UserGate Web Filter
Руководство администратора

Содержание

Введение

UserGate Web Filter - представляет собой специализированное ПО, позволяющее контролировать использование интернета на всех устройствах в локальной сети, независимо от их типа и операционной системы. Внедрение продукта обеспечивает безопасность доступа во всемирную паутину и способствует сведению к минимуму нецелевого веб-серфинга. Он может работать как сетевой шлюз, так и выступать в роли фильтрующего DNS-сервера. Кроме этого, UserGate Web Filter способен работать в распределенной отказоустойчивой сети, когда нагрузка может распределяться между узлами сети, что позволяет масштабировать систему до больших размеров. Подробнее о схемах распределения нагрузки и вариантах встраивания в любую сеть описано в специальном разделе в конце данного руководства. Также UserGate Web Filter может выступать ICAP-сервером для любого оборудования, которое поддерживает фильтрацию по протоколу ICAP.

Методы фильтрации

Блокировка сайтов с помощью Entenys URL Filtering 2.0.

UserGate Web Filter использует в работе крупнейшую базу электронных ресурсов, разделенных для удобства оперирования на 70+ категорий. Набор сайтов насчитывает более 500 миллионов адресов. Процесс наполнения базы имеет динамический характер, включая в себя:

- ежедневное обновление списка сайтов;
- повторную проверку уже внесенных ресурсов на предмет изменения контента и актуальности информации о категории.

В руках администратора находится управление доступом к таким категориям, как порнография, вредоносные сайты, онлайн-казино, игровые и развлекательные сайты, социальные сети и многие другие.

Морфологический анализ

Продукт осуществляет анализ веб-страниц на наличие определенных слов и словосочетаний. Данная технология фильтрации позволяет контролировать доступ к определенным разделам сайта, не блокируя ресурс целиком на уровне категории или домена. Подобный подход достаточно актуален для различных социальных сетей, форумов и других порталов, в наполнении которых значительную роль играют пользователи (Web 2.0).

Существует возможность подписки на обновление базы словарей, в том числе списка материалов, запрещенных Министерством Юстиции Российской Федерации, наборов слов «Суицид», «Терроризм», «Порнография», «Плохие слова», «Наркотики». Доступны словари на русском, английском и немецком языках.

Безопасный поиск

Функционал решения включает возможность принудительной активации «безопасного режима» в популярных поисковых системах (Google, Yandex, Yahoo, Bing, Rambler), а также на портале YouTube. С помощью данного инструмента блокировка нежелательного контента осуществляется средствами поисковых порталов, что позволяет добиться высокой эффективности, например, при фильтрации откликов на запросы по графическому или видеоконтенту.

Черные и белые списки

UserGate Web Filter поддерживает работу с «черными» и «белыми» списками электронных ресурсов. Доступ к сайтам, входящим в данные наборы, блокируется\разрешается независимо от других настроек продукта.

В решении реализована возможность подписки на списки сайтов, в том числе запрещенные государством на федеральном уровне.

Блокировка баннеров и всплывающих окон

Проблема всплывающих окон приобретает все большую актуальность. Зачастую переход по ссылке, скрывшейся за навязчивой картинкой, связан не с осознанным решением, а ошибочным нажатием кнопки мыши. UserGate Web Filter осуществляет блокировку подобных окон, в том числе загружаемых с других сайтов.

Вездесущие баннеры не дают покоя во время веб-серфинга. Посещение вполне безопасного сайта может быть связано с принудительным просмотром изображений порнографического характера, размещенных, например, сбоку на странице. UserGate Web Filter решает и эту проблему, выступая в качестве "баннерорезки".

Варианты исполнения

UserGate Web Filter

UserGate Web Filter доступен в качестве программного обеспечения, требующего самостоятельной установки на сервер, конфигурация которого удовлетворяет техническим требованиям продукта.

UserGate Web Filter Appliance

UserGate Web Filter Appliance - программно-аппаратный комплекс (ПАК) на основе UserGate Web Filter. Использование ПАК доступно в режиме "Быстрый старт":

- подключение устройства;
- настройка IP-адресов;
- начало использования.

Более детально о настройке и использовании UserGate Web Filter Appliance можно прочитать в соответствующей главе данного руководства.
.

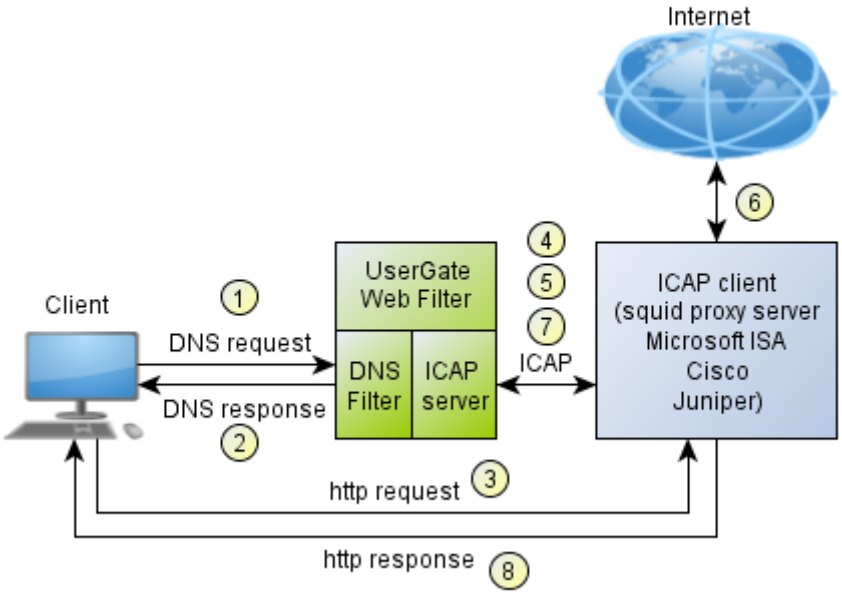
UserGate Web Filter Virtual Appliance

UserGate Web Filter Virtual Appliance - специально созданный образ, предназначенная для развертывания продукта UserGate Web Filter на виртуальной машине.

Принцип работы

Общая схема работы

UserGate Web Filter может производить фильтрацию на уровне DNS- и http-запросов. В случае фильтрации DNS-запросов, UserGate Web Filter эмулирует работу DNS-сервера с расширенными функциями фильтрации. Для фильтрации веб-трафика UserGate Web Filter работает как ICAP-сервер, принимающий на фильтрацию запросы от ICAP-клиента. В качестве ICAP-клиента могут выступать прокси-сервера Squid, Microsoft ISA server, Microsoft TMG, оборудование Cisco, Juniper и другие, поддерживающие работу по протоколу ICAP. Рассмотрим общий принцип работы UserGate Web Filter.



Фильтрация DNS-запросов

1. Клиентский компьютер посылает DNS-запрос на модуль DNS-фильтрации UserGate Web Filter.
2. UserGate Web Filter обрабатывает данный запрос в соответствии с настроенными правилами фильтрации и возвращает пользователю IP-адрес хоста запрошенного ресурса (в случае, если политика фильтрации позволяет данный интернет ресурс для просмотра), либо IP-адрес страницы блокировки (в случае, если политика фильтрации запрещает данный интернет-ресурс).

Фильтрация http-запросов

1. Клиентский компьютер посылает http-запрос на proxy-сервер, являющийся ICAP-клиентом для UserGate Web Filter.
2. Proxy-сервер передает запрос пользователя на анализ в ICAP-сервер UserGate Web Filter.

3. ICAP-сервер анализирует запрос, и если он разрешен политикой фильтрации, то разрешает proxy серверу загрузить контент.
4. Proxy-сервер загружает контент из Интернет и передает его на анализ в ICAP-сервер.
5. ICAP-сервер анализирует контент, и если он разрешен политикой фильтрации, то разрешает proxy-серверу передать контент клиенту.
6. Proxy-сервер передает контент клиенту.

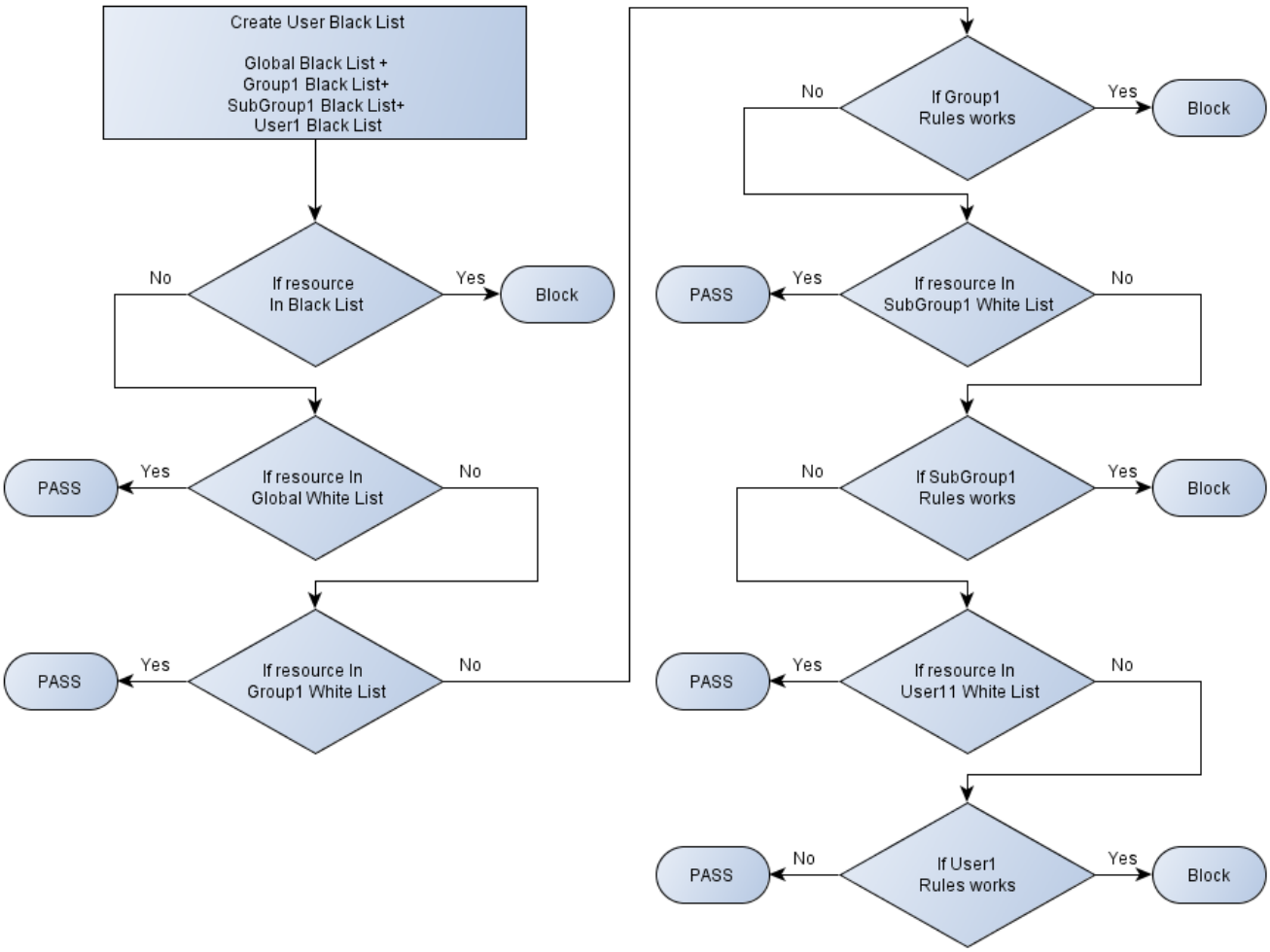
Порядок обработки запросов пользователей

На порядок обработки запросов от пользователей будет влиять наличие черных и белых списков (глобальных, на уровне группы, подгруппы и на уровне пользователя), а также наличие правил фильтрации на каждом из уровней. Порядок обработки DNS-запросов принципиально не отличается от фильтрации http-запросов, за исключением того, что:

- В правилах фильтрации DNS и http используются разные условия.
- Для http-фильтрации доступны опции блокировки рекламы (ad block) и безопасного поиска (safe search). Оба этих фильтра применяются после обработки всех остальных правил.

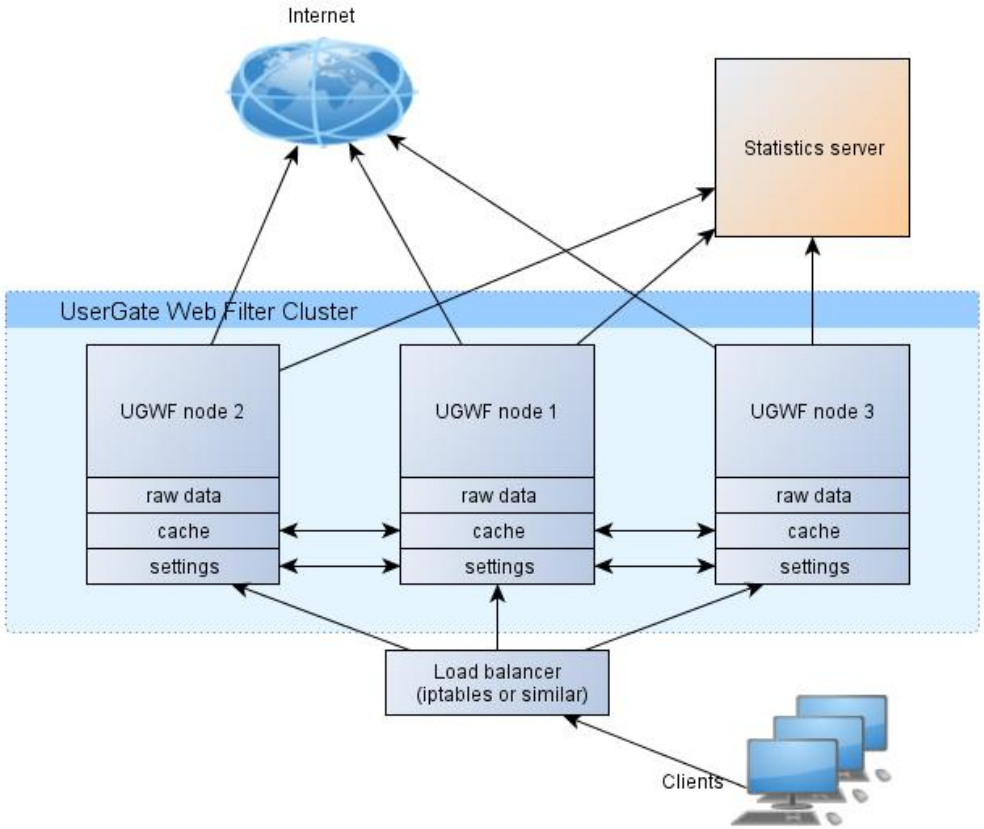
Блок-схема обработки запросов показана на рисунке ниже. В данной блок-схеме, предполагается, что пользователь User1 включен в группу SubGroup1, которая, в свою очередь, входит в группу Group1. Черные и белые списки, правила фильтрации применены к каждому уровню, как указано в следующей таблице:

Уровень	Черный список	Белый список	Применяемые правила
Глобальный уровень	Global Black List	Global White List	-
Уровень Group1	Group1 Black List	Group1 White List	Group1 Rule1 Group1 Rule2
Уровень SubGroup1	SubGroup1 Black List	SubGroup1 Black List	SubGroup1 Rule1 SubGroup1 Rule2 SubGroup1 Rule3
Уровень User1	User1 Black List	User1 Black List	User1 Rule1 User1 Rule2



Кластеризация

В продукте реализована встроенная поддержка кластеризации. Кластер состоит из нод с установленным UserGate Web Filter. Каждая нода предоставляет полноценный сервис по фильтрации DNS- и http-запросов.



Каждая из нод реплицирует настройки и свой локальный кэш со всеми остальными нодами в кластере. Информация о произведенных пользователями запросах хранится локально на каждой ноде (raw data) и не реплицируется на другие ноды. Периодически, каждая нода передает данные на сервер статистики, который обрабатывает полученные данные и генерирует отчеты.

Данная схема кластеризации позволяет объединить ноды, работающие как в одном, так и в нескольких ЦОД, что позволяет обеспечить высокую отказоустойчивость и централизованное управление всеми нодами.

Установка UserGate Web Filter

Системные требования

UserGate Web Filter работает на следующих операционных системах:

- Ubuntu Server 12.04
- Ubuntu Server 12.04 amd64
- Ubuntu Desktop 12.04
- Ubuntu Desktop 12.04 amd64
- Debian 6 i386
- Debian 6 amd64

Минимальные требования к аппаратному обеспечению зависят от количества обслуживаемых пользователей.

	Минимальные требования
До 50 пользователей	Intel® Atom™ D2500 1.86GHz, 2Gb RAM, HDD 500Gb
50-100 пользователей	Intel® Pentium Dual-Core G620 2.60GHz, 2Gb RAM, HDD 500 Gb
100-200 пользователей	Intel® Core i5 - Core i7 3550 3.30GHz, 4Gb, HDD 1Tb
200-300 пользователей	Intel® Core i7 3550 3.30GHz, 8Gb, HDD 1Tb
Более 300 пользователей	Требуется консультация разработчика

Важно! Компьютер с установленным UserGate Web Filter должен иметь доступ в Интернет по протоколам HTTP и HTTPS.

Процесс установки

Возможно 2 варианта инсталляции продукта – установка из репозитария Entensys и установка из DEB-пакетов. Установка из репозитария Entensys является более предпочтительным вариантом, и мы настоятельно рекомендуем использовать именно ее.

Для установки UserGate Web Filter из репозитория Entensys, выполните следующие команды:

Для Ubuntu:

echo 'deb http://dc.entensys.com/ubuntu precise extra' | sudo tee -a /etc/apt/sources.list
wget http://dc.entensys.com/ubuntu/entensys.gpg -O - | sudo apt-key add -
sudo apt-get update
sudo apt-get install webfilter

Для Debian:

echo 'deb http://dc.entensys.com/debian squeeze extra' | sudo tee -a /etc/apt/sources.list
wget http://dc.entensys.com/debian/entensys.gpg -O - | sudo apt-key add -
sudo apt-get update
sudo apt-get install webfilter

Если UserGate Web Filter устанавливается из DEB-пакетов, требуется выполнить команды:

sudo apt-get update
sudo dpkg -i entensys-otp.deb
sudo dpkg -i webfilter.deb

При выполнении последней команды на экране будет отображено сообщение об ошибках разрешения зависимостей пакета. Для автоматической установки зависимостей выполните команду:

sudo apt-get -f install

После этой команды сервис UserGate Web Filter будет установлен. UserGate Web Filter устанавливается в папку */usr/local/entensys*.

Для работы сервису требуются следующие порты:

3128 TCP - встроенный веб-сервер (сервер XML-RPC)

1344 TCP – ICAP-server

10053 UDP - DNS resolver

Перед установкой UserGate Web Filter необходимо убедиться, что указанные порты не используются другими сервисами.

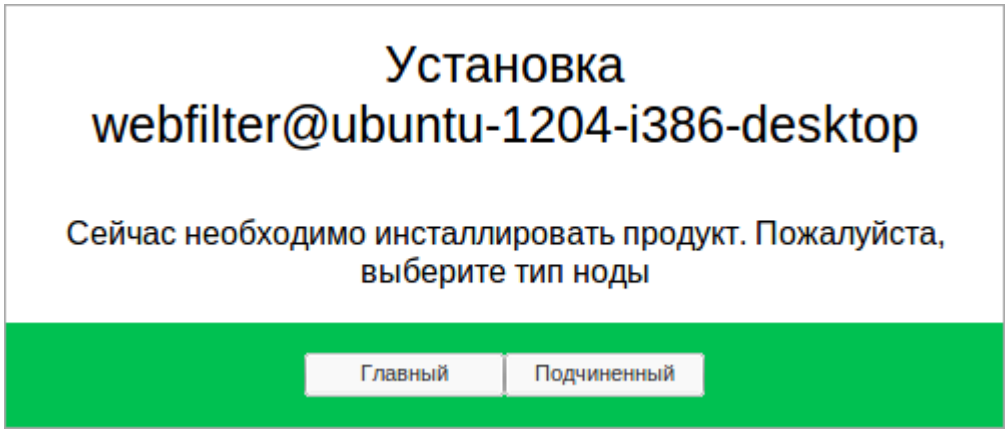
Запуск и остановка сервиса UserGate Web Filter выполняются с помощью команд:

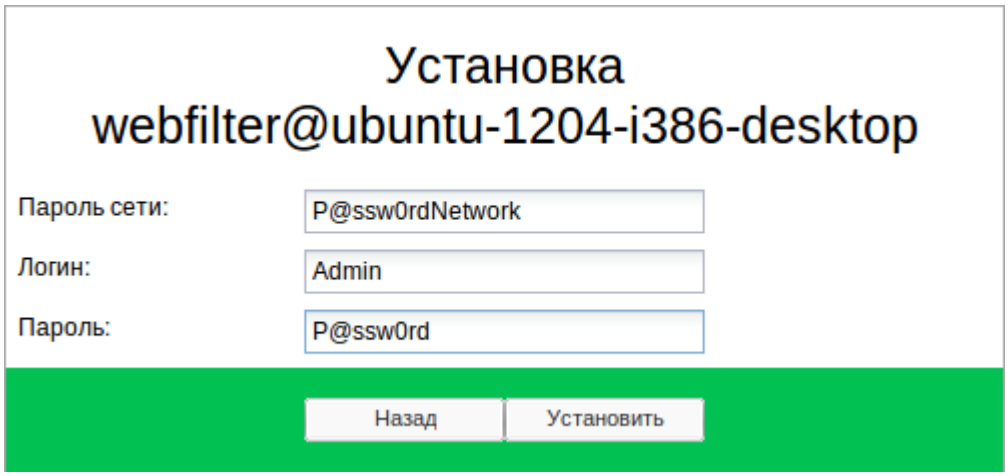
sudo service webfilter start(stop)

Входящие DNS-запросы перенаправляются на порт «DNS resolver'a» средствами *iptables* (соответствующие правила в *iptables* создает сервис */etc/init.d/webfilter_rules*).

Настройка и администрирование UserGate Web Filter выполняется через веб-консоль, доступную по ссылке http://localhost:3128/admin/.

При первом запуске консоль администратора предложит выбрать тип сервера: «Главный/Подчиненный» (master/slave), задать пароль сети, необходимый при установке кластера, и пароль администратора сервиса UserGate Web Filter. Если установка выполняется на единственный сервер, выбирается тип сервера – Главный (Master node).





Важно! Для работы UserGate Web Filter необходимо активировать триальную или полнофункциональную лицензию. Активация лицензии выполняется через консоль администратора с помощью специального пин-кода и требует подключения к сети Интернет.

Лицензия ограничивает количество пользователей в UserGate Web Filter, которые могут быть включены одновременно.

Установка кластера UserGate Web Filter

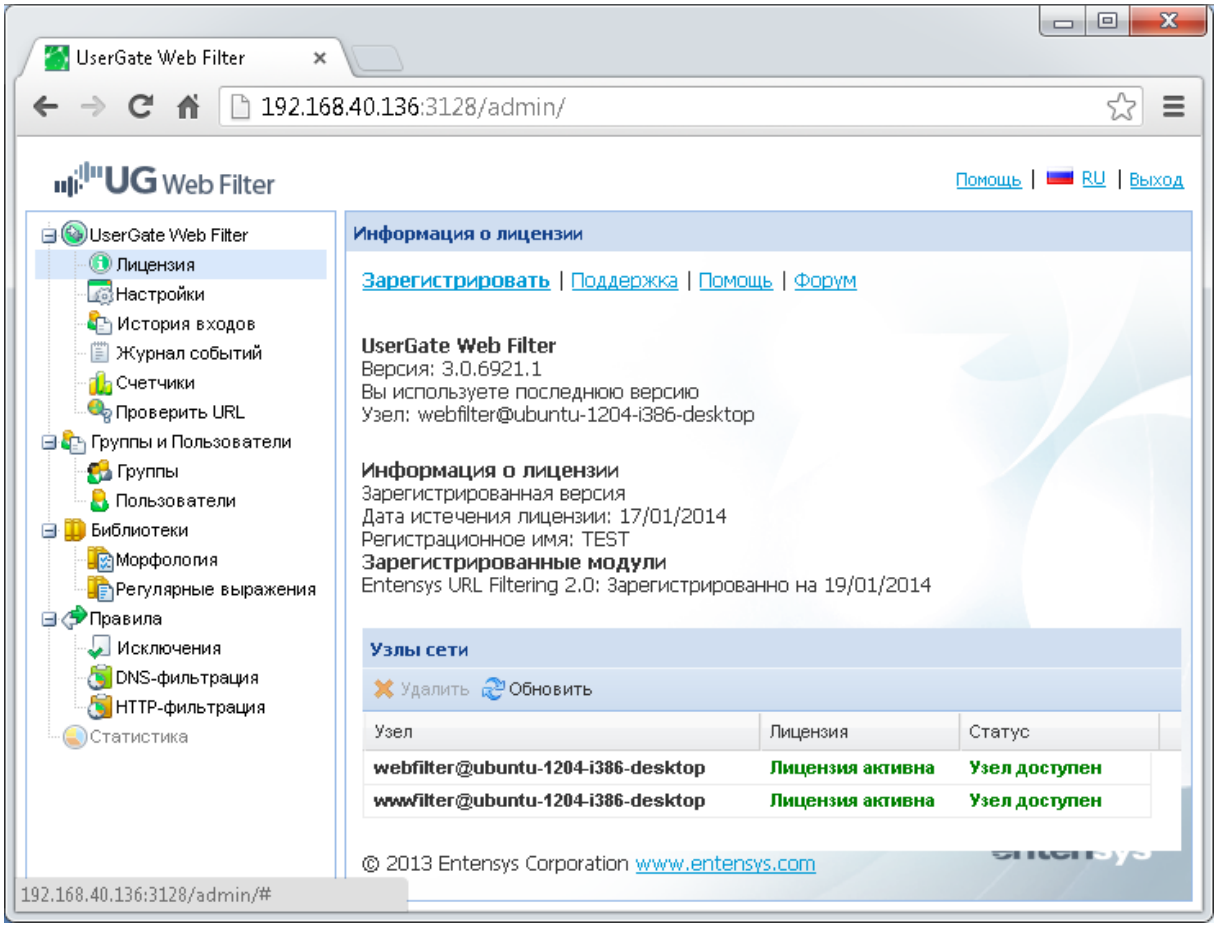
Возможности UserGate Web Filter позволяют создать распределенную систему фильтрации, состоящую из нескольких серверов (узлов). Работа UserGate Web Filter в кластере дает следующие преимущества:

- идентичность настроек на всех узлах;
- распределенный DNS-кэш;
- возможность балансировки нагрузки сторонними средствами (iptables, haproxy и т.д.).

Процедура установки кластера выглядит следующим образом:

- установить UserGate Web Filter на первый сервер;
- открыть веб-консоль администратора, выбрать тип «Главный (Master)»;
- задать пароль сети и пароль администратора;
- установить UserGate Web Filter на второй (третий и т.д.) сервер;
- открыть веб-консоль администратора на втором (третьем и т.д.) сервере;
- выбрать тип «Подчиненный (slave)», указать пароль сети и адрес master-сервера.

Адрес master-сервера указывается в формате: *webfilter@hostname*, где *hostname* - имя master-сервера. Узлы кластера UserGate Web Filter отображаются на странице «Лицензия» в консоли администратора. При работе в кластере достаточно зарегистрировать продукт на одном из узлов.



Выбор типа сервера master/slave определяет механизм создания базы настроек. При выборе типа «master» на сервере создается пустая база настроек, при типе «slave» база настроек копируется с master-узла. В дальнейшем все узлы кластера UserGate Web Filter являются равноправными.

Важно! Общение между узлами в кластере UserGate Web Filter выполняется через RPC-протокол, т.е. в общем случае используются динамические порты. Все машины кластера должны видеть друг друга по именам. Для этого достаточно обеспечить идентичность файлов */etc/hosts* на всех узлах кластера.

Удаление UserGate Web Filter

Для полного удаления UserGate Web Filter нужно выполнить команды:

sudo apt-get remove --purge webfilter

sudo apt-get remove --purge entensys-otp

Лицензирование UserGate Web Filter

Для работы UserGate Web Filter должен иметь триальную или полнофункциональную лицензию. Активация лицензии выполняется через консоль администратора с помощью специального ПИН-кода и требует подключения к сети Интернет. Лицензия ограничивает количество пользователей в UserGate Web Filter, которые могут быть включены одновременно.

Страница консоли **Лицензия** предназначена для отображения лицензионной информации о продукте и её текущем статусе. Также на странице имеются ссылки:

- *Зарегистрировать* - позволяет зарегистрировать новую лицензию;
- *Поддержка* - ссылка на портал поддержки, где можно оформить заявку в техническую поддержку и получить дополнительную информацию о продукте (примеры вариантов настроек, часто задаваемые вопросы, техническая информация);
- *Помощь* - ссылка на онлайн-руководство к программе;
- *Форум* - ссылка на сайт производителя в раздел «Форум».

Ссылка *Доступна новая версия* появляется при наличии новой версии на сайте производителя и позволяет перейти на страницу загрузок новых версий для скачивания необходимого обновления.

Обновление программного обеспечения

Разработчик постоянно работает над улучшением программного продукта. О появлении новой версии вы узнаете посредством уведомления в веб-консоли продукта в разделе **Лицензия**. Для установки новой версии вам потребуется произвести следующие действия (если установка производилась из репозитария Entensys):

1. Войти в консоль Linux.
2. Выполнить следующие команды:

   sudo apt-get update

   sudo apt-get install webfilter

3. По окончании установки перезагрузить систему.

Важно! Для выполнения обновления программного обеспечения, компьютер должен иметь доступ в Интернет.

Если установка производилась из deb-пакета, то необходимо скачать обновленные пакеты, и установить их поверх существующей версии.

Установка клиента http-фильтрации для работы с UserGate Web Filter

Для фильтрации http-трафика средствами ICAP-протокола требуется установить и настроить ICAP-клиент. В качестве ICAP-клиентов могут выступать различные прокси-сервера и оборудование, поддерживающие данный протокол, например прокси-сервер Squid, Microsoft ISA server и другие.

Рассмотрим настройку ICAP клиента на основе прокси-сервера Squid. Для установки Squid выполните команды:

sudo apt-get update

sudo apt-get install squid3

Для работы с ICAP-сервером UserGate Web Filter в файл настроек */etc/squid3/squid.conf* нужно добавить фрагмент:

icap_enable on

icap_preview_enable on

icap_preview_size 4096

icap_send_client_ip on

icap_service service_req reqmod_precache bypass=0 icap://10.0.3.10:1344/request

adaptation_access service_req allow all

icap_service service_resp respmod_precache bypass=0 icap://10.0.3.10:1344/response

adaptation_access service_resp allow all

http_port 8080 transparent

10.0.3.10 - адрес сервера UserGate Web Filter. После изменения настроек Squid нужно перезапустить сервис:

sudo service squid3 restart

Важно! Сервер UserGate Web Filter не поддерживает режим «*icap_preview_enable off*». Работа с https-трафиком в данный момент не поддерживается.

Настройки

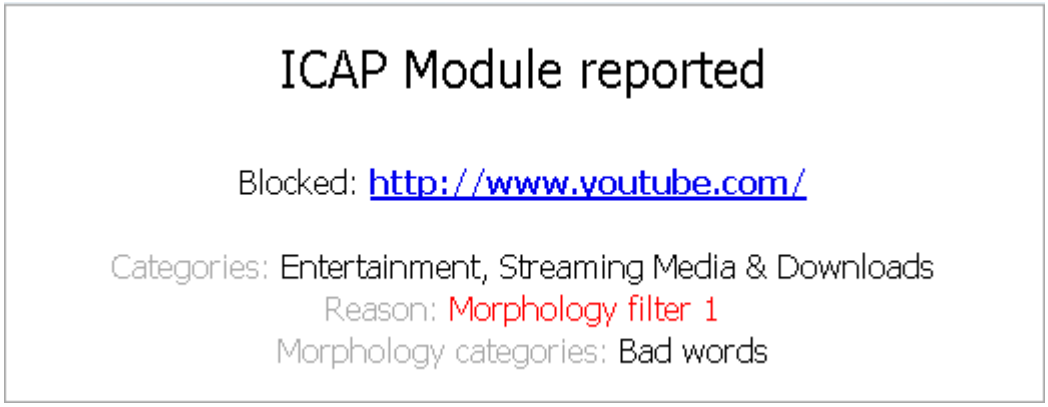
Основные настройки

Часовой пояс отвечает за корректное отображение статистики, журнала событий и истории входов (в нужном часовом поясе).

IPv4 адрес для заблокированных запросов – IP-адрес, который система будет отдавать в ответ на заблокированные запросы DNS.

IPv6 адрес для заблокированных запросов – то же, что и пункт выше, только для IPv6 адресов.

URL для заблокированных http-запросов – специальная страница для отображения информации о том, какая категория морфологии сработала при блокировке http-страницы. По умолчанию страница блокировки выводит информацию о категориях заблокированного сайта, морфологических категориях и причине блокировки.



Разрешить рекурсивные DNS-запросы – опция, которая позволяет запретить рекурсивный поиск имен.

Использовать DNS-кэш – позволяет отключить использование кэша для DNS-запросов.

Ответ на DNS-запросы от неавторизованных пользователей - при выставленном параметре «Возвращать REFUSED» все запросы, которые пришли от неизвестного пользователя (которого нет в списке на странице «Пользователи»), будут отклонены, а на странице браузера пользователя появится ошибка «невозможно обнаружить адрес узла».

Максимальный TTL-ответа от DNS-сервера – максимальное время жизни записи DNS при ответе пользователю. Более высокое значение снизит нагрузку на сервер DNS-фильтрации, но может повлиять на актуальность DNS-записей.

Настройки правил

Обработка правил – позволяет глобально выключить правила обработки правил блокировки UserGate Web Filter, например для проверки.

Действие с DNS-запросами, если облачный фильтр недоступен – задает поведение UserGate Web Filter при недоступности облачной фильтраци по

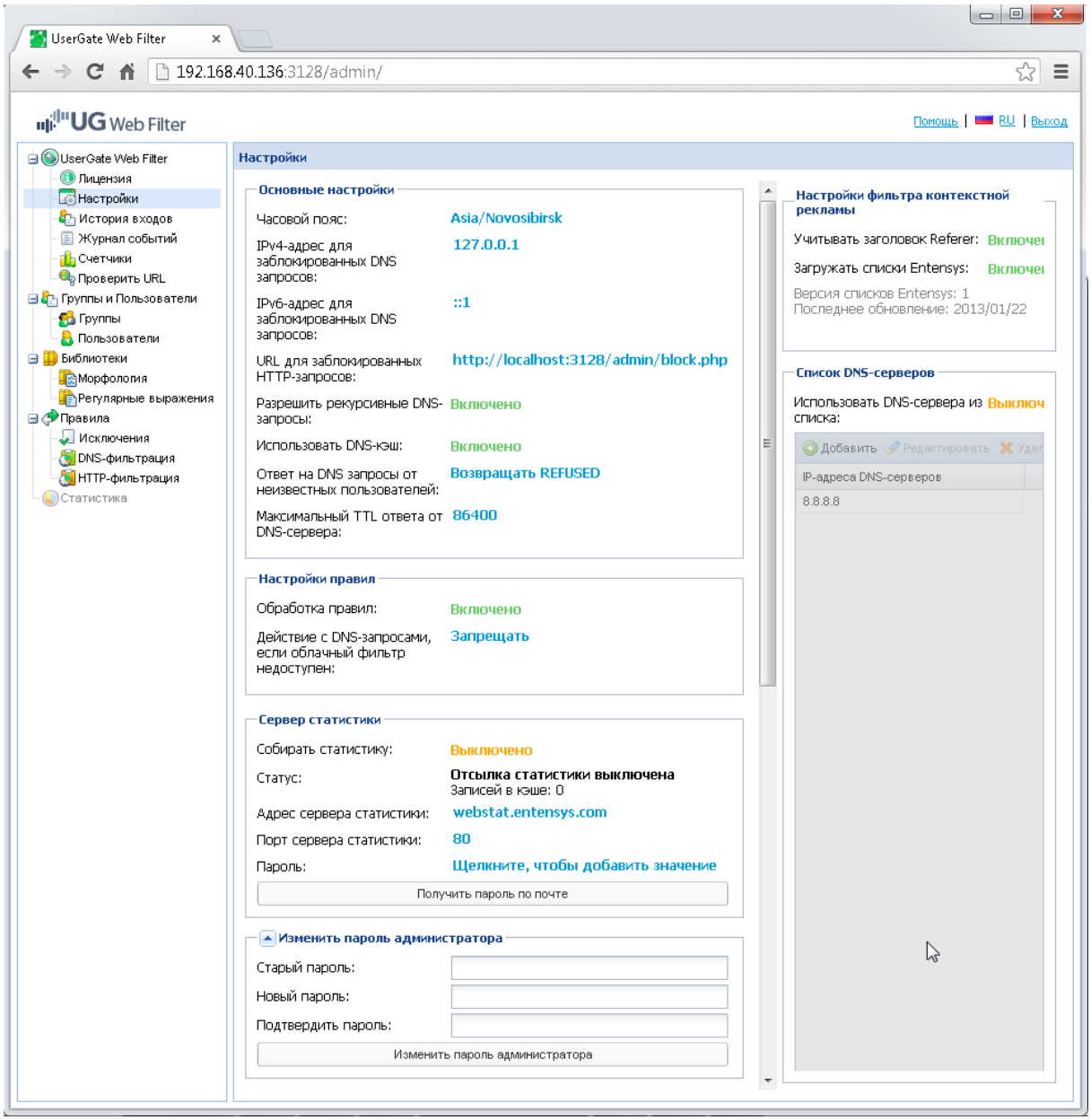
категориям сайтов Entensys URL Filter 2.0. При выставленном параметре «Возвращать REFUSED» запросы будут отклонены, а на странице браузера пользователя появится ошибка, что невозможно найти имя. При выставленном параметре «Возвращать SERVFAIL» вернется ответ о невозможности обработать запрос.

Сервер Статистики

Собирать статистику – включить или выключить сбор статистики

Статус – текущий статус кэша базы статистики и количество результатов, отосланных на сервер статистики. Имеет в качестве параметра различные способы отображения ошибок или индикацию об успешно завершенных действиях.

Пароль – уникальный хэш-код, получаемый по почте для авторизации и идентификации на сервере статистики.



Настройки фильтра контекстной рекламы

Фильтр основан на знаниях основных параметров рекламы в интернете, таких как размер баннеров, код баннеров, специальные механизмы обнаружения рекламных баннеров. Данный метод позволяет очень просто и эффективно заблокировать практически всю рекламу на любой странице интернета, и оградить вас от всплывающих окон. Например, вас когда-нибудь раздражала реклама на файловых хостингах, подобных letitbit и других?! После включения данного фильтра вы не увидите больше рекламу и всплывающие окна.

Список DNS-серверов

В настройках «Список DNS-серверов» можно указать один или несколько DNS–серверов, к которым UserGate Web Filter будет обращаться для разрешения DNS-запросов. Если сервера пересылки не указаны, то сервер будет

использовать публичные DNS-сервера, предоставляемые компаниями Google и Cisco:

8.8.8.8

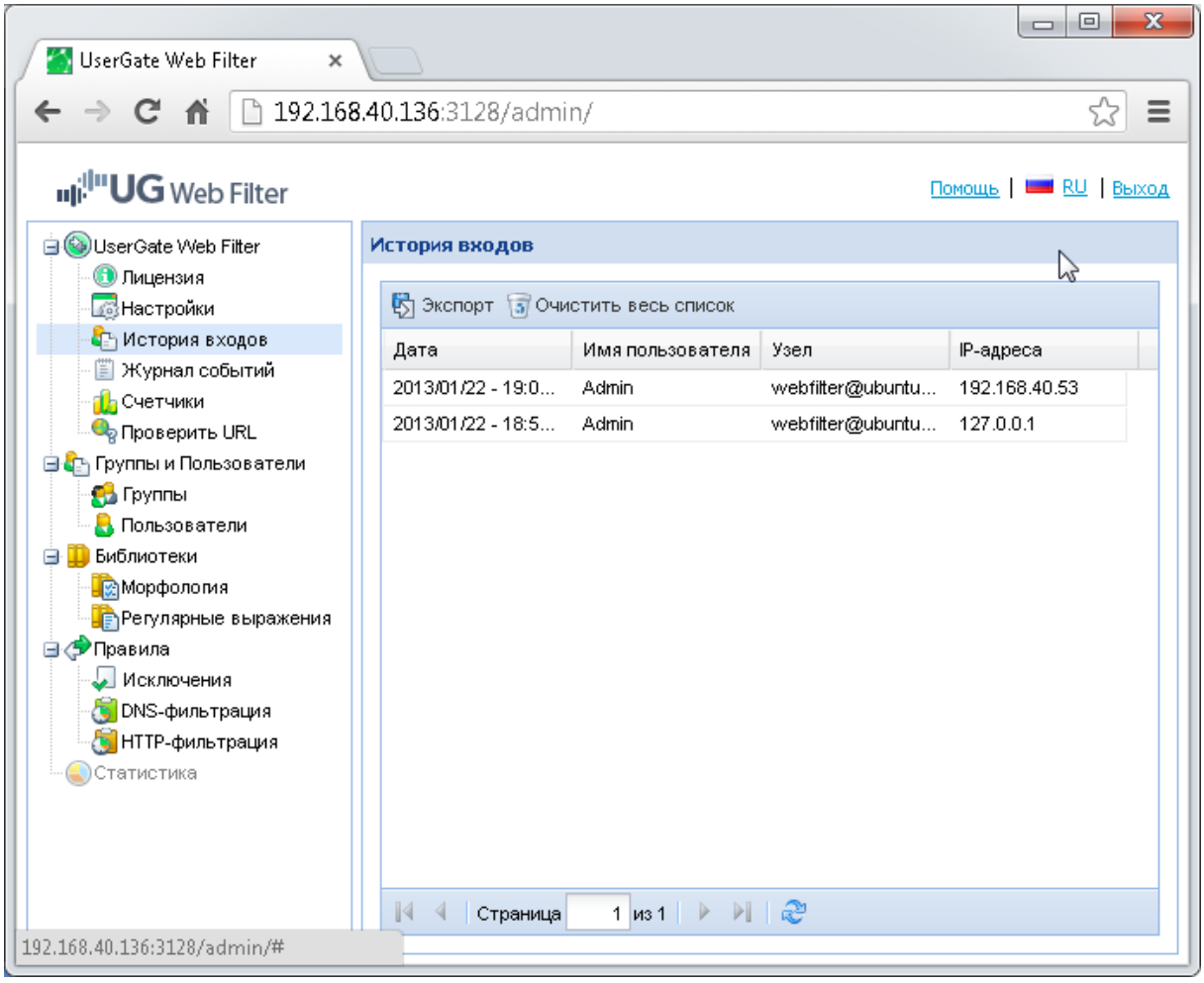
8.8.4.4

64.102.255.44

128.107.241.185

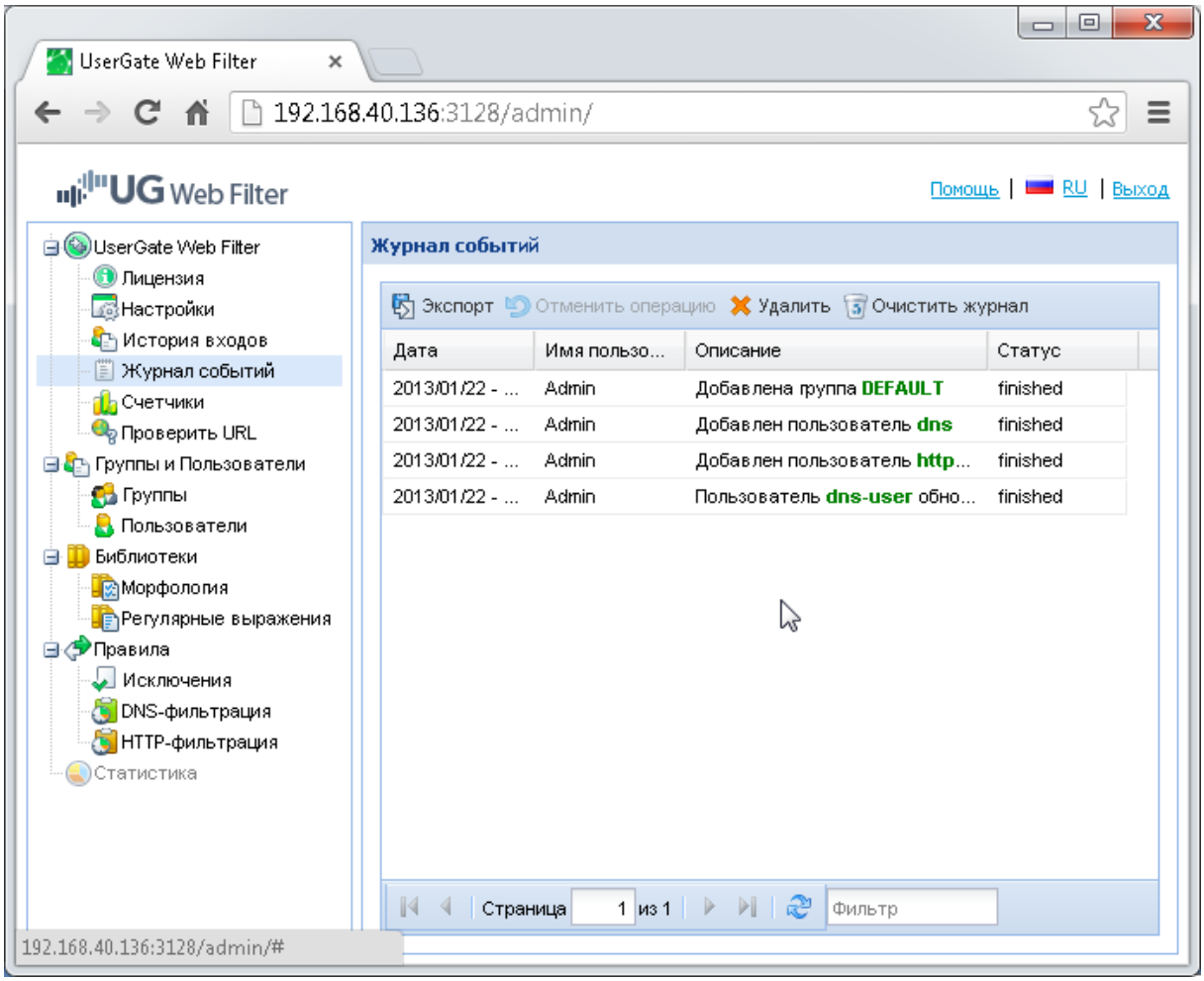
История входов

В данном разделе отображается история аутентификации на данной конкретной ноде (компьютере) или на группе компьютеров, связанных в кластер.



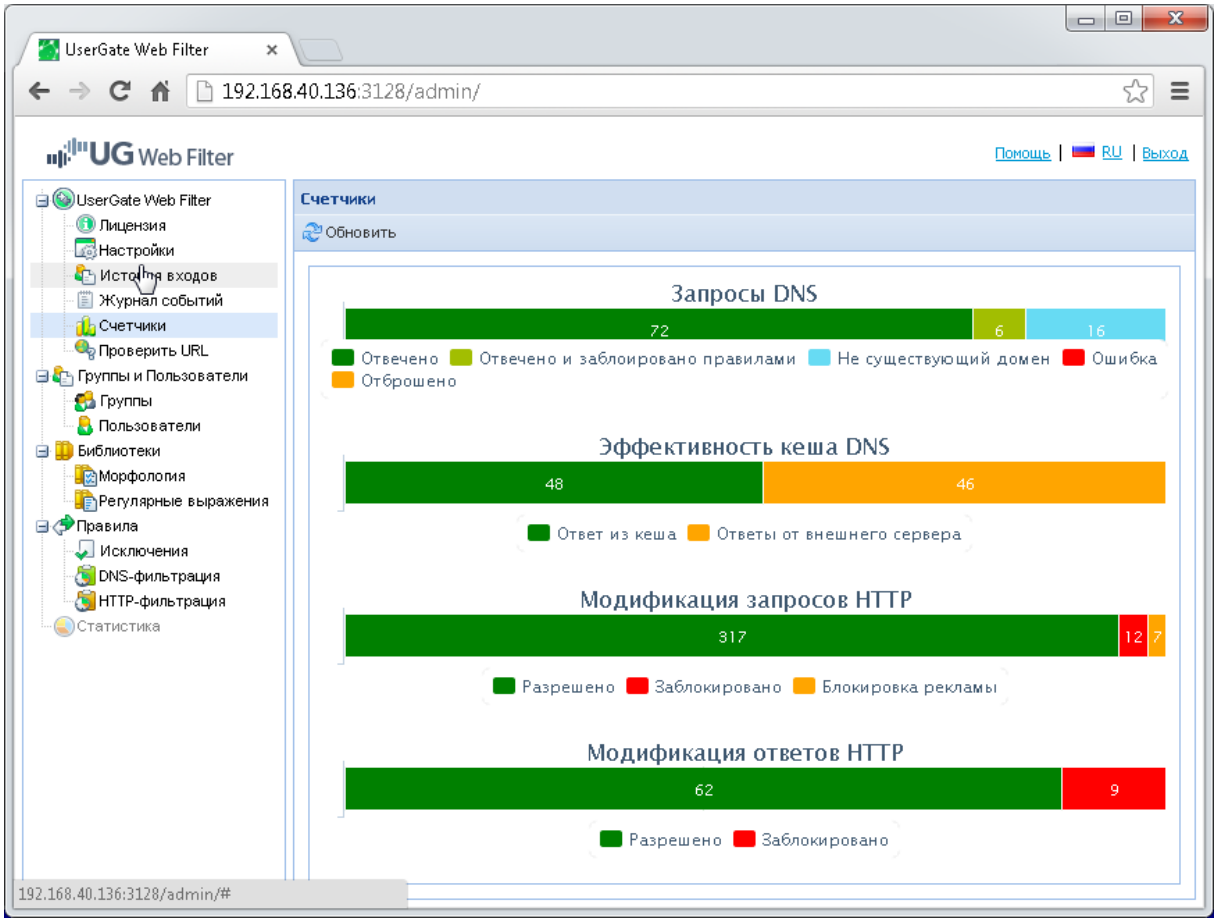
Журнал событий

Данная страница служит для отображения истории изменений настроек UserGate Web Filter и действий, произведенных администратором системы. Любое действие можно отменить, выбрав его и нажав на соответствующую кнопку.



Счетчики

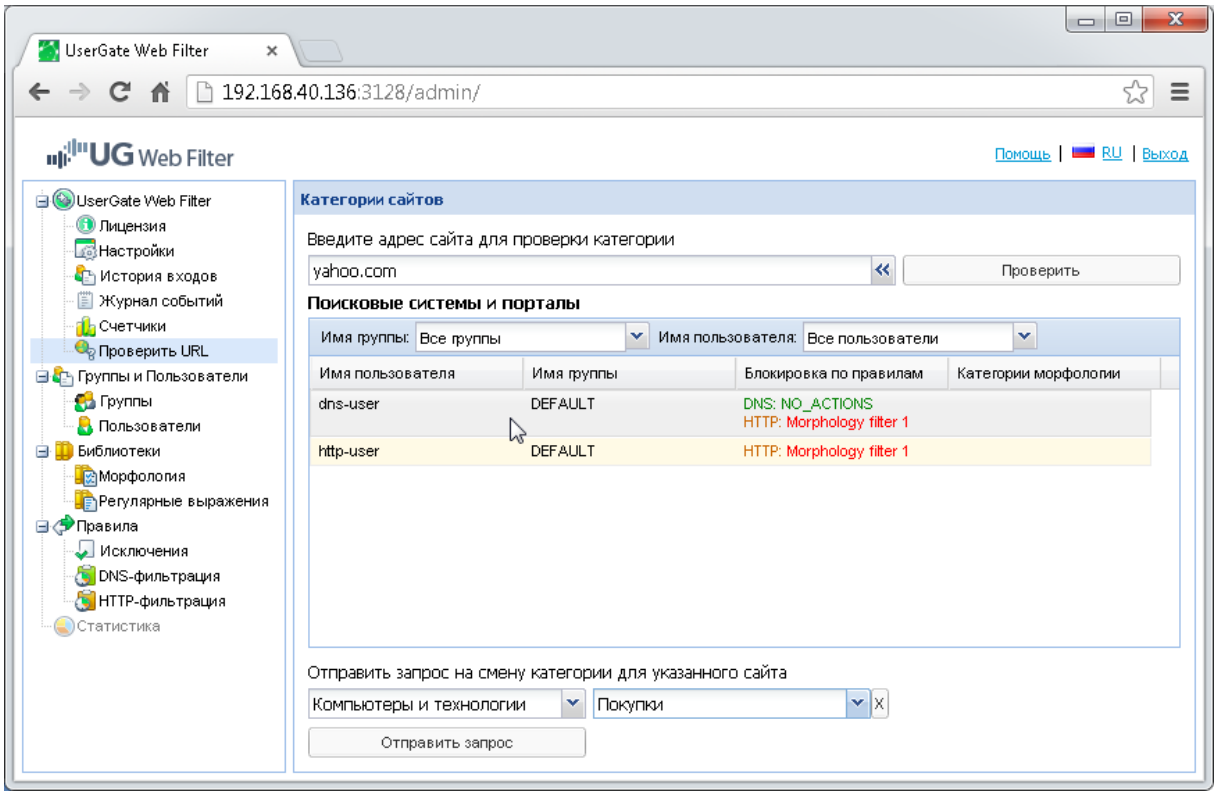
Страница предназначена для визуализации суммарной информации по основным числовым параметрам статистики UserGate Web Filter. Например, вы можете увидеть суммарное количество запросов на разрешение имен, количество заблокированных из них и количество неизвестных запрошенных DNS-запросов. В следующем графике визуализированы показатели эффективности работы кэша DNS. Последние счетчики покажут вам количество блокировок остальных методов фильтрации (Морфология, Банерорезка, Черные и белые списки, Безопасный поиск) на этапе запроса к серверу «Модификация запросов HTTP» и на этапе обработки ответа от сервера «Модификация ответов HTTP».



Проверить URL

На данной странице можно проверить, к какой категории сайтов принадлежит интересующий адрес, а также отправить запрос на смену этой категории, если вы считаете, что текущая не соответствует содержимому сайта. Здесь же реализована возможность проверить, какой морфологической базой блокируется введенный адрес (при использовании морфологического фильтра).

Обратите внимание, что DNS-правила отображаются зеленым цветом, HTTP-оранжевым.



Пользователи и группы

Для работы с сервисом UserGate Web Filter необходимо создать группы пользователей. Запросы от неавторизованных пользователей по умолчанию не обрабатываются. Поддерживаются следующие типы авторизации пользователей:

- по IP-адресу;
- по диапазону IP-адресов;
- через динамический IP-адрес.

Последний тип авторизации предполагает использование специальной программы-агента, которая устанавливается на машину пользователя. Агент авторизуется в UserGate Web Filter через логин и пароль, указанные в свойствах пользователя. При создании пользователя обязательными параметрами являются:

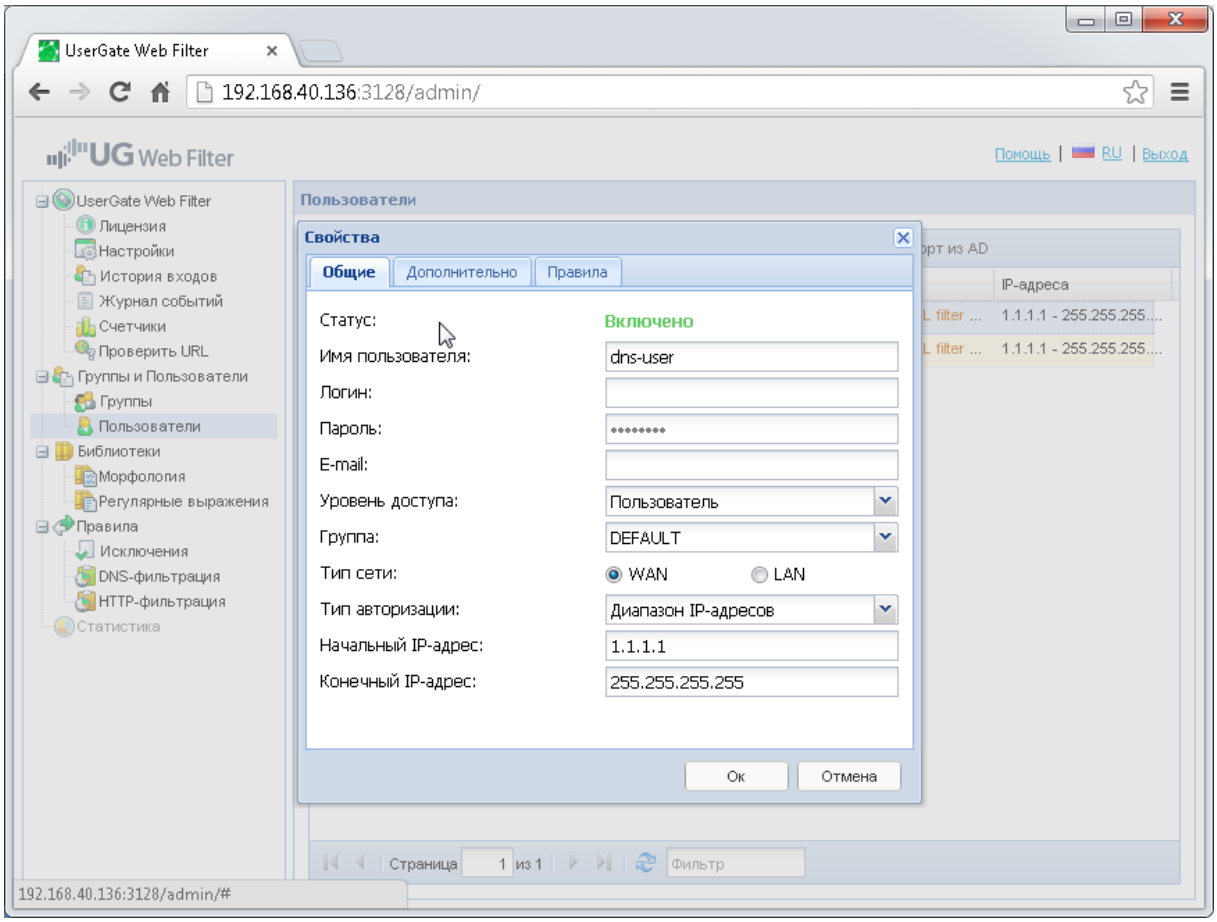
- имя пользователя;
- IP-адрес или диапазон IP-адресов.

При этом, IP-адрес пользователя, указанный как WAN-адрес, должен быть уникальным. Проверка на уникальность адреса выполняется сервисом UserGate Web Filter автоматически. Дополнительно в свойствах пользователя можно указать логин и пароль для доступа к веб-консоли, а также уровень доступа. Предусмотрено два уровня доступа:

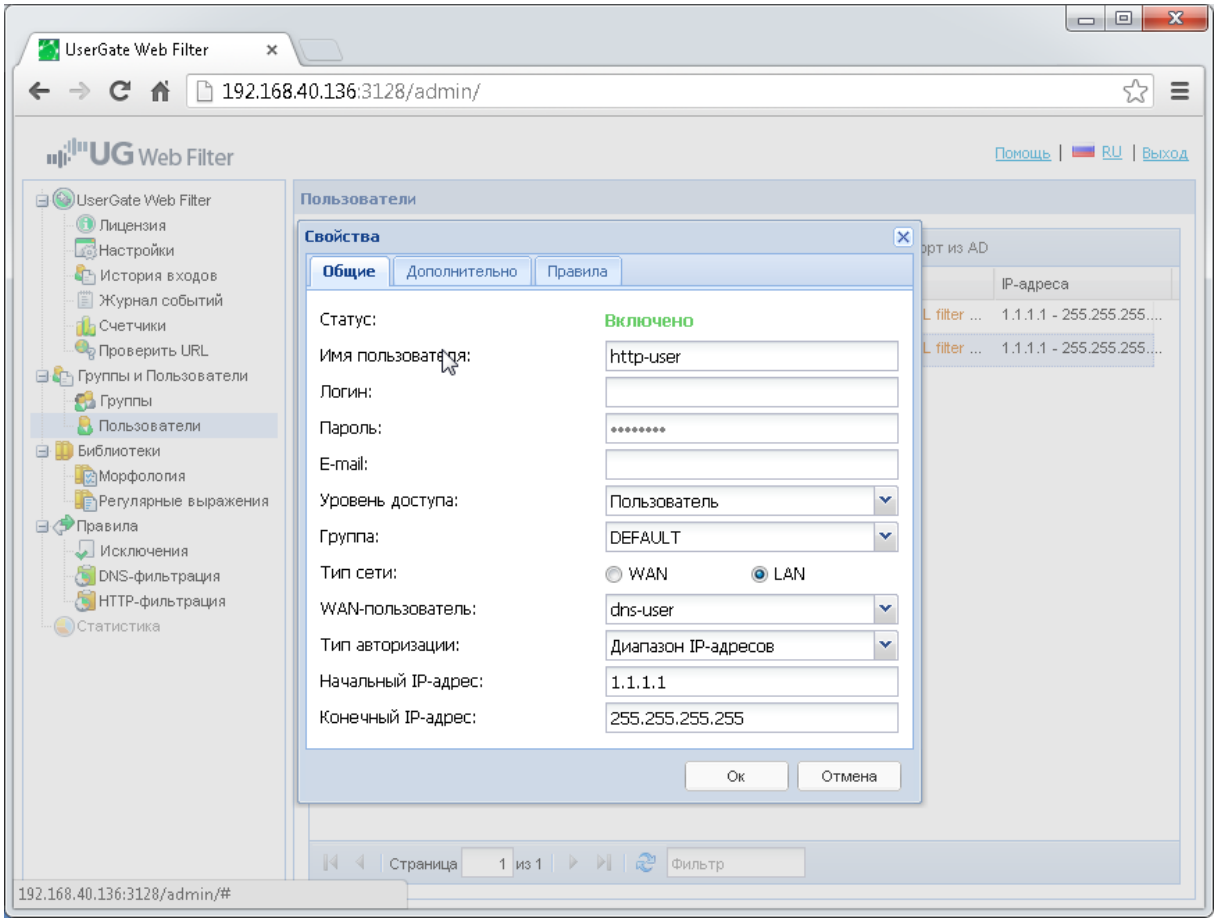
- «Пользователь»
- «Администратор»

Уровень доступа определяет возможности пользователя для создания других пользователей и групп.

Уровень «Пользователь» позволяет пользователю создавать собственные правила фильтрации. Уровень «Администратор» дает пользователю возможность создания собственных групп и пользователей, а также позволяет применять собственные правила фильтрации к другим пользователям своих групп.



При создании пользователя в UserGate Web Filter можно выбрать тип IP-адреса: WAN или LAN. Предполагается, что пользователи UserGate Web Filter могут располагаться за NAT-маршрутизатором. В этом случае пользовательские DNS-запросы будут поступать с одного IP-адреса (адреса NAT- маршрутизатора)



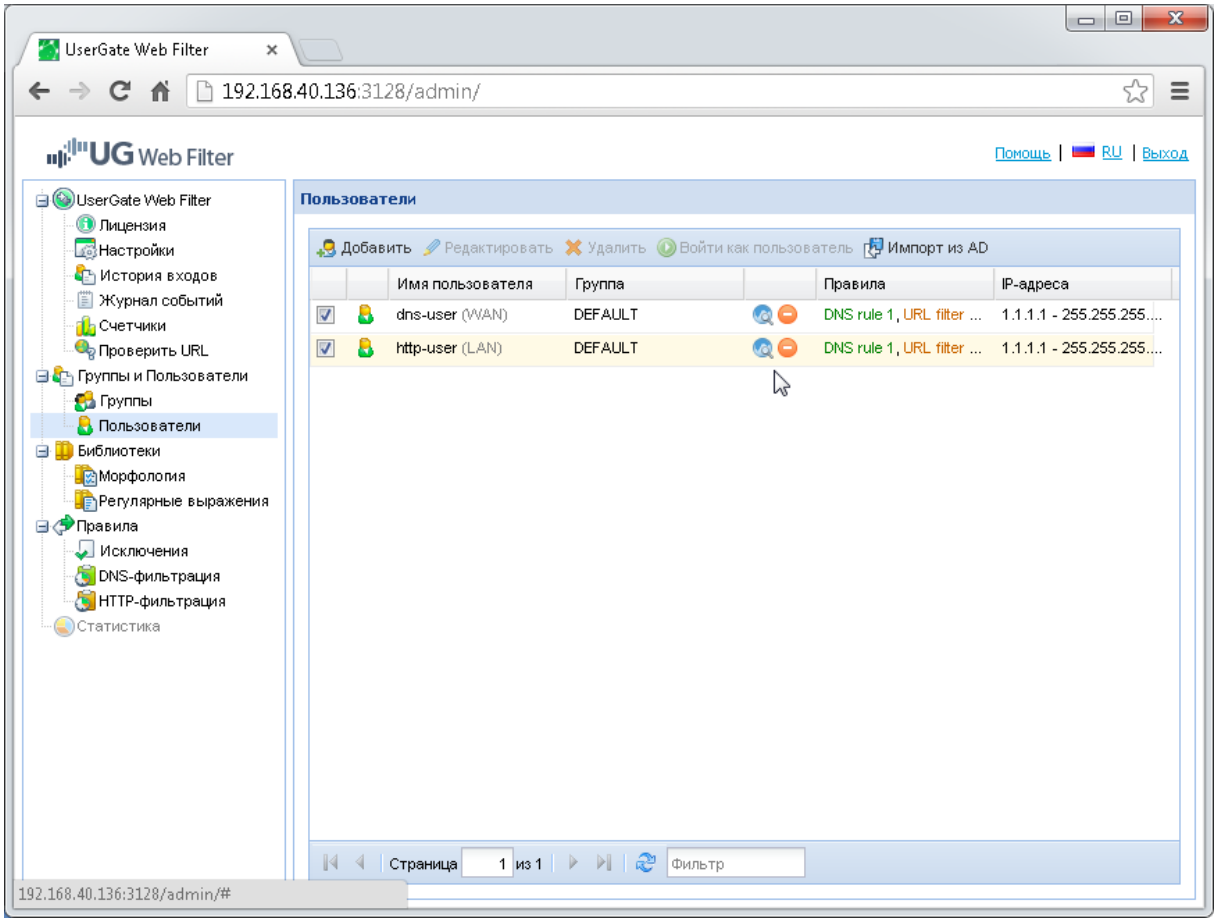
При работе с ICAP прокси-сервер Squid может быть настроен на передачу дополнительного заголовка «X-Client-IP» в самом ICAP-запросе. В этом заголовке сервису UserGate Web Filter может быть передан реальный IP-адрес пользователя, т.е. адрес пользователя в локальной сети (LAN-адрес). В этом случае авторизация ICAP-запроса выполняется по паре IP-адресов: по WAN-адресу, с которого поступил ICAP запрос, и по LAN-адресу. В настройках прокси-сервера Squid можно отключить передачу локального адреса. В этом случае пользователь будет авторизоваться по адресу, с которого фактически поступил ICAP-запрос.

Способов создания пользователей два:

1. вручную - кнопка «Добавить»;
2. импорт из ActiveDirectory (кнопка «Импорт из AD»).

Помимо правил DNS-фильтрации и HTTP-фильтрации персональная настройка позволяет настроить язык интерфейса консоли управления, а также редактировать настройки безопасного поиска и фильтра контекстной рекламы (вкладка «Дополнительно» в окне свойств пользователя).

Обратите внимание на то, что в настройках пользователя DNS-правила отображаются зеленым цветом, HTTP-правила отображаются оранжевым.



Морфология

Морфологический анализ - механизм, который распознает отдельные слова на веб-сайте. Если в них содержатся указанные слова и словосочетания, доступ к сайту блокируется.

Морфологический анализ выполняется как при проверке запроса пользователя, так и при получении ответа от веб-сервера и до его передачи пользователю. Получив ответ от веб-сервера, ICAP-клиент передает его серверу UserGate Web Filter. UserGate Web Filter просматривает текст на странице и подсчитывает его суммарный «вес», исходя из «весов» слов, указанных в морфологических категориях. Если «вес» страницы превышает «вес» морфологической категории, UserGate Web Filter возвращает ссылку о блокировке доступа. Анализ на этапе запроса позволяет блокировать доступ по самой строке запроса.

Для фильтрации по содержанию страницы требуется:

- создать одну или несколько морфологических категорий
- указать список запрещенных слов с весами для каждой категории
- указать «вес» каждой категории
- создать правило http-фильтрации, содержащее одну или несколько морфологических категорий
- применить правило к пользователю или группе пользователей

При подсчете «веса» страницы учитываются все словоформы (леммы) запрещенных слов. Для поиска словоформ UserGate Web Filter использует встроенные словари русского, английского и немецкого языков.

Страница **Библиотеки-Морфология** служит для управления морфологическими словарями. При нажатии на кнопку «Добавить» будет выведен диалог добавления новой категории морфологического анализа, в котором можно указать слова для этой категории. Чтобы импортировать готовый список слов, достаточно нажать на кнопку «Импорт». Каждое слово должно быть расположено на новой строке. В конце строки никаких символов указывать не нужно.

Условия запрета доступа на сайт по категории морфологии:

- *Включить категорию* - блокировка по данной категории морфологии будет работать, только если стоит значение «Включить».
- *«Вес» («вес» категории)* - данный параметр определяет «вес» страницы (сумму «весов» всех слов, содержащихся на странице), при достижении которого доступ на страницу будет заблокирован.

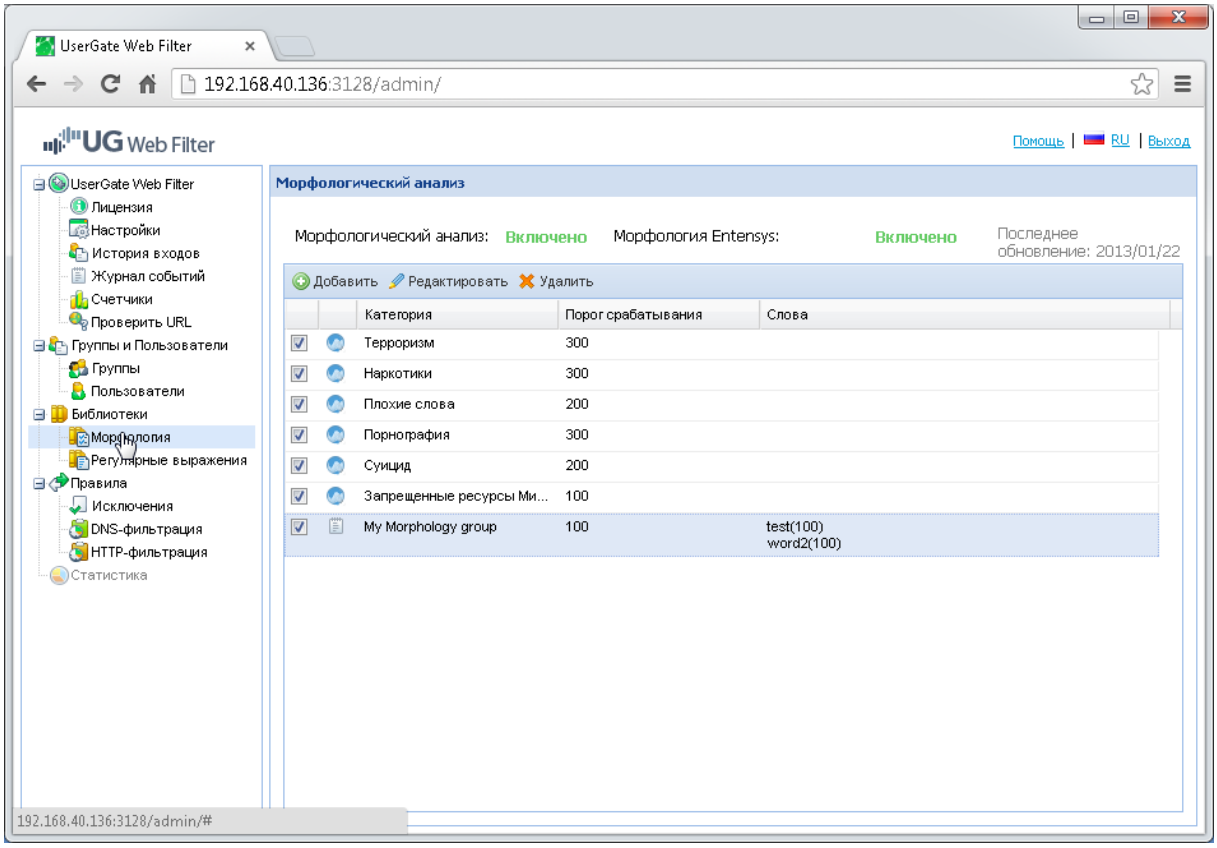
- *«Вес» («вес» слова)* - данный параметр определяет «вес» каждого конкретного слова.

Все параметры можно редактировать вручную. По умолчанию они выставляются на значении «100».

Важно! При добавлении слова в морфологический словарь, можно использовать модификатор «!» перед словом, например «!bassterd». В данном случае жаргонное слово не будет преобразовываться в словоформы, что может серьезно уменьшить вероятность ложной блокировки.

Важно! В списке слов категории можно указывать как отдельные слова, как и словосочетания.

Существует возможность подписки на словари, предоставляемые компанией Entensys, такие, как список материалов, запрещенных Министерством Юстиции Российской Федерации, наборов слов «Суицид», «Терроризм», «Порнография», «Плохие слова», «Наркотики». Данные словари нельзя редактировать, их можно включить, и использовать при определении правил http-фильтрации.



Регулярные выражения

Фильтрация по регулярным выражениям позволяет блокировать доступ к ресурсу как на этапе запроса, так и на этапе анализа ответа от веб-сервера. Для фильтрации по регулярным выражениям нужно:

- создать одно или несколько регулярных выражений;
- создать правило http-фильтрации, выбрав регулярные выражения в качестве условий;
- применить правило фильтрации к пользователю или к группе пользователей.

Для создания регулярного выражения необходимо нажать кнопку «Добавить», и заполнить поля «Шаблон» и «Имя». В поле «Шаблон» необходимо вписать само регулярное выражение.

Подробную информацию о составлении регулярных выражений можно найти в статье на сайте IBM.

Исключения

Страница предназначена для задания черных и белых списков.

Черными списками называются списки, сайты из которых будут всегда заблокированы.

Белыми списками называются списки, сайты в которых будут всегда разрешены.

Черные и белые списки можно создавать как для всех пользователей, так и для выбранных пользователей и\или групп. Это можно сделать, выбрав в выпадающих списках нужных пользователей.

Политика блокировки определяет порядок работы списков. Если выбрана политика белых списков, то будет разрешено все, что не запрещено явно (в черных списках). Если выбрана политика белых списков, то будет заблокировано все, что не разрешено явно (в белых списках).

В списках можно использовать специальные символы “*” и “?”.

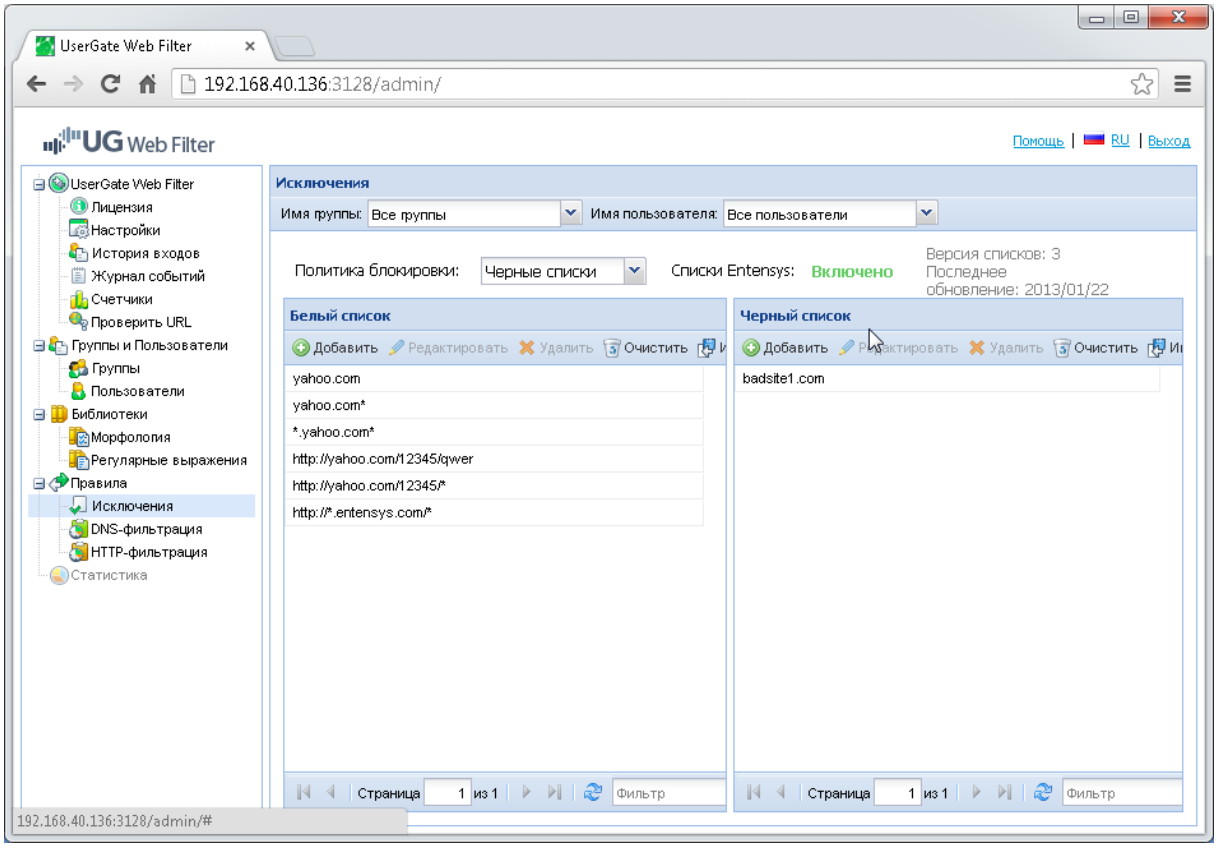
«*» – любое количество любых символов

«?» – один любой символ

Формат импортируемых списков следующий:

Пример записи	Обработка DNS-запросов	Обработка http-запросов
yahoo.com	блокируется весь домен, домены 3 уровня не блокируются	блокируется весь домен и все url этого домена, домены 3 уровня не блокируются
yahoo.com*	блокируется весь домен, домены 3 уровня не блокируются	блокируется весь домен и все url этого домена, домены 3 уровня не блокируются
.yahoo.com	блокируется весь домен, домены 3, 4 и выше уровней блокируются	блокируется http://любое.yahoo.com/любое/
yahoo.com/12345/qwer	ничего не блокируется	блок строго yahoo.com/12345/qwer
yahoo.com/12345/*	ничего не блокируется	yahoo.com/12345/ любое/

Важно! Для ускорения обработки черных и белых списков, рекомендуется вести списки без использования «*» и «?», т.е. явным образом указывать домены и url для блокировки, например: yahoo.com, www.yahoo.com, yahoo.com/qwer/123, www.yahoo.com/qwer/123



DNS-фильтрация

UserGate Web Filter предоставляет возможность фильтрации DNS запросов на основе черных и белых списков, категории хостов или времени суток.

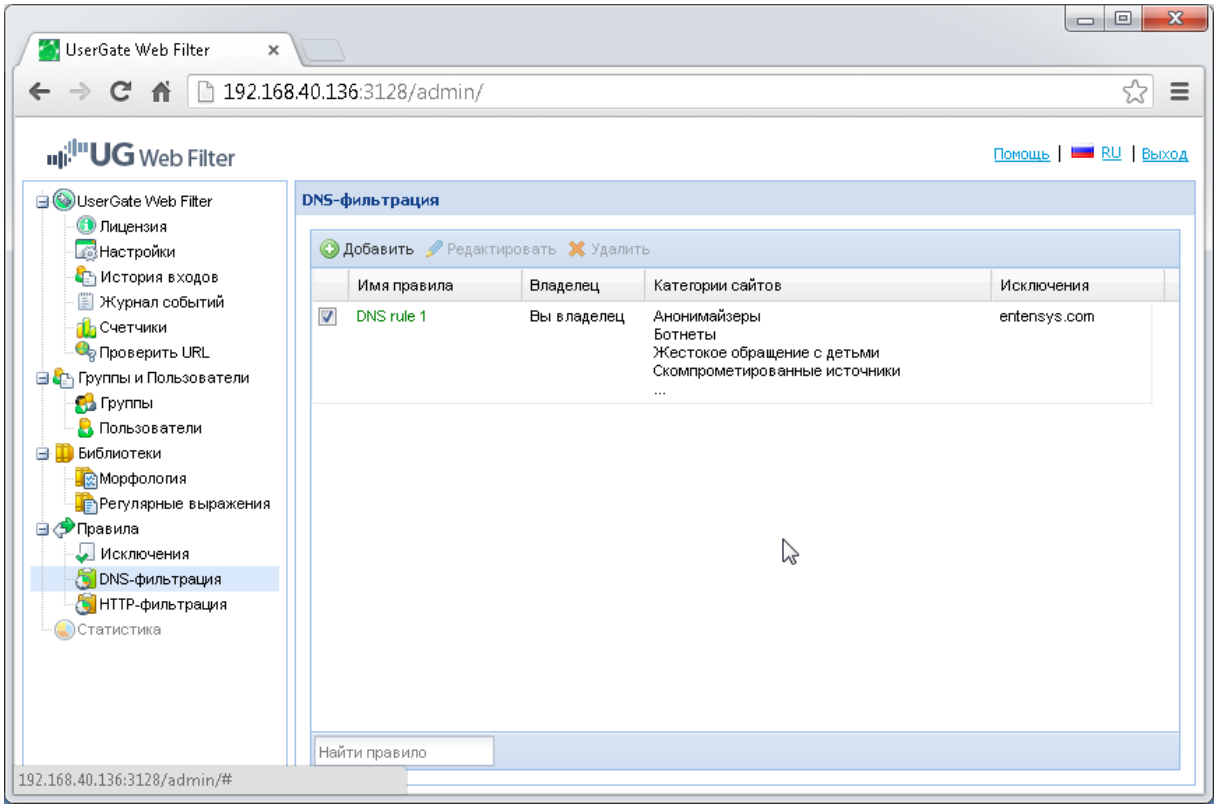
При блокировании DNS-запроса, UserGate Web Filter возвращает IP-адрес, указанный в параметре «IPv4-адрес для заблокированных DNS запросов» на странице «Настройки». По умолчанию на заблокированные запросы возвращается адрес 127.0.0.1.

Для создания фильтра, необходимо кликнуть «Добавить» и заполнить необходимые поля.

Тип логики определяет, как будут соотноситься между собой условия правила каждой вкладки. Если выбран тип логики «И», то правило будет срабатывать только при одновременном выполнении условий каждой вкладке. Если выбран тип логики «ИЛИ», то правило будет срабатывать при выполнении любого из условий.

Например, если категория «Поисковые системы и порталы» выбрана для блокировки и в качестве времени указан четверг, то при типе логики «И" поисковые запросы будут заблокированы только в четверг, при типе логики «ИЛИ» будут заблокированы все поисковые запросы, а также все запросы, сделанные в четверг.

Категории сайтов. На этой вкладке можно выбрать категории сайтов Entensys URL Filtering 2.0 для блокировки, а также добавить для них исключения.

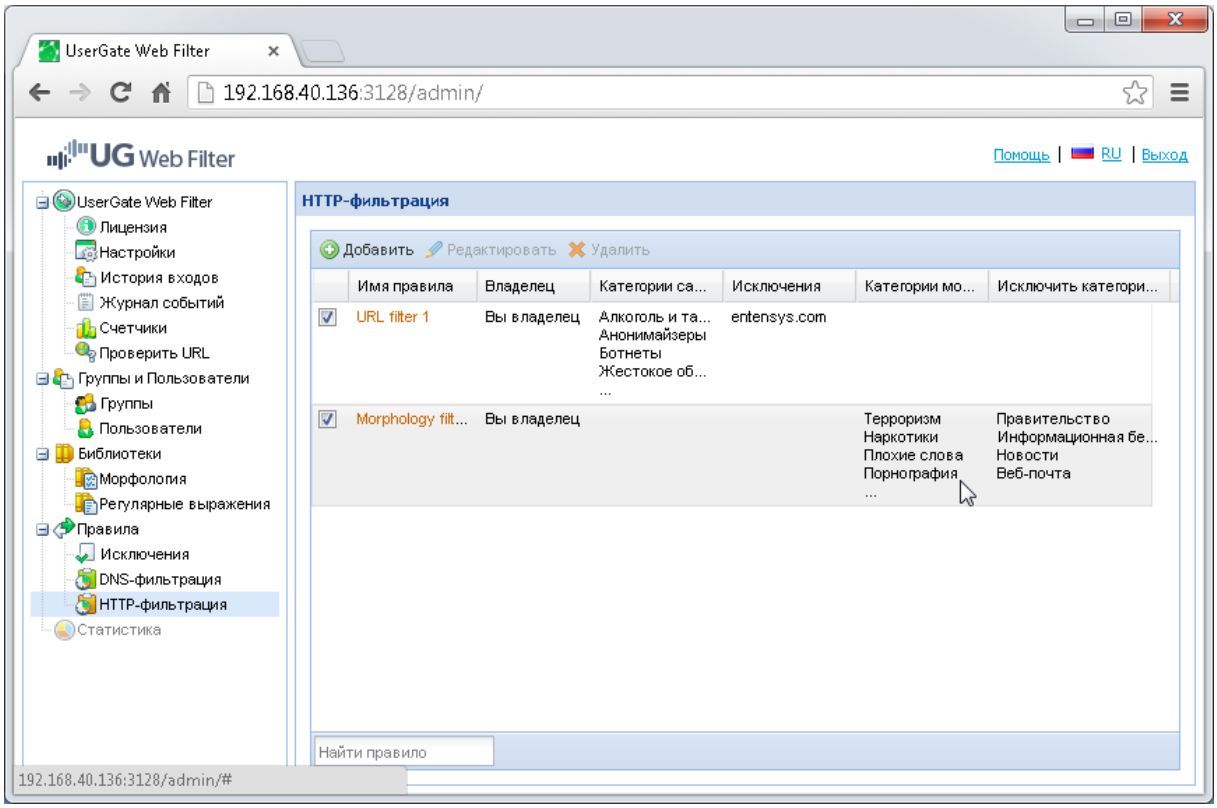


Важно! Работа правил DNS-фильтрации включается на странице Настройки (пункт «Настройки правил - Обработка правил»).

Важно! После создания правила фильтрации не забудьте его назанчить пользователю или группе пользователей в соответствующем разделе настроек.

HTTP-фильтрация

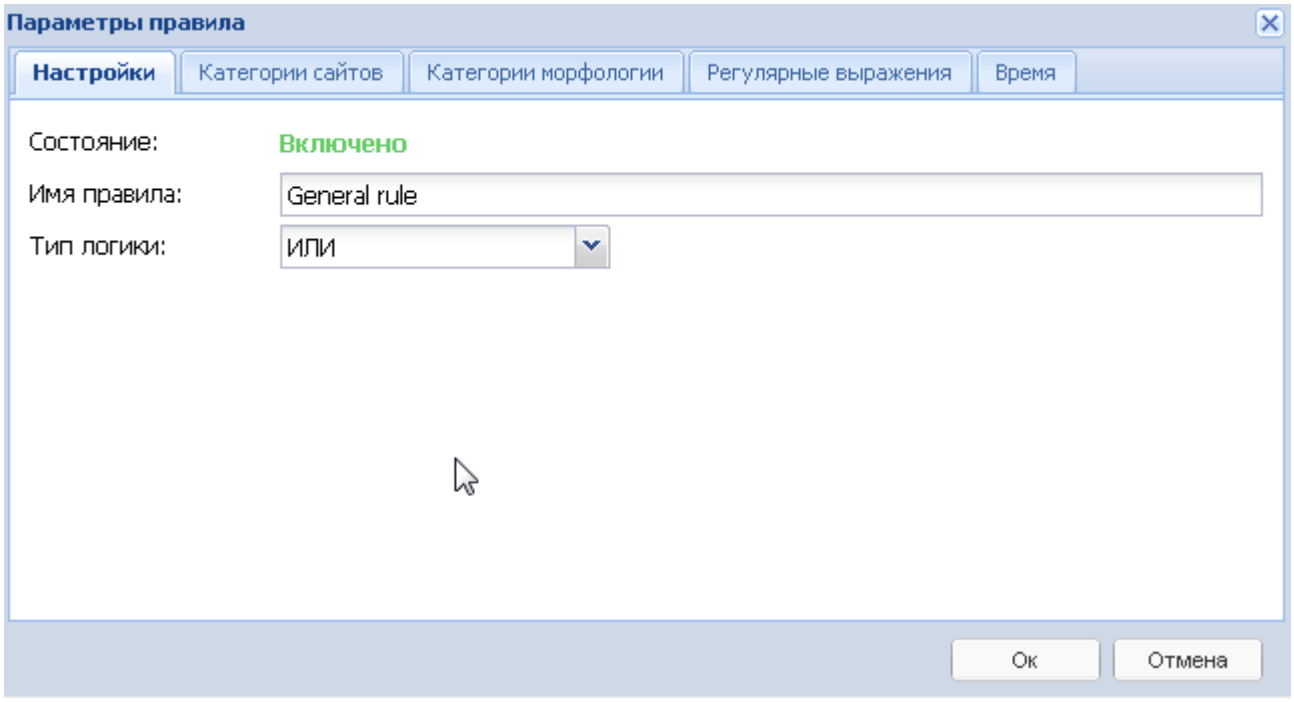
Данная страница служит для создания правил HTTP-фильтрации. HTTP-фильтрация анализирует не только DNS-имя сайта, но и его содержимое.

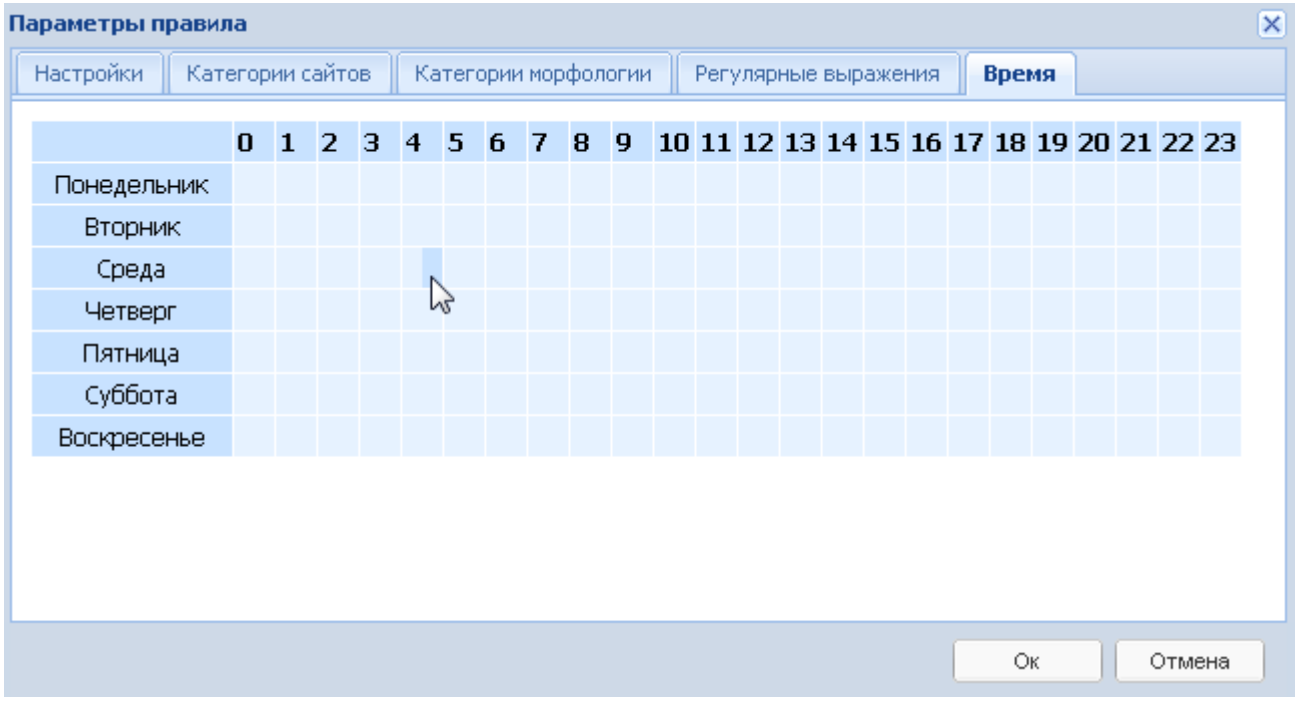


Для создания фильтра, необходимо кликнуть «Добавить» и заполнить необходимые поля.

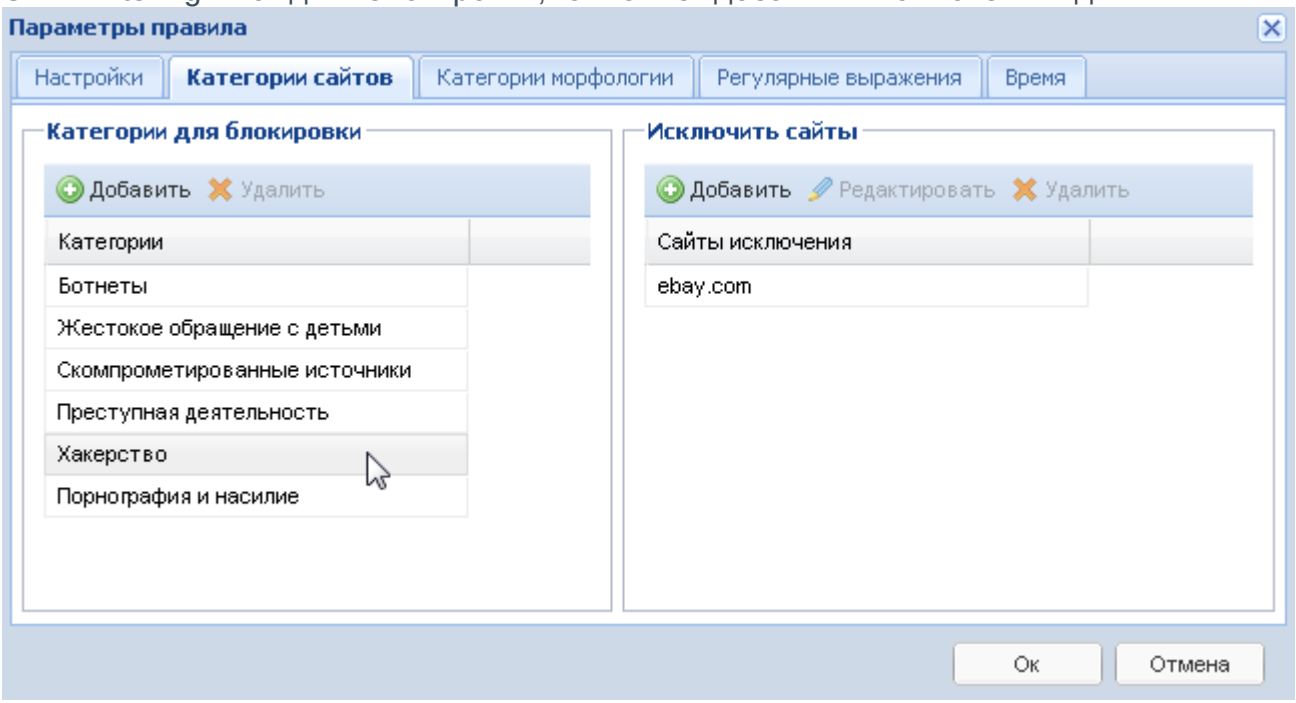
Тип логики определяет, как будут соотноситься между собой условия правила каждой вкладки. Если выбран тип логики «И», то правило будет срабатывать только при одновременном выполнении условий каждой вкладке. Если выбран тип логики «ИЛИ», то правило будет срабатывать при выполнении любого из условий.

Например, если категория «Поисковые системы и порталы» выбрана для блокировки и в качестве времени указан четверг, то при типе логики «И» поисковые запросы будут заблокированы только в четверг, при типе логики «ИЛИ» будут заблокированы все поисковые запросы, а также все запросы, сделанные в четверг.


Параметры правила
Настройки
Категории сайтов
Категории морфологии
Регулярные выражения
Время
Состояние:
Включено
Имя правила:
General rule
Тип логики:
ИЛИ
Ок
Отмена


Параметры правила
Настройки
Категории сайтов
Категории морфологии
Регулярные выражения
Время
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
Понедельник
Вторник
Среда
Четверг
Пятница
Суббота
Воскресенье
Ок
Отмена

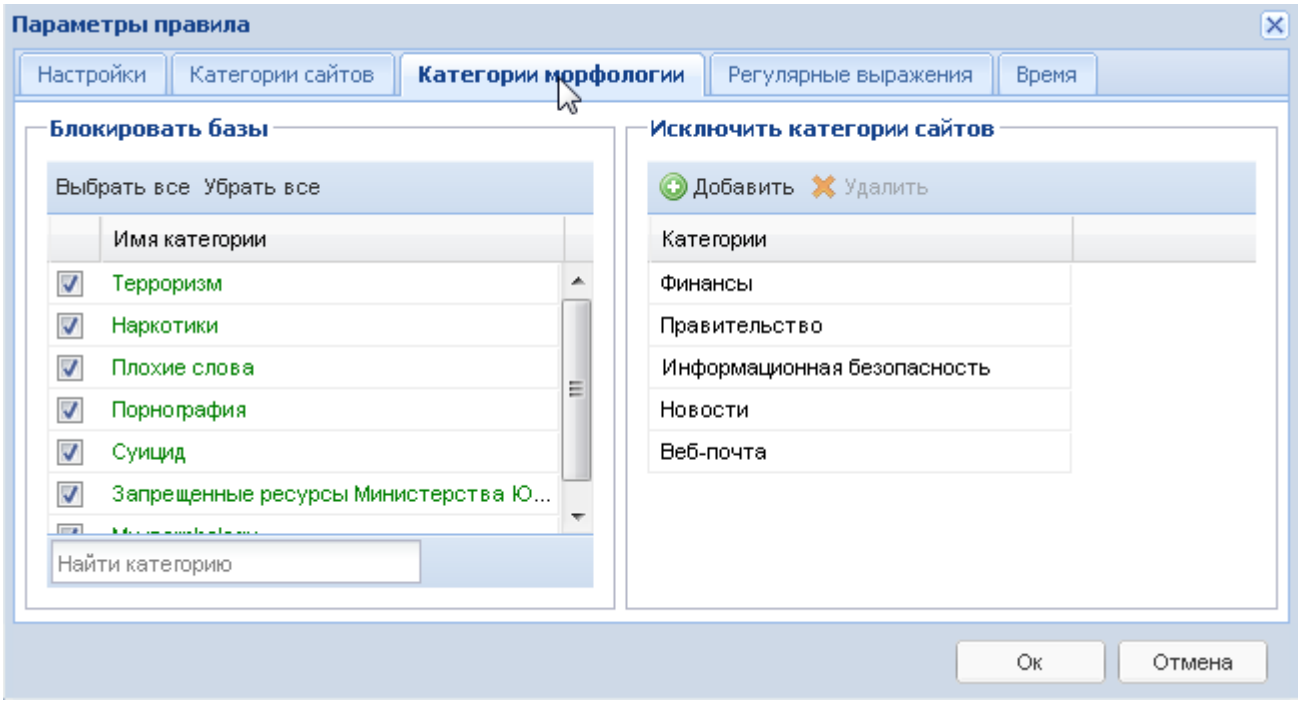
Категории сайтов. На этой вкладке можно выбрать категории сайтов Entensys URL Filtering 2.0 для блокировки, а также добавить исключения для них.



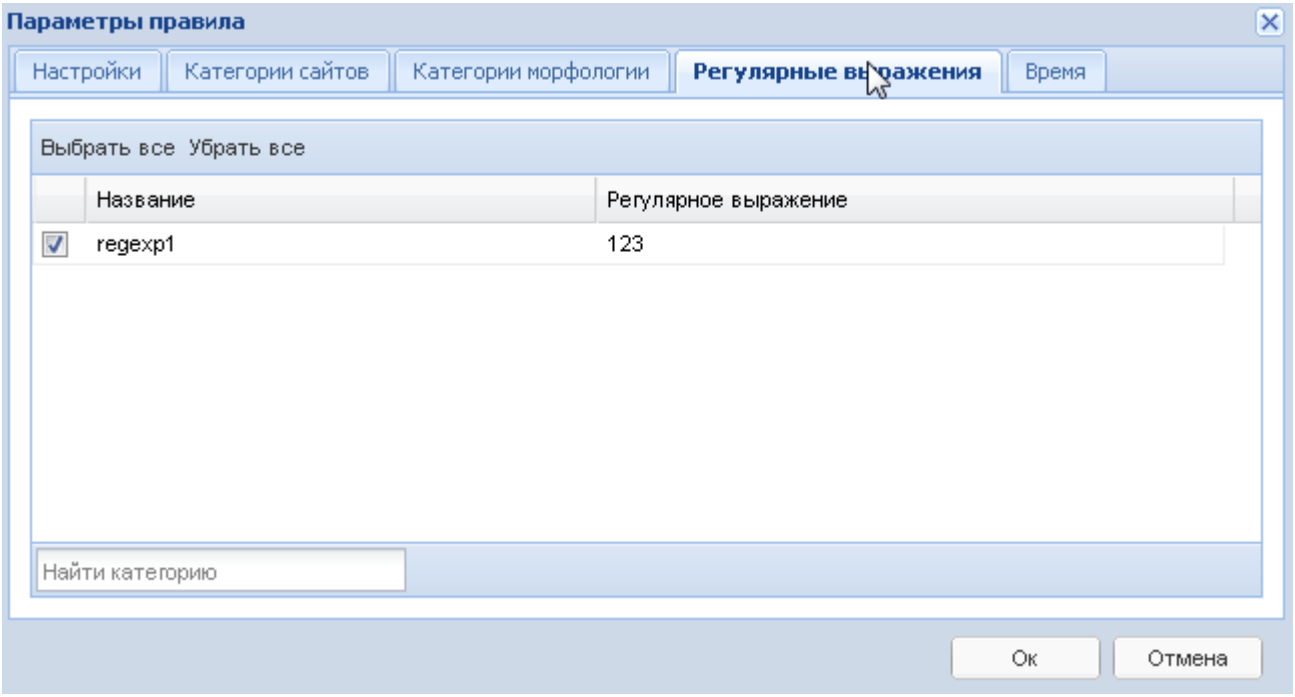
Категории морфологии. На этой вкладке можно выбрать категории морфологии, на основании которых будет анализироваться содержимое сайта, а также добавить в исключения категории сайтов, которые анализировать не нужно.

.**Важно!** Для повышения производительности и уменьшения ложных срабатываний рекомендуется исключить из проверки на морфологию следующие категории:

- Веб-почта;
- Информационная безопасность;
- Новости;
- Правительство;
- Финансы.



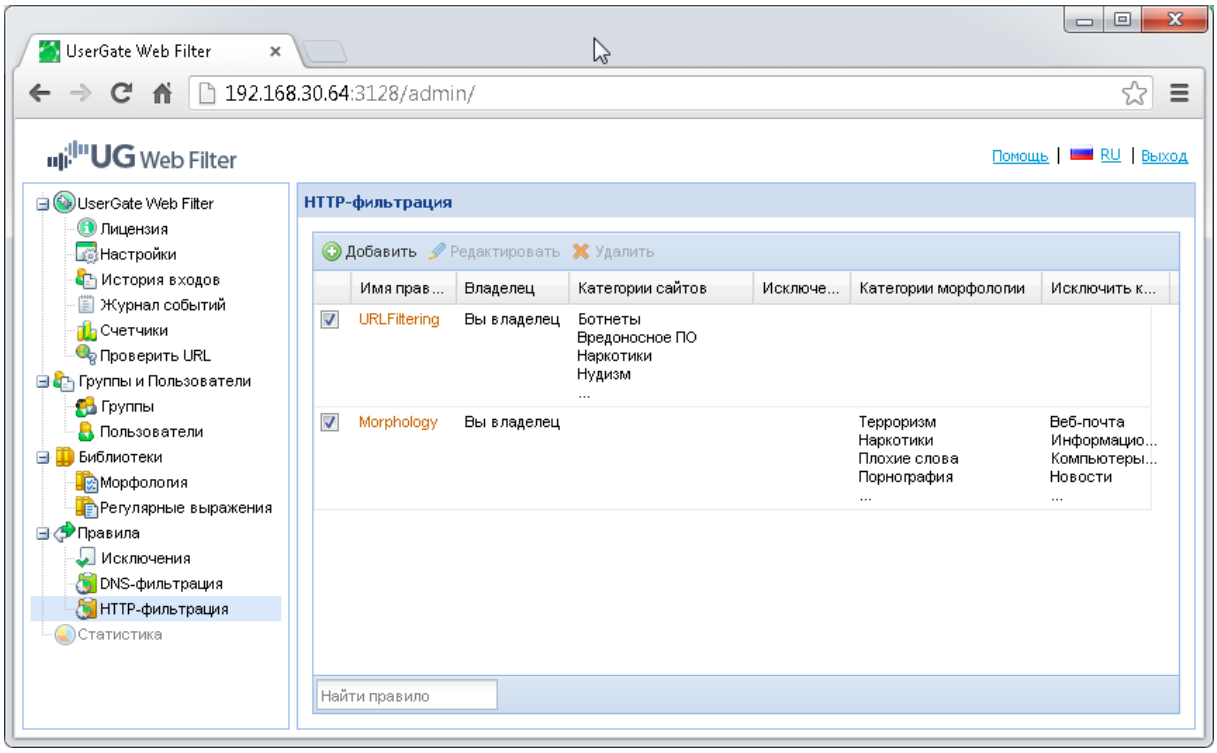
Регулярные выражения. На этой вкладке можно указывать регулярные выражения, которые будут использованы при анализе содержимого сайта.



Важно! После создания правила фильтрации не забудьте его назанчить пользователю или группе пользователей в соответствующем разделе настроек.

Важно! Если у вас создано несколько правил фильтрации, то они будут применяться в порядке, показанном в консоли. Рекомендуется создавать

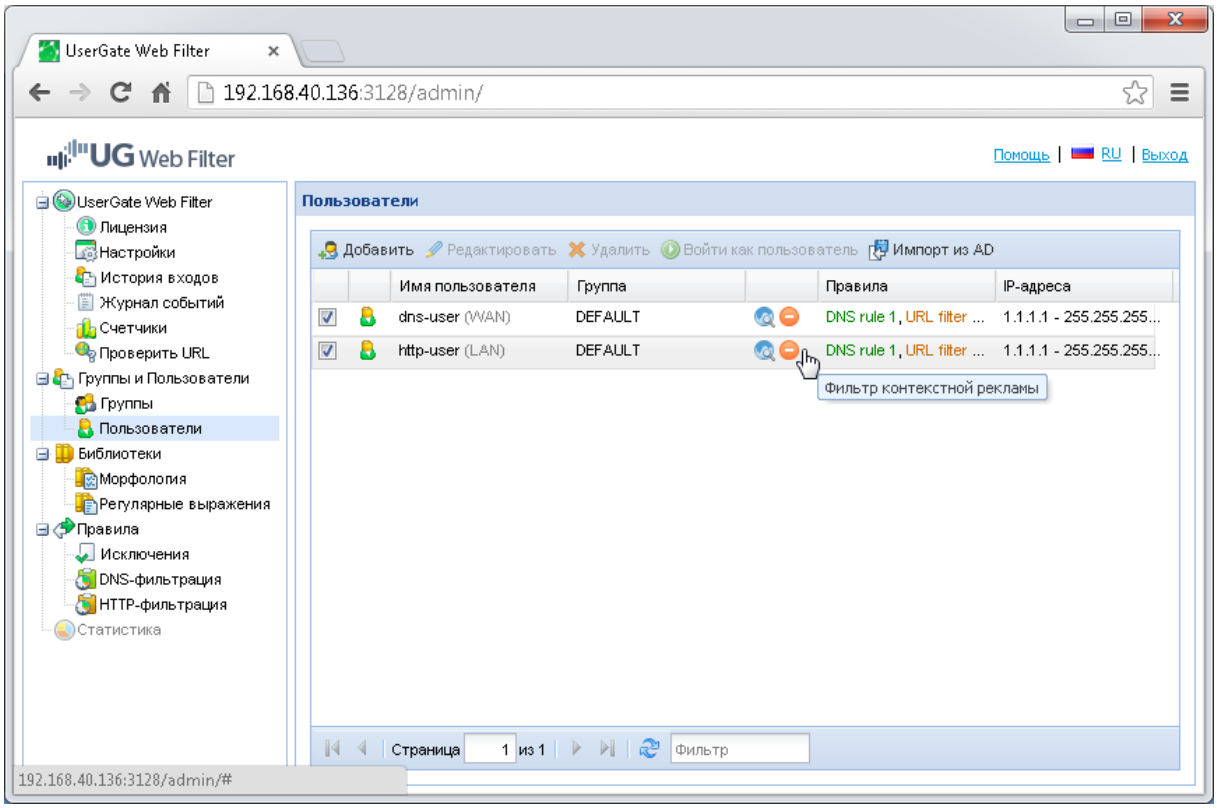
правила таким образом, что бы Морфологическая проверка проводилась в последнюю очередь, для повышения производительности системы фильтрации.



Безопасный поиск

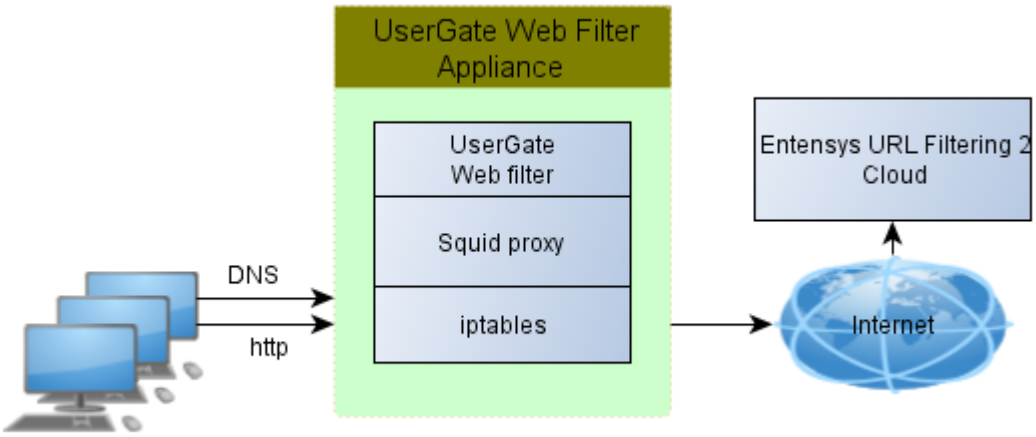
Функция «Безопасный поиск» - это фильтрация на стороне поисковой системы, которая позволяет исключить обработку поисковых запросов, связанных с запрещенным контентом. Поддержка безопасного поиска реализована для поисковых систем Google, Yandex, Yahoo, Bing, Rambler, а также на портале YouTube. С помощью данного инструмента блокировка нежелательного контента осуществляется средствами поисковых порталов, что позволяет добиться высокой эффективности, например, при фильтрации откликов на запросы по графическому или видеоконтенту.

Активация безопасного поиска производится на уровне каждого пользователя в разделе **Пользователи** во вкладке **Дополнительно**.


UserGate Web Filter
192.168.40.136:3128/admin/
UG Web Filter
Помощь | RU | Выход
UserGate Web Filter
Лицензия
Настройки
История входов
Журнал событий
Счетчики
Проверить URL
Группы и Пользователи
Группы
Пользователи
Библиотеки
Морфология
Регулярные выражения
Правила
Исключения
DNS-фильтрация
HTTP-фильтрация
Статистика
Пользователи
Добавить
Редактировать
Удалить
Войти как пользователь
Импорт из AD
Имя пользователя
Группа
Правила
IP-адреса
dns-user (WAN)
DEFAULT
DNS rule 1, URL filter ...
1.1.1.1 - 255.255.255...
http-user (LAN)
DEFAULT
DNS rule 1, URL filter ...
1.1.1.1 - 255.255.255...
Фильтр контекстной рекламы
Страница 1 из 1
Фильтр
192.168.40.136:3128/admin/#

Принцип работы

Основа продукта – UserGate Web Filter. UserGate Web Filter обеспечивает фильтрацию http-запросов и фильтрацию DNS-запросов. В качестве вспомогательных компонентов используются прокси-сервер squid и межсетевой экран iptables.



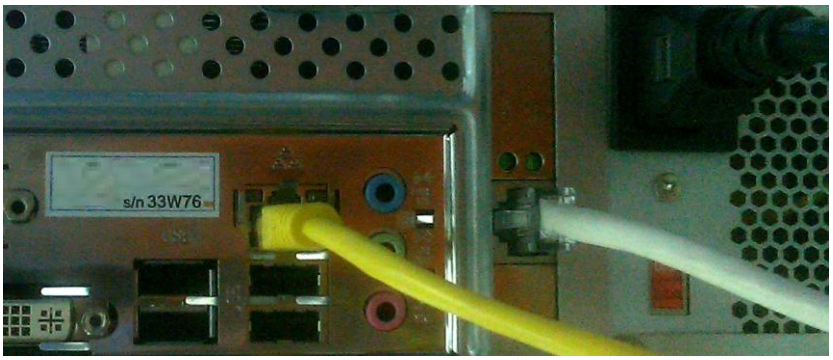
1. Iptables выполняет прозрачное проксирование http-трафика из локальной сети на прокси-сервер squid.
2. Squid, являясь ICAP-клиентом для UserGate Web Filter, передает весь контент, на фильтрацию в UserGate Web Filter.
3. UserGate Web Filter фильтрует контент согласно настроенным правилам фильтрации.
4. Кроме этого, iptables передает все DNS-запросы в UserGate Web Filter для фильтрации с помощью Entensys URL Filtering 2.

При использовании программно-аппаратного комплекса UserGate Web Filter Appliance доступен ряд дополнительных возможностей, с помощью которых администратор может управлять локальной сетью. Например, администратор может настроить сервер DHCP для контроля выдачи IP-адресов компьютерам локальной сети. Ниже перечислены возможные настройки UserGate WebFilter Appliance и дано их описание.

Быстрый запуск

UserGate Web Filter Appliance поставляется уже преднастроенным, поэтому для его запуска необходимо проделать всего несколько шагов:

1. Подключите LAN-интерфейс UserGate Filter Appliance к компьютерной сети и WAN-интерфейс к сети Интернет.

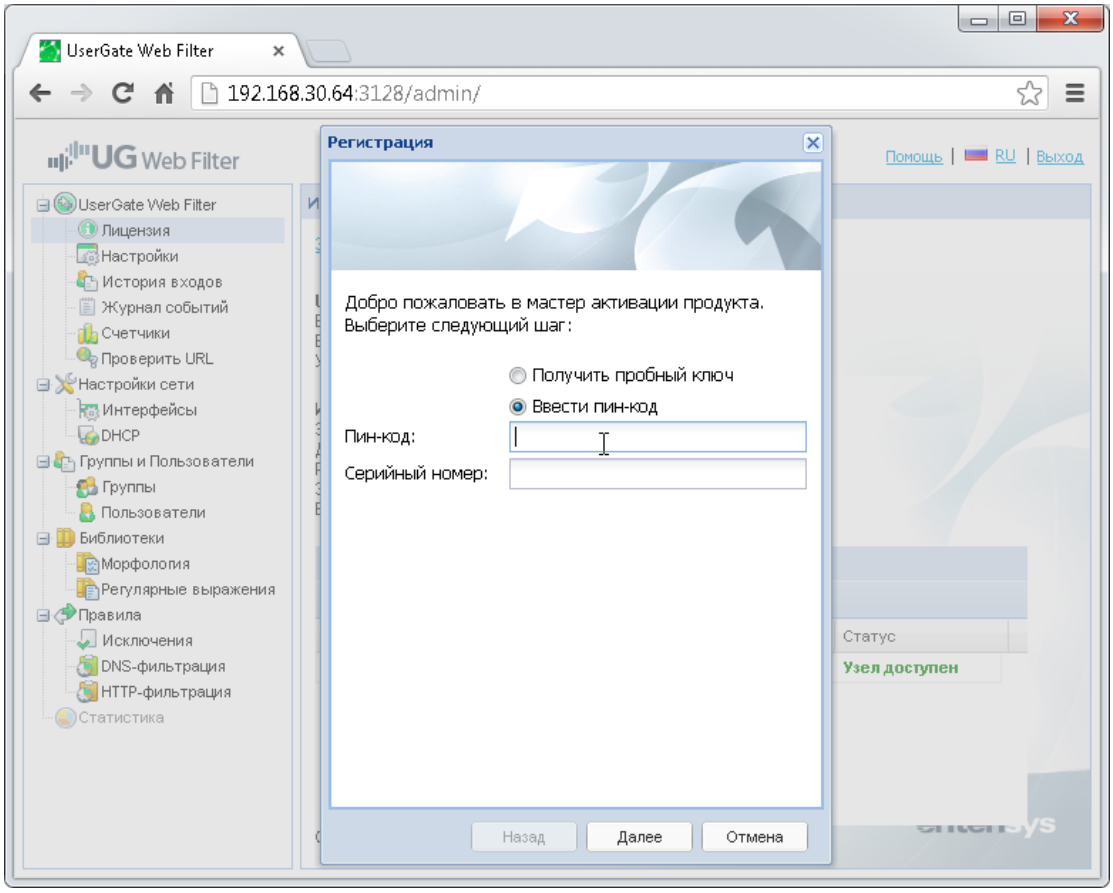


2. Убедитесь, что ваш компьютер имеет IP-адрес, относящийся к сети 192.168.1.0/24. Если это не так, то назначьте своему компьютеру адрес из диапазона 192.168.1.1-192.168.1.253, например 192.168.1.252 с маской 255.255.255.0.

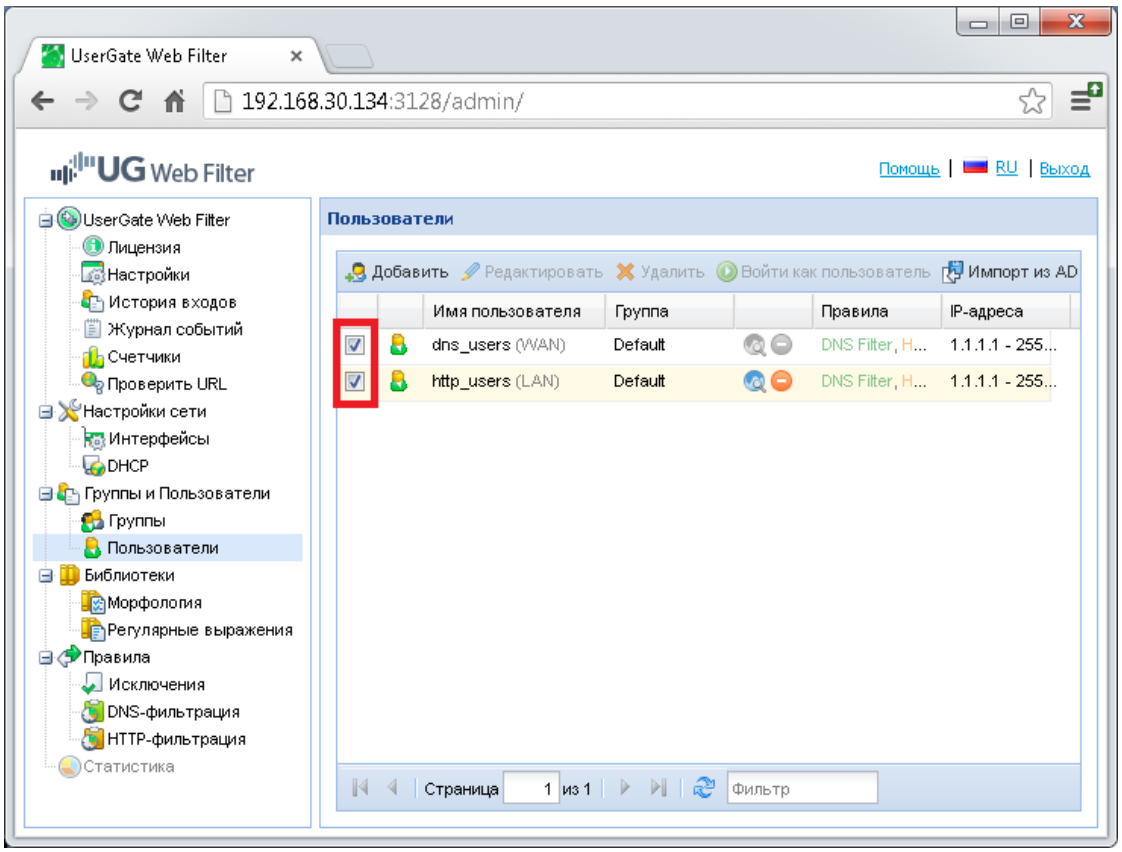
3. Подключитесь к веб-консоли UserGate Web Filter Appliance по адресу: **http://192.168.1.254:3128/admin/.** По умолчанию:

   - **адрес сервера** - http://192.168.1.254:3128/admin/;
   - **имя пользователя –** «Admin» (с большой буквы);
   - **пароль –** «admin» (с маленькой буквы).

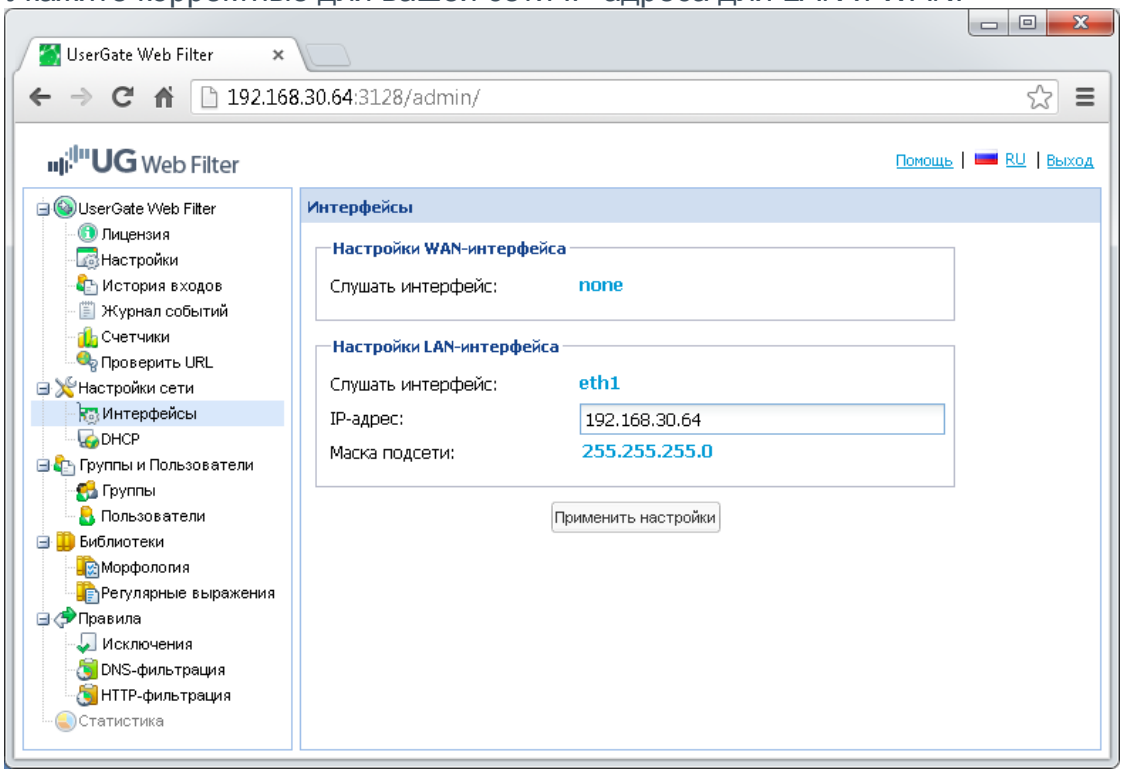
4. Зарегистрируйте продукт, введя ПИН-код продукта и серийный номер апплаенса на странице **Лицензия.** Серийный номер вы можете найти на корпусе апплаенса.



5. Активируйте пользователей **dns_users** и **http_users** на вкладке **Пользователи**



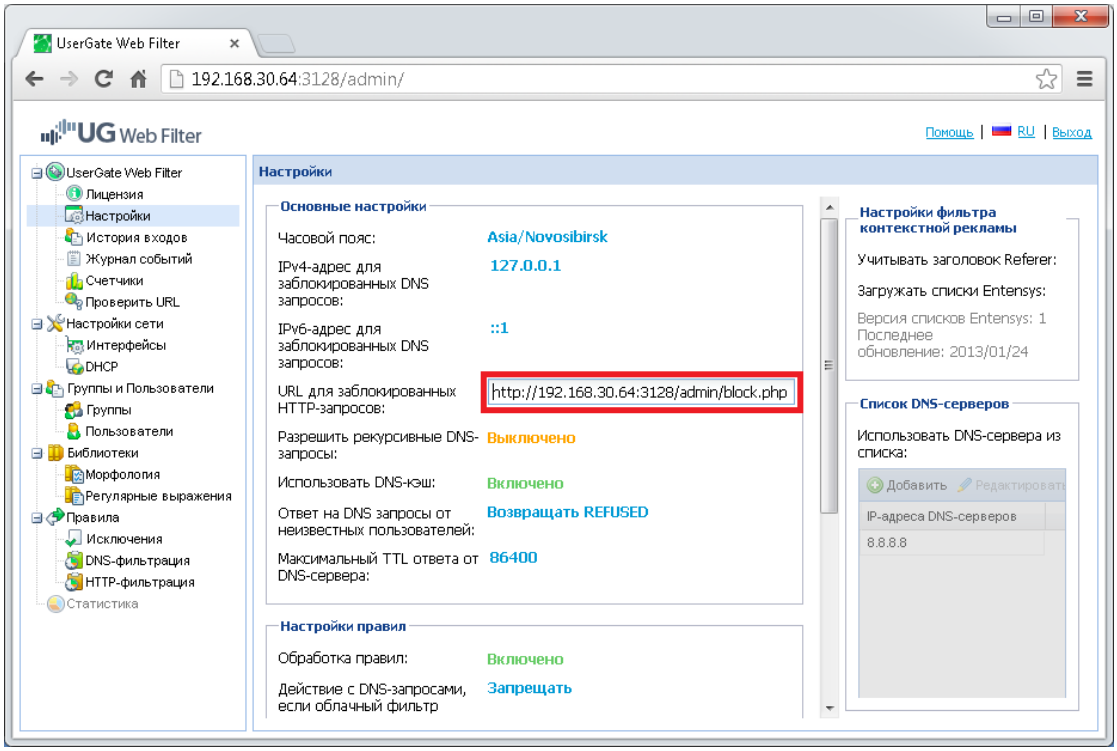
6. Укажите корректные для вашей сети IP-адреса для LAN и WAN.



Важно! Если вы измените IP-адрес локальной сети, то вам придется подключиться к веб-консоли заново, используя новый адрес - http://new-

IP-address/admin/.

7. Отредактируйте URL для заблокированных HTTP-запросов на странице **Настройки.** Укажите здесь новый адрес LAN вместо 127.0.0.1: http://NEW-LAN-IP:3128/admin/block.php



После выполнения вышеперечисленных действий UserGate Web Filter Appliance готов к работе. Для более детальной настройки обратитесь к справочному руководству.

Настройки интерфейсов

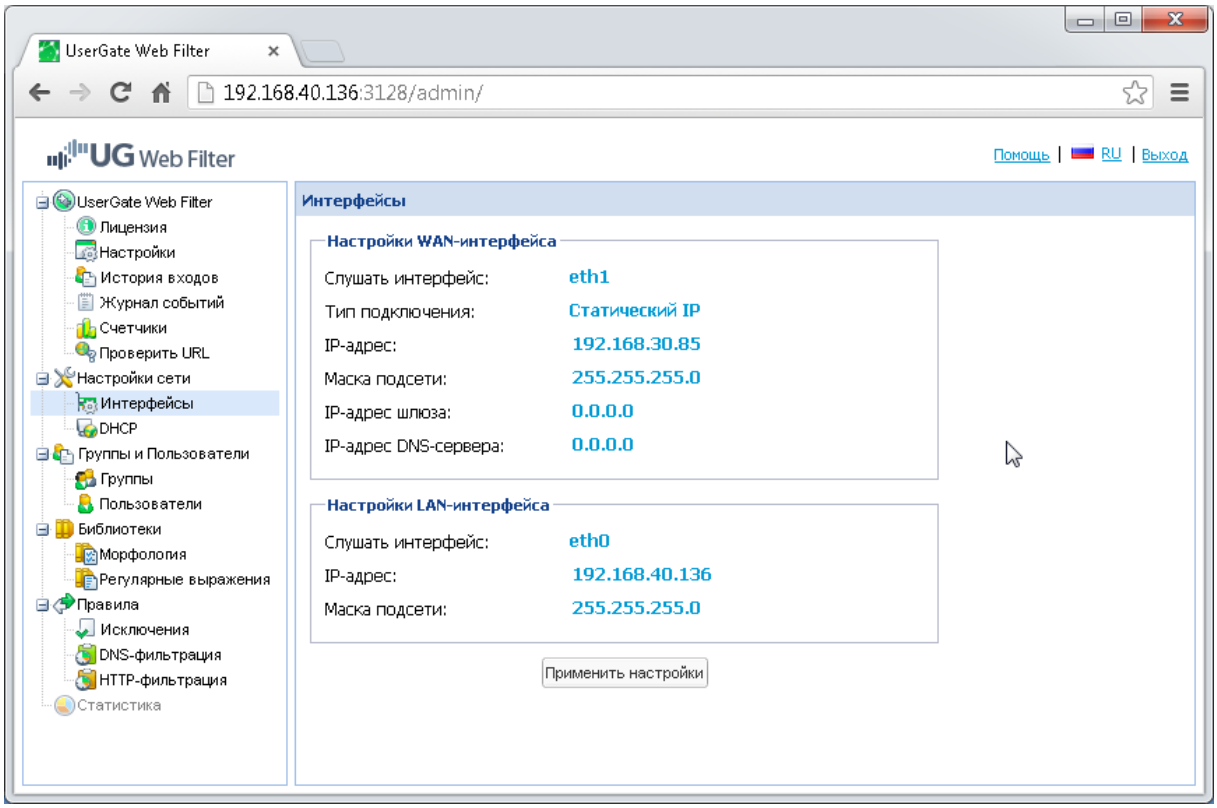
Настройки WAN-интерфейса

WAN-интерфейс - сетевой интерфейс, который подключен к Интернету.

Предполагается два типа подключения - *DHCP* и со *статическим IP*.

При типе подключения со статическим IP необходимо задать следующие параметры: IP-адрес интерфейса, маску подсети, IP-адрес шлюза по умолчанию и IP-адрес DNS-сервера.

При типе подключения DHCP все параметры будут получены от провайдера автоматически.



Настройки LAN-интерфейса

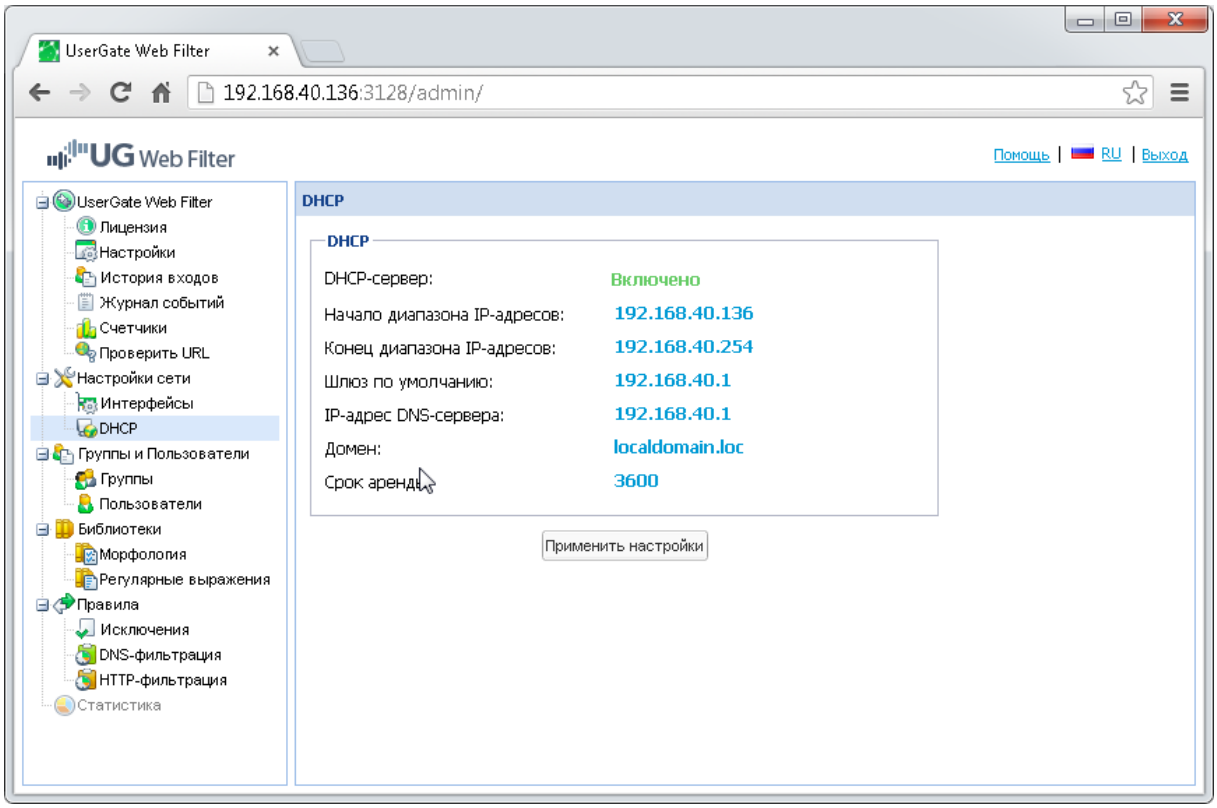
LAN-интерфейс - сетевой интерфейс, который подключен к локальной сети.

Для настройки LAN-интерфейса необходимо задать IP-адрес этого интерфейса и маску локальной подсети.

Настройки DHCP

Служба DHCP (Dynamic Host Configuration Protocol) позволяет автоматизировать процесс выдачи сетевых настроек клиентам в локальной сети. В сети с DHCP-сервером каждому сетевому устройству можно динамически назначать IP-адрес, адрес шлюза, DNS-, WINS-сервера и т.п.

Для DHCP-сервера достаточно задать следующие параметры: *Начало и конец диапазона IP-адресов* (пул адресов), из которого сервер будет выдавать адреса клиентам в локальной сети, *шлюз по умолчанию*, *IP адрес DNS сервера*, *Домен* и *срок аренды* - время, на которое будут выдаваться IP-адреса.

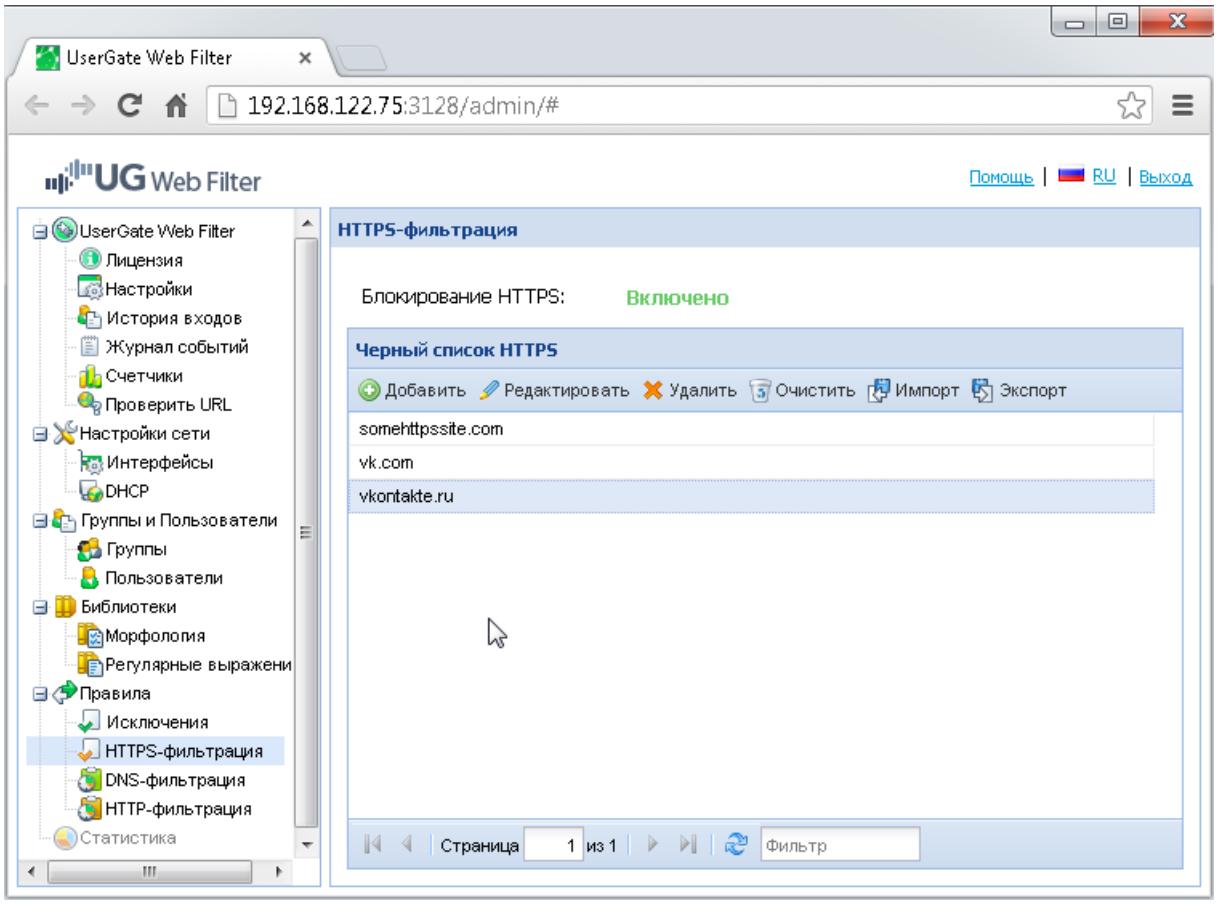


HTTPS фильтрация

Нкоторые веб-сайты предлагают контент не только по протоколу http, но и по протоколу https. Применять фильтрацию http к протоколу https не представляется возможным, поскольку протокол https шифрует передаваемый контент, но возможно заблокировать доступ по протоколу https к таким сайтам. Включите **Блокирование HTTPS** на странице **HTTPS Фильтрация** и добавьте необходимые сайты в **Черный список HTTPS**. Все попытки подключиться к этим сайтам по протокулу HTTPS будут заблокированы. Добавьте все возможные варианты сайтов в этот список, например:

- httpssite1.com
- www.httpssite1.com
- login.httpssite1.com

Не используйте символы ‘*’, ‘?’, ‘/’ в этом списке. Данный список должен содержать корректные имена интернет хостов.



Обновление программного обеспечения

Разработчик постоянно работает над улучшением программного продукта. О появлении новой версии вы узнаете посредством уведомления в веб-консоли продукта в разделе **Лицензия**. Для установки новой версии вам потребуется произвести следующие действии:

- Подключите к UserGate Web Filter Appliance монитор и клавиатуру.
- Включите Appliance и дождитесь, пока система загрузится.
- Войдите в систему, используя учетную запись webfilter и пароль, который показан на экране:

- Выполните следующие команды:
  sudo apt-get update
  sudo apt-get install webfilter

- По окончании установки перезагрузите систему.

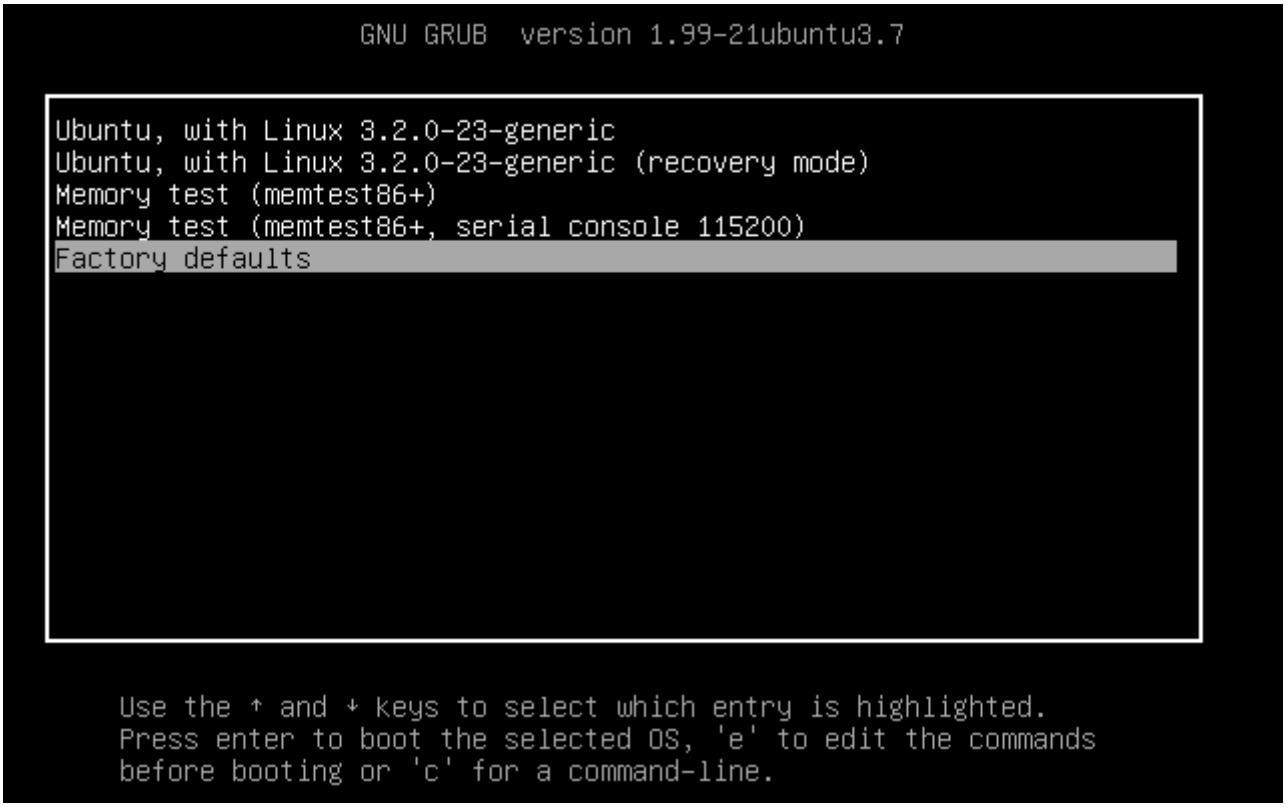
Важно! Для выполнения обновления программного обеспечения Appliance должен иметь доступ в интернет.

Восстановление настроек по умолчанию

В некоторых случаях, например, если пароль пользователя Admin утерян, может возникнуть необходимость вернуться к заводским настройкам. Следует учитывать, что в этом случае все настройки, сделанные вами, будут сброшены, и вам предстоит произвести настройку заново. Для выполнения сброса настроек проделайте следующую процедуру:

- Подключите к UserGate Web Filter Appliance монитор и клавиатуру.
- Включите Appliance и во время загрузки выберите Factory Defaults.
- Система вернет все свои настройки в заводское состояние и перезагрузится.

После перезагрузки вам необходимо произвести полную настройку продукта.



Техническая поддержка

Раздел технической поддержки на сайте компании http://entensys.ru/support содержит дополнительную информацию по настройке UserGate Web Filter. Кроме этого, здесь же Вы можете оставить заявку на решение вашей проблемы.