GateWall DNS Filter

Руководство администратора

Оглавление

ВВЕДЕНИЕ **3**

GATEWALL DNS FILTER **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 6

МОДУЛЬ АДМИНИСТРИРОВАНИЯ DNS FILTER **6**

Настройка соединений 6
Установка пароля на подключение *7*
Работа с базой статистики GateWall DNS Filter 8
Использование сторонних БД *8*
Восстановление базы данных *9*
Пользователи и группы 9
Методы авторизации пользователей *10*
Настройка DNS 10
Правила управления трафиком 11
Лог доступа и статистика запросов 11

ФИЛЬТРАЦИЯ ПО КАТЕГОРИЯМ BRIGHTCLOUD **12**

Список исключений 13
Механизм запроса категорий сайтов от BrightCloud 14
Порядок работы GateWall DNS Filter 15
Отклонение запросов на разрешение доменного имени 15
Перенаправление запрещенных запросов 16

ВЕБ–СТАТИСТИКА GATEWALL DNS FILTER **16**

ВАРИАНТЫ РАЗВЕРТЫВАНИЯ GATEWALL DNS FILTER **17**

ОТОБРАЖЕНИЕ ДОПОЛНИТЕЛЬНОЙ ОТЛАДОЧНОЙ ИНФОРМАЦИИ **19**

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, корпоративных сетях, содержащих нескольких тысяч пользователей.

GateWall DNS Filter

GateWall DNS Filter состоит из следующих модулей: сервер, консоль управления (DNS Filter Administrator), веб-сервер с поддержкой HTTPS и модуль веб-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 специальному протоколу поверх TCP/IP, что позволяет выполнять удаленное администрирование сервера. В консоли администратора доступна краткая статистика по обработке DNS запросов. Более полная статистика может быть получена через обращение к веб-статистике.

Встроенный веб-сервер используется для работы веб-статистики, 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. Так, если интенсивность составляется ~ 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 DNS Filter в директории, в которую он был установлен, останется файл настроек сервера. Если использовалась сторонняя база статистики, она не будет удалена.

Регистрация GateWall DNS Filter

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

В демонстрационном режиме сервер GateWall DNS Filter будет работать 30 дней. При обращении в 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.

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 BrightCloud) будет доступна только для 10-ти пользователей.

Лицензия на модуль BrightCloud, предназначенный для работы с категориями сайтов, включена в лицензию на GateWall DNS Filter. Срок действия лицензии на BrightCloud ограничен и составляет один год. По истечению срока действия лицензии online сервис BrightCloud станет недоступен.

Проверка доступности новой версии

В консоли администрирования, меню «Помощь» присутствует пункт «Проверить наличие обновлений». При нажатии 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 в автоматической переустановке GateWall DNS Filter.

Модуль администрирования DNS Filter

Модуль администрирования представляет собой 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», если модуль администрирования установлен на другой компьютер. Для работы с настройками необходимо подключить модуль администрирования к серверу.

Настройка соединений

При первом запуске консоль администрирования открывается на странице «Соединения», на которой присутствует единственное соединение с сервером localhost для пользователя Administrator. Пароль на подключение к DNS Filter Service не установлен. Подключить консоль администрирования к серверу можно через двойной клик на строке “localhost – Administrator” или через кнопку «Подключиться» на панели управления. В консоли администрирования можно создать несколько подключений. В параметрах подключения указываются:

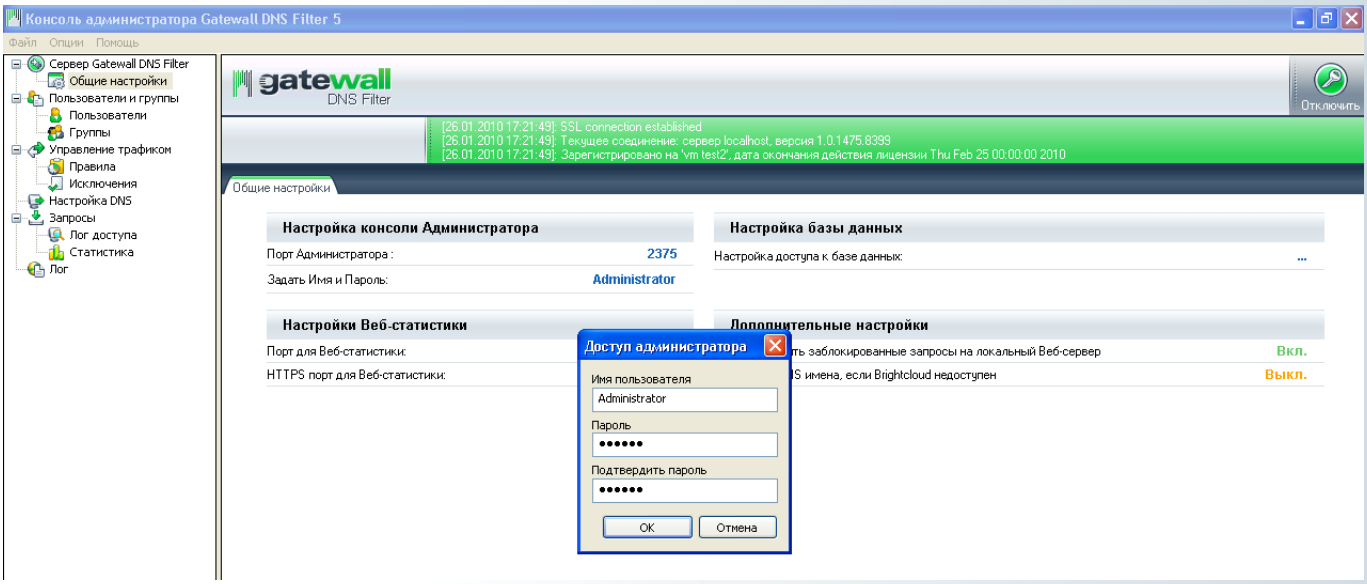
- Название сервера – это название подключения
- Имя пользователя – логин для подключения к серверу
- Адрес сервера – доменное имя или IP–адрес сервера DNS Filter
- Порт – TCP порт, используемый для подключения к серверу (по умолчанию используется порт 2375)
- Пароль – пароль для подключения

Опция «Спрашивать пароль при подключении» позволяет отображать диалог для ввода пароля при подключении к серверу. Опция «Подключаться автоматически» позволяет выполнять автоматической подключение к указанному серверу при запуске консоли администрирования.

Настройки консоли администрирования хранятся в файле *console.xml*, расположенном в директории “%DNSFilter%\Administrator”. На стороне сервера имя пользователя и пароль (в зашифрованном виде) хранятся в файле *dnsfilter.xml*, расположенном в директории %DNSFilter%.

Установка пароля на подключение

Установить «Логин/пароль» для подключения к серверу DNS Filter можно на странице «Общие настройки», раздел «Настройки консоли Администратора». В этом разделе также можно изменить TCP–порт для подключения к серверу. Для вступления новых настроек в силу необходимо перезапустить сервер DNS Filter (пункт «Перезапустить сервер DNS Filter» в меню агента). После перезапуска сервера новые настройки требуется указать и в консоли администрирования, в параметрах соединения. В противном случае администратор не сможет подключиться к серверу.



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 базами MS SQL и MySQL в состав дистрибутива GateWall DNS Filter входят дампы базы данных с требуемой структурой. Дампы расположены 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%\dnsfilter.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 *dns* раздела <*database /*> файла настройки сервера.

Важно: при работе с MySQL требуется MySQL Connector версии 3.5.

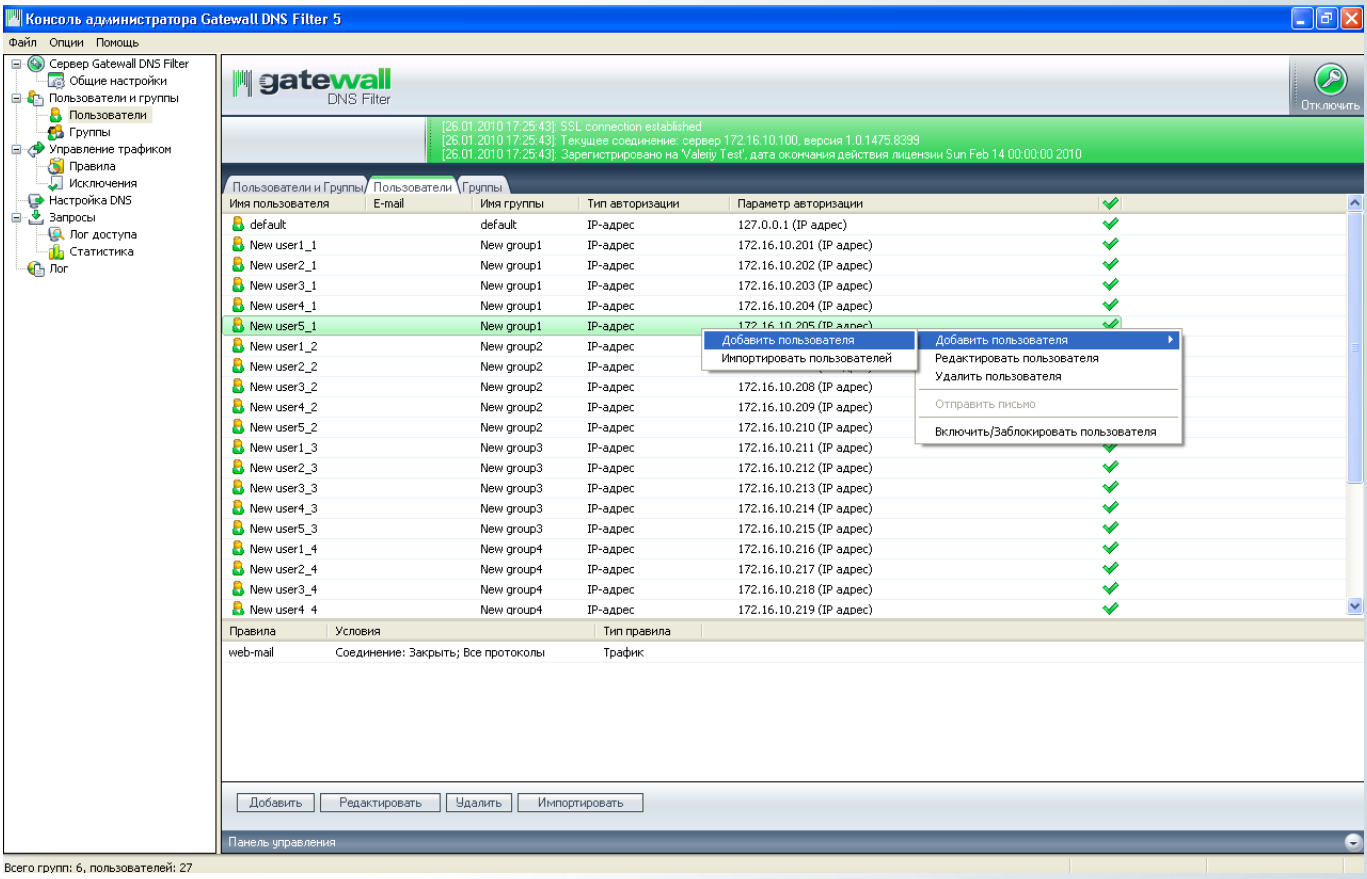
Восстановление базы данных

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%\dnsfilter.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.

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 уровням доступа, поскольку в этом случае существенно облегчается работа с правилами управления трафиком. По умолчанию в DNS Filter присутствует единственная группа – default.



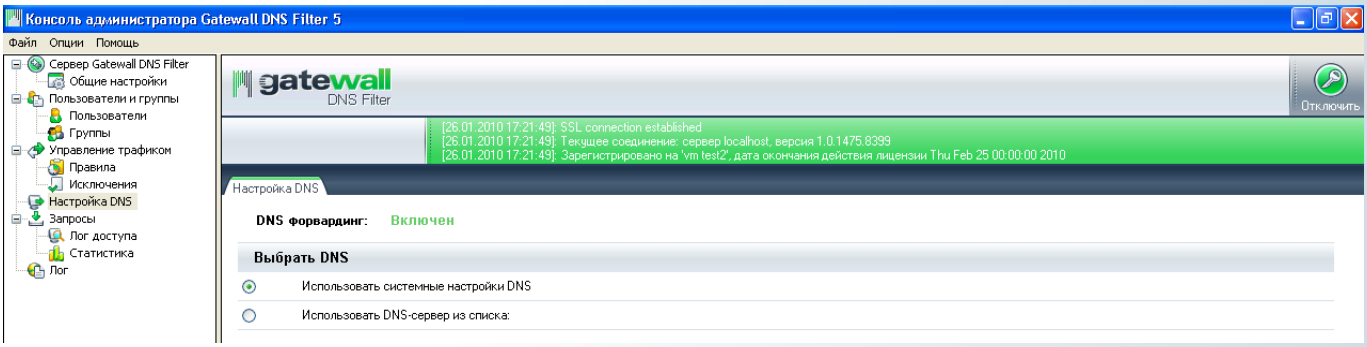
Создать нового пользователя можно через пункт «Добавить нового пользователя» или через кнопку «Добавить» в панели управления на странице «Пользователи и группы». Обязательными параметрами пользователя являются: Имя, Тип авторизации, параметр авторизации (IP–адрес, диапазон IP адресов) и группа. По умолчанию все пользователи принадлежат к группе default. Имя пользователя в DNS Filter должно быть уникальным. Дополнительно в свойствах пользователя можно разрешить или запретить доступ пользователя к веб-статистике и задать правила управления трафиком (правила фильтрации DNS запросов).

Методы авторизации пользователей

Возможность разрешения DNS имен сервером GateWall DNS Filter предоставляется для всех клиентов в локальной сети. Возможность фильтрации DNS запросов предоставляется только для авторизованных пользователей. DNS Filter поддерживает два метода авторизации: по IP–адресу и по диапазону IP–адресов.

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 *cache_size* раздела *<dns_forward />* файла настроек. По умолчанию собственный кэш может содержать не более 500 записей. Дополнительно, через файл настроек можно управлять временем жизни записи в кэш (параметры *max_cache_pos_ttl* и *max_cache_neg_ttl*).



Настройка DNS в консоли администрирования доступна в разделе «Сервисы – Настройка DNS». В настройках 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 машины, на которую установлен GateWall DNS Filter.

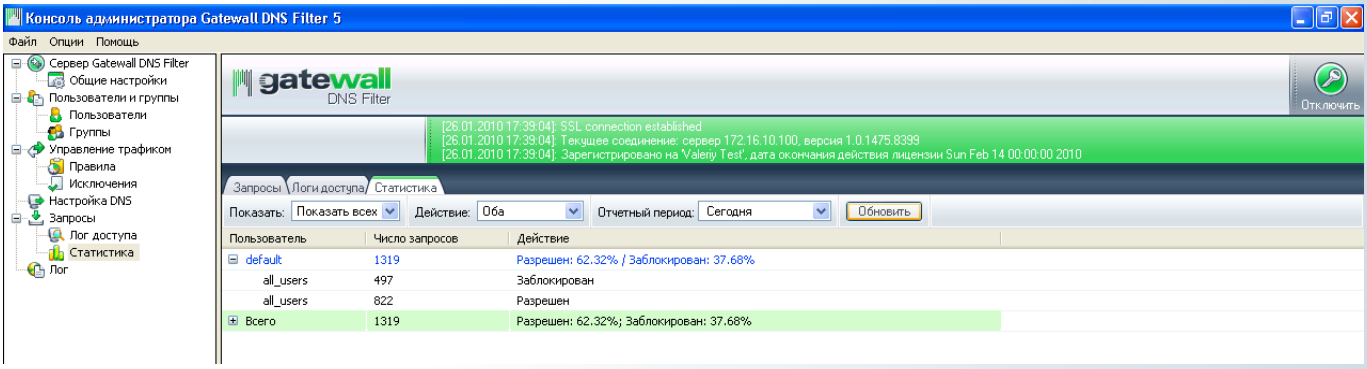
Правила управления трафиком

Правила управления трафиком предназначены для запрета доступа к сайтам в зависимости от его категории, времени суток. Дополнительно предоставляется возможность фильтрации на основе черных и белых список. 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.

Важно! В beta версии не доступна фильтрация по времени.

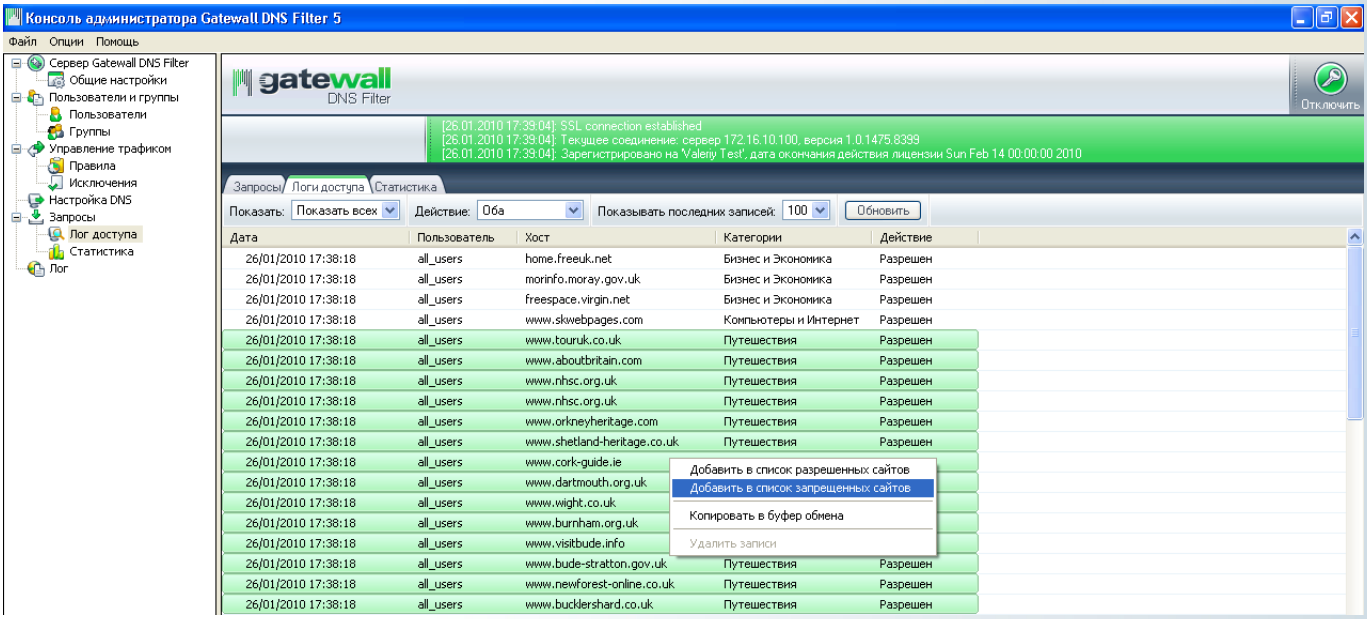
Лог доступа и статистика запросов

В разделе «Запросы» консоли администратора отображается статистика запросов, обработанных сервером DNS Filter. Страница «Статистика» отображает суммарную статистику по разрешенным и запрещенным запросам, с возможность фильтрации по пользователям, группам, действию за определенный интервал времени.



На странице «Лог доступа» отображается более детальная информация о последних запросах на разрешение имен, с отображением времени запроса, имени хоста, его категории и об

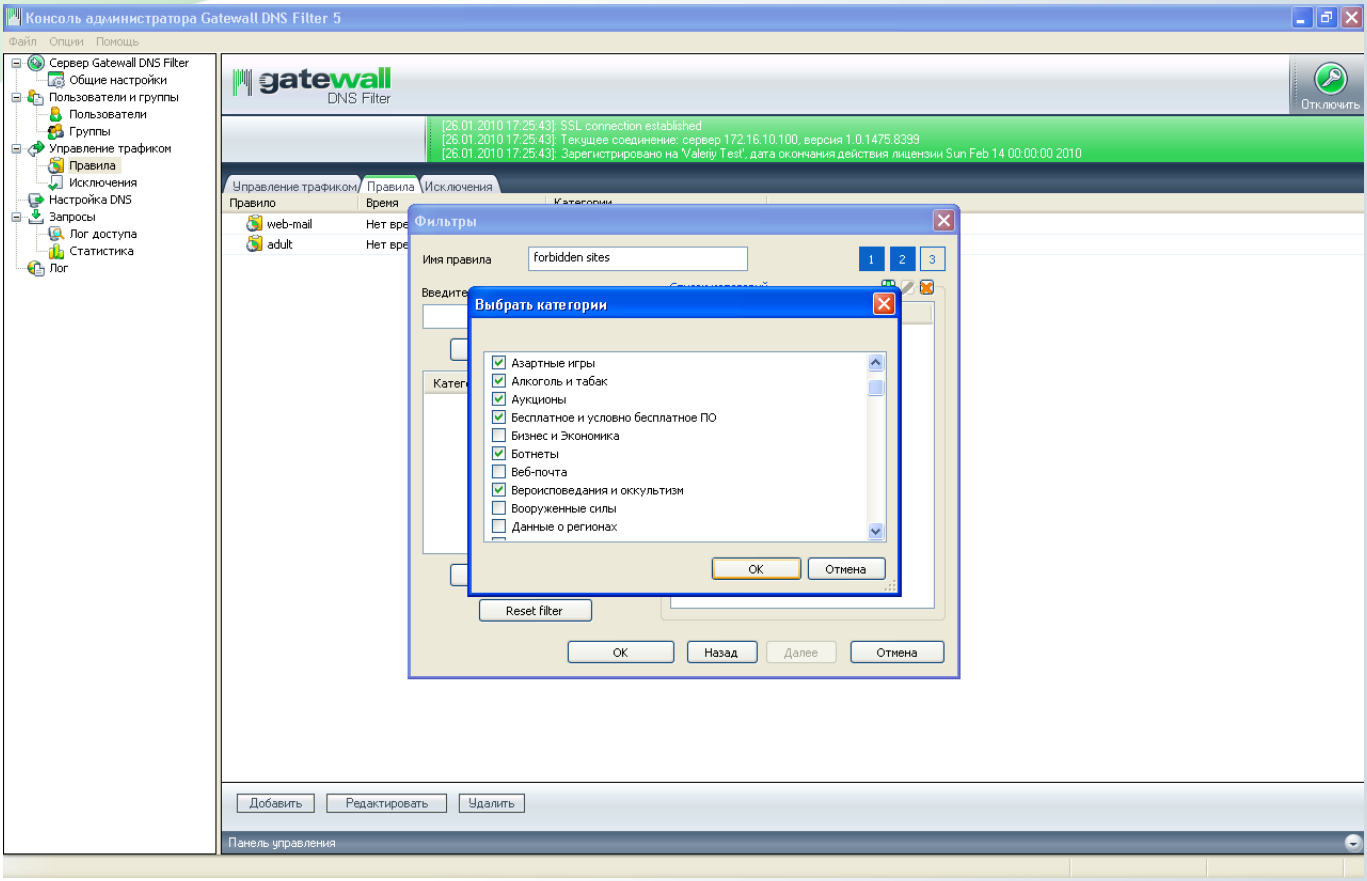
источнике запроса (пользователь/группа). Страница используется для просмотра последних 25-ти, 50-ти или 100-а запросов.



Фильтрация по категориям BrightCloud

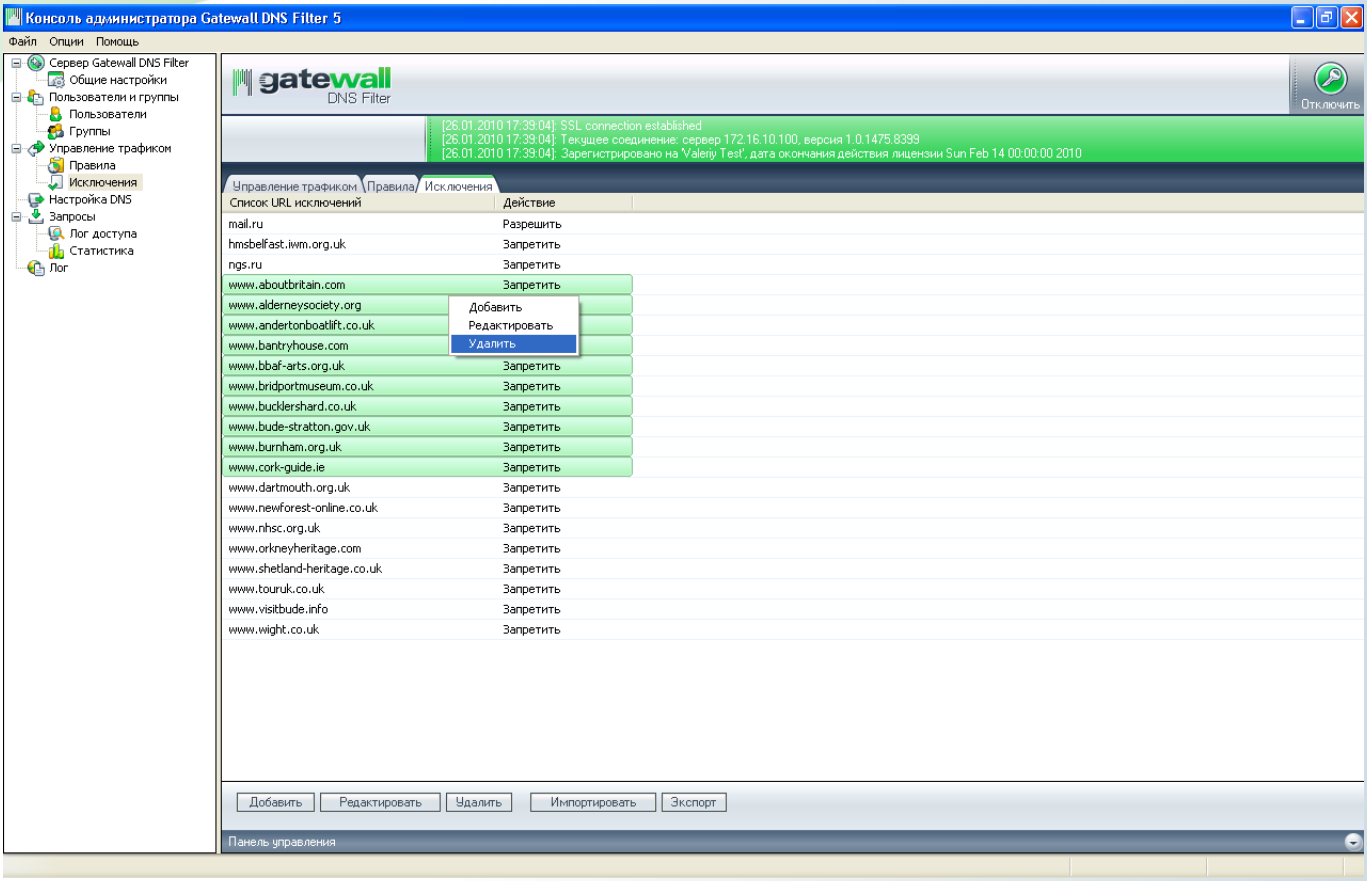
В рамках технологического сотрудничества с компанией BrightCloud Inc, в GateWall DNS Filter интегрирован инструментарий BrightCloud Service и BrightCloud Master Database. Администратор может запрещать доступ к сайтам определенного содержания без указания названия сайтов. В статистике DNS Filter можно получить отчет о категориях посещаемых сайтов, например: реклама, образование, новости и т.п. Использование категорий сайтов позволяет вести более гибкую политику управления доступом к сети Интернет.

Для запрета доступа к сайтам определенной тематики откройте раздел «Управление трафиком» – «Правила», создайте новое правило и на последней странице диалога выберите одну или несколько категорий сайтов.



Список исключений

Список исключений (пункт «Исключения» дерева настроек) позволяет добавить один или несколько хостов в черный или белый список. Имена хостов, помещенный в список исключений с действием «Разрешить», будут разрешаться всегда, даже, если указанный хост принадлежит одной или нескольким категориям в правилах управления трафиком, примененных пользователю. Имена хостов, помещенные в список исключений с действием «Запретить» не будут разрешаться на валидный IP адрес, независимо от наличия или отсутствия правил управления трафиком. Списки исключений глобальные, т.е. действует на 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, дополняю 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. При использовании GateWall DNS Filter по варианту 1 схем развертывания, рекомендуется в этой секции указать собственное доменное имя организации.

Механизм запроса категорий сайтов от BrightCloud

Запрос категорий BrightCloud выполняется через обращение к сервису BrightCloud 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 BrightCloud

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 устанавливать *min_socket_number=100*; *max_socket_number= 200* или более.

Порядок работы GateWall DNS Filter

В самом общем случае, схема работы GateWall DNS Filter выглядит следующим образом:

- от пользователя поступает запрос (DNS Request) на разрешение доменного имени
- сервер DNS Filter просматривает собственный DNS кэш, а также внутренний кэш BrightCloud, с целью определить адрес и категорию запрошенного доменного имени
- если в собственном кэш информация не найдена, DNS Filter перенаправляет запрос на указанный в настройках DNS сервер и формирует запрос к сервису BrightCloud
- DNS Filter возвращает ответ пользователю и записывает информацию о запросе в базу данных

Примечание. Для записей в БД используются транзакции (параметр *transactions="1"*), число операций SQL INSERT в транзакции задается параметром *max_transactions="50"* в файле настроек сервера. Оба параметра доступны в файле настроек сервера.

Ответ, который получает пользователь, зависит от наличия или отсутствия авторизации на сервере GateWall DNS Filter. И, если пользователь авторизован, от примененных к нему правил управления доступом, а также от списка исключений. Запросы от неавторизованных пользователей записываются в базу данных под именем Unknown.

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 BrightCloud, например, сервис недоступен.
- если запрос на BrightCloud был отклонен, закончилась лицензия.

- запрос может быть отклонен при недостаточном количестве сокетов для подключения к сервису BrightCloud

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

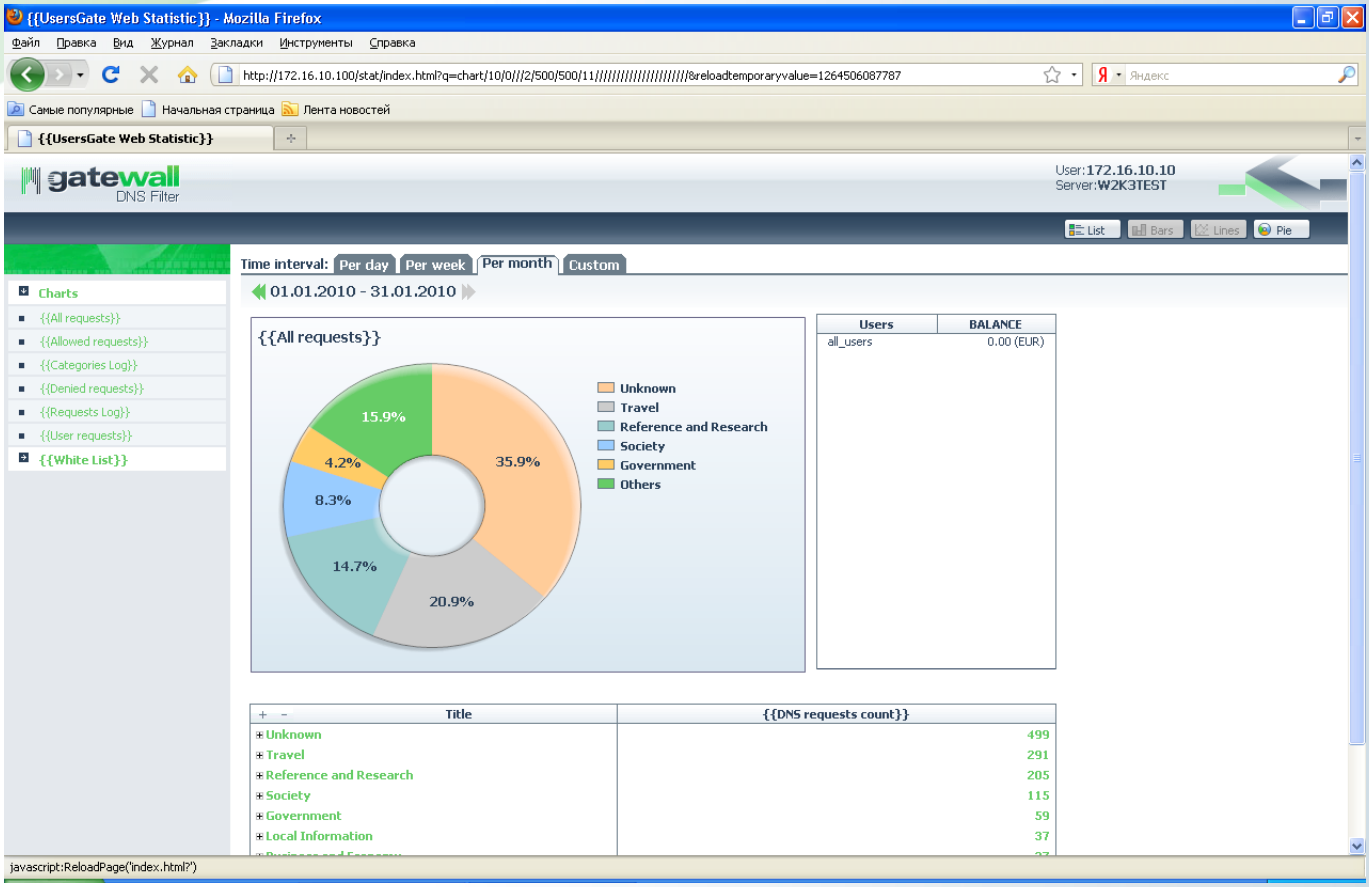
При недоступности сервиса BrightCloud можно оставить возможность разрешения DNS имен. Функция включается параметром «Разрешать DNS имена при недоступности сервиса BrightCloud» в общих настройках.

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 «Перенаправлять запросы на внутренний Веб-сервер». В этом случае, при обращении на запрещенный ресурс через браузер, пользователь попадет на специальную информационную страницу, с сообщением о запрете доступа.

Веб–статистика GateWall DNS Filter

Веб–статистика GateWall DNS Filter позволяет получать детальную информацию об обработанных DNS запросах, с разделением по пользователям, категориям, времени суток и действию («Разрешен» или «Запрещен»). Пользователю DNS Filter можно разрешить доступ к веб-статистике. В GateWall DNS Filter предусмотрено два уровня доступа: доступ к веб-статистике может быть запрещен (параметр по умолчанию) или разрешен.



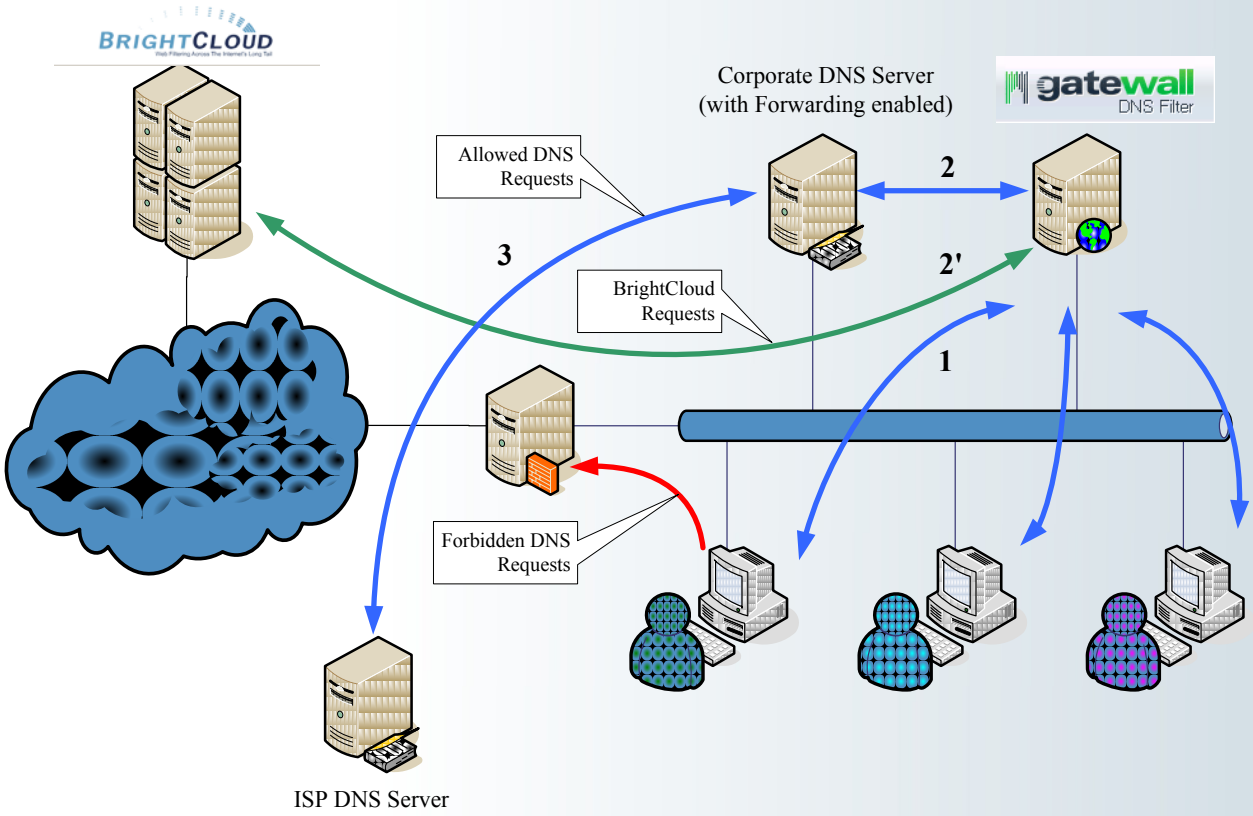
Веб-статистика доступна по ссылке http://192.168.0.1/stat/index.html, где 192.168.0.1 для примера – адрес сервера DNS Filter, или по ссылке https://192.168.0.1/stat/index.html. Порт, на котором работает веб-статистика, можно указать в разделе “Общие настройки – Настройка Веб-статистики ”. По умолчанию используются порты 80 и 443.

Отключить модуль веб-статистики можно, выставив параметр *web_stat enabled=”0”* в файле настроек сервера.

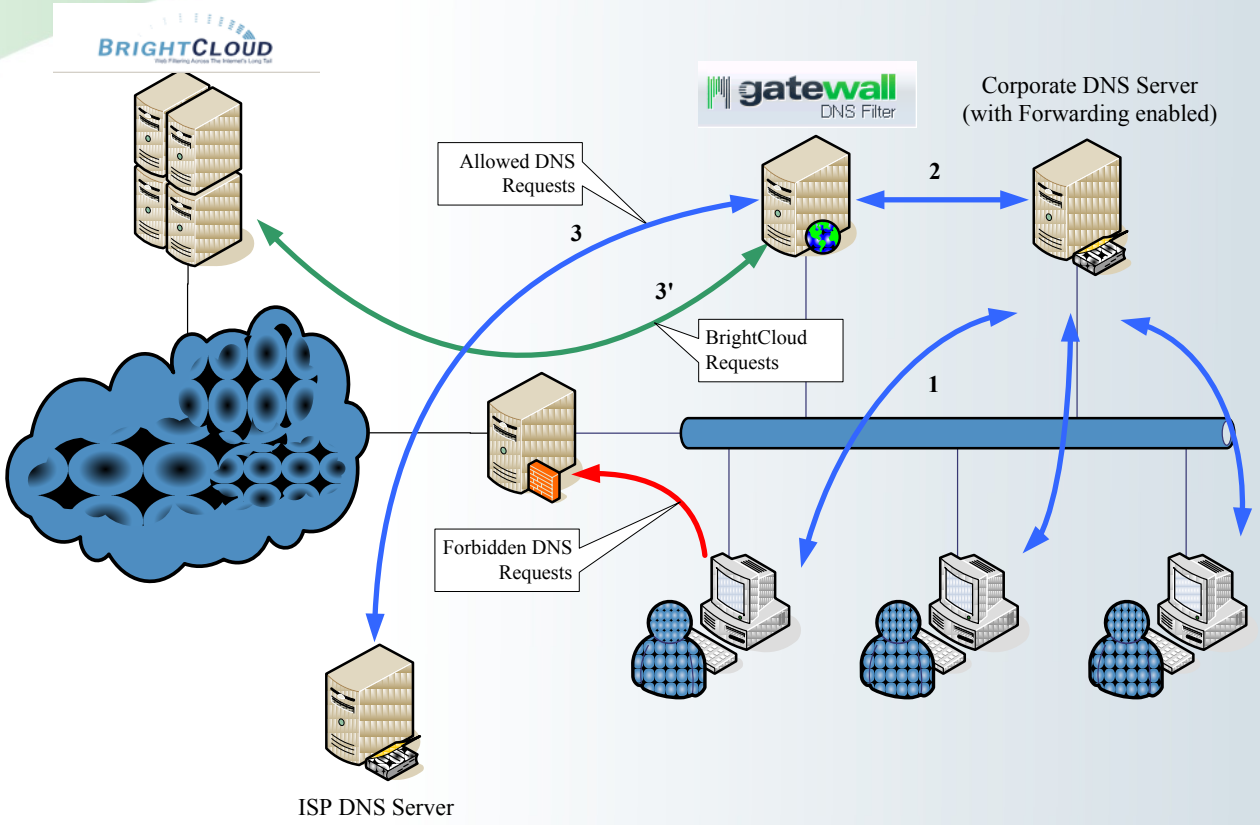
Варианты развертывания GateWall DNS Filter

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 требуется направлять на внутренний DNS сервер

компании. Машина с GateWall DNS Filter должна иметь доступ в сеть Интернет по протоколам HTTPS и BCAP (BrightCloud Control Application Protocol, TCP порт 2316). В этом варианте в GateWall DNS Filter будет доступна детальная статистика по всем пользователям (машинам) в локальной сети.



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 увеличение производительности работы GateWall DNS Filter, за счет обработки запросов от единственного пользователя. Однако детализации 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; *bclog.sem* – для вывода подробной информации о запросах BrightCloud и *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 программы *%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 Кб. При превышении размера лог файла, сервер DNS Filter создает новый лог файл *dnsfilter.log*, добавляю дату в название старого файла. Предельное количество файлов не ограничивается.

Важно! Использование SEM файлом на системах с высокой нагрузкой приведет к быстрому увеличения количества лог файлов.