование в Вашей сети двух маршрутизаторов, на каждом из которых выделяется по одному порту в сторону сервера с ZapretService.

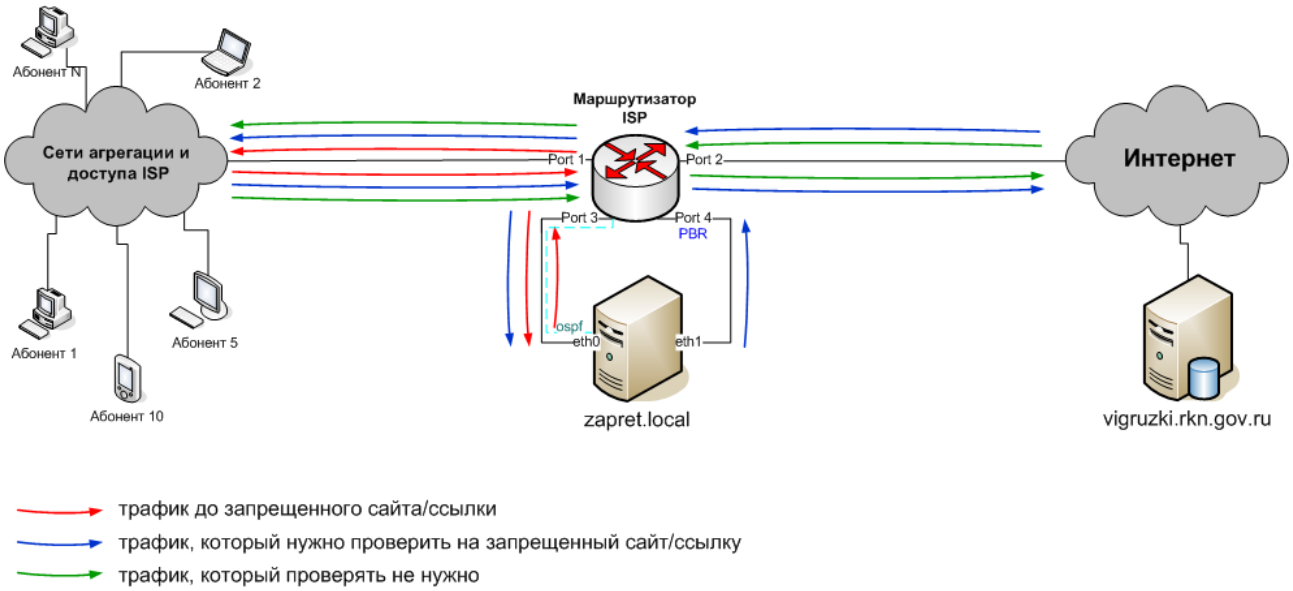


При такой схеме возможно модульное расширение, т.е. использование более одного сервера с ZapretService. Ip-адресам, анонсированные с этих серверов по протоколу OSPF, будут устанавливаться маршруты с равнозначными характеристиками, что позволит равномерно распределить трафик между серверами.

Важно! Исходящий трафик от внутреннего маршрутизатора на сервер должен поступать на первую сетевую карту (eth0), а исходящий с сервера на пограничный маршрутизатор - на вторую (eth1).

Важно! Если на сервере используется только одна сетевая карта, то можно воспользоваться технологией vlan. Для этого обратитесь в специальный раздел документации.

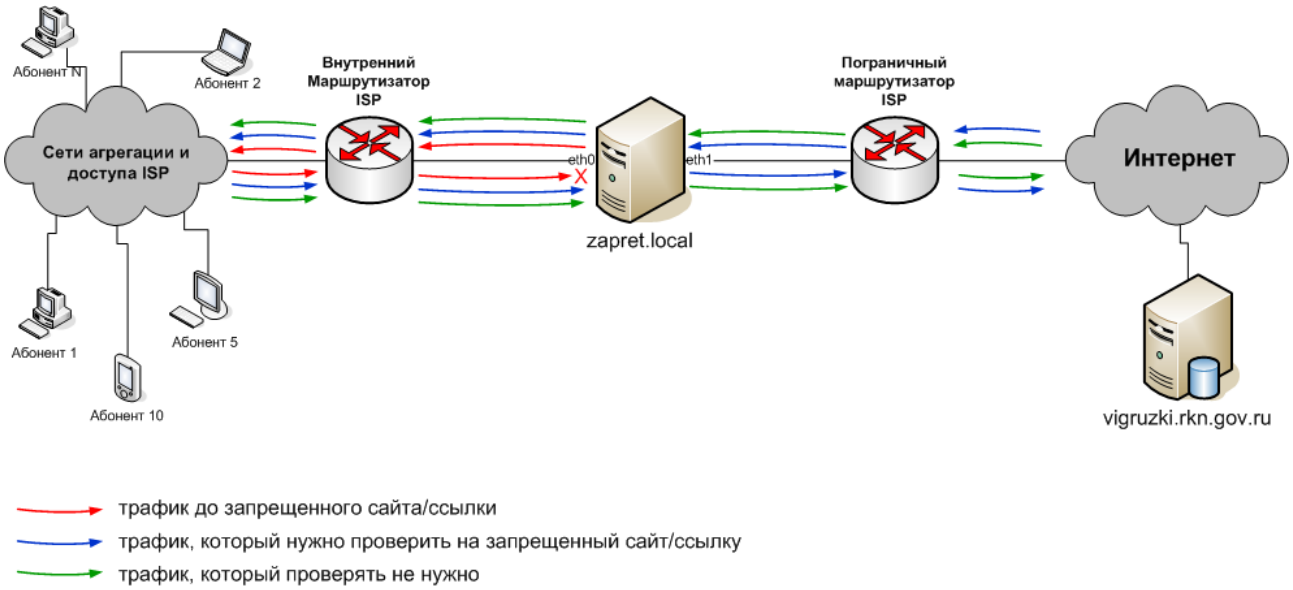
Если же в Вашей сети присутствует только один маршрутизатор (например, маршрутизатор Cisco), то возможно использование схемы с применением технологии Policy-Based Routing (PBR). Для её описания и настройки обратитесь в специальный раздел документации.



Важно! Если на маршрутизаторе используется BGP с внешними операторами, то при использовании данной схемы может возникнуть проблема с обработкой подсетей от сервера с ZapretService, а именно анонсы от внешних операторов могут быть меньше по маске или

быть более приоритетными, что приведет отправку трафика до данных подсетей не через ZapreService. В случае с запрещенными подсетями с реестра запрещенных сайтов необходимо данные подсети блокировать на самом маршрутизаторе. Это можно сделать с помощью какого-нибудь автоматического скрипта, который (используя информацию от команды «sudo ipset list block-net» у сервера с ZapretService) будет загружать, например, на CISCO в специальный access-list.

При правильно подобранной конфигурации сервера и малом интернет-трафике возможно использование упрощенной схемы, но модульное расширение будет невозможно.



Алгоритм работы

- на сервер загружается[1] реестр запрещенных сайтов от Роскомнадзора с web-сервиса интернет-портала http://vigruzki.rkn.gov.ru/;
- ZapretService путем dns-запросов вычисляет ip-адреса серверов, где располагаются запрещенные url-адреса/сайты, а так же использует ip-адреса из самого реестра;
- список вычисленных ip-адресов анонсируются на внутренний маршрутизатор по протоколу OSPF/BGP, устанавливая адрес сервера с ZapretService в качестве наилучшего маршрута;
- модуль ZapretService сравнивает url-адреса из http/https-пакетов[2] перенаправленного интернет-трафика с url-адресами из реестра;
- при совпадении url-адреса происходит перенаправление на информационную страницу сервера, а остальной трафик отправляется на пограничный маршрутизатор[3];
- обратный трафик из Интернет до абонента доходит по прямому маршруту[4].

[1] Выгрузка реестра запрещенных сайтов осуществляется не менее 2-х раз в сутки. По рекомендациям Роскомнадзора в ZapretService реализован модуль «check», который раз в 5 минут проверяет временную метку срочности на портале выгрузок. При её изменении в последующие 5 минут производится новая выгрузка реестра.
[2] В случае с HTTP производится сравнение по url-ссылке или домену, с HTTPS по sni-информации запрашиваемого домена.
[3] Информационная страница уведомляет пользователя о блокировке запрашиваемой url-страницы. Если в списках реестра запрещенных сайтов значится блокировка ресурса по ip-адресу, то пользователя так же перенаправляет на соответствующую информационную страницу. Обращаем Ваше внимание, что отображение страницы-заглушки возможно только при протоколе HTTP, при HTTPS производится сброс SSL-соединения.

[4] В отличии от 4 ветки теперь ZapretService не производит подмену адреса источника и обратный трафик из сети Интернет уже будет поступать на прямую к получателю, минуя сервер ZS.

Программный комплекс ZapretService тестировался на одном из крупных операторов связи, где данный способ не влиял на работу соц. сетей и онлайн-игр.

Установка iso-образа на сервер
Iso-образ может быть записан на CD-, DVD- или USB-носитель. При установки программного комплекса наличие доступа к сети Интернет на сервере не требуется. После загрузки с образа установщик самостоятельно попытается получить сетевые настройки по протоколу DHCP. Иначе будет предложено настроить сетевую карту самостоятельно. Если на сервере имеется несколько сетевых карт, то настройки будут производиться на первую. В следующем этапе необходимо будет выбрать часовой пояс. В дальнейшем установка происходит полностью в автоматическом режиме. Установщик сам разметит по своему усмотрению жесткий диск на сервере и установит все необходимое ПО. По окончанию установки сервер автоматически будет перезапущен.

Для ssh-входа на сервер используются следующие реквизиты:

- логин zapret
- пароль access

Для выполнения необходимых операций, требующих привилегии суперпользователя «root», используйте команду «sudo». Для изменения конфигурационных файлов можно воспользоваться редакторами «vi» или «mcedit».

Важно! После ssh-входа настоятельно рекомендуем поменять пароль для пользователя «zapret» с помощью команды «sudo passwd zapret».

Важно! Web-интерфейс ZapretService использует такие же реквизиты доступа, как и на сервис ssh. Доступ в web-интерфейс ZapretService в целях безопасности осуществляется **ТОЛЬКО** через url-ссылку http://zapret.local/manager/ (в конце обязательно должен быть знак «слеш»). Убедительная просьба не менять конфигурацию сервиса «apache», т.к. это может привести к «поломке» какого-либо функционала ZapretService.

Важно! Изменение конфигурационных файлов требует привилегии суперпользователя, т.е. чтобы отредактировать файл «/etc/hosts» нужно воспользоваться командой «sudo vi /etc/hosts» или «sudo mcedit /etc/hosts».

Важно! В целях безопасности правила сервиса «iptables» блокируют ssh-доступ с интерфейса «eth1». Если Вам все таки необходим ssh-доступ из вне, то рекомендуем Вам не менять действующие правила сервиса «iptables», а добавить разрешающие с определёнными ip-адресами.

Конфигурация интерфейсов сервера
Настройки интерфейсов сервера производятся в файле /etc/network/interfaces.

Пример конфигурации:

```
source /etc/network/interfaces.d/*

auto lo
```

```
iface lo inet loopback

auto eth0
iface eth0 inet static
    address 192.168.103.2
    netmask 255.255.255.0
    dns-nameservers 192.168.54.1 192.168.55.1
    dns-search local

auto eth1
iface eth1 inet static
    address 219.14.2.8
    netmask 255.255.255.240
    gateway 219.14.2.1
```

Для применения интерфейсам сервера новой конфигурации воспользуетесь командой «sudo /etc/init.d/networking restart».

Важно! Основной шлюз должен быть прописан у интерфейса «eth1» опцией «gateway», т.к. ZapretService создает в таблице маршрутизации маршруты до вычисленных ip-адресов с этим шлюзом. Данные маршруты экспортируются по протоколу OSPF на внутренний маршрутизатор. Для создания необходимых маршрутов на интерфейсе «eth0» в данном файле лучше воспользуетесь опцией «up route add».

Важно! Если была изменена опция dns-nameservers, то необходимо эти изменения внести в файл «/etc/resolv.conf».

Важно! Если в Вашей сети используется NAT, то необходимо отправлять трафик на сервер с ZapretService уже прошедший через него, т.к. «серый» трафик будет фильтроваться дальше вышестоящим аплинком (ZapretService не производит самостоятельно подмену адресации на «белую»).

Важно! Для равномерной нагрузки интерфейсов сервера рекомендуем добавить в конфигурацию интерфейса «eth0» маршруты до Ваших сетей опцией «up route add», чтобы обработанный трафик смог пройти обратно через тот же интерфейс.

Конфигурация сетевых карт с применением технологии vlan
В iso-образ уже включен пакет «vlan». Настройки логических подинтерфейсов так же производятся в файле /etc/network/interfaces.

Пример конфигурации:

```
source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback

auto eth0.11
iface eth0.11 inet static
    vlan_raw_device eth0
    address 192.168.103.2
    netmask 255.255.255.0
```

```
    dns-nameservers 192.168.54.1 192.168.55.1
    dns-search local

auto eth0.12
iface eth0.12 inet static
    vlan_raw_device eth0
    address 219.14.2.8
    netmask 255.255.255.240
    gateway 219.14.2.1
```

Для применения интерфейсу сервера новой конфигурации воспользуетесь командой «sudo /etc/init.d/networking restart».

Важно! В данном примере интерфейс, принимающий трафик от внутреннего маршрутизатора стал «eth0.11», а интерфейс, отправляющий трафик на пограничный маршрутизатор – «eth0.12». Необходимо отредактировать файл /etc/iptables/rules.v4, заменив «eth0» на «eth0.11», а «eth1» на «eth0.12». После изменений необходимо обновить правила сервиса «iptables» командой «sudo iptables-restore < /etc/iptables/rules.v4».

Конфигурация DNS

ZapretService использует домен «zapret.local» для перенаправления пользователя на информационную страницу при организации блокировки, а так же для работы своего web-интерфейса.

В DNS-сервисе, который используют абоненты, нужно создать этот домен, указав A-запись с ip-адресом интерфейса сервера, отправляющий трафик на пограничный маршрутизатор (стандартно – «eth1»).

Для сервиса «bind» в файле «named.conf» создается новая зона:

```
zone "zapret.local" {
        type master;
        file "/etc/namedb/master/zapret.local";
};
```

Пример файла /etc/namedb/master/zapret.local:

```
$TTL 3600
@               IN      SOA     ns.mydomain.ru. admin.mydomain.ru. (
                                        2015100314;
                                        3600;
                                        900;
                                        360000;
                                        3600;
                                )
@               IN      NS      ns.mydomain.ru.
@               IN      A       219.14.2.8
```

где 2015100314 – серийный номер зоны (обычно указывается дата до часа), 219.14.2.8 – ip-адрес интерфейса «eth1», а «mydomain.ru» – Ваш домен.

Важно! После добавления записи в DNS-сервис, на сервере с ZapretService необходимо отредактировать файл «/etc/hosts», сопоставив запись «zapret.local» с правильным ip-адресом.

После изменений необходимо перезапустить сервис «zsmon» командой «sudo /etc/init.d/zsmon restart».

Включение протокола OSPF
Важно! Для стабильной связки ZapretService с маршрутизатором рекомендуется использовать протокол «BGP» (следующий раздел). Данный раздел оставлен исключительно для случаев, когда нет возможности использовать данный протокол.

ZapretService для организации OSPF-сессии с внутренним маршрутизатором используется программный пакет «quagga», после загрузки сервера он автоматически запускается. Интерфейс его конфигурации аналогичен с интерфейсом маршрутизатора CISCO.

1. На сервере в командной строке введите команду «telnet localhost ospfd»
2. В качестве пароля введите «access»
3. Повысьте привилегии с помощью команды «enable»
4. Для входа в режим конфигурации введите команду «conf terminal»
5. Войдите в секцию «router ospf» с помощью команды «router ospf»
6. Введите команду «network x.x.x.x/y area 0.0.0.1», где x.x.x.x/y - подсеть/маска интерфейса (eth0), который принимает интернет-трафик от внутреннего маршрутизатора
7. Выйдите из режима конфигурации (нужно ввести 2 раза команду «exit»)
8. Сохраните конфигурацию командой «write mem»
9. Выйдите из режима telnet командой «exit»

После конфигурации «quagga» нужно активировать протокол OSPF на внутреннем маршрутизаторе. Для маршрутизатора CISCO:

1. Подключитесь по telnet к маршрутизатору и зайдите в режим конфигурации
2. Создайте секцию «router ospf 1», если на маршрутизаторе нет других процессов протокола OSPF
3. Задайте принадлежность LSA для маршрутизатора командой «router-id ipaddr», где ipaddr – ip-адрес интерфейса маршрутизатора, который находится в одной подсети с ZapretService
4. Выйдите в корневую секцию командой «exit»
4. Зайдите в секцию этого интерфейса на маршрутизаторе
5. Установите параметр network командой «ip ospf network non-broadcast»
6. Установите параметр dead-interval командой «ip ospf dead-interval 15»
7. Установите параметр hello-interval командой «ip ospf hello-interval 5»
8. Установите параметр priority командой «ip ospf priority 0»
9. Установите параметр retransmit-interval командой «ip ospf retransmit-interval 6»
10. Установите параметр transmit-delay командой «ip ospf transmit-delay 2»
11. Включите протокола «OSPF» на интерфейсе командой «ip ospf 1 area 1»
12. Выйдите из режима конфигурации
13. Убедитесь, что OSPF-сессия установилась с помощью команды «show ip ospf neighbor»
14. Сохраните конфигурацию командой «write mem»

При использовании маршрутизатора от другого вендора необходимо обратиться к его документации.

Использование протокола BGP
Некоторые маршрутизаторы (например, от производителя Mikrotik) плохо обрабатывают большое количество маршрутов (проблемы были замечены от 200-300 тыс. маршрутов), передаваемые по протоколу «OSPF». Вместо него можно использовать протокол «BGP». Пакет «quagga», входящий в программный комплекс ZapretService, его поддерживает.

1. На сервере в файле «/etc/quagga/daemons» установите значение параметра «bgpd» в «yes», а значение параметра «ospfd» в «no».
2. Создайте в каталоге «/etc/quagga» файл «bgpd.conf» со следующей конфигурацией:

```
!
hostname zapret
password access
log file /var/log/quagga/bgp.log
!
router bgp 65000
  bgp log-neighbor-changes
  bgp default local-preference 200
  redistribute kernel route-map bgp
  network y.y.y.y/z
  neighbor y.y.y.x remote-as 65000
  neighbor y.y.y.x next-hop-self
!
ip prefix-list bgp seq 97 deny y.y.y.w/32
ip prefix-list bgp seq 98 deny 224.0.0.0/24 le 32
ip prefix-list bgp seq 99 deny 0.0.0.0/0 le 8
ip prefix-list bgp seq 100 permit 0.0.0.0/0 le 32
!
route-map bgp permit 1
  match ip address prefix-list bgp
!
line vty
!
```

где y.y.y.y/z - подсеть/маска интерфейса (eth0), который принимает интернет-трафик от внутреннего маршрутизатора
где y.y.y.x – ip-адрес внутреннего маршрутизатора.
где y.y.y.w – ip-адрес интерфейса (eth0), который принимает интернет-трафик от внутреннего маршрутизатора (маска /32 обязательна)

Важно! На маршрутизаторах CISCO серии ASR было замечено неконтролируемое падение BGP-сессии, если в маршрутах сервера с ZapretService появлялся ip-адрес его интерфейса (eth0), например, из-за возможного его появления в резолвинге на каком-нибудь запрещенном домене. Возможно, данная проблема присутствует и на маршрутизаторах других вендоров, поэтому обязательно рекомендуем в «prefix-list» использовать правило №97.

Важно! Если на маршрутизаторе присутствуют другие neighbor, которые имеют свои анонсы, то необходимо маршрутам от сервера с ZapretService установить больший приоритет, чтобы они были приоритетными для проверяемого трафика. Сделать это можно через параметр «bgp default local-preference», добавив его в настройках сервиса «quagga» в секции «router bgp», после перезагрузить его командой «sudo /etc/init.d/quagga restart».
Так же рекомендуется «зафильтровать» на маршрутизаторе мелкие маршруты (менее /24) у всех neighbor (кроме ZapretService), если включена опция «Производить объединение ip-адресов в подсети» в web-интерфейсе ZapretService (раздел «Настройки»).

После конфигурации необходимо активировать протокол «BGP» на внутреннем маршрутизаторе.

Применение технологии Policy-Based Routing (PBR)
При использовании единственного маршрутизатора в сети необходимо дифференцировать на нем трафик, т.к. уходящий к серверу с ZapretService будет возвращаться обратно на маршрутизатор и по тем же самым маршрутам BGP/OSPF «закольцуется» на нем. Исправить данную ситуацию Вам поможет технология Policy-Based Routing.
Суть этой технологии заключается в установке принудительного маршрута для обратного трафика, приходящего обратно с сервера с ZapretService, не используя основную маршрутизацию. В теории состоит из фильтра отбора трафика и механизма назначения ему основного маршрута.
В фильтр добавляются «внешние» ip-адреса Ваших абонентов и ip-адрес второго интерфейса сервера с ZapretService. При использовании «серых» ip-адресов у абонентов необходимо предварительно трафик, уходящий на сервер с ZapretService, провести на маршрутизаторе через NAT. Ip-адрес, используемый в NAT, необходимо тоже добавить в фильтр.

На маршрутизаторе вендора Cisco данная технология реализуется с помощью функционала access-list (фильтр):

```
ip access-list standard zapret
   permit ip_адрес_второго_интерфейса_сервера
   permit внешний_ip_адрес_nat
   permit внешний_ip_адрес_абонента_1
   permit внешний_ip_адрес_абонента_x
```

и route-map (назначение маршрута), который назначается на втором интерфейсе маршрутизатора до сервера с ZapretService (Port 4 на схеме с одним маршрутизатором):

```
route-map hoptoinet permit 10
   match ip address zapret
   set ip next-hop ip_адрес_ISP_1 ip_адрес_ISP_2
```

На маршрутизаторах других вендоров принцип конфигурации подобен, поэтому необходимо обратиться к их документации для подбора нужных команд.

Важно! При использовании технологии PBR необходимо маршрутам от сервера с ZapretService установить больший приоритет с помощью параметра «bgp default local-preference».
Так же рекомендуется «зафильтровать» на маршрутизаторе мелкие маршруты (менее /24) у всех neighbor (кроме ZapretService), если включена опция «Производить объединение ip-адресов в подсети» в web-интерфейсе ZapretService (раздел «Настройки»).

Отправка уведомлений на внешнюю почту
ZapretService по умолчанию отправляет все уведомления локальному пользователю «zapret», которые можно наблюдать в файле «/var/mail/zapret». Для перенаправления уведомлений на внешнюю почту в файле «/etc/aliases» необходимо указать почтовый адрес для пользователя «zapret», пример:

zapret: user@mydomain.ru

Если почтовый адрес располагается, например на web-сервисе «yandex.ru», то необходимо настроить сервис «exim4» на отправку через удаленный smtp-сервер.

1. В файле «/etc/exim4/update-exim4.conf.conf» измените переменную dc_eximconfig_configtype на значение «smarthost», а переменную dc_smarthost адресом удаленного smtp-сервера (если есть SSL-авторизация, то через «::», двойное двоеточие, нужно указать номер SSL-порта удаленного smtp-сервера).

dc_eximconfig_configtype='smarthost'
dc_smarthost='smtp.yandex.ru::587'

3. В файле «/etc/exim4/passwd.client» пропишите реквизиты подключения к smtp-серверу

smtp.yandex.ru:логин@yandex.ru:пароль

4. Многие внешние почтовые web-сервисы отбрасывают приходящие письма, у которых в качестве отправителя указан локальный почтовый ящик. Для этого нужно в файле «/etc/exim4/conf.d/rewrite/00_exim4-config_header» указать замену на достоверный почтовый ящик.

begin rewrite
@ логин@yandex.ru Ffr

5. Перезагрузите сервис exim4 командой «sudo /etc/init.d/exim4 restart».

Важно! Содержимое в файле «/etc/mailname» должно совпадать с «/etc/hostname», иначе уведомления отправляться не будут.

Активация пробного режима
Данный режим используется изначально для демонстрации работы программного комплекса ZapretService и оформляется на нашем сайте (http://www.zapretservice.ru/). На почтовый ящик, указанный в заказе, должно поступить письмо с url-адресом лицензии, который необходимо ввести в web-интерфейсе ZapretService (http://zapret.local/manager/).
Данный режим не ограничен каким-либо функционалом и действует в течение 60 календарный дней. По истечению его срока действия Вы можете оформить заказ на режим «Trial» (подписка по оплаченному времени) или «Full» (бессрочное использование).

Важно! Если активация не производится, необходимо проверить доступность нашего сайта на сервере с ZapretService, а так же корректность времени, например с помощью команды «sudo /usr/sbin/ntpdate -u ru.pool.ntp.org».

Активация режима «Trial»
Данный режим не является ограниченным каким-либо функционалом и предоставляется после оформления договора, который позволяет производить оплату за желаемый период (месяц, квартал, полгода и т.д.). Заказ на него можно оформить на нашем сайте (http://www.zapretservice.ru/) в период и после действия пробного периода при условиях, что настройка была произведена в соответствии данной документации, наше решение Вам подходит и устраивает по заявленному функционалу.
За 10-6-3-2-1 дней до истечения оплаченного срока действия данного режима отправляются уведомления на электронный ящик, указанный при регистрации пробного периода. Так же срок действия можно наблюдать в web-интерфейсе ZapretService (раздел «Лицензия»).

Активация режима «Full»
Данный режим активируется автоматически при наличии на сервере специального usb-ключа. К сожалению, продажи данного режима не производятся из-за нюансов использования

нового алгоритма ГОСТ 2012 в usb-носителях для защиты ПО (старый алгоритм ГОСТ 94 на текущий момент не предоставляется авторизированными УЦ).

Настройка ZapretService
По требованиям Роскомнадзора необходимо иметь личную электронную подпись (ЭЦП) на специальном usb-носителе (ruToken или eToken). Её можно приобрести у любого аккредитованного удостоверяющего центра (список смотрите по ссылке http://minsvyaz.ru/ru/activity/govservices/2/).

Важно! В web-интерфейсе ZapretService так же существует возможность загрузки уже готовых файлов запроса и его цифровой подписи, поэтому следующие шаги по данному разделу можно не совершать. Данные файлы можно загрузить на странице «Настройки» в web-интерфейсе ZapretService, выбрав соответствующую опцию.

На локальной машине под управлением Windows с этого usb-носителя нужно установить сертификат электронной подписи:

1. Установите необходимые драйвера с сайта производителя usb-носителя
2. Установите ПО КриптоПро CSP (версию не ниже 3.6) с сайта http://www.cryptopro.ru/
3. Подключите usb-носитель
4. Выберите «Пуск/Панель управления/КриптоПро CSP», перейдите на вкладку «Сервис» и кликните по кнопке «Просмотреть сертификаты в контейнере»
5. В открывшемся окне кликните на кнопку «Обзор», чтобы выбрать контейнер для просмотра, и после выбора контейнера (если их несколько, то самый последний) кликните на кнопку «ОК»
6. Кликните по кнопке «Далее»
7. В следующем окне кликните на кнопку «Установить», после чего утвердительно ответьте на уведомление о замене сертификата (если оно появится)
8. Кликните по кнопке «Готово»
9. Не отключайте usb-носитель, т.к. он будет нужен для следующей операции

На той же локальной машине под управлением Windows нужно экспортировать установленный сертификат электронной подписи в pfx-файл (в формате PCKS#12). К сожалению, средствами КриптоПро CSP сделать такую выгрузку нет возможности, т.к. он формирует формат файла понятный только ему. Сделать это возможно только с помощью утилиты «P12FromGostCSP» (http://soft.lissi.ru/products/utils/p12fromcsp/). Обращаем Ваше внимание, чтобы для ее скачивания необходимо пройти процедуру лицензирования, т.к. утилита является платной. Шаги выгрузки:

1. Запустите утилиту «P12FromGostCSP»
2. В открывшемся окне выберите установленный ранее сертификат (его можно идентифицировать по сроку действия) и кликните по кнопке «ОК»
3. Утилита запросит доступ к usb-носителю, где нужно будет ввести pin-код
4. В следующем окне задайте придуманный пароль для экспортируемого файла в формате PCKS#12 и сохраните этот файл на локальной машине
5. Отключите usb-носитель

Полученный файл нужно загрузить в ZapretService, чтобы программный комплекс мог автоматически приступить к выполнению своих функций:

1. Зайдите в web-интерфейс ZapretService (http://zapret.local/manager/)
2. Перейдите на страницу «Настройки»

3. Заполните поля «Название компании», «ИНН», «ОГРН», «E-mail», т.к. эти данные нужны для формирования специального файл-запроса, с помощью которого будет осуществляться загрузка реестра запрещенных сайтов от Роскомнадзора
4. Кликните по кнопке «Обзор» и выберите файл, который был экспортирован в предыдущей операции
5. В поле «Пароль к PCKS#12» введите пароль к файлу, который был задан при его экспорте
6. Кликните по кнопке «Обновить»
7. Удалите используемый файл с локальной машины

Важно! После активации режима работы и настройки ZapretService каждому его модулям необходимо выполнить свою задачу по одному разу, чтобы web-фильтрация по реестру запрещенных сайтов заработала в полную силу. При выборе минимальной конфигурации сервера это занимает примерно 3-4 часа.

Новый механизм выгрузки реестра
С ноября 2017 года Роскомнадзор анонсировал новый механизм организации выгрузки реестра без использования ЭЦП. Данный механизм так же предоставляет возможность использования «дельта-пакетов» (упрощенные xml-файлы, в котором отражаются только изменения вместо целого реестра) для оперативного обновления фильтров на стороне операторов связи, но при этом сохранена возможность получения и полного xml-файла реестра.
Начиная с версии 5.2, ZapretService поддерживает использование данного механизма, который можно включить в web-интерфейсе (раздел «Настройки»). Для получения реквизитов доступа (логин и пароль) необходимо обратиться на специальный раздел портала выгрузки - https://vigruzki.rkn.gov.ru/auto-delta/.

Важно! С версии 5.0 в ZapretService была внедрена упрощенная обработка реестра - самостоятельное отслеживание новых/измененных/удаленных контентных записей, что позволило оперативно применять обновления реестра за несколько минут.
Совместно с представителями Роскомнадзора в декабре 2017 года была проведена тщательная проверка данного функционала на новом механизме (посредством тестирования у некоторых операторов связи), которая полностью удовлетворила все требования, применяемые при использовании «дельта-пакетов», в том числе и оперативность.
Было решено использовать данный функционал при новом механизме, чтобы исключить в будущем нюансы, например, сбой выдачи «дельта-пакета» на портале выгрузок.

Использование другого домена вместо zapret.local
В ZapretService существует возможность использования другого домена вместо «zapret.local». Для этого необходимо добавить опцию «redirect_domain» в конфигурационный файл «/etc/zsmon/zsmon.conf», например:

redirect_domain=mydomain.ru

Дополнительно необходимо сервису «apache» добавить опцию «ServerAlias» в конфигурационном файле «/etc/apache2/sites-available/000-default.conf» после строки «ServerName zapret.local», пример:

```
<VirtualHost *:80>
        ServerAdmin www@zapret.local
        ServerName zapret.local
        ServerAlias mydomain.ru
…
```

Важно! Другие секции «VirtualHost», где есть опция «ServerName» с доменом отличным от «zapret.local», корректировать не нужно, т.к. тем самым можно «сломать» работу web-интерфейса ZapretService.

После всех операций необходимо перезапустить сервисы «apache» (команда «sudo /etc/init.d/apache2 reload») и «zsmon» (командами «sudo /etc/init.d/zsmon stop» и «sudo /etc/init.d/zsmon start»).

Важно! Если необходимо поменять домен в файле «/etc/hostname», то это нужно отразить и в файле «/etc/mailname», иначе уведомления будут отправляться от домена, указанного в данном файле, а не от нового.

Описание основных модулей ZapretService
«generate»: модуль для генерации файла запроса, который загружается на web-сервис интернет-портала http://vigruzki.rkn.gov.ru/ модулем «request». Данный файл генерируется на основе данных, заполненных в разделе «Настройки» web-интерфейса ZapretService, и подписывается файлом в формате PCKS#12 (сертификатом электронной подписи). Запускается при загрузке файла (в формате PCKS#12) в разделе «Настройки» и каждый первый день месяца в 04:50. При сроке действия сертификата электронной подписи менее 60 дней генерируется соответствующее уведомление.

«rkn»: модуль для взаимодействия с web-сервисом интернет-портала http://vigruzki.rkn.gov.ru/. Производит обязательные выгрузки реестра, а также проверку срочности выгрузки. Запускается каждые 5 минут. Обязательная выгрузка производится в 9 часов (утром и вечером) по московскому времени, т.е. учитывается часовой пояс. Если у Вас часовой пояс +2, то обязательная выгрузка будет производиться в 11 часов утра и вечера. Можно выполнить принудительную выгрузку, если запустить модуль в shell с ключом «p».

«parser»: модуль обработки файла реестра запрещенных сайтов, который был загружен модулем «rkn». Запускается каждые 5 минут, если в этот момент модуль не выполняет свою задачу. При запуске проверяет файл дампа реестра и начинает его обрабатывать, если он изменился с момента последней обработки. При первом запуске после установки ZapretService используется полный алгоритм для обработки всего файла реестра, что занимает довольно много времени (от 2 до 6 часов в зависимости от конфигурации сервера). При последующих запусках применяется упрощенный алгоритм, который обрабатывает только изменения реестра, что в свою очередь снижает время общей работы модуля до нескольких минут. Каждый понедельник в 00 часов по местному времени данный модуль запускает полный алгоритм для организации проверки целостности БД. Данную процедуру можно выполнить принудительно, если запустить модуль в shell с ключом «p». Так же модуль использует полный алгоритм обработки реестра, если предыдущий запуск был выполнен с ошибкой.

«routing»: модуль корректировки маршрутов для протокола OSPF/BGP и таблиц сервиса iptables. Запускается каждые 5 минут. Выполняет обработку таблицы маршрутизации сервера при соблюдении одного из 4 условий: статус модуля отличен от «complete»; количество маршрутов на сервере менее 1000; запуск модуля в промежутке времени с 6.30 до 6.35 ночи (по местному времени); запуск модуля с ключом «p» в shell.

«stat»: модуль сбора статистики по общей работе сервера для отображения графиков в web-интерфейсе ZapretService. Запускается в начале каждого часа.

«resolver»: модуль обнаружения новых ip-адресов у запрещенных ресурсов (которые активно используют технологию CDN). Запускается каждую минуту, если в этот момент модуль не выполняет свою задачу. Помимо этого, дополнительно запускается в начале каждого часа для выявления ресурсов, которые начали использовать технологию CDN. Данный модуль использует dns-сервера, прописанные в файле /etc/resolv.conf, а также дополнительно dns-сервера от Google (8.8.8.8) и Yandex (77.88.8.8).

Блокировка запрещенных ip-адресов и ip-подсетей
7 октября 2015 года Роскомнадзор вынес операторам связи распоряжение о полном ограничении доступа до ip-адреса или ip-подсети, включая все их сетевые порты, если это требуется в выгрузке.
ZapretService оснащен возможностью автоматического выполнения этого требования без Вашего вмешательства. Посмотреть актуальный список блокированных ip-адресов или ip-подсетей можно с помощью команд «ipset list block-ip» и «ipset list block-net».

Агрегация маршрутов (routes)
Начиная с версии 7.1, в ZapretService были добавлены 3 режима агрегации маршрутов с целью снижения их числа для передачи в OSPF/BGP-связку. Выбрать необходимый можно в web-интерфейсе - раздел «Настройки», опция «Производить объединение ip-адресов в подсети для OSPF/BGP»:

«грубое (с маской 24)» - все маршруты с маской /32 переводятся в маску /24;
«гибкое (с масками 24 и 32)» - создается маршрут с маской /24, если маршруты с маской /32 превышают установленный процент вхождения в данный маршрут, при этом сами маршруты /32 удаляются;
«стандартное (с разной маской)» - агрегация маршрутов производится по стандартному алгоритму суммирования всех маршрутов.

Важно!!! Режимы, кроме «грубое (с маской 24)», были протестированы только в «лабораторных условиях». Настоятельно рекомендуем после включения одного из них понаблюдать за работой сервера ZS в течение нескольких дней, а так же за отчетами АС Ревизора.

О методе фильтрации https-трафика
Модуль «zsmon» использует специальную технологию анализа HTTPS-трафика. Если ZapretService обнаружит в sni-информации запрещенный домен из реестра, то будет производиться сброс SSL-соединения.

Важно! К сожалению, при SSL-соединении технически невозможно без вмешательства в само соединение передать клиенту код ответа сервера (например, 451), а также произвести перенаправление на страницу-заглушку, т.к. такое соединение заблокирует сам браузер.

URL-ссылки сервиса Youtube
В реестре запрещенных сайтов на данный момент занесены только HTTP-ссылки сервиса Youtube. Можно заметить, что данные ссылки открываются. Происходит это из-за технологии HSTS (https://ru.wikipedia.org/wiki/HSTS), т.е. при входе на HTTP-ссылку Ваш браузер автоматически будет перенаправлять Вас на HTTPS.
АС «Ревизор» не использует данное перенаправление, поэтому проверяет только HTTP-ссылки без всякого перехода на HTTPS.

Логирование попыток переходов на запрещенные ресурсы
Начиная с версии 6.0 в ZapretService по умолчанию отключено информирование о

блокированном ресурсе в лог-файле «/var/log/zsmon/zsmon.log», т.к. при интенсивной блокировке может возникнуть деградация дисковой подсистемы сервера.

Но этот функционал можно включить опцией «log_inform_blocked=true» в файле «/etc/zsmon/zsmon.conf». После необходимо перезагрузить сервис zsmon командой «sudo /etc/init.d/zsmon restart». Для отслеживания блокировок в режиме реального времени можно воспользоваться командой «tail -F /var/log/zsmon/zsmon.log».

Обнаружение новых ip-адресов у запрещенных ресурсов
В лог-файле «/var/log/zsmon/foundip.log» заносится информация о новых ip-адресах запрещенных ресурсов, которые ZapretService смог обнаружить при их резолвинге. Для просмотра данного файла в режиме реального времени можно воспользоваться командой «tail -F /var/log/zsmon/foundip.log».

Удаленный мониторинг параметров модулей ZapretService
Для организации мониторинга параметров модулей ZapretService, например, с помощью системы мониторинга Zabbix, разработан модуль «getinfo». Листинг модуля в командной строке на сервере:

/usr/local/zapret/getinfo [target]

где target:

list	количество записей в реестре
urls	количество запрещенных ссылок в БД
dmns	количество запрещенных доменов в БД
ips	количество запрещенных ip-адресов в БД
lans	количество запрещенных ip-подсетей в БД
block	количество попыток перехода на запрещенные ресурсы за прошлый час
dcr [unixtime]	дата последнего формирования списков на web-сервисе интернет-портала http://vigruzki.rkn.gov.ru/
dnl [unixtime]	дата последней выгрузки дампа реестра с web-сервиса интернет-портала http://vigruzki.rkn.gov.ru/
version	версия программного комплекса

Особую благодарность мы хотели бы выразить Кожевникову Виктору (ООО "Север-Связь" г. Ноябрьск), а именно за предоставленные нам его наработки для сервиса zabbix-agent:

- скрипты взаимодействия с нашим модулем getinfo (/etc/zabbix/scripts)
- конфигурационный файл (/etc/zabbix/zabbix_agentd.d/zapretservice.conf)
- шаблон для web-интерфейса Zabbix (/etc/zabbix/zs_template.xml)

Данные наработки уже включены в состав программного комплекса ZapretService. Мы так же в него включили установочный файл сервиса zabbix-agent (/etc/zabbix/zabbix-agent_2.2.9-1+wheezy_amd64.deb).
Вам лишь необходимо установить сервис zabbix-agent на сервере с помощью команды «sudo dpkg -i /etc/zabbix/zabbix-agent_2.2.9-1+wheezy_amd64.deb» и импортировать шаблон zs_template.xml в web-интерфейсе Zabbix.

«Список РКН»
Данный функционал позволяет просматривать актуальный реестр Роскомнадзора. В поисковый запрос можно указать url-ссылку, домен или ip-адрес. В найденных результатах можно свободно перемещаться по объектам реестра.

«Черный список»
Данный функционал позволяет формировать собственные списки по блокировке определенных ресурсов. В качестве блокируемого ресурса можно указать url-ссылку, домен или ip-адрес.

«Глобальный черный список»
Иногда в реестр запрещенных сайтов попадают ресурсы с некорректными символами, например, url-ссылки с символом «двойная кавычка». Нами не предполагалось, что такой символ когда-нибудь мог бы появиться, т.к. он является совсем не типичным, а по стандарту RFC недопустимым. Данный момент был учтен в ZapretService версии 5.2.
Однако при проявлении подобного случая, чтобы не нужно было ожидать очередного обновления ZapretService, с версии 5.3 был добавлен функционал «глобальный черный список». Данный функционал позволяет ZapretService автоматически получить «ресурс-заглушку» с нашего удаленного сервера, чтобы Вы не делали этого вручную. После выпуска соответствующего обновления данный функционал автоматически удалит «ресурс-заглушку».

«Белый список»
Данный функционал позволяет исключить из блокировки/проверки программным комплексом ZapretService необходимые ресурсы, если они находятся в реестре запрещенных сайтов или в черном списке. В качестве ресурса можно указать url-ссылку, домен, ip-адрес или подсеть.
При указании url-ссылки/домена модуль фильтра не будет перенаправлять абонента на страницу-заглушку.
При указании ip-адреса модуль фильтра исключит его из маршрутизации. Тем самым пограничный маршрутизатор не получит его по протоколу OSPF/BGP и не будет отправлять трафик до данного ip-адреса на сервер с ZapretService.
При указании подсети модуль фильтра не будет проверять трафик, который отправляется на указанную подсеть. Т.е. трафик до указанной подсети будет проходить через сервер «сквозным» методом. К сожалению, пока по технической причине данная возможность не исключает из маршрутизации ip-адреса, которые сгенерировались на сервере с ZapretService и входят в указанную подсеть.

Интеграция с местными dns-серверами (на BIND)
В качестве дополнительной защиты фильтрации запрещенных сайтов в версии 4.3 ZapretService был добавлен модуль genfakezones, который генерирует для dns-сервиса, основанный на пакете BIND, специальные файлы с «фейковыми» зонами. Данный функционал позволяет подставлять в запрещенных доменах ip-адрес сервера с ZapretService (или другого сервера со страницей-заглушкой) вместо своих ip-адресов.

Важно! В сети лучше использовать два dns-сервиса чтобы, при отказе первого (при применении данных), второй подхватил запросы абонентов.

Важно! После завершения настройки данного функционала мы рекомендуем на Ваших BRAS’ах сделать перенаправление на Ваш dns-сервер всех запросов 53 порта (tcp и udp) от Ваших абонентов. Тем самым, если абонент пропишет у себя какой-нибудь другой dns-сервер, то все равно обработкой dns-запросов будет заниматься Ваш dns-сервер.

Модуль genfakezones необходимо скопировать из каталога «/usr/local/zapret» с сервера ZapretService на сервер с dns-сервисом. На сервере с dns-сервисом должен быть установлен пакет php5-cli версии не ниже 5.4, т.к. модуль должен запускаться как исполняемый файл. Скопировать модуль genfakezones можно в любой каталог сервера. Файл модуля должен иметь права на запуск (755). Синтаксис запуска модуля:

./genfakezones -d <path> [-i <ip>], где ключ d является обязательным.

<path> - каталог для формирования специальных файлов «фейковых» зон. Желательно указать каталог расположения конфигурационных файлов BIND, например, /etc/namedb.
<ip> - ip-адрес сервера, где расположена страница-заглушка. Если не указывать данный параметр, то модуль будет использовать ip-адрес домена zapret.local.

Важно! Ключ «i» не является обязательным. Его можно использовать, если Вы желаете снизить нагрузку на сервер ZS, перебросив запросы к запрещенным сайтам на отдельный сервер, где у Вас расположена страница-заглушка. Данный файл модуля можно так же скопировать на этот сервер, переименовав его в index.php и расположить его в каталоге, где должна храниться страница-заглушка. При использовании файла модуля сервисом apache или nginx, он будет генерировать правильную страницу-заглушку с необходимым кодом статуса 451.

Модуль генерирует два файла: «zapret.db» (файл «фейковой» зоны) и «zapret.zones» (файл с зонами запрещенных сайтов). После генерации файлов необходимо добавить в конец конфигурационного файла «named.conf» пакета BIND строку «include "/etc/namedb/zapret.zones";», где /etc/namedb/ - каталог расположения сгенерированных файлов модуля genfakezones.
После необходимо перезапустить сервис BIND, например, командой «sudo /etc/init.d/named restart».

Важно! Убедитесь, что перезапуск сервиса BIND прошел удачно и dns-сервис начал отвечать на домены запрещенных сайтов ip-адресом сервера страницы-заглушки.

Модуль необходимо запускать на сервере периодично, хотя бы раз в сутки, например, в 4:30 ночи. Это можно сделать, добавив вызов в сервис CRON, например, командой

«echo '30 4 * * * root /etc/namedb/genfakezones -d /etc/namedb && команда_reload_для_bind' > /etc/cron.d/genfakezones», где команда_reload_для_bind – команда сброса кэша или перезапуска сервиса bind, например, «/etc/init.d/named reload»

Проделайте аналогичные действия на сервере со вторым dns-сервисом.

Важно! Необходимо понимать, что данный функционал перенаправляет все url-ссылки сайта на страницу-заглушку, даже если в реестре запрещенных сайтов находится только одна его url-ссылка. Со временем в реестре запрещенных сайтов может появиться и сам домен сайта, как показывает практика. Но Вы можете в web-интерфейсе ZapretService (в разделе DNS-интеграция) добавить необходимый домен в исключение. Тогда перенаправление для необходимого сайта отключится, и ZapretService будет проводить его фильтрацию по стандартным правилам, т.е. по url-ссылкам при http-трафике и по доменам при https-трафике.

Важно! При добавлении домена в исключение необходимо вручную запустить модуль genfakezones на Вашем dns-сервере, а так же произвести перезагрузку самого сервиса DNS. Либо дождаться срабатывания на Вашем dns-сервере сервиса CRON.

Важно! В ОС Linux необходимо изменить значение команды «ulimit -n», если оно меньше 4096. Для этого необходимо в файл /etc/security/limits.conf добавить строку «root - nofile 4096», и выполнить команду «ulimit -n 4096» под учетной записью root.

Важно! В ОС FreeBSD для корректного запуска модуля genfakezones под CRON необходимо прописать в файле /etc/crontab (в переменную PATH) абсолютный путь директории, где располагается обработчик языка PHP. Например, было
PATH=/etc:/bin:/sbin:/usr/bin:/usr/sbin
стало:
PATH=/etc:/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin/

Интеграция с местными dns-серверами (на UNBOUND)
Настройка данного функционала для интеграции с dns-сервером на базе пакета UNBOUND осуществляется аналогично, как и с пакетом BIND.
Для генерации конфигурационного файла для пакета UNBOUND необходимо использовать дополнительный ключ -t со значением «unbound», т.е.

./genfakezones -d <path> -t unbound [-i <ip>], где ключ d является обязательным.

Модуль генерирует один файл: zapret.zones (файл с зонами запрещенных сайтов). После генерации файла необходимо добавить в конфигурационный файл «unbound.conf» пакета UNBOUND (обычно в начале файла) строку «include: "/etc/unbound/zapret.zones"», где /etc/unbound/ - каталог расположения сгенерированного файла модуля genfakezones. После необходимо перезапустить сервис UNBOUND, например, командой «sudo service unbound restart».

Модуль необходимо также запускать на сервере периодично, например, через сервис CRON.

Важно! В ОС Linux необходимо изменить значение команды «ulimit -n», если оно меньше 4096. Для этого необходимо в файл /etc/security/limits.conf добавить строку «root - nofile 4096», и выполнить команду «ulimit -n 4096» под учетной записью root.

Важно! В ОС FreeBSD для корректного запуска модуля genfakezones под CRON необходимо прописать в файле /etc/crontab (в переменную PATH) абсолютный путь директории, где располагается обработчик языка PHP. Например, было
PATH=/etc:/bin:/sbin:/usr/bin:/usr/sbin
стало:
PATH=/etc:/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin/

Отключение поиска ip-адресов у запрещенных ресурсов
В связи с рекомендательным письмом Роскомнадзора №10513-02/66 от 09.06.2017 и многочисленными обращениями наших клиентов по реализации возможности, указанной в этом письме, в web-интерфейсе ZapretService версии 4.10 была добавлена опция «Не производить поиск ip-адресов у запрещенных ресурсов». Данная опция отключает модуль «resolver», а модуль «routing» переводит в режим генерации маршрутов только по ip-адресам из списка запрещенных сайтов.

Поддержка IPv6
Программный комплекс ZapretService не имеет поддержку протокола IPv6.

Установка дополнительных пакетов на сервере с ZapretService
В составе программного комплекса ZapretService включены модифицированные пакеты некоторых сервисов, которые специально заточены под нужды взаимодействия с интернет-порталом Роскомнадзора и для фильтра запрещенных сайтов.
Мы не рекомендуем использовать команды «aptitude» и «apt-get» для установки

дополнительных пакетов или обновления системы в целом, т.к. есть риск замены модифицированных пакетов, что в свою очередь может привести к отказу работы сервиса фильтрации в целом.
Если Вы желаете установить необходимый пакет, то лучше скопировать его на сервер и воспользоваться командой «dpkg», или же сообщите нам через обратную связь на нашем сайте, и мы сами произведем необходимые действия на Вашем сервере с ZapretService.

Использование резолвинга
Обращаем Ваше внимание, что использование резолвинга запрещенных доменов производится только с целью снижения отправки количества проверяемого трафика на сервер с ZapretService (вместо отправки всего исходящего с маршрутизатора), тем самым позволяет не использовать дорогостоящий сервер для такой нагрузки. На текущий момент доля проверяемого трафика составляет не более 10-15% от общего, т.к. остальной трафик это видео или игровой, где никогда не появится запрещенный ресурс.
Основная фильтрация производится уже на самом сервере с ZapretService согласно последним требованиям Роскомнадзора, а именно ZapretService не производит блокирование по ip-адресу, если того явно не требует сам реестр, или ресурс не был добавлен Вами в «черный список».

Решение проблем
Q. После установки iso-образа на сервер не могу попасть в web-интерфейс ZapretService.
A. В целях безопасности вход в web-интерфейс возможен только через домен zapret.local, а именно через url-ссылку http://zapret.local/manager/. Необходимо данный домен добавить в свой dns-сервис или прописать на своем ПК в файле hosts, указав ему ip-адрес сервера с ZapretService.

Q. При вводе url-ссылки пробного ключа в web-интерфейсе ZapretService выводится ошибка «По введенной url-адресу ZapretService не смог обнаружить актуальную лицензию».
A. Проверьте доступность нашего сайта http://www.zapretservice.ru/ и корректность времени командой «sudo /usr/sbin/ntpdate -u ru.pool.ntp.org» на сервере с ZapretService.

Q. Есть ли возможность провести тестирование решения без загрузки в него ЭЦП или файлов для запроса.
A. Такая возможность имеется, если у Вас есть в наличии xml-файл реестра. Данный файл можно разместить в каталоге «/var/spool/zapret» сервера под именем dump.xml. При следующем запланированном запуске модуль parser начнет его обработку.

Q. Где можно посмотреть логи модулей ZapretService.
A. Данная информация предоставляется в web-интерфейсе ZapretService на главной странице, кликнув по названию нужного модуля.

Q. Нет пинга до ресурса, трафик которого проходит через сервер с ZapretService.
A. Убедитесь, что ip-адрес ресурса не включен в список заблокированных ip-адресов реестра. Для этого Вы можете воспользоваться разделом «Список РКН» web-интерфейса ZapretService или командой «sudo ipset list block-ip». Так же необходимо убедиться в отсутствии ip-адреса ресурса в разделе «Черный список» web-интерфейса ZapretService.

Q. Трассировка до ресурса обрывается после сервера ZapretService.
A. Такое возможно при использовании NAT. Убедитесь, что на сервер с ZapretService отправляется трафик от Ваших клиентов, уже прошедший через NAT.

Q. Не фильтруется ни один сайт из реестра.

A. Убедитесь, что OSPF/BGP-сессия установлена с Вашим пограничным маршрутизатором, и трафик до открываемого ресурса отправляется на сервер с ZapretService. При использовании технологии VLAN на сервере, необходимо убедиться в правильности указания интерфейсов в файле «/etc/iptables/rules.v4». Точно такую же информацию должна выдавать команда «sudo iptables-save».

Q. При использовании ZapretService не открывается сайт сервиса Youtube или подобный. При отключении сервера сайт начинает открываться.
A. Необходимо проверить, что url-ссылки или сам домен данного ресурса не добавлены в «Черный список», а так же не присутствуют ли ip-адреса данного ресурса в реестре РКН (можно посмотреть через «Список РКН»).

Q. При входе на сайт n-ресурса не выводится страница-заглушка.
A. Проверьте наличие url-ссылки сайта, на которую Вы заходите, в разделе «Список РКН» web-интерфейса ZapretService. Если url-ссылка там присутствует, то убедитесь, что трафик до данного ресурса проходит через сервер ZapretService. Возможно, Вы недавно добавили ресурс или его ip-адрес в «Белый список». Обращаем Ваше внимание, что страница-заглушка может выводиться только при HTTP-протоколе. При HTTPS вывод страницы-заглушки невозможен, т.к. это шифрованный протокол, в который нет возможности подменить данные, поэтому имеется только возможность сбросить соединение.

Q. Где можно точно посмотреть, что ресурс является запрещенным.
A. Вы можете воспользоваться разделом «Список РКН» в web-интерфейсе ZapretService или «Универсальным сервисом проверки ограничения доступа к сайтам и (или) страницам сайтов сети «Интернет»» - http://blocklist.rkn.gov.ru/.

Q. В лог-файле «/var/log/messages» и выводе команды «dmesg» присутствуют записи «nf_queue: full at 16384 entries, dropping packets(s)».
A. Данные записи говорят о переполнении очередей обрабатываемого трафика и та часть, что вышла за пределы, не была обработана и не отправилась далее по маршрутизации. Такое случается, если до какого-то ресурса сети Интернет из Вашей сети была произведена DDOS-атака (генерация большого трафика), либо на Вашем сервере с ZapretService закончились системные ресурсы и необходимо их увеличение. Рекомендуем обратиться к нам для получения рекомендаций, возможно, потребуется всего лишь небольшой «тюнинг» ОС.

Q. Имеется проблема, которая тут не описана. Куда обращаться.
A. Вы можете воспользоваться формой «Обратная связь» на сайте http://www.zapretservice.ru/ или отправить письмо на электронный ящик answer@zapretservice.ru. В тексте обращения необходимо подробно описать суть проблемы, а при необходимости выполнения каких-либо действий на Вашем сервере – реквизиты ssh-доступа (ip-адрес сервера, пароль для логина zapret). Реагирование на обращение производится согласно регламенту - http://www.zapretservice.ru/files/reglament.pdf.

История изменений
7.1 (19.08.2019)
* Добавлено 3 режима агрегации routes (подробнее в документации - раздел "агрегация маршрутов (routes)")
* Добавлена дополнительная проверка на задвоение default gw
* Убрана проверка целостности БД, запускаемая ночью каждого понедельника недели
* Исправлена проблема обнуления лицензии при вводе неверной url-ссылки в web-интерфейсе ZS
* Оптимизирован процесс чистки БД от старой адресации модуля resolver

* Увеличен лимит на количество запрещенных ip-адресов в ipset с 800000 до 2000000
* Добавлена фильтрация ssl-трафика расширенного протокола TLS

7.0 (10.06.2019)

* Переход на новую платформу разработки: открыта 7 ветка ZS
* Переработана логика обработки xml-файла реестра: уменьшено в 3 раза потребление памяти модулем parser
* Добавлена дополнительная проверка состояния БД, которая не допускает считать ее "некорректной" при невозможности чтения xml-файла реестра
* Увеличен лимит на количество запрещенных ip-адресов в ipset с 400000 до 800000 (на текущий момент в реестре находятся более 350 тыс. запрещенных ip-адресов и они все еще добавляются)
* Исправлен подсчет разрешенных ресурсов из белого списка у модуля zsmon

6.6 (21.03.2019)

* Исправлена фильтрация некорректных url-ссылок с конечной последовательностью символов "?#"
* Оптимизирована работа модуля parser на плановой задаче проверки всего реестра РКН
* Уменьшено время хранения ip-адресации в БД до 45 дней
* Мелкая оптимизация модулей generate и trialkey
* Добавлена поддержка ГОСТ2012 при импорте pfx-файла ЭЦП
* Увеличен лимит на количество запрещенных ip-адресов в ipset с 200000 до 400000

6.5 (23.01.2019)

* Добавлен контроль над появлением ip-адресов сервера в генерируемых маршрутах
* Добавлен контроль над некорректными доменами с символом "\": такие домены теперь не экспортируются для модуля genfakezones
* Добавлен фильтр ip-адресов из подсетей 127.0.0.0/8 и 255.0.0.0/8 при экспорте в маршрутизацию сервера
* Исправлен баг обработки url-ссылок с числом "0" после знака "?": такие url-ссылки считались некорректными и приводились к виду без query_string
* Добавлена подсветка количества обработанных строк в разделе "история реестра" web-интерфейса ZS
* Исправлен мелкий баг отображения данных при поиске в разделе "история реестра" web-интерфейса ZS
* Откорректирован размер буфера БД для внесения больших данных: при превышении модуль parser может получить критическую ошибку и инициировать процедуру проверки БД с xml-файлом выгрузки
* Добавлен контроль над количеством tcp-портов в фильтрующих правилах iptables
* Оптимизирован код модуля routing для ускорения наполнения фильтров данными по проверяемым ip-адресам
* Структурирование кода и исправление мелких ошибок в модуле main

6.4 (16.09.2018)

* Добавлена поддержка формата 2.4 файла выгрузки РКН (изменения на портале выгрузки РКН с 1 ноября 2018 - http://vigruzki.rkn.gov.ru/docs/description_for_operators_actual.pdf)
* Добавлена возможность просмотра в web-интерфейсе (раздел "Список РКН") ipv6-адресов и ipv6-подсетей, включенных в выгрузку РКН у запрещенных ресурсов
* Добавлен контроль случайного попадания ipv6-адресов в тегах xml-файла выгрузки
* Добавлен контроль количества tcp-портов для правил iptables (при более 15 возникала системная ошибка обновления iptables)
* Исправлен баг при контроле количества маршрутов в модуле routing (не срабатывала проверка всей таблицы маршрутизации при обнаружении менее 1000 маршрутов)

6.3 (24.08.2018)

* Добавлены графики "Средняя скорость обработки трафика в секунду" и "Средняя

скорость обработки eth-пакетов в секунду" (раздел "статистика" в web-интерфейсе)
* Добавлена возможность просмотра статистики в web-интерфейсе за месяц
* Исправлена возможная ошибка при добавлении локальных подсетей интерфейсов сервера модулем routing
* Мелкая оптимизация кода в разных модулях

6.2 (06.06.2018)
* Добавлена правильная обработка и корректировка неразрешенного символа "\" в url-ссылках
* Исправлена сортировка результатов поиска в функционале "история реестра"
* Исправлена возможная ошибка, приводящая к зависанию модуля parser
* Увеличение лимита на количество запрещенных ip-адресов в ipset с 65000 до 200000
* Мелкая оптимизация системы резолвинга

6.1 (25.04.2018)
* Заменено информирование о произведенной блокировке ресурса на обычный их подсчет в логах модуля zsmon, т.к. при увеличении частоты таких сообщений страдает дисковая подсистема, а так же нагрузка на сервер
* Оптимизирована библиотека сборки фрагментированных tcp-пакетов
* Доработано исключение из проверки трафика до ip-адреса, включенного в "белый список", если данный ip-адрес входит в запрещенную подсеть
* Добавлен функционал "история реестра" в web-интерфейсе ZS для оперативного отслеживания изменений реестра РКН
* Отключена проверка ssl-сертификата портала при использовании нового механизма выгрузки

6.0 (03.04.2018)
* Произведен "рефакторинг" с добавлением функционала сборки фрагментированных tcp-пакетов
* Добавлен к алгоритму "резолвинга" дополнительный функционал защиты от dns-атаки (частое изменением А-записей у "нехорошего" запрещенного домена)
* Добавлена в web-интерфейсе возможность просмотра изменения реестра по произведенным выгрузкам
* Исправлена ошибка, по которой сервис squid запускался и генерировал ненужные сообщения о сбое в его работе
* Убрана из web-интерфейса опция "Производить обработку https-трафика сервиса Youtube" по причине отсутствия ее полезности

5.5 (21.03.2018)
* Страница-заглушка генерируется в кодировке UTF-8
* Исправлена повышенная нагрузка при работе функционала "DNS-интеграция"

5.4 (21.03.2018)
* Откорректирована страница-заглушка согласно новым требованиям приказа РКН от 14.12.2017 №249 "http://ordercom.ru/treb.doc" (зарегистрирован Минюстом 15.03.2018)
*Добавлены дополнительные проверки в модуль rkn для более стабильной его работы при организации выгрузки (проблема была плавающей и возникла только в единичном случае)
* Email-сообщения, содержащие информацию о каких-либо ошибках (в том числе о невозможности выгрузки), теперь имеют тему «Warning from ZapretService» вместо «Notice from ZapretService»

5.3 (30.01.2018)
* Добавлена поддержка новой версии xml-файла выгрузки 2.3
* Оптимизирован алгоритм сравнения xml-файлов модуля "parser"
* Добавлена система "глобального черного списка"
* Передвинута проверка таблицы маршрутизации сервера с 4 на 6 часов ночи, чтобы снять лишнюю нагрузку на сервер во время полной проверки АС Ревизора

* Исправлен баг, который допускал пропуск маршрутов при полной проверки таблицы маршрутизации сервера

5.2 (06.01.2018)

* Добавлена поддержка нового механизма выгрузки реестра без использования ЭЦП
* Переработан алгоритм обработки xml-файла выгрузки, что позволило снизить его время работы в 2 раза
* Переработан алгоритм проверки запрещенных ресурсов в модуле "zsmon", что увеличило его производительность
* Оптимизированы модули "resolver" и "routing"
* Заменена сторонняя функция на собственную для правильной корректировки неразрешенных символов в url-ссылках, таких как одинарная или двойная "кавычка"
* Исправлен баг при фильтрации запрещенный доменов с большими русскими буквами

5.1 (28.08.2017)

* Переработан web-интерфейс добавления домена в список исключения функционала "DNS-интеграция".
* Добавлена опция "Включать в список функционала "dns-интеграция" только домены, которые имеют явный признак полного блокирования" в разделе "Настройки".
* Добавлена опция "Производить объединение ip-адресов в подсети с маской 24 для OSPF/BGP" в разделе "Настройки" (Внимание!!! Данная опция способствует увеличению поступаемого трафика на сервер ZS).
* Добавлена опция redirect_domain для модуля zsmon. Подробнее в разделе "Использование другого домена вместо zapret.local" нашей документации.
* Добавлена опция redirect_at_block для модуля zsmon, которая может принимать значение true или false. При значении false модуль zsmon будет выдавать сразу страницу-заглушку вместо редиректа. (Внимание!!! Данная опция экспериментальная, т.к. не была оттестирована под высокими нагрузками).
* Исправлена обработка url-ссылок, который содержат в себе 80 порт.
* Исправлен баг при проверке запрещенных ресурсов типа "маска домена".

5.0 (27.07.2017)

* Заменен сервис squid на модуль zsmon, в котором используется принцип DPI: сквозная проверка трафика без подмены адреса источника. При открытии запрещенного https-ресурса производится сброс ssl-соединения. При открытии запрещенного http-ресурса модуль умеет пока отправлять только редиректы на страницу-заглушку. В последующих обновлениях мы планируем вместо этого сделать отображение страницы-заглушки как у сервиса squid, т.е. без редиректа.
* Добавлен упрощенный алгоритм обработки реестра в модуль parser. Теперь при появлении свежей выгрузки модуль parser обрабатывает только новые или измененные контентные записи. Для сохранения целостности БД модуль каждый понедельник в 00 часов, и в случае появления ошибки при новом алгоритме запускает старый алгоритм обработки реестра.

4.10 (11.06.2017)

* Добавлена возможность добавлять подсети в "Белый список"
* Добавлена опция "Не производить поиск ip-адресов у запрещенных ресурсов" в web-интерфейсе ZS (в документации раздел "Отключение поиска ip-адресов у запрещенных ресурсов")
* После обновления в "Белый список" добавятся подсети ресурса ВКонтакте и ip-адреса из xls-файла РКН
* Исправлена проблема пропусков с запрещенными ресурсами "http://pro100farma.net\stanozolol\" и "http://alkogol61.accountant"
* Продолжается разработка 5 ветки нашего решения, где метод "проксирование" заменится на "сквозную проверку трафика" (DPI), где адрес источника не будет подменяться (проблема с сервисом ВКонтакте)

4.9 (31.05.2017)

* Оптимизирован модуль "trial" для подключения к нашему серверу лицензий.
* Добавлена возможность выбрать ip-адрес сервера, с которого будут производиться запросы к серверам РКН для организации выгрузок.
* Раздел "Список РКН" в web-интерфейсе ZS теперь может искать ip-адрес в запрещенных подсетях.
* Исправлен баг в разделе "Список РКН" web-интерфейса ZS, при котором не отображалась информация о запрещенной подсети.
* Исправлен баг с символом "\" в url-ссылках запрещенных ресурсов.

4.8 (16.05.2017)

* Добавлен функционал, который следит за изменением default-маршрута на сервере ZS. При его смене производится обновление генерируемых маршрутов на новый default-маршрут.
* Теперь модуль parser не зависит от модуля rkn, что позволяет подменять xml-файл выгрузки в директории /var/spool/zapret без организации выгрузки с портала РКН.
* Добавлен ключ "p" для модулей rkn и routing для принудительного выполнения их операций в командной строке.
* Генерация уведомления от самого ПО (не от нашего сайта) об истечении срока действия режима Trial перенесено с 5 на 8 утра.
* Увеличено число файлов для логов сервиса squid до 9.
* Исправлен баг, который при особых обстоятельствах работы модуля parser не останаливал его при обнаружении новой выгрузки.
* Исправлен баг, приводящий к сбросу работы модуля parser при включенной опции "Производить выгрузку реестра РКН каждый час".
* Исправлен баг, приводящий к зависанию сервиса apache при повышенной нагрузки http/https-запросов.
* Исправлен баг в модуле genfakezones, приводящий к краху запуска dns-сервиса на базе bind или unbound при появлении символа "обратный слэш" в домене ресурса. Рекомендуем обновить модуль genfakezones на своих dns-серверах с данного обновления.

4.7 (19.04.2017)

* Отказ от домена zapret.local за пределами сервера ZS. Теперь данный домен не нужно прописывать в своем dns-сервисе, чтобы производилось перенаправление на страницу-заглушку или отображался логотип компании на ней. Для входа в web-интерфейс ZS достаточно прописать домен zapret.local локально на своем ПК, с которого будет осуществляться вход.
* Добавлена возможность указания url своей страницы-заглушки в web-интерфейсе ZS
* Улучшен алгоритм модуля "resolver" для поиска ip-адресов у запрещенных доменов. Теперь данный модуль сам опрашивает dns-сервера без использования штатной команды nslookup, которые указаны в файле /etc/resolv.conf. Это ускорило работу модуля, а так же позволяет делать опрос с нескольких dns-серверов за раз, чем ранее с одного.
* Если в момент работы модуля "parser" произвелась срочная выгрузка реестра, то модуль перезапустит свой процесс, чтобы приступить к обработке свежего xml-файл реестра.
* Добавлено дополнительное правило в iptables для контроля ресурсов типа "newcamd".
* Добавлена возможность удаления логотипа компании из БД ZS.
* Исправлен баг зацикливания модуля "resolver" при цикле опроса всех доменов запрещенных ресурсов, из-за чего происходила лишняя нагрузка на сервер ZS.
* Исправлен баг при чистке сведений об ip-адресах, которые находятся в БД более 180 дней, приводящая к остановки модуля "parser".

4.6 (21.02.2017)

* Разработан модуль "rkn", который объединяет работу модулей "check", "request" и "dumps". Теперь он проверяет каждые 5 минут параметр срочности на портале выгрузок

и в случае его изменения производится срочная выгрузка дампа реестра.
* Обязательная выгрузка теперь производится в 9 часов (утром и вечером) по московского времени, т.е. учитывается часовой пояс. Если у Вас часовой пояс +2, то обязательная выгрузка будет производиться в 11 часов утра и вечера.
* Запуск модуля "parser" теперь производится каждые 5 минут, если в этот момент он не выполняет свою работу.
* Исправлен баг с доступом по https к запрещенному ip-адресу
* Исправлена ошибка инициализации функции, которая проверяет наличие кириллицы у ресурсов типа "маска домена", в связи, с чем такие ресурсы исключались из фильтрации.

4.5 (02.02.2017)
* Добавлена дополнительная проверка на пустой символ при обработке url-ссылок
* Исправлен баг с кодировкой в письме уведомления об успешной выгрузке
* Переназначены права на запуск модуля check

4.4 (31.01.2017)
* В web-интерфейсе внедрена система доступа для пользователей
* Добавлена функция, позволяющая организовывать выгрузки реестра РКН каждый час
* Добавлена функция, позволяющая отправлять вместе с уведомлением на электронную почту файл дампа выгрузки
* Добавлен фикс, контролирующий изменения, произведенные на АС Ревизор от 19 января
* Модуль genfakezones теперь может генерировать конфигурационные файлы для unbound (подробнее описано в документации)
* Снижено количество отправляемых сообщений на электронную почту при невозможности получения лицензии с нашего сайта
* Модуль parser теперь тоже добавляет ip-адреса в таблицу маршрутизации при обработки реестра РКН, что позволяет быстрее реагировать на его изменения
* В логах модуля dumps теперь можно увидеть кому засчитывается выгрузка реестра РКН
* Добавлены дополнительные параметры expurls и expdmns для модуля getinfo, позволяющие делать выгрузки url-ссылок и доменов из БД
* Подправлены некоторые информационные сообщения в разных модулях

4.3 (02.01.2017)
* Алгоритм нахождения новых ip-адресов теперь работает постоянно, а так же дополнительно опрашивает dns-сервера от google.
* Добавлен просмотр реестра РКН в web-интерфейсе.
* Разработан новый функционал интеграции с местным dns-сервером на базе BIND для дополнительной надежности фильтрации (подробнее описано в нашей документации).
* Теперь модуль parser следит за не концептуальными tcp-портами и добавляет их автоматически в правила iptables.
* Добавлен функционал сохранения успешных выгрузок реестра РКН (включается в web-интерфейсе).

4.2 (06.12.2016)
* Переписан алгоритм обнаружения новых ip-адресов у запрещенных ресурсов на основе анализа характера их смены (ранее алгоритм с TTL показал себя менее эффективно).
* Добавлен на проверку неконцептуальный tcp-порт 8081.
* Добавлен дополнительный лог-файл /var/log/squid3/foundip.log для мониторинга обнаружения новых ip-адресов у запрещенных ресурсов.

4.1 (21.11.2016)
* Разработан новый экспериментальный алгоритм быстрого обнаружения новых ip-адресов у запрещенных ресурсов на основе записи TTL.
* Часть функционала модуля routing было перенесено в модуль resolver, в связи с чем

удалось избавиться от периодичной 100% загрузки сервера от этого модуля.
* Теперь модуль routing проверяет таблицу маршрутизации на корректность только в 4:30 ночи или когда были внесены изменения в черном/белом списках, а не при каждом его запуске.
* Подкорректированы параметры сервиса mysql для уменьшения потребления памяти.
* Переписан скрипт контроля за утечкой памяти сервиса SQUID, который позволит более гибко контролировать данный процесс.
* Мелкие исправления в модуле redirector в частности формирования лог-файла.

4.0 (01.11.2016)
* Добавлен модуль SNI, позволяющий отказаться от подмены сертификата в связи, с чем мы и изменили мажорную версию нашего решения. Теперь при ssl-соединении с сервером ZapretService будет смотреть на домен, указанный в сертификате. Если домен присутствует в реестре РКН, то такое соединение будет сбрасываться.
* Добавлен новый список ssl-net для ipset, где будут добавляться подсети для проверки https-трафика. В связи с чем список ssl был переименован в ssl-ip.
* Отключены бинарные логи сервиса mysql для повышения эффективности дисковой подсистемы.
* Доработана обработка url-ссылок по маске домена формата "*.domain.ru"

3.5 (13.10.2016)
* Оптимизирован модуль "resolver". Теперь данному модулю достаточно всего 4 потока для выполнения своей задачи, но при желании количество потоков все так же можно поменять в разделе "Настройки"
* Исправлена обработка ресурса типа домен в функционале "Белый список". Ранее не всегда корректно исключался из фильтра внесенный домен
* В раздел "Статистика" добавлен новый график по мониторингу загрузки CPU

3.4 (05.10.2016)
* Добавлен функционал "Белый список"
* Добавлена дата в заголовок оповещения
* В некоторых случаях неправильно обрабатывались фигурные скобки и символ | в url-ссылках запрещенных ресурсов
* В web-интерфейсе добавлена возможность менять количество потоков для модуля "resolver"

3.3 (21.09.2016)
* В web-интерфейсе добавлено отображение данных о готовом xml-файле запроса для РКН
* Модуль "parser" теперь начинает свою работу, только если дамп реестра РКН был изменен
* Модуль "resolver" при нахождении нового ip-адреса для проверки сразу добавляет его в таблицу маршрутизации для оперативного внесения его в OSPF
* Добавлены отдельные правила в iptables для сетей 52.28.0.0/16, 52.29.0.0/16, 52.57.0.0/16 и 52.58.0.0/16, которые используют сайты по игровым автоматам
* Количество потомков модуля "redirector" снижено до 15 для уменьшения нагрузки на память сервера, в связи с ранней оптимизацией самого модуля
* Добавлены мелкие доработки по обработке русских символов в доменах

3.2 (26.08.2016)
* Исправлен обработчик доменов, у которых присуствует точка как последний символ
* Добавлен временный фикс, убирающий подмену сертификата у ресурса «www.ya.ru» (запрещенный ресурс «slotomaniya.su» иногда «резолвит» ip-адрес 213.180.193.3, который принадлежит домену «www.ya.ru»)

3.1 (13.08.2016)
* Исправлен обработчик для url-ссылок типа "https://37.220.4.154" и с русскоязычными символами

3.0 (10.08.2016)

* Заменен экспериментальный функционал по борьбе с сайтами, которые активно используют технологию CDN (частая смена ip-адреса), на улучшенный и доработанный (новый модуль «resolver»)
* Небольшая рекомендация: на сервере с ZapretService в файле /etc/resolv.conf необходимо указать ip-адрес Вашего DNS-сервера, который Вы даете своим абонентам (особенно для «Ревизора»), чтобы ZapretService мог оперативно контролировать ресурсы с технологией CDN
* Переработан алгоритм обработки реестра под новые рекомендации РКН (памятка оператора 4.7)
* Добавлена экспериментальная поддержка фильтрации ресурсов по маске домена (новое требование РКН)
* Улучшено взаимодействие с сервисом РКН. Ранее у некоторых наших клиентов возникала ошибка Timeout при отправки запроса на сервис РКН
* Добавлено слежение за не стандартными tcp-портами сайтов: 81,8001,16869

2.4 (10.06.2016)

* Добавлен экспериментальный функционал по борьбе с сайтами, которые активно используют технологию CDN (частая смена ip-адреса)
* Страница-заглушка выдает http-статус 451, вместо 200 (необходимо для системы "Ревизор")
* Добавлены новые фильтры для обработки "корявых" url-ссылок
* Добавлено «слежение» за https-ссылками сервиса Youtube (экспериментальный функционал)
* Исправлена глупая орфографическая ошибка на странице "Статистика"
* Оптимизирован запуск модулей за счёт упрощения системы очистки БД

2.3 (27.04.2016)

* Добавлена возможность загрузки уже готовых файлов для запроса в РКН вместо PCKS#12-сертификата
* Добавлена возможность загрузки логотипа компании для страницы блокировки
* Создан модуль "stat" для сбора статистики по серверу (время запуска - каждый час)
* Добавлен раздел "Статистика" в web-интерфейсе, в котором отображатся графики на основе данных модуля "stat"
* Добавлен функционал включения/отключения обработки https-трафика сервиса Youtube.
* Переработаны файлы модулей. Теперь их можно запускать вручную как обычные программы без указания интерпретатора php
* Файлы для запроса в РКН и дамп реестра теперь располагаются в папке /var/spool/zapret
* Исправлено обнуление файлов запроса для РКН, если во время их генерации возникала какая-либо ошибка
* Модифицирован темплейт /etc/zabbix/zs_template.xml для сервиса zabbix в связи со сменой местоположения файла дампа реестра на сервере

2.1 (28.03.2016)

* Переработан web-интерфейс: теперь он стал намного приятнее и адаптирован под экраны мобильных устройств
* Убрана колонка "результат" в таблице на главной странице web-интерфейса: данную информацию можно узнать, нажав на статус модуля
* Добавлен новый функционал "Черный список"
* Добавлена возможность отключить уведомления о загрузки дампа с сервиса http://vigruzki.rkn.gov.ru/
* В модуль getinfo добавлена возможность узнать дату последней выгрузки с сервиса http://vigruzki.rkn.gov.ru/
* Изменен порядок запуска модуля routing: теперь он выполняется каждые 5 минут для

быстрого реагирования на изменение ip-адресов у запрещенных ресурсов

1.3 (21.02.2016)

* Переработан модуль parser: обработка дампа начинается с конца. Теперь доступ к новым запрещенным ресурсам будет блокироваться быстрее
* Оптимизирован метод определения ip-адресов в модуле parser. Теперь время работы модуля сократилось на 60%
* Добавлены конфигурационные файлы для сервиса zabbix-agent

1.2 (11.02.2016)

* Добавлена загрузка маршрутов из базы при старте OS
* Разработан свой кэш в модуле фильтрации http/https
* Создан модуль getinfo
* Мелкие изменения в параметрах сервисов sysctl, mysql и SQUID

1.1 (21.09.2015)

* Мелкие исправления в модулях parser и routing

1.0 (29.07.2015)

* Выпуск первой версии