

GateWall DNS Filter

Руководство администратора

Оглавление

Оглавление	2
Введение	3
Системные требования	3
Установка GateWall DNS Filter	4
Обновление и удаление DNS Filter	4
Регистрация GateWall DNS Filter	4
Политика лицензирования GateWall DNS Filter	5
Проверка доступности новой версии	5
Модуль администрирования DNS Filter	6
Вход в систему	6
Установка пароля на подключение	7
Работа с базой статистики GateWall DNS Filter	7
Использование сторонних БД	8
Восстановление базы данных	8
Настройка DNS	8
Пользователи и группы	9
Методы авторизации пользователей	11
Правила управления трафиком	11
Список исключений	12
Категории сайтов	13
Список категорий с пояснениями	13
Лог доступа и статистика запросов	19
Лог доступа	19
Статистика запросов	20
Статистика по категориям	20
Популярные категории	21
Механизм запроса категорий сайтов Entensys URL Filter Master Database	22
Отклонение запросов на разрешение доменного имени	23
Перенаправление запрещенных запросов	23
Варианты развертывания GateWall DNS Filter	23
Вариант 1	23
Вариант 2	24
Отображение дополнительной отладочной информации	25

Введение

GateWall DNS Filter представляет собой модуль перенаправления DNS-запросов (DNS Forwarder), снабженный дополнительными возможностями, такими как: определение категории запрошенного хоста, учет и ведение статистики обрабатываемых запросов, работа с правилами управления трафиком. Встроенная система правил позволяет управлять доступом в сеть Интернет на основе списков разрешенных/запрещенных хостов, времени, а также на основе категорий сайтов. GateWall DNS Filter не является шлюзовым решением, поэтому его можно использовать в крупных сетях, содержащих несколько тысяч пользователей.

GateWall DNS Filter состоит из следующих модулей:

- сервер,
- веб-консоль управления (DNS Filter Administrator),
- веб-сервер с поддержкой HTTPS и модулем статистики.

Сервер DNSFilter (процесс DNSFilter.exe) реализован в виде системной службы Windows. Сервер предоставляет возможность для разрешения DNS запросов пользователей, выполняет фильтрацию и ведет статистику запросов.

Консоль администрирования DNS Filter предназначена для управления сервером GateWall DNS Filter. Консоль общается с серверной частью по средствам веб-сервера с технологиями PHP + Ajax, что позволяет выполнять удаленное администрирование сервера. В консоли администратора доступна статистика по обработке DNS-запросов.

Встроенный веб-сервер используется для работы консоли управления, а также может быть использован для перенаправления HTTP-запросов пользователей. В этом случае, если пользователь пытается открыть в браузере запрещенный сайт, ему будет отображена страница с соответствующим информационным сообщением.

Системные требования

Сервер GateWall DNS Filter рекомендуется устанавливать на компьютер с операционной системой Windows XP/2003/Vista/2008/Windows7, подключенный к сети Интернет. Требования к аппаратной части компьютера зависят от интенсивности обрабатываемых DNS-запросов. Если интенсивность запросов составляет ~ 1000 запросов/сек, рекомендуется CPU 2 ГГц и ОЗУ порядка 2Гб. Объем дискового пространства определяет предельный размер базы данных статистики. Для крупных сетей рекомендуется наличие нескольких десятков Гб свободного места на диске.

Установка GateWall DNS Filter

Для установки GateWall DNS Filter запустите инсталляционный файл. Если GateWall DNS Filter устанавливается впервые, следует оставить опции Мастера установки по умолчанию. По умолчанию GateWall DNS Filter устанавливается в директорию “%Program Files%\Entensys\GateWall DNS Filter” (в дальнейшем %DNSFilter%). После установки перезагрузка компьютера не требуется.

После установки в списке системных служб появится две дополнительные службы: GateWall DNS Filter и GateWall DNS Filter DB Service. Первая служба представляет собой сам DNS Filter (процесс DNSFilter.exe), вторая используется для работы со встроенной базой данных (БД). В качестве встроенной БД используется FireBird. Обе службы будут запущены автоматически сразу после установки. Для удобства управления в системный трей будет помещена иконка агента , через контекстное меню которого можно запустить консоль администрирования, остановить или перезапустить сервер DNS Filter, а также получить доступ к файлу логов.

Обновление и удаление DNS Filter

Перед установкой новой версии рекомендуется удалить предыдущую версию DNS Filter, сохранив при необходимости файл настроек сервера (файл dnsfilter.xml из директории, в которую установлен DNS Filter) и дамп базы статистики. Удаление DNS Filter выполняется через соответствующий пункт меню «Пуск – Программы» или через консоль «Установка и удаление программ» в панели управления. При удалении в директории %DNSFilter% останется файл настроек сервера. Если использовалась сторонняя база статистики, база не будет удалена.

Регистрация GateWall DNS Filter

При первом подключении консоли администрирования появится диалог для регистрации с двумя доступными опциями: запрос демонстрационного ключа (триальная версия) и запрос полнофункционального ключа (ввод ПИН-кода). Запрос ключа выполняются online (протокол HTTPS), через обращение к сайту usegate.ru. При запросе полнофункционального ключа требуется ввести специальный пин-код, который выдается при покупке GateWall DNS Filter. Кроме того, при регистрации потребуются ввести дополнительную персональную информацию (имя пользователя латиницей, адрес электронной почты, страна, регион). Персональная информация используется исключительно для привязки лицензии к пользователю и никоим образом не используется вовне. После получения полного или демонстрационного ключа сервер DNS Filter будет автоматически перезапущен.

В демонстрационном режиме сервер GateWall DNS Filter будет работать 30 дней. При обращении в компанию Entensys можно запросить специальный ПИН-код для расширенного тестирования. Например, можно запросить демонстрационный ключ на три месяца. Повторный запрос демонстрационного ключа без специального ПИН-кода невозможен.

При работе DNS Filter периодически выполняется проверка статуса регистрационного ключа. Для корректной работы DNS Filter необходимо разрешить доступ в сеть Интернет по протоколу HTTPS. Это требуется для online проверки статуса ключа. В противном случае программа станет незарегистрированной.

Политика лицензирования GateWall DNS Filter

Лицензионный ключ GateWall DNS Filter не ограничивает количество обрабатываемых DNS-запросов. Ограничение касается только работы с пользователями. Так, если вы приобрели лицензию на 10 пользователей, вы сможете создать не более 10-ти различных пользователей. Соответственно и отчет (статистика запросов, общее количество запросов, количество заблокированных запросов, распределение запросов по категориям Entensys URL Filter) будет доступен только для 10-ти пользователей.

Лицензия на модуль Entensys URL Filter, предназначенный для работы с категориями сайтов, включена в лицензию на GateWall DNS Filter. Срок действия лицензии на Entensys URL Filter ограничен и составляет один год. По истечении срока действия лицензии online сервис Entensys URL Filter станет недоступен и фильтрация по категориям прекратит действовать.

Проверка доступности новой версии

В консоли администрирования, в меню «Лицензия» присутствует пункт «DNS Filter». При входе на эту страницу сервер DNS Filter формирует запрос на сайт производителя, запрашивая номер последней доступной версии. Если установленная версия оказывается младше той, которая доступна на сайте производителя, консоль администрирования отображает соответствующее сообщение. В этом случае администратор может скачать последнюю версию с сайта и установить ее. Проверка новой версии не приводит к автоматической переустановке GateWall DNS Filter.

Модуль администрирования DNS Filter

Модуль администрирования представляет собой веб-приложение, предназначенное для управления локальным или удаленным сервером GateWall DNS Filter. Для использования DNS Filter Administrator необходимо запустить службу DNS Filter, выбрав пункт «Запустить сервер DNS Filter» в меню агента. Запустить модуль DNS Filter Administrator можно и через пункт меню «Пуск – Программы». Для удаленного управления настройками, необходимо открыть браузер, набрать там адрес <http://192.168.0.1:8080>, где 192.168.0.1, IP-адрес того компьютера, на который установлен DNS Filter. Если подключиться удаленно не удастся, стоит проверить настройки антивирусов и фаерволлов.

Вход в систему

При запуске консоли администрирования открывается страница «Авторизация», на которой необходимо ввести имя пользователя и пароль. По умолчанию имя пользователя Admin, а пароль на подключение к DNS Filter не установлен.

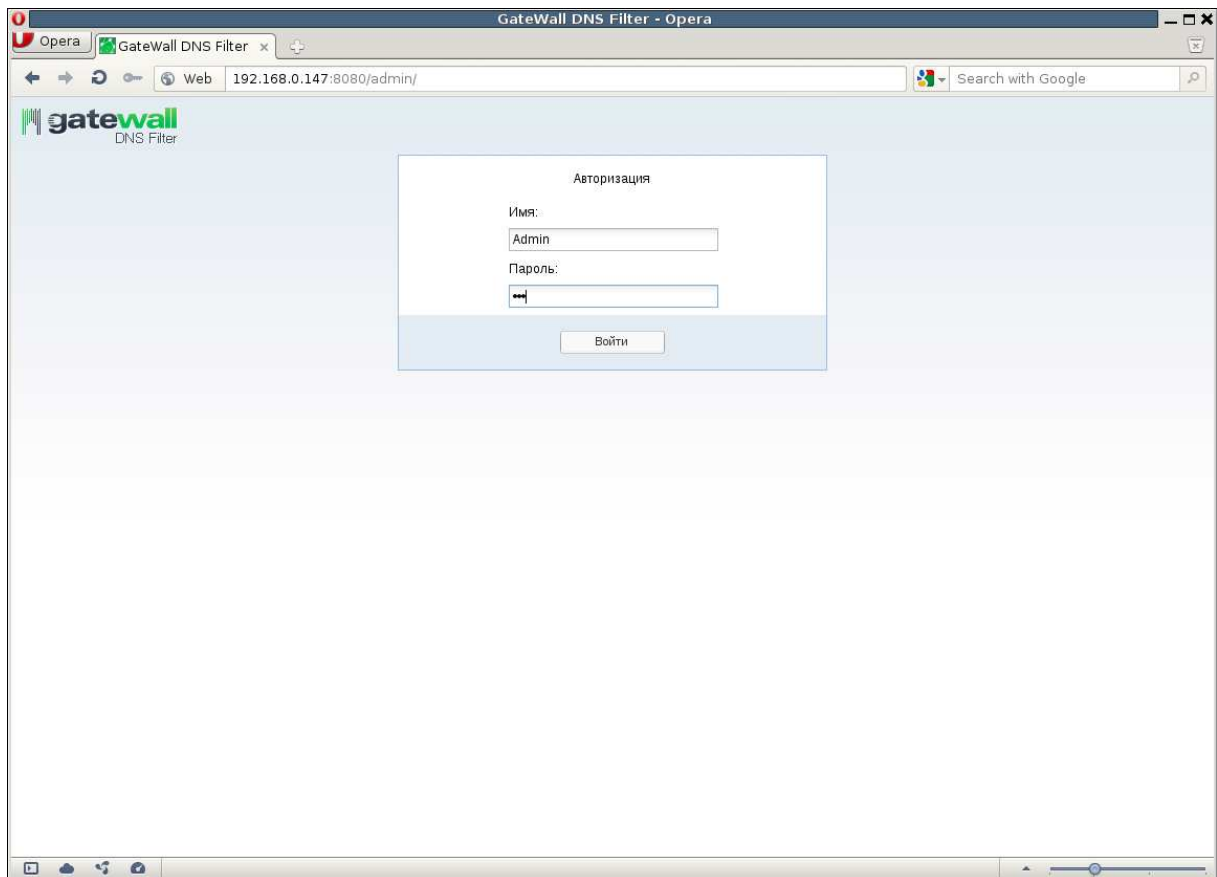


Рисунок 1. Вход в систему

Установка пароля на подключение

Установить «Логин/пароль» для подключения к серверу DNS Filter можно на странице «Настройки DNS», раздел «Основные настройки». Для вступления новых настроек в силу необходимо перезапустить сервер DNS Filter (пункт «Перезапустить сервер DNS Filter» в меню агента). После перезапуска сервера необходимо указать новые настройки и при подключении на странице «Авторизация».

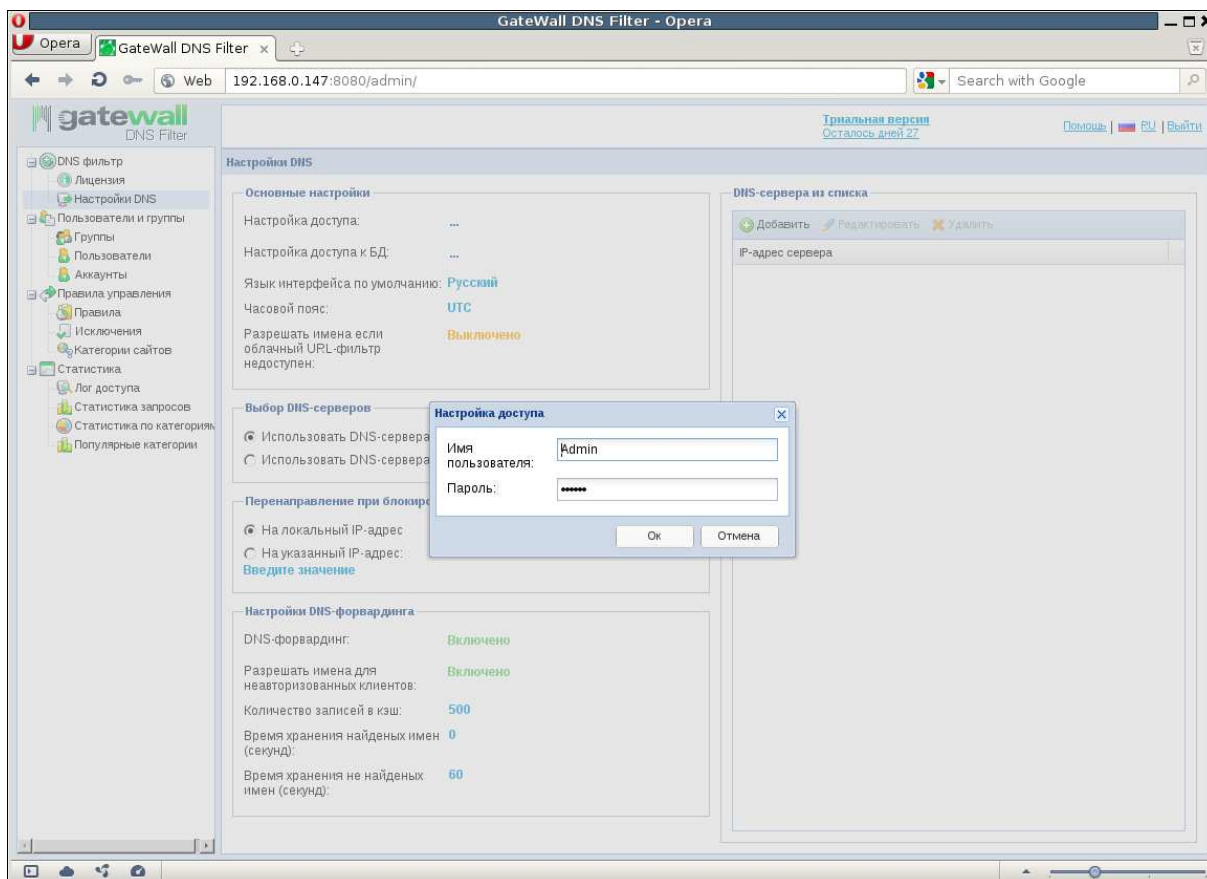


Рисунок 2. Установка пароля на подключение

Работа с базой статистики GateWall DNS Filter

Статистика DNS-запросов – запрашиваемый хост, время, результат запроса (разрешен или запрещен) – записывается сервером DNS Filter в специальную базу данных. Доступ к базе данных осуществляется через API-интерфейс, если используется встроенная БД, или через ODBC-драйвер, если используется сторонняя БД.

По умолчанию, используется встроенная база формата FireBird (файл %DNSFilter%\dnsfilter.fdb). Для работы с базой FireBird используется логин "SYSDBA" и пароль "masterkey".

Использование сторонних БД

Поддержка ODBC позволяет работать с базами практически любого формата (MS Access, MS SQL, MySQL). Для работы с базой MySQL в состав дистрибутива GateWall DNS Filter входит дамп базы данных с требуемой структурой. Дамп расположен в директории "%DNSFilter%\db_dumps". Для настройки GateWall DNS Filter на работу со сторонней базой данных необходимо выполнить следующие шаги:

- в разделе "Общие настройки – Настройка базы данных" в консоли администратора нужно указать логин и пароль для подключения к базе данных
- остановить службу GateWall DNS Filter (пункт "Остановить сервер DNSFilter" в меню агента)
- открыть файл настроек сервера (*%DNSFilter%\dnfilter.xml*) и в секции `<database />` выставить параметр `firebird = 0`
- в консоли Windows "Администрирование – Источники ODBC" нужно создать системный DSN (Data Source Name) с названием *DNSFILTER*, указывающий на нужную базу данных (MySQL, MS SQL)
- запустить службу GateWall DNSFilter

Примечание: По умолчанию, для DSN используется название DNSFilter. Это название можно изменить через параметр `dsn` раздела `<database />` файла настройки сервера.

Важно! При работе с MySQL требуется MySQL Connector версии 3.5.

Восстановление базы данных

При работе со встроенной базой данных (FireBird) GateWall DNS Filter может автоматически создавать новую, пустую базу статистики. Для этого достаточно остановить сервер DNS Filter и удалить файл базы статистики *%DNSFilter%\dnfilter.fdb*.

Если используется сторонняя база данных (`firebird="0"`) и при запуске GateWall DNS Filter не смог обнаружить соответствующий системный DSN, DNS Filter создаст базу данных формата MS Access и соответствующий DSN автоматически.

Настройка DNS

Разрешение имен в сервере DNS Filter обеспечивается за счет перенаправления DNS-запросов (DNS forwarding) на вышестоящий DNS-сервер. Ответы на DNS-запросы кэшируются в оперативной памяти, тем самым, повышая скорость разрешения имен при повторных обращениях. Отключить кэширование DNS можно, выставив параметр `dns_cache_enable="0"` в файле настроек сервера. Максимальное количество записей, помещаемых в собственный DNS-кэш, определяется параметром "Количество записей в кэш" раздела "Настройки DNS форвардинга". По умолчанию, собственный кэш может содержать не более 500 записей. Дополнительно на странице "Настройка DNS" можно задать такие параметры, как время жизни записи в кэш

(параметры "Время хранения найденных имен" и "Время хранения не найденных имен").

Настройка DNS в консоли администрирования доступна в разделе «DNS фильтр – Настройки DNS». В настройках («Выбор DNS-серверов») можно указать один или несколько DNS-серверов, к которым DNS Filter будет обращаться для разрешения клиентских запросов. По умолчанию, сервер DNS Filter будет использовать DNS-сервер, указанный в сетевых настройках компьютера, на котором он установлен.

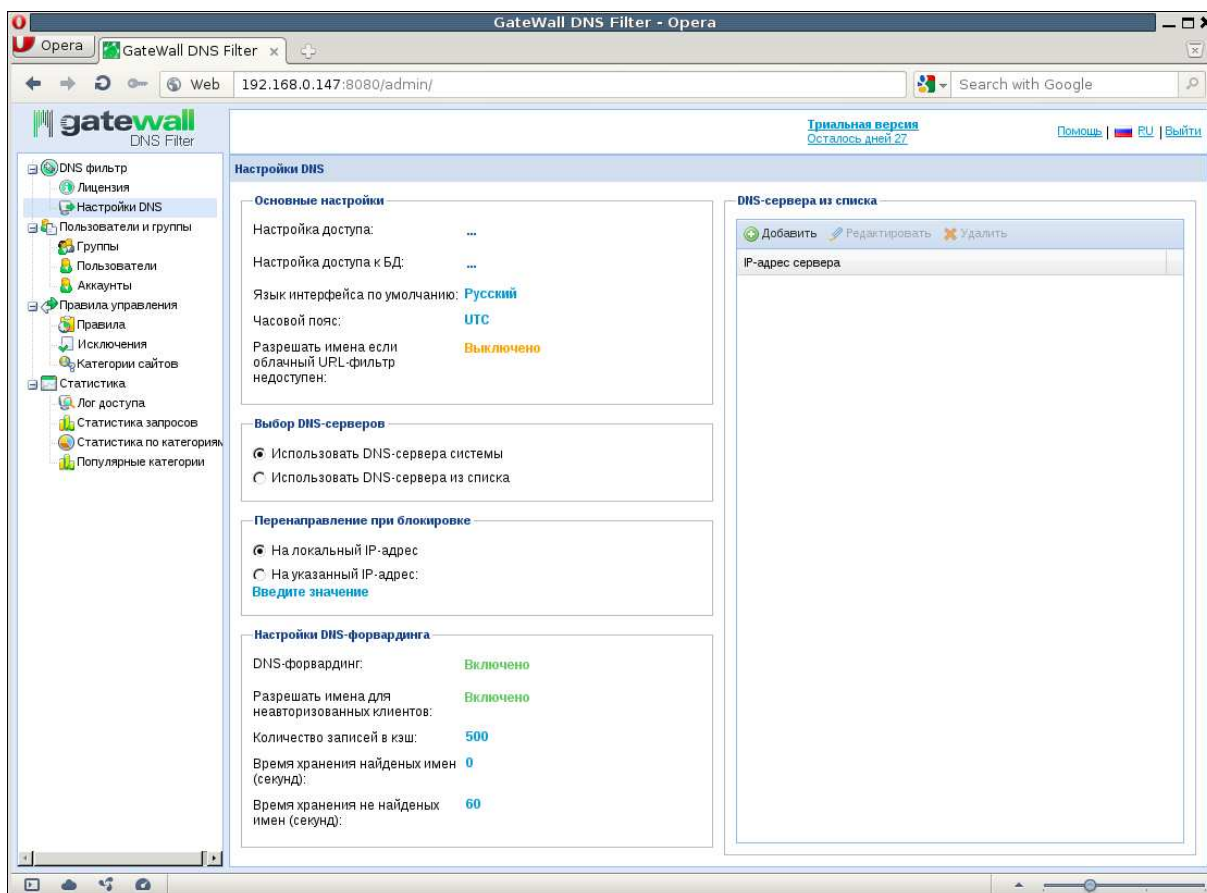


Рисунок 3. Настройка DNS

Пользователи и группы

Для предоставления возможности фильтрации DNS-запросов, а также для ведения статистики запросов, необходимо создать пользователей в GateWall DNS Filter. Для удобства администрирования пользователей можно объединять в группы по территориальному признаку или по уровню доступа. Логически наиболее правильным является объединение пользователей в группы по уровню доступа, поскольку в этом случае существенно облегчается работа с правилами управления трафиком. По умолчанию в DNS Filter присутствует единственная группа – default.

Создать нового пользователя можно через кнопку «Добавить» на странице «Пользователи и группы». Обязательными параметрами пользователя

являются: Имя, Тип авторизации, параметр авторизации (IP-адрес, диапазон IP адресов) и группа. По умолчанию все пользователи принадлежат к группе default. Имя пользователя в DNS Filter должно быть уникальным. Дополнительно в свойствах пользователя можно задать «Имя для входа в веб-интерфейс» и пароль, тем самым разрешив доступ пользователя к личной странице консоли управления, где могут задаваться индивидуальные правила управления трафиком. В DNS Filter 2.0 была добавлена возможность выставления уровня доступа для пользователя: «Пользователь», «Администратор группы» и «Администратор».

- "Администратор" имеет полные права на DNS Filter и может управлять всеми настройками программы.
- "Администратор группы" может управлять всеми правилами и подгруппами, которые находятся в его группе.
- "Пользователь" наследует правила родительской группы и может управлять только личными правилами.

Внимание! Правила унаследованные от группы пользователя не могут быть отредактированы самим пользователем группы, т.к. они имеют более высокий приоритет над правилами пользователя. Такие правила для группы НЕ будут отображены в веб-интерфейсе пользователя.

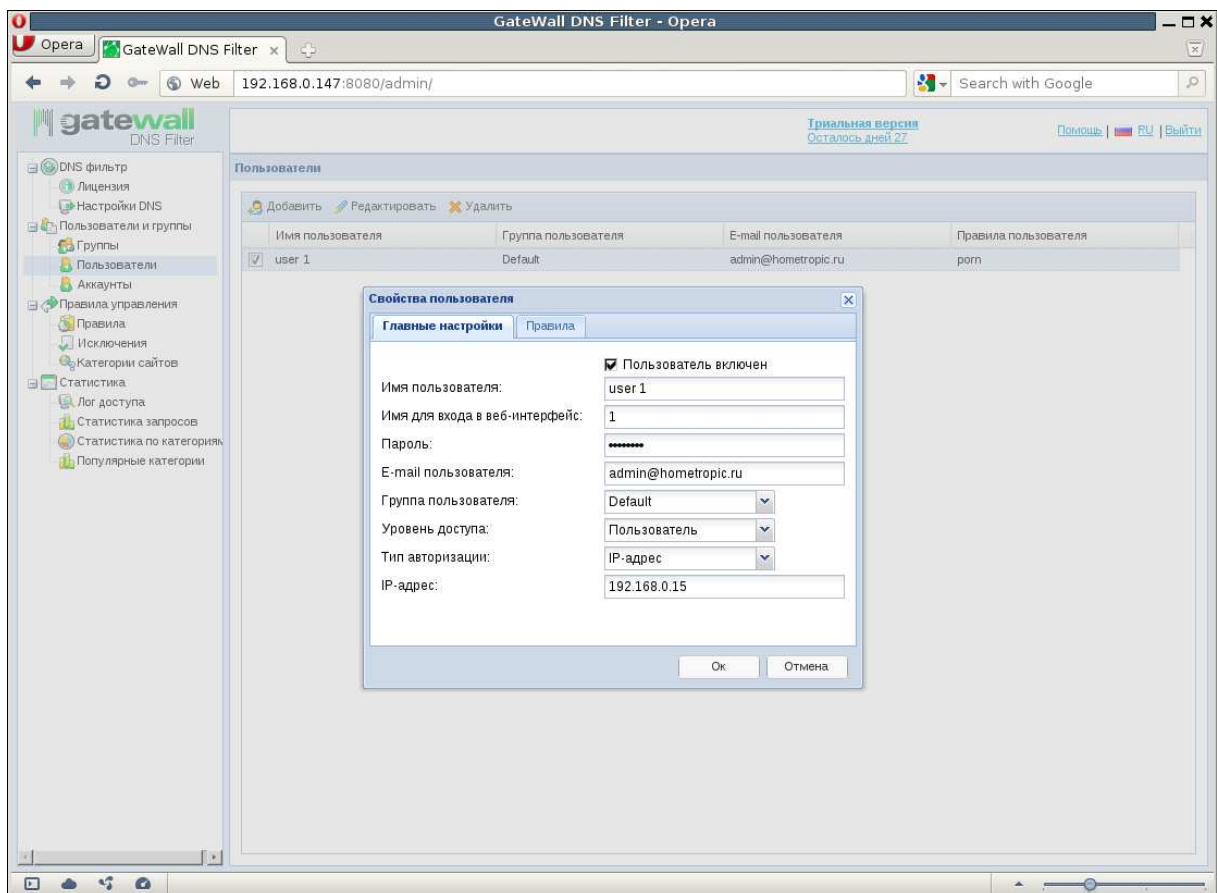


Рисунок 4. Пользователи и группы

Методы авторизации пользователей

Возможность фильтрации DNS-запросов предоставляется для всех пользователей совершающих запросы к DNS Filter. Если пользователь авторизован, то его запросы и статистика будут записаны на его имя. Если пользователь не был авторизован, его статистика НЕ будет записана в базу данных DNS Filter.

Поддерживаются два метода авторизации: по IP-адресу и по диапазону IP-адресов.

Правила управления трафиком

Правила управления трафиком предназначены для запрета доступа к сайтам в зависимости от категории или времени суток. Дополнительно предоставляется возможность фильтрации сайтов на основе черных и белых списков. В качестве условий в правилах можно указать время, день недели, одну или несколько категорий сайтов. Созданные правила управления трафиком должны быть применены к пользователям или к группе пользователей в DNS Filter.

Для запрета доступа к сайтам определенной тематики следует открыть раздел «Управление трафиком» – «Правила», создать новое правило и на второй странице диалога выбрать одну или несколько категорий сайтов.

Пользователи, которым заданы «Имя для входа в веб-интерфейс» и «пароль», могут создавать правила блокировки и исключения. Для этого им необходимо войти в веб-консоль управления по адресу <http://192.168.0.1:8080>, ввести логин и пароль, полученный от администратора сервера. В консоли управления можно создавать правила для категорий сайтов, доменных имен и временные ограничения, либо по комбинации этих условий. Если администратор сервера выставил для пользователя права доступа «Администратор групп», то этот пользователь может редактировать и управлять пользователями своей и всех дочерних подгрупп данной группы пользователей.

Внимание! Правила, унаследованные от группы пользователя, не могут быть отредактированы самим пользователем группы, т.к. они имеют более высокий приоритет перед правилами пользователя. Более того, они не будут отображены в веб-интерфейсе управления пользователя.

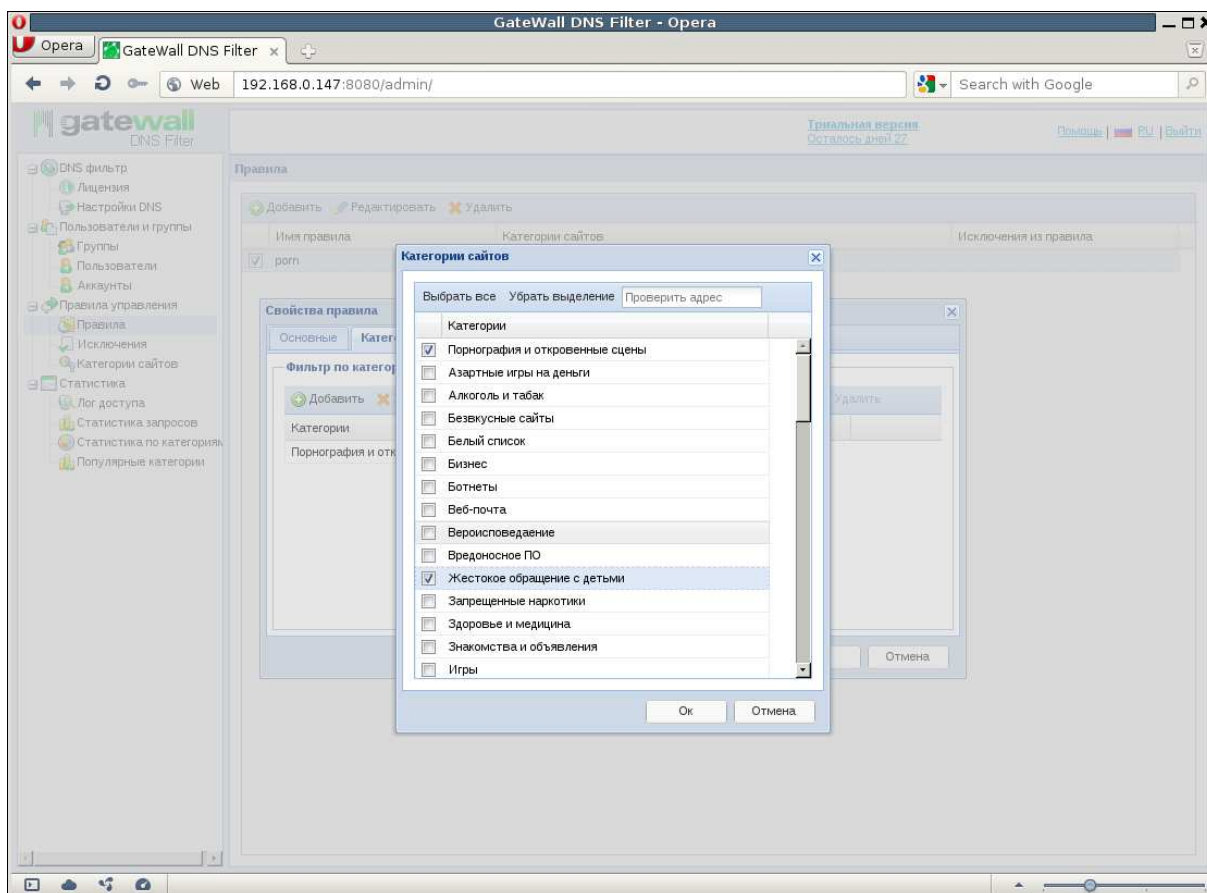


Рисунок 5. Правило управления трафиком

Список исключений

Список исключений (пункт "Исключения" дерева настроек) позволяет добавить один или несколько хостов в черный или белый список. Имена хостов, помещенных в список с действием "Разрешить", будут разрешаться всегда, даже если указанный хост принадлежит одной или нескольким категориям, доступ к которым запрещен. Имена хостов, помещенных в список с действием "Запретить" не будут разрешаться на валидный IP-адрес, независимо от наличия или отсутствия правил управления трафиком. Списки исключений глобальные, т.е. действуют для всех пользователей GateWall DNS Filter.

В файле настроек сервера имена хостов, указанные в списке исключений, помещаются в секции `<white_list />` и `<black_list />` раздела `<brightcloud />`. В этих секциях имена хостов можно указывать не полностью, дополняя часть символом `"*"`. В файле настроек сервера доступна еще одна секция, в которой можно указать хост, принадлежащий белому списку (действие "Разрешить"). Этот список указывается в секции `<exclude_domains>` раздела `<brightcloud />`. В этом списке указывается только полное доменное имя хоста.

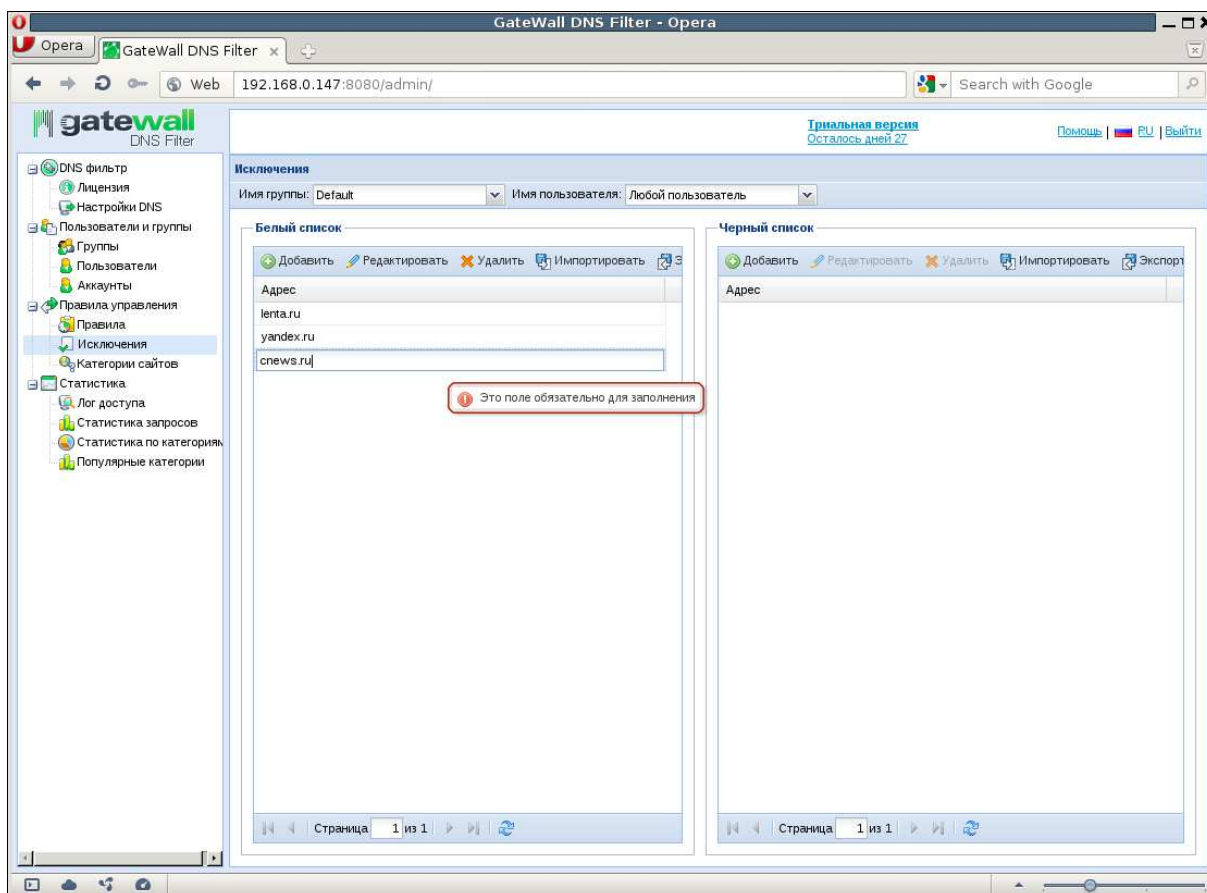


Рисунок 6. Список исключений

Категории сайтов

В этом разделе можно просмотреть, к какой категории сайтов относится конкретный URL, а также отправить запрос на изменение категории.

На данной странице для проверки категории сайта введите в окно URL и нажмите Enter. После выполнения запроса Вы увидите список текущих категорий, к которым принадлежит адрес.

Если Вы считаете, что данная информация не соответствует действительности, то в выпадающем списке можно выбрать категорию, которая, по Вашему мнению, лучше подходит для данного URL. Можно выбрать одну или две категории.

Далее остается только нажать кнопку "Запрос на смену категории" и Ваши пожелания будут приняты в рассмотрение.

Список категорий с пояснениями

- Азартные игры на деньги - Азартные игры и лотереи, сайты, предлагающие игру на реальные или виртуальные деньги. Информация и рекомендации по размещению ставок, участию в лотереях, азартных играх. Виртуальные казино и рискованные предприятия, спортивные пари

и тотализатор. Виртуальные виды спорта и вымышленные содружества, предлагающие крупные награды и требующие значительных ставок.

- Алкоголь и табак - Сайты, содержащие информацию по данной тематике, продвигающие либо продающие алкогольные напитки или табачные изделия, а также сопутствующие аксессуары.
- Безвкусные сайты - Сайты с оскорбительным или безвкусным контентом, таким как туалетный юмор, ужасный или даже пугающий контент: шокирующие изображения крови, ран или жестокого обращения животных.
- Белый список - Сайты, добавленные Вами в белые списки на вкладке "Исключения".
- Бизнес - Коммерческие компании, корпоративные сайты, деловая информация, экономика, маркетинг, управление и предпринимательство.
- Ботнеты - URL-адреса, IP-адреса, которые определены как принадлежащие к сетям программ ботов, запускающих сетевые атаки, а также могут включать спам-сообщения, DOS-атаки, SQL инъекции, появление промежуточного (незаконного) прокси, с целью перехвата чужого трафика и другие угрозы.
- Веб-почта - Сайты, предлагающие веб-интерфейс доступа к почтовым ящикам, почтовые клиенты.
- Вероисповедание - Сайты, связанные с нетрадиционными религиозными практиками ("культы"), которые считаются ложными, неортодоксальными, экстремистскими или принудительными, члены часто живут под руководством харизматического лидера.
- Вредоносное ПО - Установка нежелательного программного обеспечения на компьютере пользователя с намерением внести в систему изменения и позволить сторонним разработчикам мониторинг без согласия пользователя.
- Жестокое обращение с детьми - Сайты с изображениями или обсуждениями сексуальных или других оскорбительных действий с детьми
- Запрещенные наркотики - Обсуждение, ответственность за использование запрещенных или незаконных препаратов или наркотиков, таких, как героин, кокаин или других наркотических веществ. Информация по «легальным наркотикам»: клей, неправильное применение или злоупотребление лекарственными препаратами.
- Здоровье и медицина - Общее здоровье, фитнес, самочувствие, включая традиционные и нетрадиционные методы и темы. Медицинская информация о заболеваниях, лечение зубов, психиатрия, оптометрия и другие специализации. Больницы и врачебные кабинеты. Медицинская страховка. Косметическая хирургия.
- Знакомства и объявления - Сайты знакомств, направленные на установление личных отношений между людьми.

- Игры - Загрузка игр, видео игры, компьютерные игры, электронные игры, рекомендации и советы по ведению нечестной игры (получение кодов).
- Информационная безопасность - Компьютерная безопасность, Интернет-безопасность, форумы и Интернет-сообщества, обсуждения информационной безопасности.
- Искусство - Сайты с художественным содержанием, связанные с такими институтами как театры, музеи, галереи, танцевальные коллективы, фотографии, графические и цифровые ресурсы.
- Компьютеры и технологии - Сайты, которые содержат информацию, такую, как обзоры продуктов, обсуждения и новости о компьютерах, программном обеспечении, оборудовании, компьютерных услугах.
- Мода и красота - Журналы о моде, красоте, одежде, косметике, стиле.
- Нагота - Изображения обнаженных или полубнаженных тел, не обязательно сексуального характера, также может включать сайты, содержащие изображения с росписью по телу или галереи художественного фото. Данная категория также включает сайты, содержащие фотографии обнаженных людей.
- Насилие и жестокость - Сайты, которые содержат изображения, описание или пропаганду физического насилия против людей, животных. Сайты, содержащие ненормативную лексику.
- Недвижимость - Информация об аренде, покупке или продаже недвижимости или земельных участков. Рекомендации по покупке или продаже жилых помещений. Агентства недвижимости, услуги по аренде, переезду, улучшению жилищных условий.
- Неизвестная - Данных сайтов пока нет в базе данных.
- Некоммерческие и неправительственные организации - Сайты клубов, сообществ, союзов и некоммерческих организаций. Многие из них существуют в образовательных или благотворительных целях.
- Нелегальное ПО - Сайты, которые незаконно распространяют программное обеспечение, незаконные серийные номера, генераторы лицензионных ключей или защищенные авторским правом материалы (фильмы или музыка).
- Ненависть и нетерпимость - Сайты, которые пропагандируют угнетение людей на основании их расы, религии, пола, возраста, инвалидности, сексуальной ориентации или национальности.
- Новости - Новости и актуальные события дня. Также включает радиостанции и журналы, новостные онлайн газеты, заголовки новостей, новостные службы, порталы прогноза погоды.
- Обмен картинками - Сайты, принимающих цифровые фотографии и изображения, онлайн-фотоальбомы и фотообменники.

- Обмен мгновенными сообщениями - Сайты, которые позволяют войти в службы мгновенных сообщений, такие как ICQ, AOL Instant Messenger, IRC, MSN, Jabber, Yahoo Messenger и тому подобные.
- Образование - Сайты по поддержке учебных заведений и школ всех типов, включая дистанционное обучение. Включает в себя общие образовательные и справочные материалы, такие как словари, энциклопедии, интерактивные курсы, учебные пособия.
- Общая категория - Сайты, которые явно не попадают ни в какую категорию, например, пустые веб-страницы.
- Оружие - Продажа оружия, обзоры, описания оружия, например, огнестрельного и холодного оружия, предметов военного искусства, информация об их использовании, аксессуарах и модификациях.
- Отдых и свободное время - Информация, сообщества, форумы и публикации об отдыхе, времяпровождении и хобби, таких, как коллекционирование, авиатехника, туризм, кемпинг, скалолазание, искусства, ремесла, изделия, технологии, информация о животных и их содержании, включая породы и родословные, перевозку, выставки и сообщества по интересам.
- Переводчики - Сайты, на которых возможен онлайн-перевод сайтов на другие языки. Данные сайты могут использоваться для обхода заданных ограничений так просмотр страниц осуществляется с URL сайта онлайн-переводчика.
- Персональные сайты - Персональные сайты, созданные отдельными людьми или группами лиц, блоги.
- Пиринговые сети - Клиенты P2P доступа. Включает торренты, программы загрузки музыки.
- Поздравительные открытки - Сайты с поздравительными открытками.
- Поиск работы - Помощь в поиске занятости, инструментарий для поиска работодателя и подбора соискателя.
- Поисковые системы и информационные порталы - Сайты, предназначенные для поиска в Интернете новостей, изображений, каталогов и другого онлайн-контента.
- Покупка товаров - Интернет-магазины, каталоги, онлайн заказ, аукционы, рекламные объявления. Исключает торговлю товарами и услугами, относящимися к другим категориям, таким как здравоохранение и медицина.
- Политика - Сайты, продвигающие политические партии. Политическая пропаганда, информация о выборах, законодательстве или лоббировании. Также включает в себя сайты, которые предлагают правовую информацию.
- Половое воспитание - Информация о процессе размножения, половое развитие, правила безопасного секса, болезни, передающиеся половым

путем, сексуальность, регулирование рождаемости, советы и товары для улучшения сексуальной жизни, контрацептивы.

- Порнография и откровенные сцены - Материалы эротического содержания, эротические игрушки, CD-ROMы и видеозаписи. Сообщества и новостные группы, включая форумы, носящие сексуальный характер. Эротические истории и описания половых актов. Сервисы эротического характера, например, видеоконференции, эскорт, стриптиз-клубы. Искусства, вызывающие сексуальное возбуждение.
- Потоковое вещание и скачки - Сайты загрузки потокового контента, например, интернет-радио, интернет-телевидение или MP3. Включает фан-сайты или официальные сайты музыкантов, групп или звукозаписывающих компаний.
- Правительство - Информация о правительстве, государственных органах и правительственных службах, таких, как налоговая служба и налогообложение, коммунальные услуги и услуги скорой помощи. Также включает сайты, обсуждающие законы и различные государственные организации, а также федеральные, региональные и национальные правительственные сайты.
- Преступная деятельность - Советы о том, как совершить противоправные или преступные действия: совершение убийства, создание бомбы, взламывание замков и т.д. Также включает сайты с информацией о незаконной манипуляции электронными устройствами, хакерстве, мошенничестве и незаконном распространении программного обеспечения.
- Припаркованные домены - Сайты, которые неактивны, как правило, зарезервированы для дальнейшего использования. Они чаще всего не имеют собственное содержание, может быть просто сказано "под строительство", "купить этот домен" или показывать рекламные объявления.
- Прокси-сервера и анонимайзеры - Прокси-сервера и другие способы получить доступ в Интернет в обход установленным политикам и слежению. Веб-приложения для обхода фильтрации сайтов.
- Путешествия - Авиакомпании, агентства по бронированию авиабилетов, планирование поездок, предварительные заказы, аренда транспортных средств, описания мест назначения, реклама гостиниц и казино. Аренда машин.
- Развлечение - Кинофильмы, видео, телевидение, музыка и книги, комиксы, театр, галереи, актеры и обзоры представлений. Театральное искусство (театр, водевиль, опера, симфонии и другие).
- Реклама и всплывающие окна - Реклама, объявления, анонсы, баннеры.
- Религия - Сайты, которые имеют дело с верой, духовностью и религиозными убеждениями, в том числе сайты церквей, синагог, мечетей и других молитвенных домов.

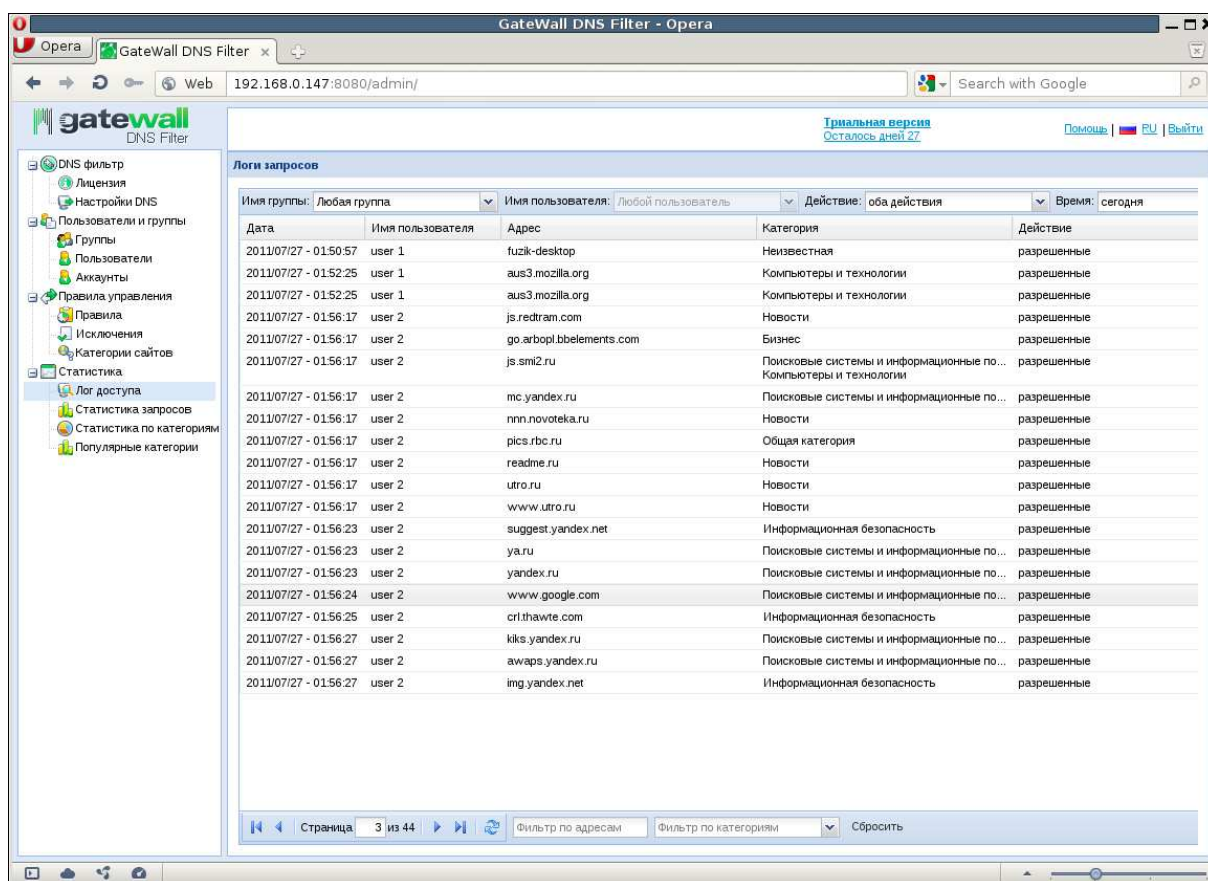
- Рестораны и еда - Обзор, обсуждение или реклама пищи или услуг общественного питания. Включает в себя сайты для рецептов сайтов, приготовление пищи, инструкции и советы, продукты питания.
- Сайты со СПАМом - URL-адреса, содержащиеся в спам-сообщениях.
- Сетевые ошибки - Сайты, которым не соответствует ни один IP-адрес
- Социальные сети - Сайты социальных сетей, пользователи которых могут общаться, взаимодействовать, обмениваться сообщениями, файлами.
- Спорные ресурсы - Инструкции по защите от нанесения вреда и ущерба частным лицам и группам. Также данная категория включает описания враждебности, агрессии, клеветы и дискриминации на основе расовых, религиозных, половых, национальных и этнических различий. Также содержит некорректный юмор, преступную деятельность, плагиат и вводящие в заблуждения сайты типа «стань миллионером прямо сейчас».
- Спорт - Сайты команд или спортивных ассоциаций, международные и национальные, спортивные колледжи, баллы, очки, расписания игр, спортивные журналы и газеты, виртуальный спорт и спортивные лиги.
- Транспорт - Сайты, которые включают информацию об автотранспортных средствах, таких как автомобили, мотоциклы, лодки, грузовые автомобили, внедорожники и т.п., в том числе сайты онлайн покупки. Включает в себя производителя, дилеров, обзоры, цены, клубы и т.д.
- Файлообменники - Сайты, содержащие загружаемое программное обеспечение, будь то условно-бесплатные, бесплатные или за плату. Включает в себя некоторые пиринговые сайты.
- Финансы - Банковские услуги и другие виды финансовой информации о таких операциях, как ссуда и заем, ипотеки, а также бухгалтерский учет, банки, актуарии, страховые компании. Не включает сайты, которые предлагают информацию о рынке, брокерских операциях или торговых услугах.
- Фишинг и мошенничество - Порталы, выдающие себя за сайты с хорошей репутацией, однако собирающие личную информацию о пользователе.
- Форумы и списки рассылки - Сайты для обмена информацией: новости, форумы, доски объявлений. Не включает в себя персональные блоги.
- Хакерство - Нелегальный или сомнительный доступ к данным, использование аппаратных или программных средств для нелегального доступа. Разработка и распространение программ, использование которых подвергает риску сети или системы. Нелегальное использование программ, уклонение от оплаты, использование пиратских копий ПО.

- Частные IP-адреса - Включает наборы IP-адресов, предназначенных для определенных организаций или субъектов.
- Чаты - Сайты, которые позволяют веб-обмен сообщениями в режиме реального времени, чаты.
- Школьные мошенничества - Сайты, которые способствуют плагиату, содержат ответы на тесты, готовые эссе, исследовательские или курсовые работы.

Лог доступа и статистика запросов

Лог доступа

На странице «Лог доступа» отображается более детальная информация о последних запросах на разрешение имен, с отображением времени запроса, имени хоста, его категории и данных об источнике запроса (пользователь/группа). Страница используется для просмотра последних 20-ти запросов с возможностью листать остальные страницы логов доступа путем нажатия соответствующих кнопок.



Дата	Имя пользователя	Адрес	Категория	Действие
2011/07/27 - 01:50:57	user 1	fuzik-desktop	Неизвестная	разрешенные
2011/07/27 - 01:52:25	user 1	aus3.mozilla.org	Компьютеры и технологии	разрешенные
2011/07/27 - 01:52:25	user 1	aus3.mozilla.org	Компьютеры и технологии	разрешенные
2011/07/27 - 01:56:17	user 2	js.redtram.com	Новости	разрешенные
2011/07/27 - 01:56:17	user 2	go.arbopl.bbelements.com	Бизнес	разрешенные
2011/07/27 - 01:56:17	user 2	js.smi2.ru	Поисковые системы и информационные по... Компьютеры и технологии	разрешенные
2011/07/27 - 01:56:17	user 2	mc.yandex.ru	Поисковые системы и информационные по...	разрешенные
2011/07/27 - 01:56:17	user 2	nnn.novoteka.ru	Новости	разрешенные
2011/07/27 - 01:56:17	user 2	pics.rbc.ru	Общая категория	разрешенные
2011/07/27 - 01:56:17	user 2	readme.ru	Новости	разрешенные
2011/07/27 - 01:56:17	user 2	utro.ru	Новости	разрешенные
2011/07/27 - 01:56:17	user 2	www.utro.ru	Новости	разрешенные
2011/07/27 - 01:56:23	user 2	suggest.yandex.net	Информационная безопасность	разрешенные
2011/07/27 - 01:56:23	user 2	ya.ru	Поисковые системы и информационные по...	разрешенные
2011/07/27 - 01:56:23	user 2	yandex.ru	Поисковые системы и информационные по...	разрешенные
2011/07/27 - 01:56:24	user 2	www.google.com	Поисковые системы и информационные по...	разрешенные
2011/07/27 - 01:56:25	user 2	cri.thawte.com	Информационная безопасность	разрешенные
2011/07/27 - 01:56:27	user 2	kiks.yandex.ru	Поисковые системы и информационные по...	разрешенные
2011/07/27 - 01:56:27	user 2	awaps.yandex.ru	Поисковые системы и информационные по...	разрешенные
2011/07/27 - 01:56:27	user 2	img.yandex.net	Информационная безопасность	разрешенные

Рисунок 7. Лог доступа

Статистика запросов

Страница «Статистика» отображает суммарную статистику по разрешенным и запрещенным запросам с возможностью фильтрации по пользователям, группам и действию за определенный интервал времени.

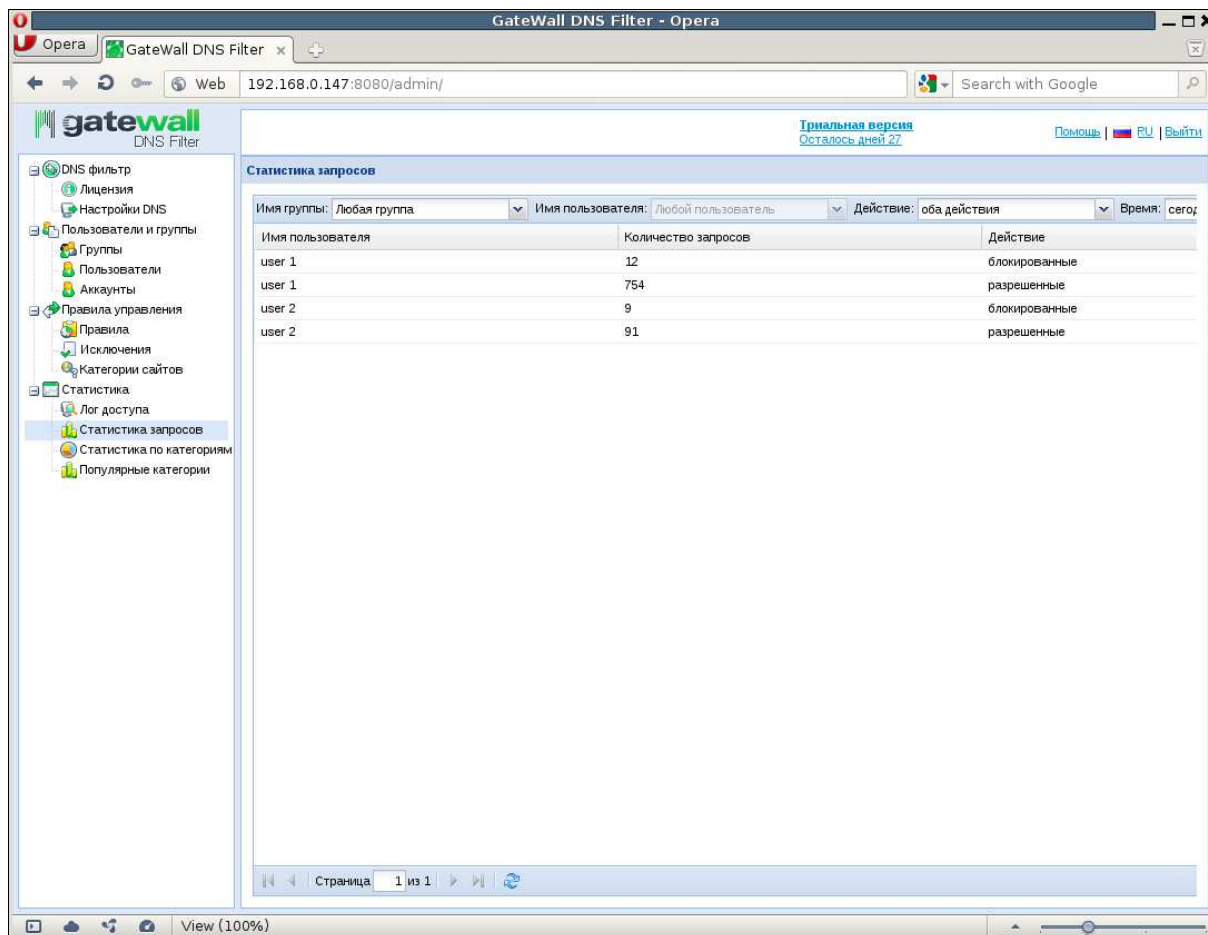


Рисунок 8. Статистика запросов

Статистика по категориям

Кроме управления правилами доступа через веб-консоль пользователям доступна статистика запросов, лог доступа и статистика по категориям сайтов для себя или для своей группы, если пользователю были даны права "Администратор группы". "Администратор" видит статистику по всем пользователям или по выбранным через фильтр группам/пользователям.

В левой части окна статистики отображаются процентные составляющие категорий сайтов от общего количества запросов. Если щелкнуть на определенной доле этой диаграммы, то в правой части окна вы увидите детализацию: применение фильтра только к выбранной вами категории сайтов.

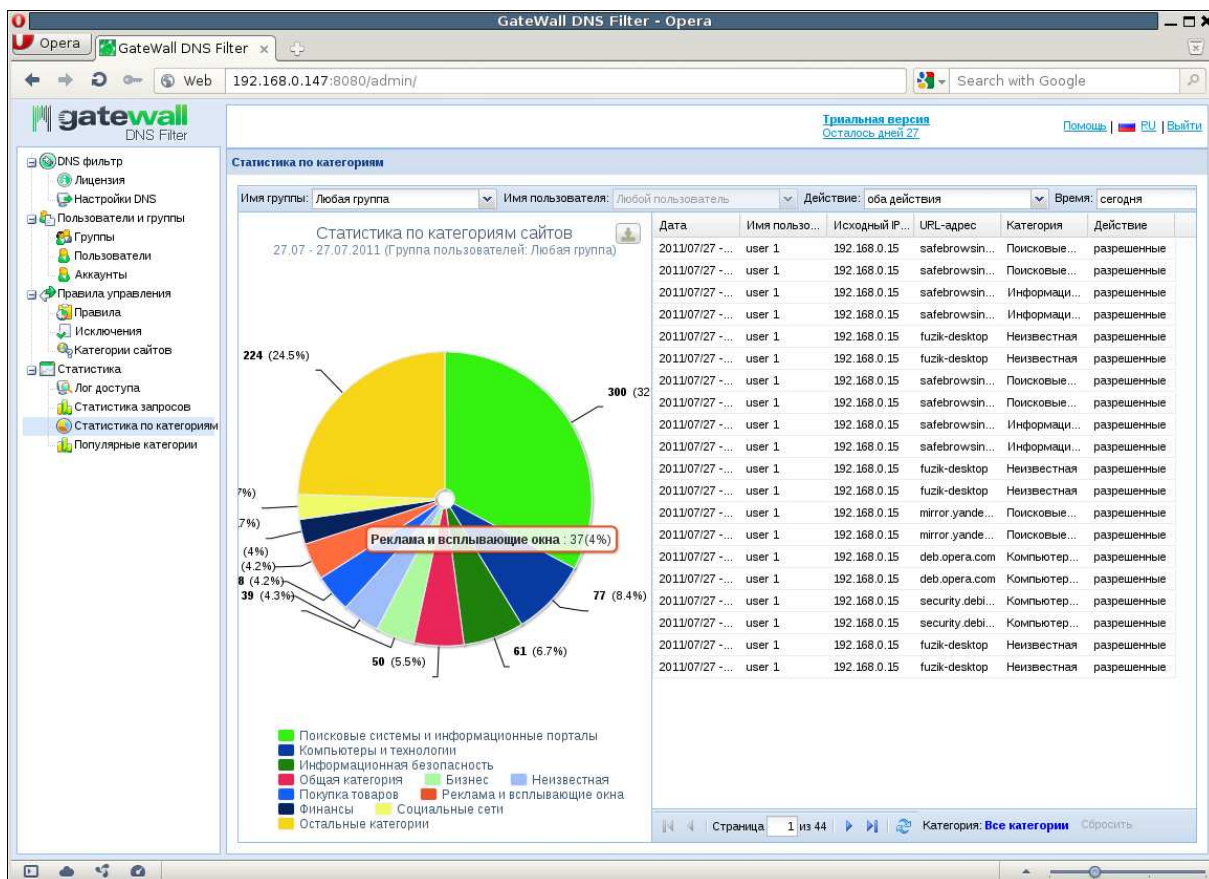


Рисунок 9. Статистика по категориям

Популярные категории

На данной вкладке можно просмотреть статистику по десяти самым популярным категориям за сегодня, последнюю неделю или месяц.

На графике отображается количество запросов на сайты из самых посещаемых категорий по часам (статистика за день) или дням (статистика за неделю/месяц). Столбцы графика разбиты на цветные сектора, каждый из которых соответствует одной из категорий.

Есть возможность фильтровать по группе, пользователю, а также по типу примененного правила: "разрешено", "заблокировано".

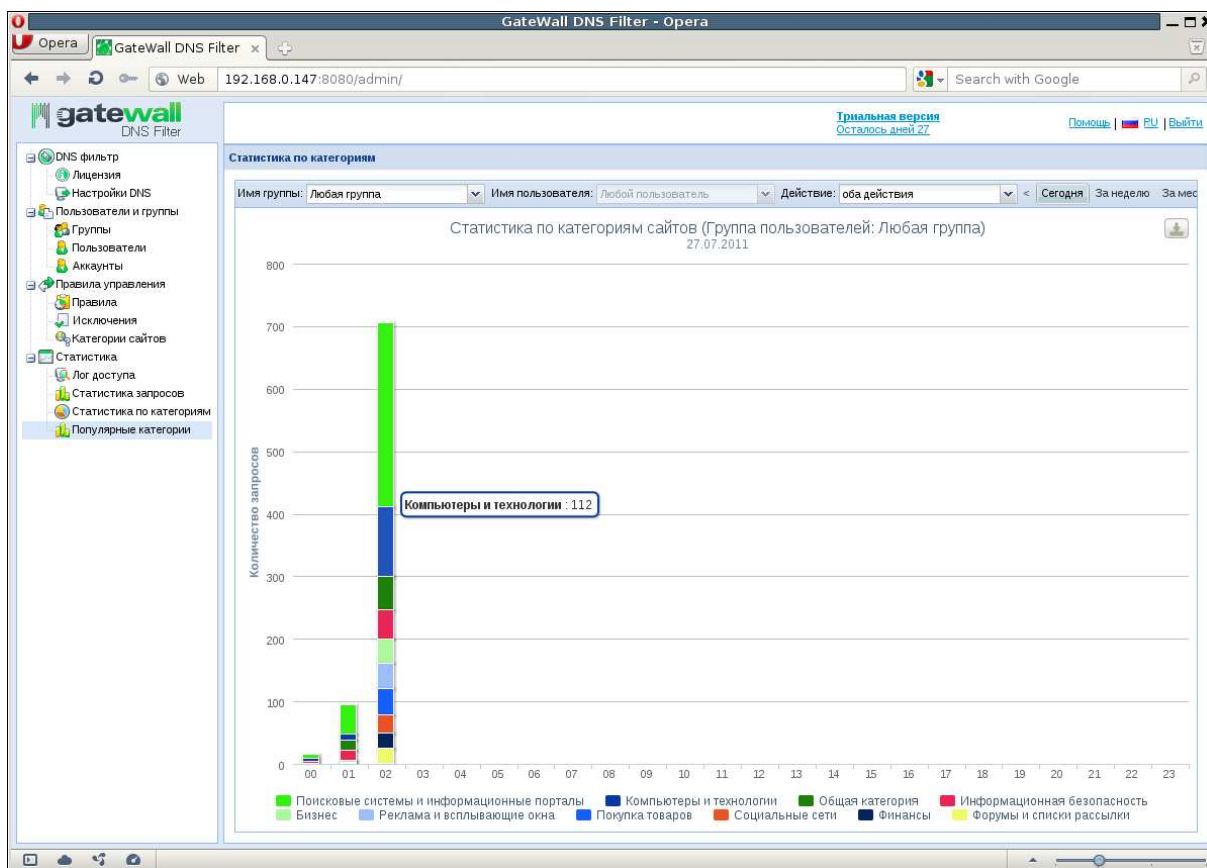


Рисунок 10. Популярные категории

Механизм запроса категорий сайтов Entensys URL Filter Master Database

Запрос категорий выполняется через обращение к сервису Entensys URL Filter Master Database. DNS Filter обращается к сервису, адрес которого задан параметром *server_name*, указанный в разделе `<brightcloud />` файла настроек.

Запрос на разрешение категорий выполняется в асинхронном режиме через пул сокетов. Минимальное и максимальное количество сокетов для подключения к сервису Entensys URL Filter Master Database задается параметрами *min_socket_number* и *max_socket_number* в разделе `<brightcloud />` файла настроек. Количество сокетов может увеличиваться автоматически по мере возрастания нагрузки.

Важно! Для крупных сетей рекомендуется увеличить значение параметров *min_socket_number* и *max_socket_number* в соответствии с нагрузкой на сервер.

Отклонение запросов на разрешение доменного имени

Запрос на разрешение доменного имени может быть отклонен. В этом случае пользователю вернется специальный адрес 127.0.0.1 или собственный адрес GateWall DNS Filter. Запрос может быть отклонен при следующих вариантах:

- не удается получить категорию от Entensys URL Filter, например, сервис недоступен.
- если запрос на Entensys URL Filter был отклонен, закончилась лицензия.
- запрос может быть отклонен при недостаточном количестве сокетов для подключения к сервису Entensys URL Filter

Примечание. При недостаточном количестве сокетов, отклоненные DNS-запросы помещаются в специальную очередь. Запросы из этой очереди могут быть обработаны с некоторой задержкой.

При недоступности сервиса Entensys URL Filter, можно оставить возможность разрешения DNS-имен. Функция включается параметром "Разрешать имена, если облачный URL-фильтр недоступен" в общих настройках.

Перенаправление запрещенных запросов

Если доступ к хосту запрещен, пользователю возвращается адрес 127.0.0.1 или собственный адрес GateWall DNS Filter. Собственный IP-адрес GateWall DNS Filter возвращается тогда, когда в общих настройках включена опция "На локальный IP-адрес". В этом случае при обращении на запрещенный ресурс через браузер пользователь попадет на специальную информационную страницу с сообщением о запрете доступа.

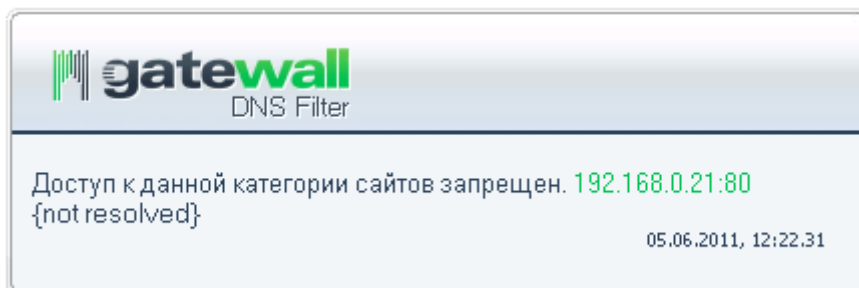


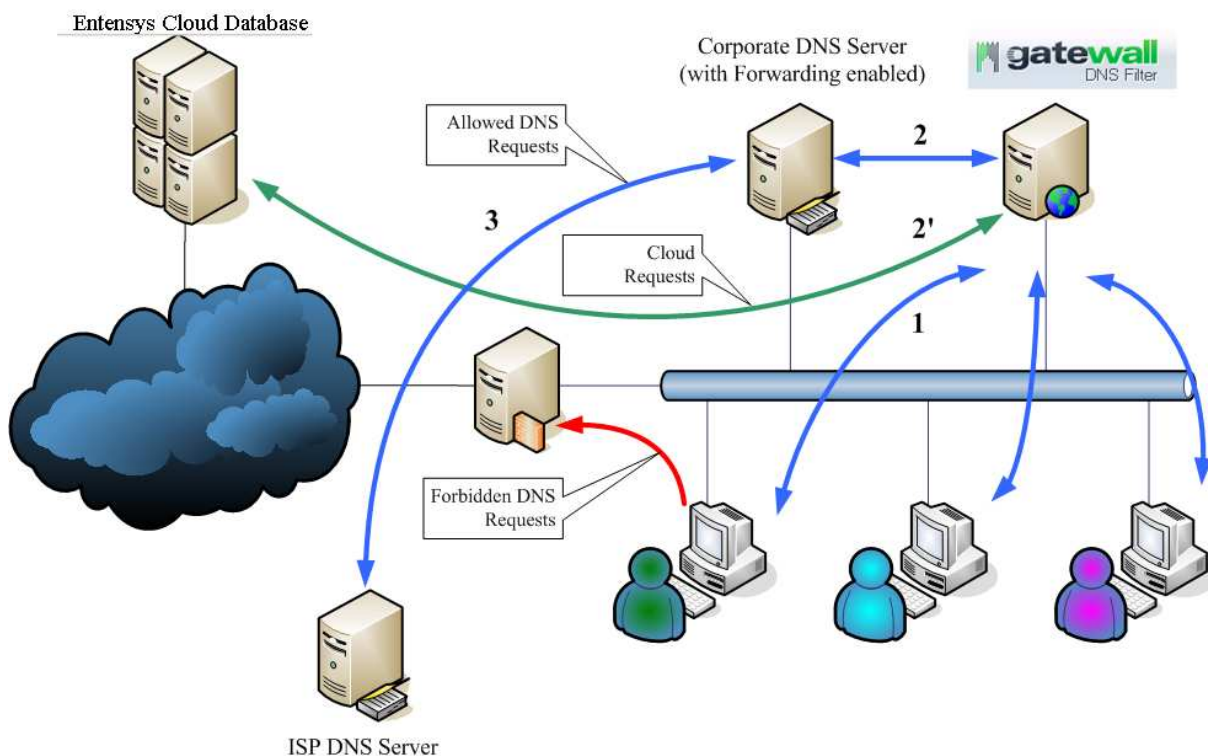
Рисунок 11. Отклоненный запрос

Варианты развертывания GateWall DNS Filter

Вариант 1

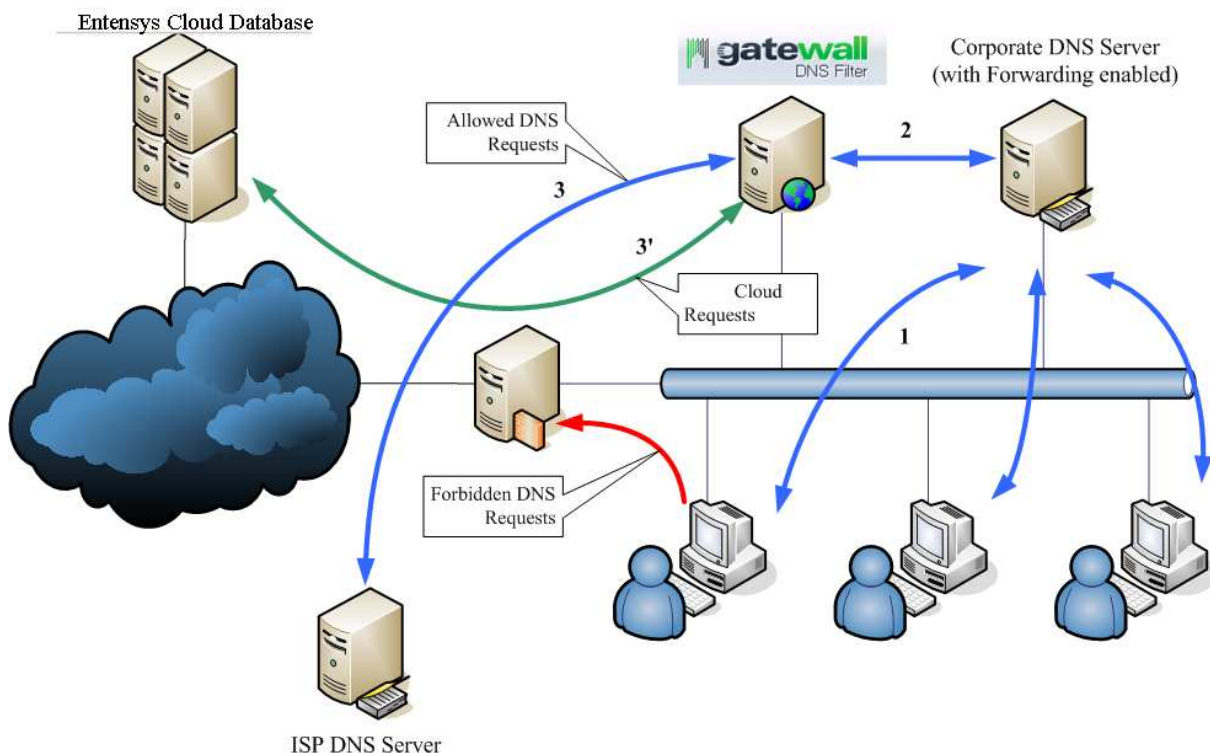
В корпоративных сетях можно использовать два варианта развертывания сервера GateWall DNS Filter. В первом варианте сервер GateWall DNS Filter располагается перед корпоративным DNS-сервером. Предполагается, что на корпоративном DNS-сервере разрешено перенаправление DNS-запросов на DNS-сервер(а) Интернет-провайдера. В консоли DNS Filter Administrator

создаются пользователи локальной сети, с авторизацией по IP-адресу. Доменное имя организации помещается в параметр *exclude_domains* секции *<brightcloud />* файла настроек сервера. В настройках DNS указывается, что DNS-запросы необходимо направлять на внутренний DNS-сервер компании. Машина с GateWall DNS Filter должна иметь доступ в сеть Интернет по протоколам HTTPS и BCAP (TCP порт 2316). В этом варианте в GateWall DNS Filter будет доступна детальная статистика по всем пользователям (машинам) в локальной сети.



Вариант 2

Во втором варианте сервер GateWall DNS Filter устанавливается непосредственно за корпоративным DNS-сервером. Предполагается, что в настройках корпоративного DNS-сервера указан адрес GateWall DNS Filter в качестве сервера для пересылки запросов (Forwarder). В настройках DNS Filter создается единственный пользователь с IP-адресом, соответствующим корпоративному DNS-серверу. В качестве DNS-серверов для пересылки запросов в настройках DNS Filter указывается DNS сервер(а) Интернет-провайдера. В этом варианте возможно снижение нагрузки на GateWall DNS Filter за счет дополнительного кэширования на корпоративном DNS-сервере. Однако статистика запросов по пользователям локальной сети будет недоступна.



Важно! Поскольку GateWall DNS Filter не является шлюзовым решением, в обоих вариантах необходимо запретить прохождение DNS-запросов в сеть Интернет непосредственно с машин пользователей.

Отображение дополнительной отладочной информации

Если требуется получить дополнительную информацию о работе GateWall DNS Filter, администратор может создать специальные *.sem файлы в корневой директории DNS Filter. SEM файл представляет собой пустой файл с расширением *.sem и со строго определенным названием. Доступны следующие файлы:

- dnslog.sem – для вывода подробной информации о разрешении DNS-имен
- bblog.sem – для вывода подробной информации о запросах Entensys URL Filter
- dblog.sem – для вывода информации о работе с базой данных

После создания SEM-файлов необходимо перезапустить сервер DNS Filter. Отладочная информация будет записываться в лог файл %DNSFilter%\Logging\dnsfilter.log. Параметры логирования работы программы задаются в разделе <logs /> файла настроек сервера. Предельный размер одного лог файла определяется параметром *max_size* и по умолчанию составляет 20 Мб. При превышении размера лог файла, сервер DNS Filter

создает новый лог файл *dnsfilter.log*, добавляя дату в название старого файла. Предельное количество файлов не ограничивается.

Важно! Использование SEM-файлов на системах с высокой нагрузкой приведет к быстрому увеличению количества лог файлов и к увеличению загрузки ЦПУ.