Компания «Риланс»

RProxy

Система управления доступом

к ресурсам сети Интернет

ТЕХНИЧЕСКАЯ ДОКУМЕНТАЦИЯ

Оглавление

Термины и определения

Термин	Значение
Интернет	Всемирная система объединённых компьютерных сетей, построенная на использовании протокола IP и маршрутизации пакетов данных.
Система	Система управления доступом к ресурсам сети Интернет
Клиентский компьютер	Компьютер пользователя, запросы которого обрабатывает Система
Кэширование	Сохранение прокси-сервером получаемых файлов, с целью их предоставления их локальных копий при повторном запросе
Кэш	Локальные копии файлов, полученные при кэшировании

1. Введение

1.1. Общее описание

Система управления доступом к ресурсам сети Интернет (далее Система) представляет собой полнофункциональный непрозрачный кэширующий прокси-сервер, работающий под управлением операционных систем Windows и Linux.

Система имеет следующий **функционал**:

- управление доступом пользователей к запрашиваемым Интернет-ресурсам на основании установленных администратором правил;
- антивирусная проверка трафика средствами бесплатного антивирусного модуля clamav или Антивируса Касперского;
- возможность ограничения потребляемого пользователем объема трафика за определенный промежуток времени (установка лимитов);
- подсчет объема потребленного трафика по пользователям, дням и категориям сайтов (ведение статистики);
- оповещение администратора о попытках нарушения установленных им правил доступа;
- мониторинг активности пользователей при работе с Интернет-ресурсами.

1.2. Возможности

Система имеет следующие возможности:

1. Управление с помощью веб-интерфейса.

2. Антивирусная проверка трафика антивирусным модулем (clamav или Антивирус Касперского).

3. Кэширование запросов.

4. Проверка HTTPS-трафика.

5. Система управления доступом к Интернет-ресурсам на основе правил, в которых может быть использовано сочетание следующих параметров:
   - IP-адрес клиентского компьютера;
   - логин пользователя (поддерживаются схема basic и авторизация в Active Directory, протоколы NTLM и Kerberos);
   - DNS-имя клиентского компьютера;
   - доменная группа пользователя в Active Directory;
   - тематика ресурса (33 предустановленные категории);
   - адрес ресурса (URL);
   - часть адреса ресурса;
   - расширение запрашиваемого файла;
   - тип содержимого (content type) запрашиваемого файла;
   - HTTP-метод;
   - максимальный размер запрашиваемого файла;
   - время работы правила.

6. При принятии решения об отнесении запрашиваемого ресурса к определенной категории используются следующие методы:

- поиск в собственных базах данных (более 40 миллионов сайтов);
- анализ адреса ресурса (URL);
- лингвистический анализ текста (поиска характерных словоформ) с поддержкой всех русских кодировок.

7. Регулярное автоматическое обновление баз данных сайтов и терминов анализатора текста.

8. Установка лимитов на объем скачиваемого трафика с использованием сочетания следующих параметров:
- IP-адрес клиентского компьютера;
- логин пользователя;
- DNS-имя клиентского компьютера;
- временной интервал (месяц, неделя, день);

9. Предоставление статистических отчетов с возможностью выборки и группировки по следующим данным:
- IP-адрес клиентского компьютера;
- логин пользователя;
- DNS-имя клиентского компьютера;
- DNS-имя сервера;
- поисковый запрос;
- группа (отдел);
- тематика сайта;
- временной интервал (год, месяц, неделя, день, произвольный диапазон);

10. Назначение для всей Системы либо для конкретного правила доступа ответственного лица, получающего уведомления о попытках нарушения установленных правил.

11. Назначение группе пользователей или клиентских компьютеров (например, отделу) ответственного лица (например, начальника отдела), имеющего возможность просматривать статистику и получать уведомления о событиях, связанных с членами данной группы;

12. Импорт списка пользователей из Active Directory;

13. Предоставление пользователю его текущих статистических данных (имеющиеся ограничения, текущее потребление трафика и т.д.).

1.3. Преимущества и достоинства

К преимуществам и достоинствам Системы относятся:
- низкие системные требования;
- высокая скорость обработки запросов;
- русскоязычный веб-интерфейс;
- ориентация на русский сегмент сети Интернет;
- поддержка всех русских кодировок;
- работа с пониженными привилегиями (не от root);
- проверка HTTPS-трафика;
- отсутствие ограничения на количество правил доступа, предоставляющее возможность максимально гибкой настройки Системы;

- возможность работы в режиме мониторинга, т.е. без каких-либо запретов, с последующим предоставлением отчетов о тематике посещаемых пользователями сайтов;
- возможность управления и получения отчетности с использованием групп объектов, объединенных по определенному признаку (например, отделы предприятия);
- возможность использования различных методов авторизации (поддерживаются схема basic и авторизация в Active Directory, протоколы NTLM и Kerberos) одновременно;
- интеграция с Active Directory (возможность построения правил доступа на основе доменных групп, импорт списка пользователей);
- мощная система построения отчетов с возможностью группировки;
- предоставление отчета о поисковых запросах пользователей;
- гибкая система настройки оповещений с возможностью запуска пользовательских программ в качестве реакции на возникновение событий.

1.4. Тематические категории

Система имеет следующие предустановленные категории:

- сайты содержащие вредоносный код (вирусы);
- порно и эротические сайты, секс-шопы;
- юмористические сайты (анекдоты, шутки, розыгрыши, комиксы);
- музыка и танцы;
- сайты о кино (продажа и обзоры кинофильмов, кинотеатры, киноафиши, сайты киноактеров, аниме, мультфильмы);
- игры (продажа и обзоры игр, online-игры, online-казино);
- спортивные сайты;
- сайты о природе (животные, охота, рыбалка);
- книги, литература;
- рефераты, дипломные работы, шпаргалки;
- варез (торренты, cracks, serials, hacking, p2p);
- путешествия и туризм (туристические агентства, отели, санатории, пансионаты);
- сигареты и алкоголь;
- медицина (клиники, продажа медикаментов, препараты и методики увеличения различных частей тела);
- автомобили;
- сайты знакомств;
- коллекции картинок, скринсэйверов, обоев для рабочего стола, постеров;
- женские сайты (косметика, парфюмерия, украшения, макияж, мода, белье);
- сайты по поиску работы;
- чаты и irc;
- полифония (мелодии, игры и картинки для сотовых телефонов);
- кулинария (рецепты, бары, рестораны);
- гороскопы, эзотерика, магия;
- электронные поздравительные открытки;
- отдых (дайвинг, бильярд, боулинг, ночные клубы, хобби, коллекционирование);
- социальные сети;
- развлекательные сайты (блоги, развлекательные порталы, домашние странички);
- почтовые web-сервера;
- открытые прокси-сервера и web-анонимайзеры;
- баннеры и счетчики;
- антисоциальные сайты (аборты, изготовление наркотиков и взрывчатых веществ, способы самоубийства, саентология, экстремизм);

- сервера сервисов мгновенного обмена сообщениями (ICQ, AOL Instant Messenger, MSN Messenger, Yahoo Messenger, Google Talk, Rambler ICQ, Mail.ru Agent, Jabber);
- "белые" сайты (kernel.org, squid-cache.org, microsoft.com и т.д.).

2. Требования и установка

2.1. Аппаратные и программные требования

Аппаратные требования:

- необходимая мощность процессора зависит от количества подключений и обрабатываемых запросов, в минимальном варианте соответствует требованиям операционной системы;
- 50-750 Мб свободной оперативной памяти (объем потребления зависит от количества используемых тематических категорий, методов анализа и антивирусного модуля);
- 250 Мб свободного места на жестком диске.

Программные требования:

- Linux (ядро 2.6.x, glibc 2.7 и выше);
- Windows Server 2003 R2 и выше;
- Windows XP SP2 и выше - только для локального тестирования (XP имеет ограничение на 5 одновременных подключений);
- Windows 7 – только для тестирования.

2.2. Установка приложения

Установка приложения производится стандартным для операционной системы образом:

- Windows: msi-инсталлятор (перед запуском установить Microfost Visual C++ SP1 Redistributable Package)
- Rpm-based Linux (RedHat, Fedora, Mandriva, SuSE): rpm -i rproxy-1.0-xxxx.i386.rpm
- Deb-based Linux (Debian, Ubuntu, AltLinux): dpkg –i rproxy-1.0.xxxx.i386.deb

Все файлы приложения располагаются в каталоге установки:

- C:\Program Files\RProxy (Windows по умолчанию)
- /usr/local/rproxy (Linux по умолчанию)

В дистрибутив включена тестовая лицензия на 5 IP-адресов сроком действия один месяц (лицензия на большее количество предоставляется по запросу на адрес sales@relans.ru).

3. Конфигурация

Конфигурационный файл rproxy.conf по умолчанию расположен в папке установки и имеет формат ini-файла. При указании значений:

- в качестве разделителя используется запятая;
- в качестве положительных значений параметров логического типа могут быть использованы yes, y, on, 1, true, отрицательных no, n, off, 0, false;
- адреса серверов указываются без протокола, домен верхнего уровня включает в себя домены нижних уровней;
- в списке адресов для обозначения всех интерфейсов системы возможно использование символа *;
- в качестве значения параметра допустимо указание имени файла, содержащее значения по одному в строке;
- при указании размеров файла возможно использование единиц измерения (Kb, Mb или Gb).

Секции и параметры конфигурационного файла приведены в таблице 1.

Таблица 1 – Секции и параметры конфигурационного файла

Параметр	Формат	Описание	По умолчанию
Секция **common** (Общие параметры)			
listen	Список адресов	Адрес и порт, которые использует процесс прокси-сервера.	*:12345
dir	Имя каталога	Каталог установки. Значение также передается в переменную $dir, которая используется для указания относительных путей.	Linux: /usr/local/rproxy Windows: каталог, из которого запущен процесс
hostname	Строка	Внутреннее имя сервера	rproxy
ctlsocket	Номер порта	Порт на локальном интерфейсе, используемый для передачи управляющих команд процессу прокси-сервера	12346
connect_ports	Номера портов	Порты, к которым разрешен метод CONNECT через прокси-сервер	443, 5190
peer_address	IP-адрес:порт	Адрес и порт следующего прокси-сервера в цепочке	
temp_dir	Имя каталога	Каталог для хранения временных файлов	$dir\tmp

stat_enable	Логический	Необходимость сбора статистических данных	yes
stat_userid	Выбор	Данные для идентификации пользователя на странице статистики. Возможные варианты выбора: ip (IP-адрес), login (логин), dns (DNS-имя компьютера), client (пользователь)	ip
dns_domain	Строка	Локальный домен, значение добавляется к DNS-именам клиентских компьютеров	
mail_domain	Строка	Почтовый домен, значение добавляется к адресам рассылки уведомлений, если они указаны без символа @	
direct_urls	Список	Список серверов, доступ на которые осуществляется напрямую, т.е. не через peer_address	
unlimited	Список	Список серверов, для которых не ведется статистика посещений и, как следствие, трафик которых не учитывается в лимитах	
Секция **auth** (Авторизация)			
default_scheme	Выбор	Схема авторизации, используемая по умолчанию. (см. Схемы авторизации)	none
realm	Строка	Текст, отображаемый в заголовке диалогового окна basic-авторизации	Proxy Authorization
unauth_urls	Список	Список серверов, доступ на которые осуществляется без авторизации	
smb_servers	Список IP-адресов	Список IP-адресов контроллеров домена (необходим только для настройки протокола авторизации NTLM на Linux)	
Секция **av** (Антивирус)			

engine	Выбор	Используемый антивирусный модуль, доступные значения: none – не используется; clamav – ClamAV (Clam AntiVirus); kav – Антивирус Касперского. После изменения значения параметра необходим рестарт прокси-сервера (см. Антивирусная проверка).	none
behavior	Выбор	Поведение прокси-сервера в случае невозможности проверки полученного файла антивирусным модулем, доступные значения: stop – не возвращать файл пользователю; pass – пропустить без проверки.	pass
max_check_size	Размер файла	Максимальный размер файла, который будет передан на проверку антивирусному модулю	100Mb
quarantine_dir	Имя каталога	Каталог «антивирусного карантина», в котором сохраняются копии зараженных файлов	$dir/av/quarantine
Секция **cache** (Кэш)			
enable	Логический	Необходимость кэширования	yes
cache_dir	Имя каталога	Каталог для сохранения кэша	$dir/cache
max_cache_size	Размер	Максимальный размер кэша	1Gb
max_object_size	Размер файла	Максимальный размер кэшируемого файла	512Kb
not_cache_ext	Список	Расширения файлов, которые не сохраняются в кэше	asmx, asp, aspx, cgi, do, php, php4, php5, pl, shtml
Секция **db** (База данных)			
engine	Выбор	Используемая СУБД: sqlite (входит в дистрибутив), mysql, pgsql, mssql. После изменения значения параметра необходим рестарт прокси-сервера	sqlite

server	Имя или IP-адрес сервера	Сервер базы данных. Для СУБД sqlite указывать не нужно	
database	Строка	Название базы данных	rproxy
login	Строка	Логин для доступа к базе данных	
password	Строка	Пароль для доступа к базе данных	
Секция **dns** (DNS)			
dns_servers	Список	Список DNS-серверов (если параметр не указан, то используются системные)	
client_lookups	Логический	Необходимость получения ptr-записей компьютеров пользователей	no
ptr_servers	Список	Список DNS-серверов для получения ptr-записей компьютеров пользователей	
Секция **ldap** (LDAP)			
servers	Список	Список DNS-имен LDAP-серверов (контроллеров домена Windows)	
domain	Строка	Имя домена Windows	
login	Строка	Логин учетной записи, имеющей права для доступа на чтение к LDAP-каталогу (любой пользователь домена)	
password	Строка	Пароль учетной записи, имеющей права для доступа на чтение к LDAP-каталогу	
filter	Строка	Фильтр LDAP (без указания параметров DC, например CN=Users или OU=IT-otdel,OU=filial1)	
Секция **license** (Лицензии)			
keys_dir	Имя каталога	Каталог с файлами лицензий	$dir/data/licenses

check_clients	Имя файла	Файл с IP-адресами, которые участвуют в лицензировании (см. Лицензирование)	$dir/data/licenses/checked
auto	Логический	Необходимость автоматического формирования списка лицензированных IP-адресов	yes
dhcp_mode	Логический	Автоматическое обнуление один раз сутки списка лицензированных IP-адресов	no
Секция **logs** (Логи)			
logfile	Имя файла	Файл лога прокси-сервера	$dir/logs/rproxy.log
loglevel	Число	Уровень детализации лога. Не рекомендуется использовать значение отличное от 0.	0
append	Логический	Необходимость добавления в существующий лог, не обнуляя его на старте	yes
show_all	Логический	Необходимость записи всех событий	yes
banners	Логический	Необходимость записи запросов баннеров и счетчиков	yes
Секция **notify** (Оповещения)			
admin_address	email-адрес	Адрес администратора для отправки оповещений об окончании лицензии и других важных событиях	
smtp_server	IP-адрес:порт	Адрес smtp-сервера для отправки оповещений администратору	127.0.0.1:25
timeout	Число	Минимальное время в секундах, которое должно пройти между попытками отправки уведомлений	0
Секция **ssl** (Проверка HTTPS)			
enable	Логический	Необходимость проверки HTTPS-трафика	no

allow_untrusted	Логический	Разрешать доступ к сайтам, сертификаты которых не проходят проверку (подписаны не доверенным центром сертификации, истек срок годности, не соответствуют доменному имени и т.д.)	yes
trusted_urls	Список	Список серверов, HTTPS-трафик которых не должен проверяться	
Секция **webctl** (Веб-интерфейс)			
listen	Список адресов	Адрес и порт для доступа к веб-интерфейсу (логин/пароль по умолчанию admin/admin)	*:12347
language	Выбор	Язык веб-интерфейса: RU – русский, EN – английский	RU
logfile	Имя файл	Файл лога веб-интерфейса	$dir/logs/webctl.log
cron_logfile	Имя файла	Файл лога выполняемых действий	$dir/logs/execs.log
rss_len	Число	Количество записей в верхней области веб-интерфейса, предназначенной для отображения последних событий	5

4. Управление доступом

4.1. Правила доступа

Управление доступом основано на применении правил. Решение по каждому запросу (разрешить/запретить) выносится при срабатывании первого правила, таким образом порядок их указания имеет значение.

Правила формируются с использованием следующих параметров:

- данные о пользователе;
- данные о сайте;
- данные о ресурсе;
- HTTP-метод (GET, POST, HEAD и т.д.);
- размер запрашиваемого файла;
- время работы правила.

Параметры объединяются логическим оператором «И».

В качестве данных может выступать информация о:

- пользователе – логин (без указания домена при авторизации в Active Directory), IP-адрес (допустимо указание подсети в формате x.x.x.x/x или диапазона в формате x.x.x.x-x.x.x.x), DNS-имя компьютера или доменная группа (необходима настройка параметров доступа к LDAP-серверам, см. Конфигурация, секция ldap);
- сайте – категория, адрес сервера, часть URL;
- ресурсе – расширение или тип содержимого (content type).

Данные объединяются логическим оператором «ИЛИ».

В качестве значений могут быть использованы объекты следующих типов:

- пользователи;
- категории сайтов;
- адреса сайтов;
- типы содержимого;
- расширения файлов.

Объект представляет собой сочетание свойств и их значений. Объекты используются для удобства администрирования и восприятия. Все объекты имеют следующие свойства:

- Активно. Предназначено для временного отключения объекта, который в выключенном состоянии остается в конфигурации, но не учитывается при обработке правил.
- Название. Например, ФИО пользователя. Используется при отображении объекта в редакторах и статистических отчетах;
- Метка. Например, название отдела. Данное свойство не объединяет пользователей в одну группу, а только помечает их, что может быть использовано для фильтрации и при составлении отчетов.

Пользователь имеет следующие дополнительные свойства:

- администратор, который будет получать соответствующие уведомления;
- адрес электронной почты для отправки пользователю уведомлений;
- схема авторизации (см. Схемы авторизации);
- пароль (при использовании схемы авторизации basic);
- запрет пересылки запросов пользователя через следующий прокси-сервер в цепочке, т.е. разрешение прямого доступа.

Пользователь может включать в себя другие объекты аналогичного типа, т.е. являться групповым (например, отдел).

Правило доступа имеет следующие дополнительные свойства:

- активно, используется для временного отключения правила;
- администратор, который будет получать уведомления о сработке правила;
- исполняемый файл, который необходимо выполнить для рассылки оповещения;
- информация, которая будет предоставлена пользователю на странице блокировки.

Категория сайтов имеет следующие дополнительные свойства:

- порог чувствительности анализатора текста;
- информация, предоставляемая пользователю на странице запрета доступа;
- используемые методы блокировки (базы данных, анализ URL ресурса, временный список заблокированных сайтов, лингвистический анализ текста).

4.2. Лимиты

Ограничение объема предоставляемых пользователю данных (лимит) может быть установлено:

- на день;
- на неделю (с понедельника по воскресенье включительно);
- на месяц (с первое по последнее число месяца включительно);
- разово (ограничение будет действовать до тех пор, пока администратор не отменит запрет).

Ограничения определяются с помощью создания правил лимитов, которые могут быть применены к пользователю, логину, IP-адресу (подсети или диапазону) или DNS-имени компьютера.

Порядок указания правил имеет значение, т.к. потребленный пользователем трафик учитывается в первом правиле, содержащем его логин, IP-адрес или DNS-имени компьютера пользователя. Например, если в первым правилом указать лимит для подсети, а вторым для IP-адреса, входящего в эту подсеть, то второе правило никогда не сработает, т.к. трафик будет увеличиваться для первого правила. Таким образом, если необходимо установить один лимит для всех пользователей и другой для нескольких, то правило с исключениями должно находиться выше общего.

По умолчанию ограничение действует на каждого участника, но правило лимита также может быть групповым. В этом случае лимит устанавливается на всех участников правила суммарно. Т.е. обычное правило для, например, подсети означает «n мегабайт каждому IP-адресу из указанной подсети», а групповое «данная подсеть суммарно не должна потребить больше n мегабайт трафика».

Правило лимита имеет следующие дополнительные свойства:

- Администратор, который будет получать уведомления о срабатывании правила;
- Исполняемый файл, который необходимо выполнить для рассылки оповещения;

5. Дополнительная информация

5.1. Схемы авторизации

RProxy поддерживает следующие схемы авторизации:

- basic – запрос логина/пароля у пользователя при каждом запуске браузера;
- ad – прозрачная авторизация в домене Windows;
- ad/basic – попытка авторизации в домене Windows и использование схемы basic в случае неудачи.

Перечисленные варианты могут быть использованы в качестве схемы по умолчанию (значение параметра default_scheme секции auth конфигурационного файла). Параметр авторизации у клиентов по умолчанию имеет значение default, т.е. используется схема, указанная для всей системы.

Авторизация в Active Directory на Linux-серверах

Для использования авторизации в домене Windows на серверах под управлением ОС Linux прокси-серверу RProxy необходимы файлы krb5.conf и krb5.keytab, которые могут быть получены **одним** из следующих способов:

1. Скачать с сайта набор утилит makekeytab.zip, на компьютере под управлением серверной ОС Windows, который является членом домена, распаковать архив и выполнить с правами администратора домена скрипт makekeytab.vbs со следующими параметрами:

cscript makekeytab.vbs /dns:<DNS-имя сервера RProxy> /ip:<IP-адрес сервера RProxy> /mask:<Маска подсети> /dc:<IP-адрес контроллера домена>

Созданные файлы krb5.conf и krb5.keytab скопировать в каталог установки RProxy.

Для отмены изменений, произведенных makekeytab.vbs необходимо выполнить:

cscript makekeytab.vbs /u /dns:<DNS-имя сервера RProxy> /ip:<IP-адрес сервера RProxy>

2. На компьютере под управлением ОС Linux, который является членом домена Windows (установлен Samba-сервер), выполнить команды:

net ads keytab add HTTP

net ads keytab create

В каталоге установки RProxy создать ссылки, выполнив команду:

ln -s /etc/krb5.conf /usr/local/rproxy/krb5.conf

ln -s /etc/krb5.keytab /usr/local/rproxy/krb5.keytab

В конфигурационном файле Samba-сервера smb.conf указать:

[global]

kerberos method = secrets and keytab

ВНИМАНИЕ! Для корректной работы протокола Kerberos на сервере Linux также необходимо выполнение следующих условий:

1. Наличие в /etc/hosts строки:

<Локальный IP-адрес сервера> <Полное DNS-имя> <Имя хоста (hostname)>

, например

10.0.0.1 rproxy.relans.ru rproxy

2. Имя хоста (hostname) должно быть указано без домена и должно совпадать с NetBIOS-именем компьютера в домене Windows (имя хоста устанавливается с помощью команды sysctl, либо через конфигурационные файлы /etc/hostname, /etc/sysconfig/network и т.п.).

5.2. Антивирусная проверка

Во время загрузки антивирусного модуля поведение RProxy регламентируется параметром behavior (см. Конфигурация, секция av). По умолчанию значение параметра pass, т.е. некоторые запросы могут быть обработаны без проверки антивирусным модулем.

Clamav

В состав дистрибутива для Linux не входит антивирусный модуль clamav. Для возможности его подключения необходимо:

- установить пакет clamav из репозитория операционной системы;
- убедиться в том, что модуль libclamav.so находится в одном из каталогов /lib, /usr/lib, /usr/local/lib;
- настроить обновление антивирусных баз по расписанию (исполняемый файл freshclam);
- для того чтобы после обновления антивирусных баз их перечитывал модуль clamav в RProxy необходимо в конфигурационном файле /etc/freshclam.conf указать OnUpdateExecute /usr/local/rproxy/rproxy -C /usr/local/rproxy/rproxy.conf –a

Clamav поставляется в составе дистрибутива для Windows, который также включает антивирусные базы, актуальные на момент его сборки. Необходимо настроить расписание действия «Обновление clamav» (рекомендуется не реже одного раза в сутки).

Антивирус Касперского

Модуль Антивируса Касперского входит в состав дистрибутива для Linux и Windows без антивирусных баз, поэтому до его использования необходимо выполнить действие «Обновление Антивируса Касперского» и настроить его расписание.

5.3. Лицензирование

Лицензирование RProxy основано на подсчете уникальных IP-адресов компьютеров, для запросов с которых проводились проверки. Таким образом на привилегированных пользователей (см. Конфигурация по умолчанию) лицензии не используются.

Если параметр auto секции license установлен в yes, то администратору необходимо вручную внести IP-адреса в файл, указанный в параметре check_clients, в противном случае их список будет формироваться автоматически (во время работы RProxy список хранится в памяти и сохраняется на диск только при релоаде или рестарте).

Если параметр dhcp_mode секции license установлен в yes, то список лицензированных IP-адресов будет автоматически сбрасываться один раз в сутки.

Рекомендуется использовать данную опцию, если в сети используется DHCP, т.е. IP-адреса компьютеров пользователей периодически изменяются.

По окончании срока действия всех лицензий, а также для IP-адресов с порядковым номером больше допустимого в активной лицензии, прокси-сервер:

- не производит фильтрацию;
- перестает вести лог;
- не ведет статистику посещений сайтов.

Оповещение администратора по электронной почте, при условии указания параметров admin_address и smtp_server, производится при следующих условиях:

- использовано 90% текущей лицензии;
- до окончания лицензии с максимальным сроком действия осталось 20 дней;
- до окончания лицензии с максимальным сроком действия осталось 5 дней;
- все лицензии истекли.

Лицензия предоставляется в текстовом виде и может быть сохранена администратором в каталоге, указанном в параметре keys_dir секции license (по умолчанию каталог_установки/data/licenses) в файле с расширением lic, либо добавлена через репозиторий с помощью веб-интерфейса (пункт меню «Управление - Лицензии»). После окончания текущей лицензии новая будет активирована автоматически.

Лицензия для антивирусного модуля Лаборатории Касперского предоставляется в виде файла с расширением key, который должен быть сохранен в папку каталог_установки/av. После окончания текущей лицензии новая будет активирована автоматически.

В состав дистрибутива входит тестовая лицензия на 5 IP-адресов сроком действия один месяц (лицензия на большее количество предоставляется по запросу на адрес sales@relans.ru).

5.4. Ключи командной строки

Ключи командной строки исполняемого файла rproxy приведены в таблице 2.

Таблица 2 – Ключи командной строки

Ключ	Назначение
-l, --log	Лог-файла
-p, --listen	Занимаемый порт
-t, --ctl	Адрес локального управляющего сокета
-d, --debug	Уровень детализации лога
-C, --config	Конфигурационный файл
-g, --generate-config	Экспорт всей конфигурации прокси-сервера в файл
-v, --version	Просмотр версии приложения
-c, --check	Проверка текущей конфигурации

-m, --tmp	Действия со списками текущих блокировок: clear - сборосить, save - сохранить, load – загрузить
-a, --avreload	Отдать команду перечитать базы антивирусные модулю
-r, --reload	Перечитать конфигурацию
-R, --restart	Перечитать базы
-s, --status	Получить данные о текущем состоянии системы: db – количество записей в базах данных, block - блокировки, common – общая информация, all – все вышеперечисленные.
-q, --quit	Завершить работу
-h, --help	Показать помощь по ключам командной строки

6. Веб-интерфейс

Веб-интерфейс по умолчанию доступен на порту 12347 (URL доступа http://IP-адрес_сервера:12347 либо, при настройке использования RProxy в качестве прокси-сервера в браузере, http://rproxy:12347, логин/пароль admin/admin).

Страница статистики пользователя доступна по адресу http://IP-адрес_сервера:12347/user либо, при настройке использования RProxy в качестве прокси-сервера в браузере, http://rproxy:12347/user.

Разделы меню и их предназначение приведены в таблице 3.

Таблица 3 – Пункты меню веб-интерфейса

Параметр	Назначение
Конфигурация	Изменение параметров конфигурационного файла
Объекты	Создание и изменение объектов
Управление – Правила доступа	Создание и изменение правил доступа
Управление – Правила лимитов	Создание и изменение правил лимитов
Управление – Действия	Настройка расписания и запуск различных утилит и функций (стоп/старт прокси-сервера, обновления баз RProxy и антивируса, рассылка оповещений и т.п.)
Управление – Лицензии	Репозиторий лицензий
Управление – Импорт пользователей	Импорт списка пользователей с контроллеров домена Windows (каталога Active Directory)
Данные – Статус	Информация о текущем состоянии прокси-сервера
Данные – Кол-во записей	Информация о текущем количестве записей в базах данных фильтрации
Данные – Блокировки	Информация о текущем количестве блокировок по категориям и методам фильтрации
Данные – Статистика	Предоставление статистических отчетов с широкими возможностями фильтрации и группировки. Максимальный уровень детализации – сайты, посещенные пользователем за день
Данные – Поисковые фразы	Предоставление отчета о том, что искали пользователи на поисковых сайтах с возможностью выборки

Данные – Лимиты	Предоставление данных о текущем потреблении трафика пользователями применительно к установленным администратором правилам лимитов
Данные – Логи	Просмотр журналов событий прокси-сервера, веб-интерфейса, утилиты обновления и задач, запускаемых по расписанию

В последней колонке списков находятся пиктограммы, выполняющие следующие действия:

- включить/выключить;
- переместить выше;
- переместить ниже;
- удалить;
- редактировать.

Изменить местоположение строки можно также с помощью элементов, которые появляются при нажатии на ее номер.

Также внизу и вверху таблиц расположены элементы для выполнения следующих действий:

- добавление объекта в начало списка;
- добавление объекта в конец списка;
- удалить выбранные объекты;
- присвоить значение свойствам «Метка» и «Активно» выбранных объектов.

7. Конфигурация по умолчанию

После установки RProxy имеет следующие значения основных параметров и настройки по умолчанию:

- порт прокси-сервера: 12345
- порт веб-интерфейса: 12347 (URL доступа http://IP-адрес_сервера:12347 либо, при настройке использования RProxy в качестве прокси-сервера в браузере, http://rproxy:12347, логин/пароль admin/admin)
- страница статистики пользователя доступна по адресу http://IP-адрес_сервера:12347/user либо, при настройке использования RProxy в качестве прокси-сервера в браузере, http://rproxy:12347/user
- запрещен доступ к следующим категориям: порно, насилие, наркотики, варез, алкоголь и курение
- список доверенных сайтов, ресурсы которых не должны проходить проверку, доступен для редактирования через веб-интерфейс, меню «Объекты – Адреса сайтов – Доверенные сайты»
- привилегированных пользователей (IP-адреса, логины, DNS-имена компьютеров), запросы которых должны обрабатываться без фильтрации, можно указать через веб-интерфейс, меню «Объекты – Клиенты – Привилегированные пользователи»
- антивирусная проверка не производится (для включения необходимо указать антивирусный модуль в параметр engine секции av конфигурационного файла, или через веб-интерфейс пункт меню «Конфигурация - Антивирус»)
- авторизация не используется (для включения необходимо указать тип авторизации по умолчанию в параметре default_scheme секции auth конфигурационного файла, или через веб-интерфейс пункт меню «Конфигурация - Авторизация»)
- кэширование запрашиваемых ресурсов включено
- обновления баз производятся один раз в сутки с ресурса rproxy.ru/updates

Для получения уведомлений администратору рекомендуется указать свой адрес и сервер электронной почты в параметрах admin_address и smtp_server секции notify конфигурационного файла, или через веб-интерфейс пункт меню «Конфигурация - Оповещения»