

GateWall DNS Filter 2.0

Administrator Manual

Contents

Contents	2
Introduction	3
System Requirements	3
GateWall DNS Filter Installation	3
DNS Filter Update and Removal	4
GateWall DNS Filter Registration	4
GateWall DNS Filter Licensing Policy	4
Program Update	5
Administrator Console	5
System Login Procedure	5
Connection Password Setup	6
GateWall DNS Filter Statistics Database Management	7
Using Third-Party Databases	7
Database Recovery	8
Users and Groups	8
User Authorization Methods	9
DNS Setup	10
Traffic Control Rules	10
Exception List	11
Website Categories	12
Access Log and Request Statistics	13
Statistics by Category	13
Popular Categories	14
Requesting URL Categories from Entensys URL Filter	15
GateWall DNS Filter Operation	15
Declining Domain Name Resolution Requests	16
Forwarding Forbidden Requests	17
GateWall DNS Filter Deployment Options	17
Displaying Additional Debug Information	19

Introduction

GateWall DNS Filter is a DNS forwarder application with enhanced functionality, including requested host category identification, tracking and recording processed requests, as well as traffic rules management. An integrated system of rules allows Internet access management based on the lists of authorized/unauthorized hosts, time and URL categories. GateWall DNS Filter is not a gate solution, which makes it a good choice for large networks with thousands of users.

GateWall DNS Filter is made up of the following modules: server, administrator console (DNS Filter Administrator), web-server with HTTPS support and statistics module.

DNS Filter server (DNSFilter.exe) is a Windows system service. The server allows users' DNS requests through, functions as a filter and records requests statistics.

DNS Filter administrator console is used to control the GateWall DNS Filter server. The console communicates with the server via a PHP + Ajax web-server, which allows remote server administration. Brief statistics of DNS requests can be viewed from the administrator console.

Integrated web-server is used to manage the administrator console and can serve as a forwarder for users' HTTP requests. For example, when a user is trying to access a prohibited web site in a browser application, a corresponding notification will appear on the screen.


System Requirements

Install your GateWall DNS Filter server on a Windows XP/2003/Vista/2008/Windows7 system with Internet connection capability. Specific hardware requirements depend on the rate of DNS requests. We recommend using a system with a 2 GHz CPU and 2 Gb RAM if the approximate request rate is 1,000 req/sec. The disk space requirements depend on the maximum size of statistics database. We recommend that companies with large networks have several dozen gigabytes of free disk space.

GateWall DNS Filter Installation

Launch the setup file to install GateWall DNS Filter. When installing GateWall DNS Filter for the first time, leave all default Setup Wizard settings. By default, GateWall DNS Filter will be installed to folder "%Program Files%\Entensys\GateWall DNS Filter" (further used as "%DNSFilter%"). No system restart will be required after installation.

When the application is installed, three additional services will appear on the system services list: GateWall DNS Filter, GateWall DNS Filter Router and Entensys database service. The first service is the DNS Filter (DNSFilter.exe process), the second service supports the web-server and administrator console, and the third

service is used to administer the integrated database (DB). The program uses FireBird as the integrated DB. All these services will launch automatically after installation. The agent icon  will appear in the system tray for convenience. You may use the agent's quick menu to start the administrator console, stop or restart DNS Filter server or access the log file.

DNS Filter Update and Removal

We recommend removing any previous version of DNS Filter before you install the new version. If necessary, you can save the server settings file (dnsfilter.xml from the DNS Filter folder) and statistics database dump file, or the complete database itself (dnsfilter.fdb). To remove DNS Filter, go to Start – Applications, find the application and select Uninstall or use the Applications utility in the Control Panel. Server settings file will not be deleted from %DNSFilter% folder during the uninstall process.

GateWall DNS Filter Registration

When you first start the administrator console, a registration window will pop up requesting you to enter either your demo key (for a trial version), or full license key (pin code). The key request is performed online (via HTTPS protocol), through a query to usergate.ru website. If you are prompted to enter the full license key, enter the special pin code provided with your GateWall DNS Filter software. Besides, you will be additionally asked for personal data (user name in Latin letters, email, country, and region) during the registration process. Your personal data is requested only to link the license to the user and will not be disclosed to third parties. DNS Filter will automatically restart after you register your demo or full license key.

You can use GateWall DNS Filter in demo mode for 30 days. Entensys may issue a special extended trial pin code upon your request. For example, you may request a 3-month demo key. However, you will not be able to repeat your request unless you have a special pin code.

When DNS Filter is active, it occasionally checks the registration key status. For DNS Filter to function properly, allow the application web access via HTTPS protocol for online key status checks. Otherwise, the application status will be changed to "unregistered."

GateWall DNS Filter Licensing Policy

Your GateWall DNS Filter license key does not limit the quantity of DNS requests processed by the server, but it restricts the number of users. For example, if your license covers ten users, you can create no more than ten individual users. The report containing the request statistics, total number of requests, the number of blocked requests, and distribution of requests according to Entensys URL categories will also be generated for maximum ten users.

GateWall DNS Filter license includes the license for Entensys URL Filter module, which is a URL category filter. Entensys URL Filter license is a limited license valid for one year. The online Entensys URL Filter service will become unavailable upon expiry of this license, and URL filtering capability will no longer be available.

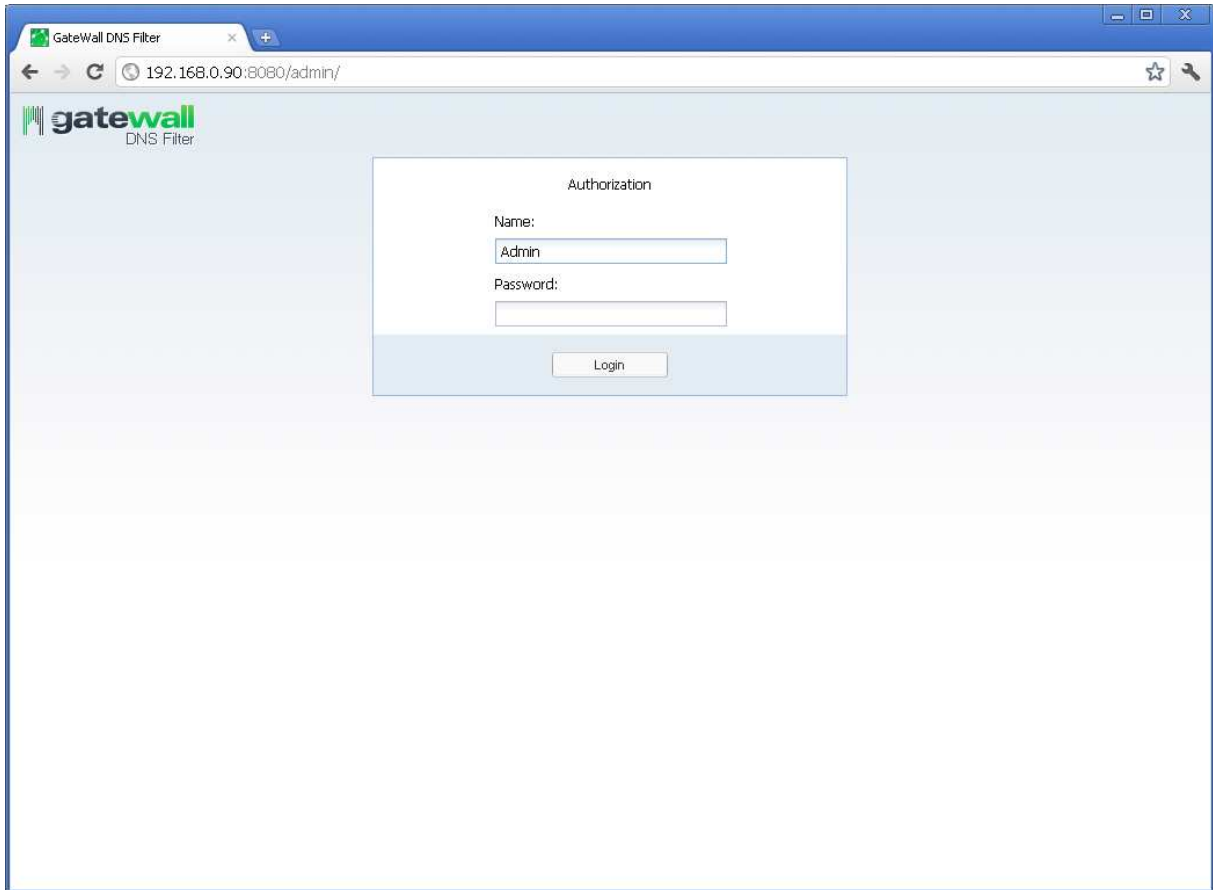
Program Update

Click on “DNS Filter” in the License menu of the administrator console. When this page is loaded, DNS Filter will request the number of the latest software version from the vendor’s website. If the current installed version is older than the version available on the website, a notification will appear in the administrator console window. The administrator can download and install the latest version from the website. When you complete the update check, the system will not reinstall GateWall DNS Filter automatically.

Administrator Console

System Login Procedure

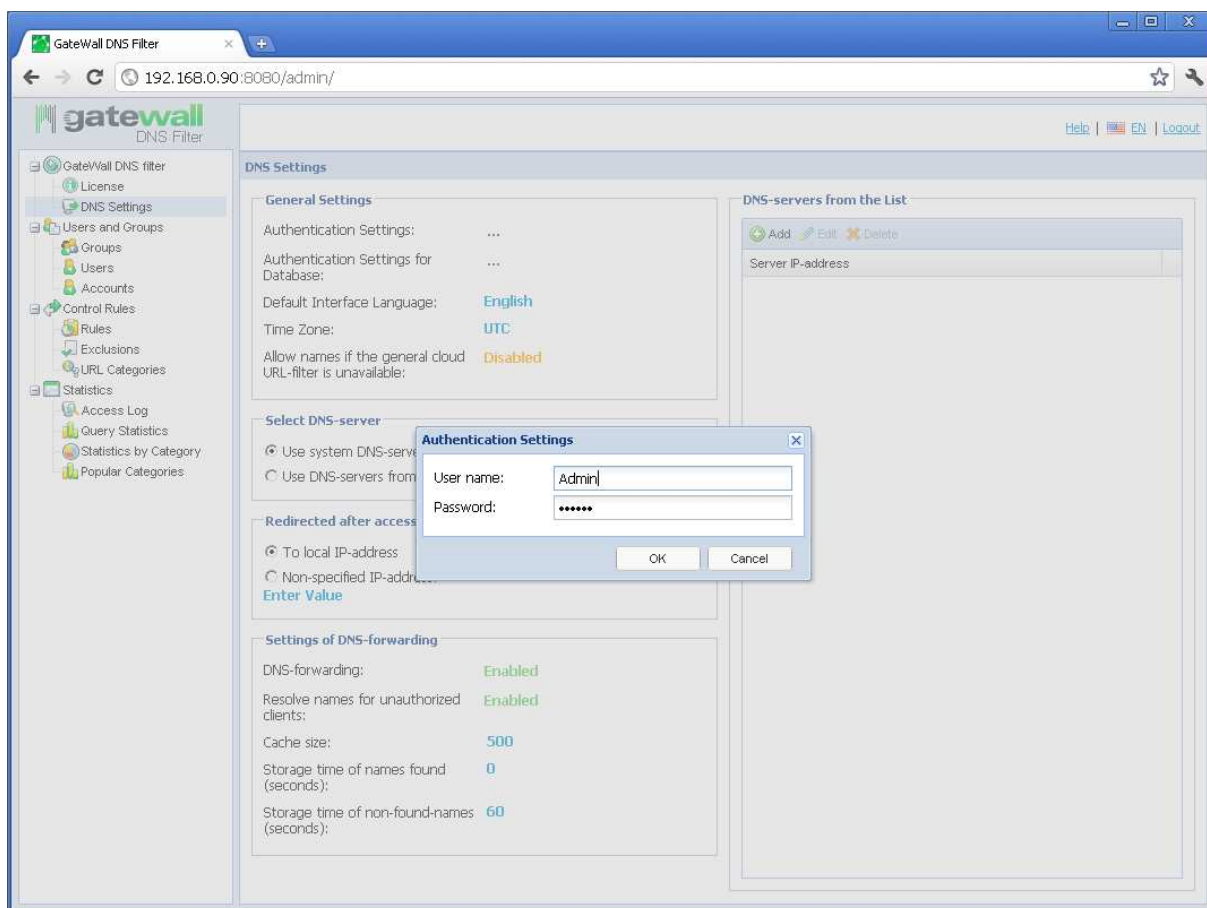
Administration module is a web-based application designed to manage GateWall DNS Filter’s local and remote servers. To launch DNS Filter Administrator, start DNS Filter service by clicking on “Start DNS Filter server” in the agent’s menu. You can also start DNS Filter Administrator from the corresponding menu in Start – Applications. To manage server settings from a remote location, open a web-browser and enter the following address: <http://192.168.0.1:8080>, where 192.168.0.1 is the IP address of the computer where DNS Filter is installed. If remote connection fails, check antivirus and firewall settings.



When you launch the administrator console, “Authorization” page will open. Enter your username and password in this window. Default username is Admin. No password is required by default to connect to DNS Filter server.

Connection Password Setup

To assign login/password to DNS Filter server connection, open General Settings page in the DNS Settings window. Restart DNS Filter server for the changes to take effect (click “Restart DNS Filter server” in the agent’s menu). When the server has restarted, enter new login/password on the Authorization page when establishing connection.



GateWall DNS Filter Statistics Database Management

DNS Filter server records the statistics of DNS requests, including the requested host and request time and result (allowed or blocked), in a special database. You can access the database via an API interface if you are using an integrated DB or through an ODBC driver if you are using a third-party DB.

An integrated FireBird database is used by default (file %DNSFilter%\dnsfilter.fdb). To access FireBird database, enter “SYSDBA” for login and “masterkey” for password.

Using Third-Party Databases

Due to ODBC support, you can use almost any type of database (MS Access, MS SQL or MySQL). For MySQL databases, GateWall DNS Filter installation package contains a dump of database with the appropriate structure. This dump is placed in folder “%DNSFilter%\db_dumps.”

If you need to configure your GateWall DNS Filter to work with a third-party database, follow the steps below:

- Specify the database login and password in “General Settings – Database Settings” window of the administrator console.
- Stop GateWall DNS Filter service (select “Stop DNS Filter server” in the agent’s menu).

- Open server settings file (%DNSFilter%\dnsfilter.xml) and set firebird = "0" in <database/> section.
- Go to "Administration – ODBC Sources" Windows console and create a system DSN (Data Source Name) named "DNS Filter" that would refer to the appropriate database (MySQL, MS SQL).
- Start GateWall DNSFilter service.

Note: "DNS Filter" is the default name for DSN. You may change this name by changing the value of DSN parameter in <database /> section of the server settings file.

Important: MySQL Connector 3.5 is required for a MySQL database.

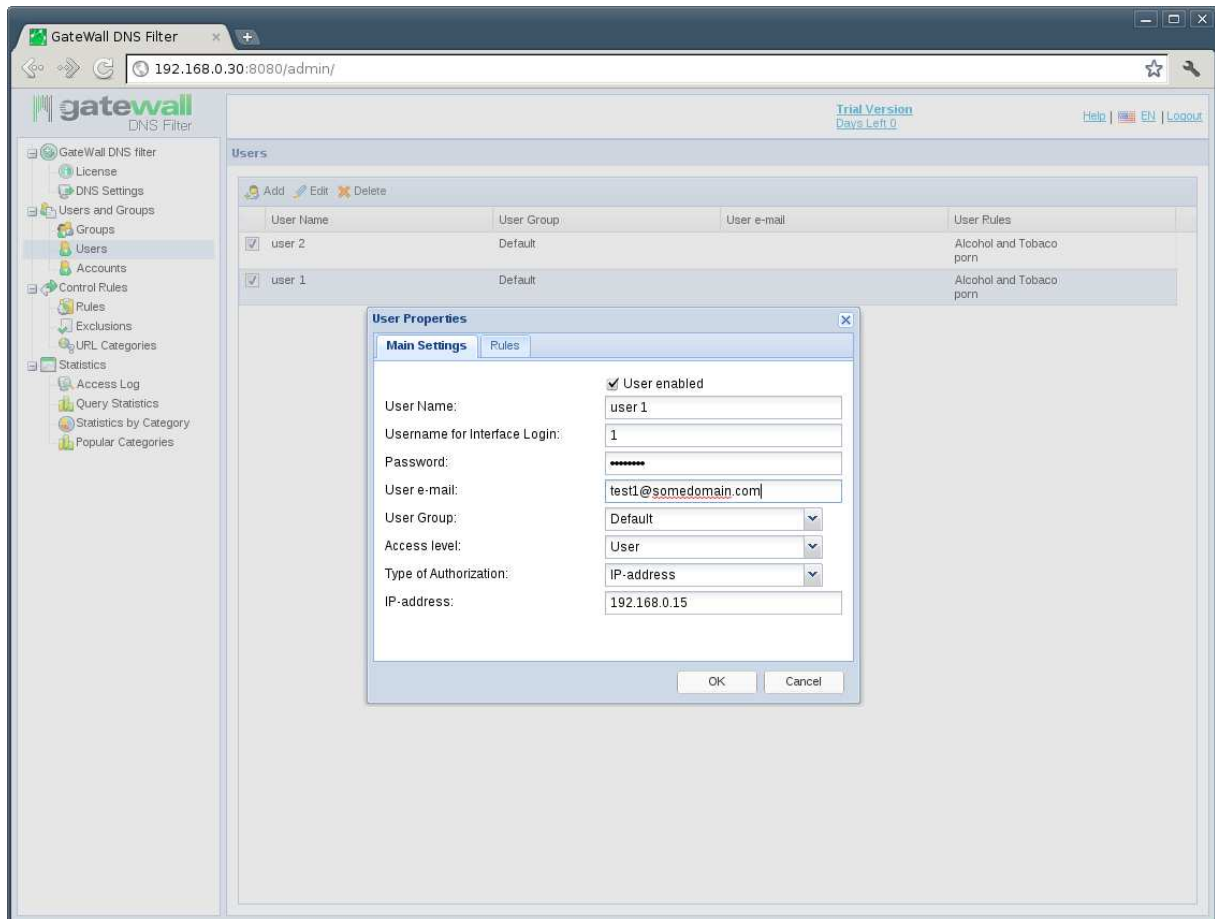
Database Recovery

If you are using the integrated database (FireBird), GateWall DNS Filter can automatically create a new empty statistics database. To do this, stop DNS Filter server and remove the statistics database file %DNSFilter%\dnsfilter.fdb.

If you are using a third-party database (firebird="0"), and GateWall DNS Filter fails to detect the appropriate system DSN on start, DNS Filter will automatically create an MS Access database and a corresponding DSN.

Users and Groups

Create GateWall DNS Filter users to enable DNS request filtering and recording of request statistics. You may unite users into groups by location or access rights for convenience. Grouping users by access rights is the most logical approach. This approach will make traffic rules management task much simpler. "Default" is the only group available in DNS Filter by default.



To create a new user, click the “Add” button on “Users and Groups” page. Required user parameters include: Name, Authorization type, authorization parameter (IP address, IP range) and group. By default, all users belong to the “default” group. Each user must be assigned a unique name in DNS Filter. Additionally, you can assign web-interface login and password on user properties page to allow users access to their private administrator console page where individual traffic management rules may be created. In DNS Filter 2.0, you can also assign access level to each user; the appropriate access level may be “User,” “Group administrator” or “Administrator.”

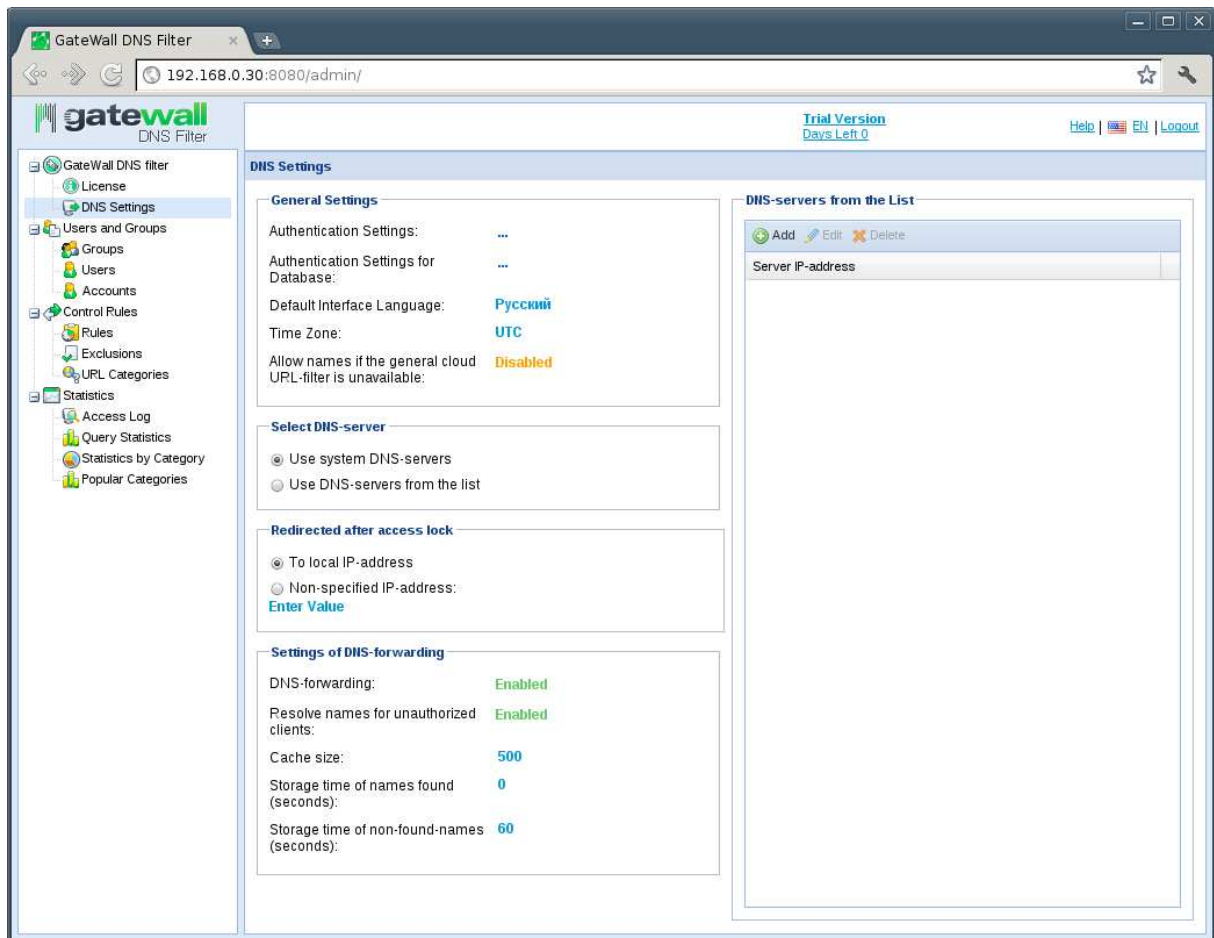
- “Administrator” has unlimited rights within DNS Filter and can manage all program settings;
- “Group administrator” can manage all rights and groups within the appropriate group and all subgroups of this group;
- “User” submits to the rules of the appropriate parent group and can only manage private rules.

User Authorization Methods

DNS names resolution capability in GateWall DNS Filter server is available to all server clients in the local area network or on the Internet. DNS Filter supports two authorization methods: by a specific IP address and by a range of IP addresses.

DNS Setup

Name resolution in DNS Filter server is accomplished through forwarding DNS requests (DNS forwarding) to an upstream server. Responses to DNS requests are cached in RAM to make name resolution faster during repeat requests. To disable DNS caching, set `dns_cache_enable="0"` in the server settings file. The maximum number of entries that can be stored in the program's DNS cache is set in "Number of cache entries" parameter located in the "DNS Forwarding Settings" section. The default cache size is maximum 500 entries. One of the additional parameters you can set on DNS Setup page is the cached entry lifetime ("Found names lifetime" and "Missing names lifetime" parameters).



To configure DNS in the administrator console, go to DNS Filter – DNS Settings. On the settings page (DNS Server Selection), you may list one or more DNS servers where DNS Filter will send client requests. By default, DNS Filter will use the DNS server listed in the network settings of the computer where the application is installed.

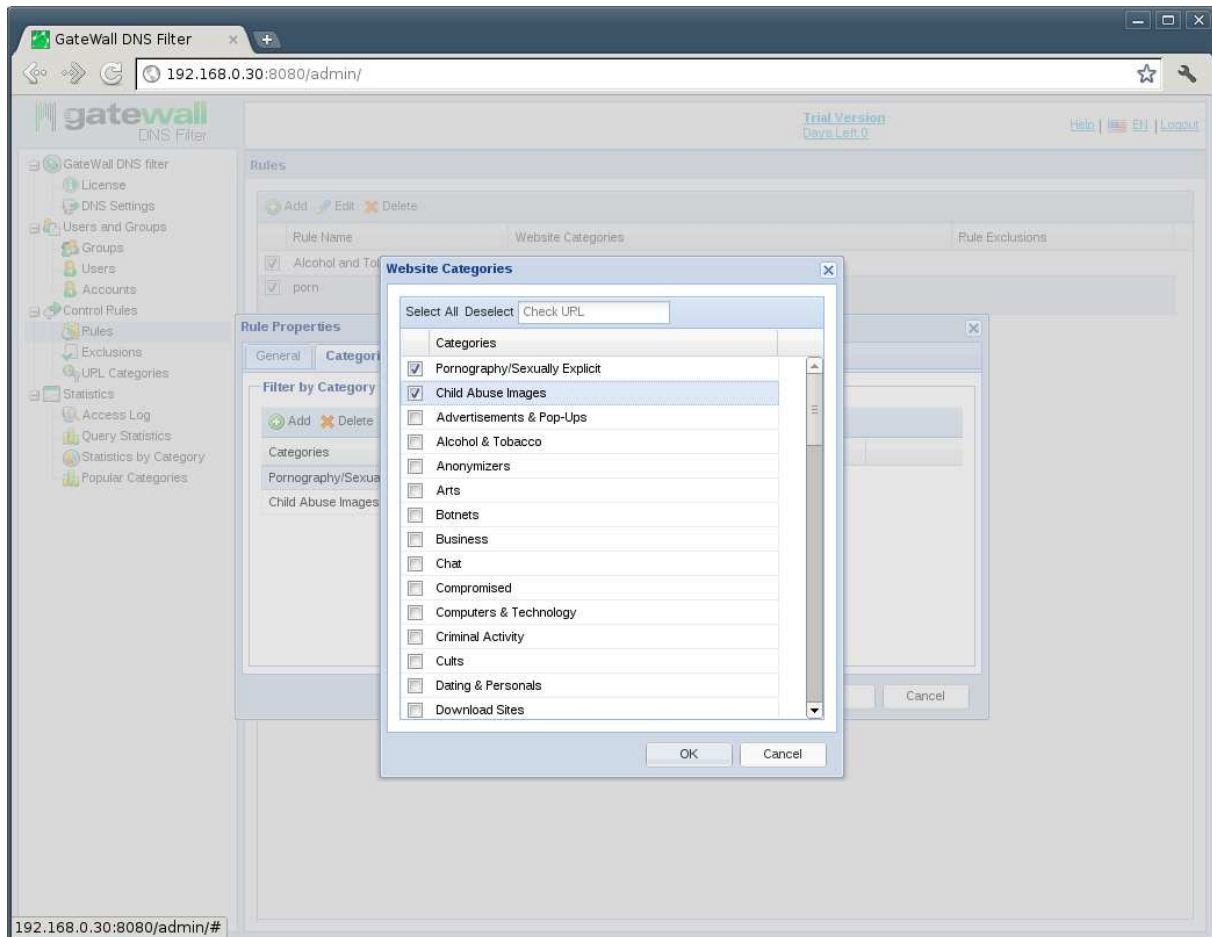
Traffic Control Rules

Traffic control rules are used to deny access to web sites of certain categories or in a given time of the day. These rules also enable URL filtering using blacklists and whitelists. Rule criteria may include time, day of the week or one or more URL categories. After you have created a traffic control rule, apply this rule to individual users or a group of users in DNS Filter.

To deny access to websites belonging to a certain thematic category, go to Traffic Control – Rules, create a new rule and select one or more URL categories on the second page of the dialog window.

Users with assigned web interface login and password may create block rules and exceptions. To do so, such users need to open the web-based administrator console at <http://192.168.-.1:8080>, where 192.168.0.1 is the IP address of the server where DNS Filter is installed, and enter the login and password provided by the server administrator. Once in the administrator console, users may create rules for website categories and domain names, set time restrictions, or create rules with different combinations of these conditions. If server administrator assigned "Group administrator" access level to a given user, this user can edit rules and manage user settings within this user's group and all subgroups belonging to that group of users.

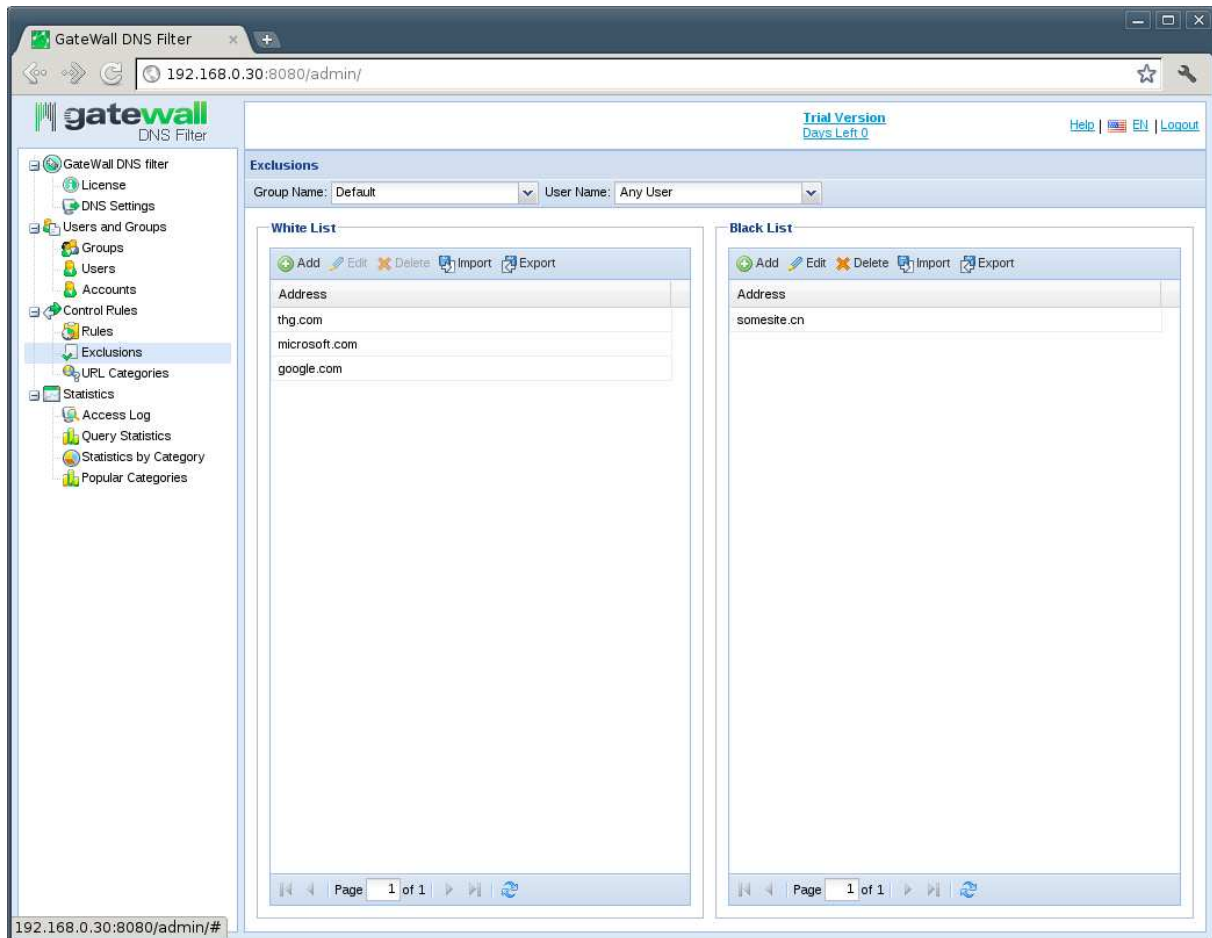
Caution! User cannot edit rules that are inherited from this user's group because such rules prevail over the rules created by the user. Besides, these rules will not be displayed in the user's administration web-interface.



Exception List

You may add one or more hosts to your blacklist or whitelist using the exception list (see "Exceptions" in the settings menu). Host names listed as "Allowed" will always be allowed, even if a certain host is listed in one or more forbidden categories. Host names listed as "Forbidden" will not be allowed to a valid IP address regardless of

the applicable traffic control rules. The exception lists are global lists, i.e. they apply to all GateWall DNS Filter users.



In the server settings file, host names specified in the exception list are located in the `<white_list />` and `<black_list />` subsections of `<Entensys URL Filter />` section. These subsections may contain incomplete host names with an asterisk (*) that may replace any beginning or ending of a URL address.

The server settings file contains another subsection where you can specify whitelist hosts ("Allowed" option). Such hosts will be listed in `<exclude_domains>` subsection of `<Entensys URL Filter />` section. This list may only contain full domain host names.

Website Categories

In this section, you may look up which URL category a specific URL belongs to and submit a category change request.

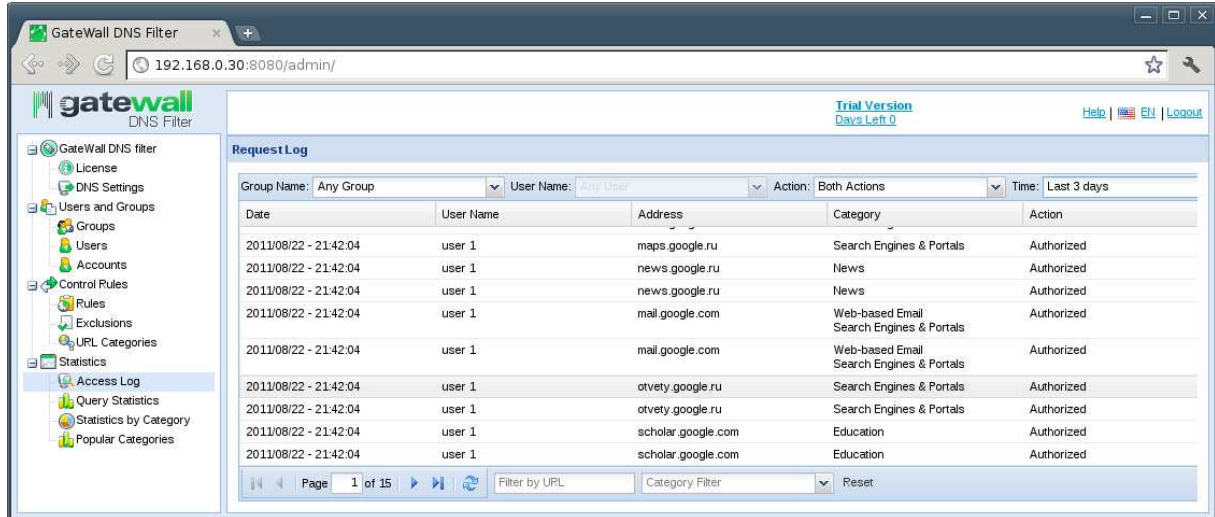
To look up a website category, type the URL in the corresponding box in the window and press Enter. When the system has finished processing your request, you will see a list of current categories to which this address belongs.

If you think that the provided information is no longer valid, you may select the category that you believe fits this URL the best in the dropout list. Only one or two categories may be selected from the provided list.

When you have selected the required category, press "Category change request" button, and your suggestion will be submitted for review.

Access Log and Request Statistics

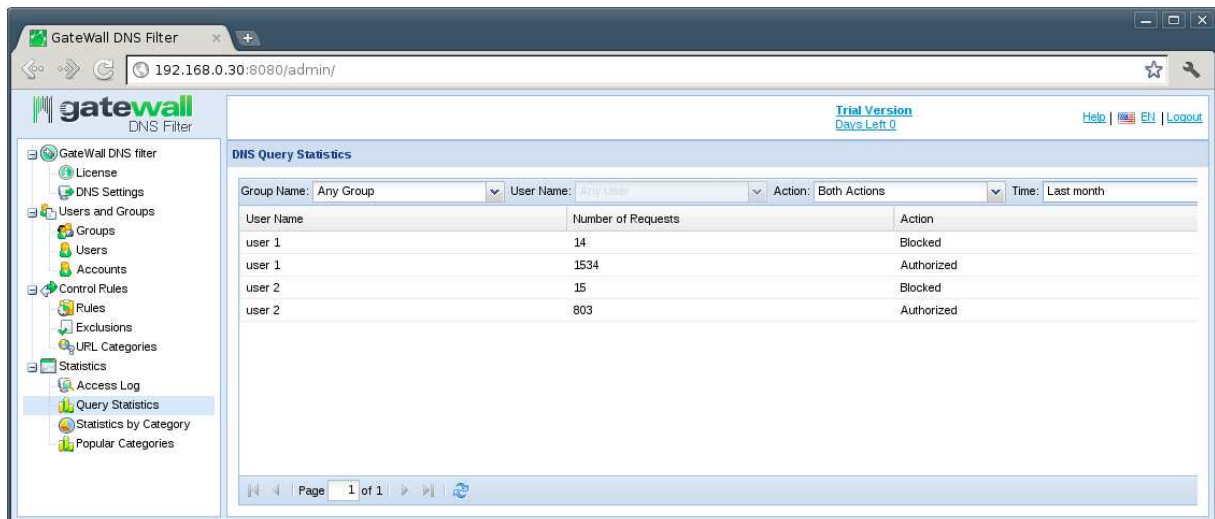
The Statistics page shows summary statistics of all allowed and blocked requests. The statistics may be sorted by user, group or activity over a certain period of time.



The screenshot shows the 'Request Log' page in the GateWall DNS Filter web console. The page includes a navigation menu on the left and a main content area with a table of request logs. The table has columns for Date, User Name, Address, Category, and Action. The data shows several requests from 'user 1' for various Google services, all of which were 'Authorized'.

Date	User Name	Address	Category	Action
2011/08/22 - 21:42:04	user 1	maps.google.ru	Search Engines & Portals	Authorized
2011/08/22 - 21:42:04	user 1	news.google.ru	News	Authorized
2011/08/22 - 21:42:04	user 1	news.google.ru	News	Authorized
2011/08/22 - 21:42:04	user 1	mail.google.com	Web-based Email	Authorized
2011/08/22 - 21:42:04	user 1	mail.google.com	Search Engines & Portals	Authorized
2011/08/22 - 21:42:04	user 1	otvety.google.ru	Search Engines & Portals	Authorized
2011/08/22 - 21:42:04	user 1	otvety.google.ru	Search Engines & Portals	Authorized
2011/08/22 - 21:42:04	user 1	scholar.google.com	Education	Authorized
2011/08/22 - 21:42:04	user 1	scholar.google.com	Education	Authorized

The Access Log page contains more detailed information about the latest name resolution requests, including the time of request and host name and category, as well as about the source of request (user/group). One page contains the last 20 requests, and you may browse through the other Access Log pages by pressing the corresponding navigation buttons.



The screenshot shows the 'DNS Query Statistics' page in the GateWall DNS Filter web console. The page includes a navigation menu on the left and a main content area with a table of query statistics. The table has columns for User Name, Number of Requests, and Action. The data shows the number of requests for different users and their actions (Blocked or Authorized).

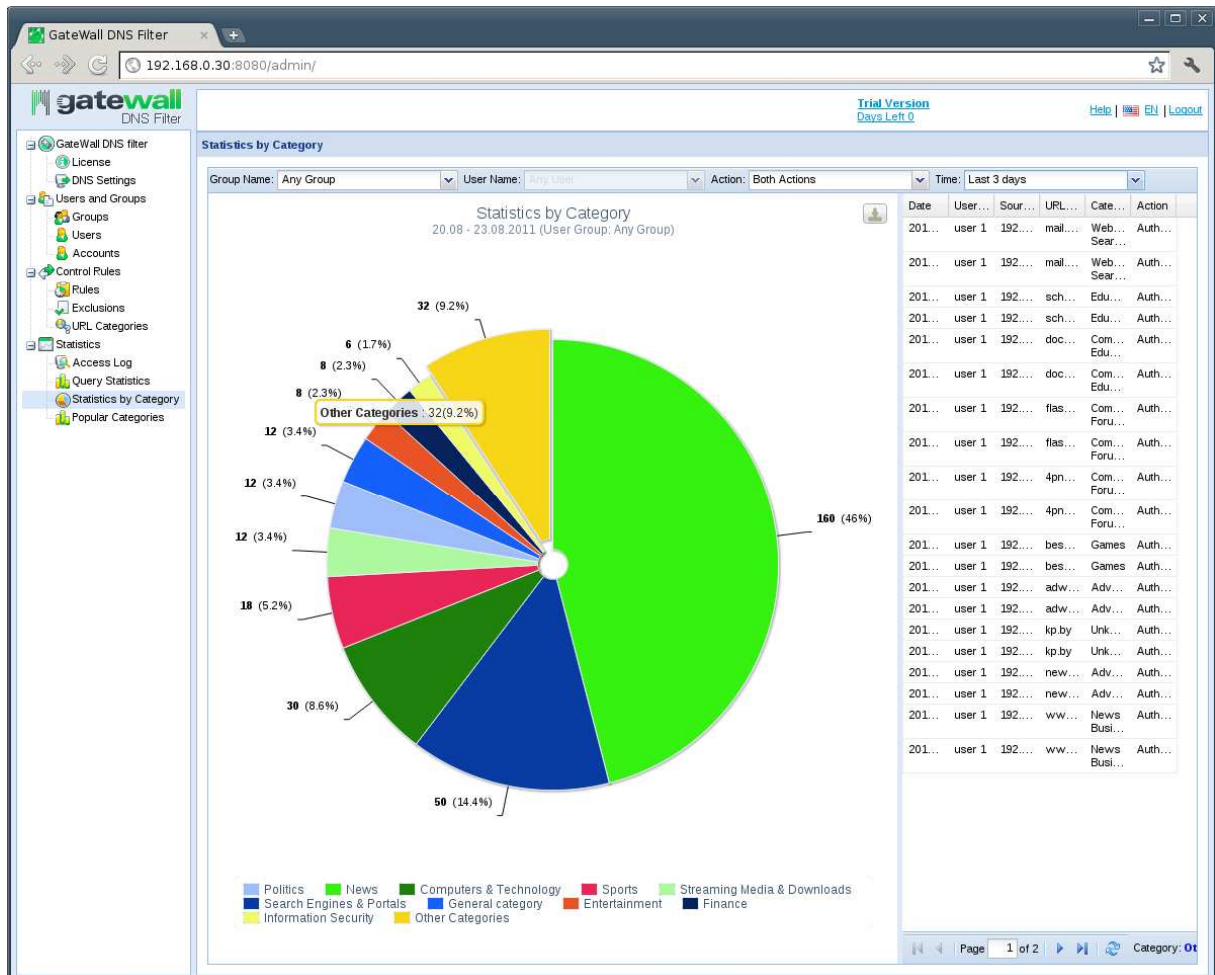
User Name	Number of Requests	Action
user 1	14	Blocked
user 1	1534	Authorized
user 2	15	Blocked
user 2	803	Authorized

Statistics by Category

Besides being able to manage access rights, users with Group Administrator rights may view their own and their group users' request statistics, access log and statistics by URL categories in the web console. Server administrator may view statistics for all users or filtered statistics.

The graph in the left section of the window showing segments of website categories in the overall number of requests has filter functionality. Click on a segment of the graph to view filtered statistics results only for the selected URL category. This functionality is very convenient when you need a more detailed report.

An “Export report” button has been added above the URL category graph for a better visualization and easier reporting. You may now export your reports into files with different formats, such as PNG, JPG or SVG.

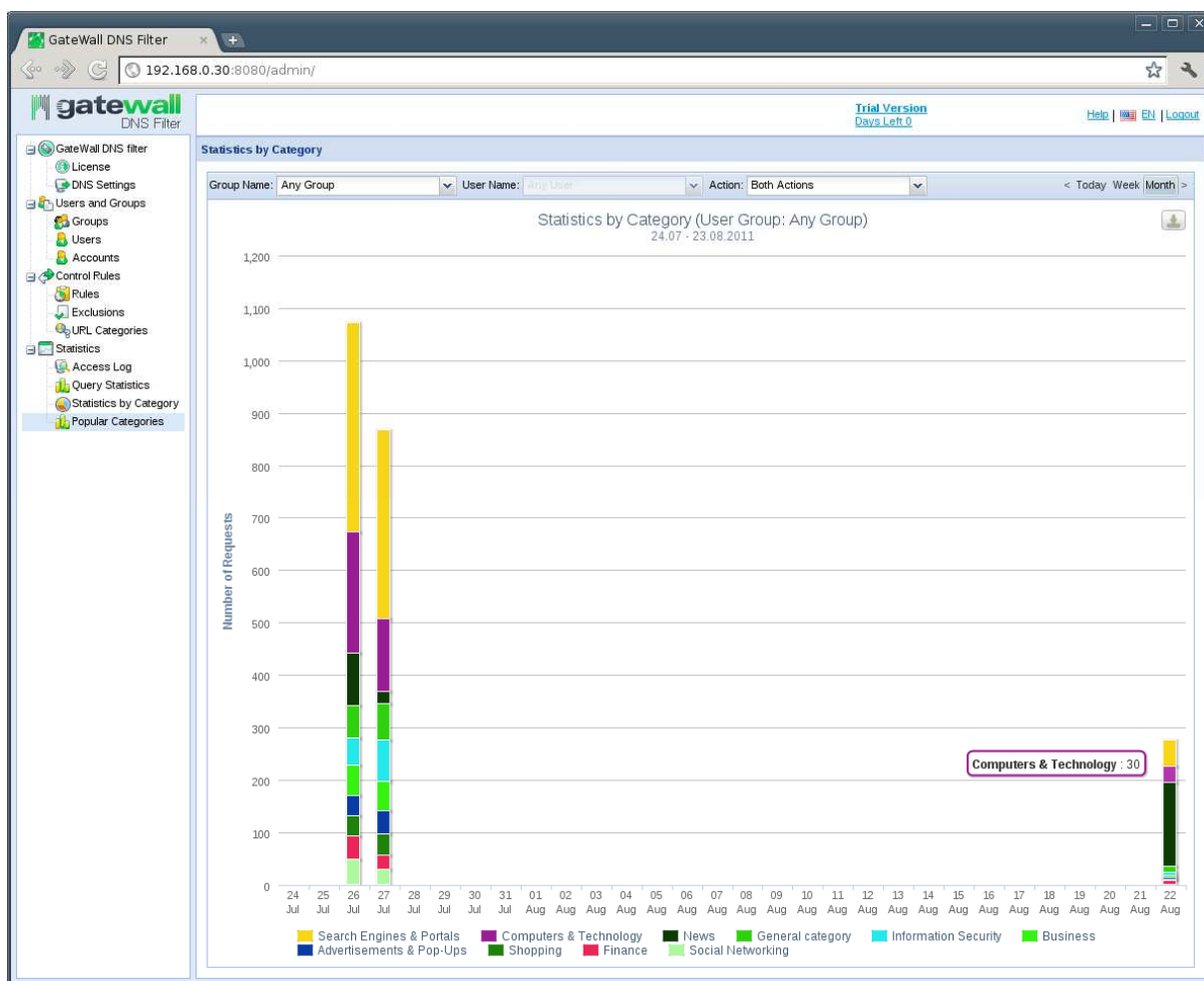


Popular Categories

This tab can be used to view statistics for ten most popular categories in any given day, last week or last month.

The graph shows the number of requests to websites from the most popular categories by hours (daily statistics) or by days (weekly/monthly statistics). Graph columns are broken down into color sectors, each representing one of the categories.

You may filter requests by group, user or the type of rule applied (“allowed” or “blocked”).



Requesting URL Categories from Entensys URL Filter

Entensys URL Filter categories are requested through a query to Entensys URL Filter Master Database service. DNS Filter submits a request to the service whose address is specified in the `server_name` parameter (see <Entensys URL Filter /> section of the settings file).

Category resolution request is run asynchronously via a socket pool. The minimum and maximum number of sockets used for connection to Entensys URL Filter service is set in the `min_socket_number` and `max_socket_number` parameters in the <Entensys URL Filter /> section of the settings file. The number of sockets may increase automatically along with the increase of load.

Important! We recommend setting higher values for `min_socket_number` and `max_socket_number` parameters for large networks in accordance with the server load.

GateWall DNS Filter Operation

In general, GateWall DNS Filter functions as described below:

- A user sends a DNS request for a domain name resolution.
- DNS Filter server scans through its own DNS cache and the integrated Entensys URL Filter cache to define the address and category of the requested domain name.
- If no data is available in the integrated cache, DNS Filter forwards the request to the DNS server specified in the settings and generates a request to Entensys URL Filter service.
- DNS Filter returns the response to the user and registers the request-related data in the database.

Note! Transactions are used for database entries (transactions="1"). The number of SQL INSERT operations in a transaction is set in the max_transactions="50" parameter in the server settings file. You may find both these parameters in the server settings file.

The response received by the user depends on whether the user is authorized by GateWall DNS Filter. If the user is authorized, it also depends on the access rights applied to this user and the exception list parameters. Requests sent by unauthorized users are registered in the database as unknown requests.

Declining Domain Name Resolution Requests

A domain name resolution request may be declined. A user will then be forwarded to a special address 127.0.0.1 or GateWall DNS Filter's own address. A request may be declined if one of the following occurs:

- The server is unable to define Entensys URL Filter category, for example, if the service is unavailable.
- The request to Entensys URL Filter is rejected due to license expiration.
- The number of sockets is insufficient to connect to Entensys URL Filter service.

Note: In case of insufficient number of sockets all declined DNS requests will be placed in a separate queue. Requests from this queue may be processed with a delay.

You can allow DNS name resolution when Entensys URL Filter service is unavailable. This feature is enabled in the "Allow DNS names cloud-based URL filter is unavailable" parameter of DNS Settings – General Settings menu.

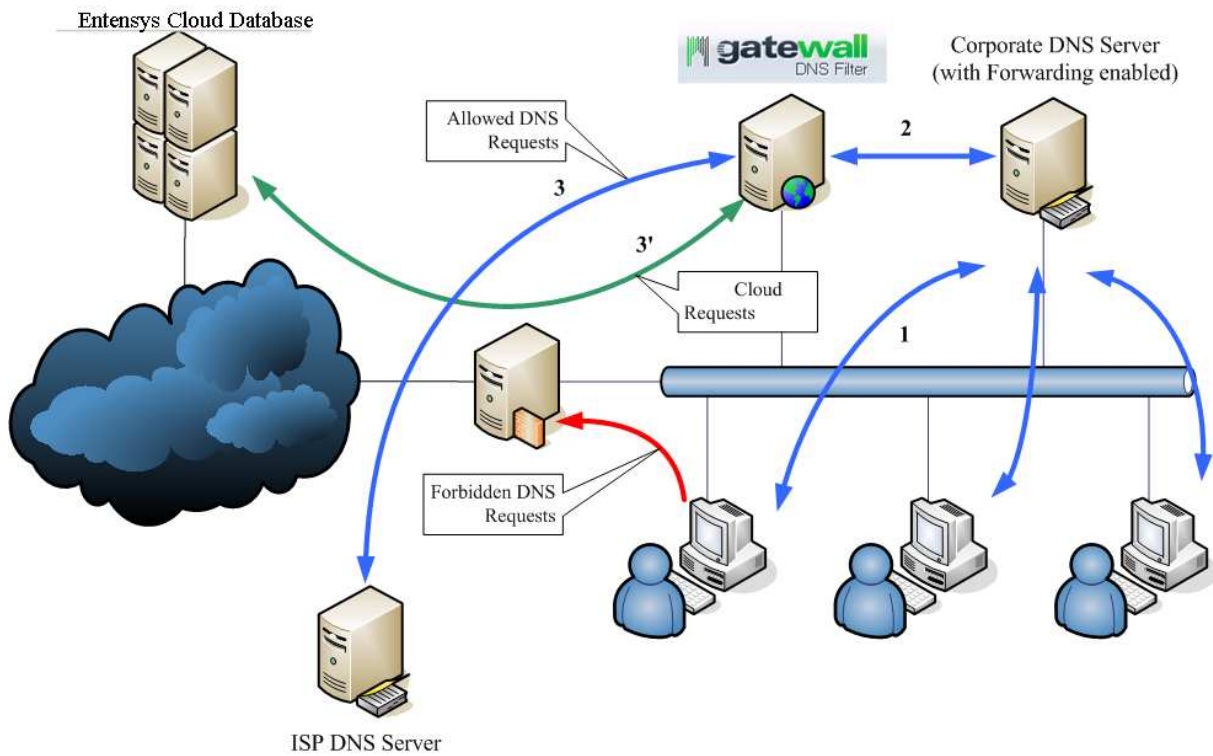


Forwarding Forbidden Requests

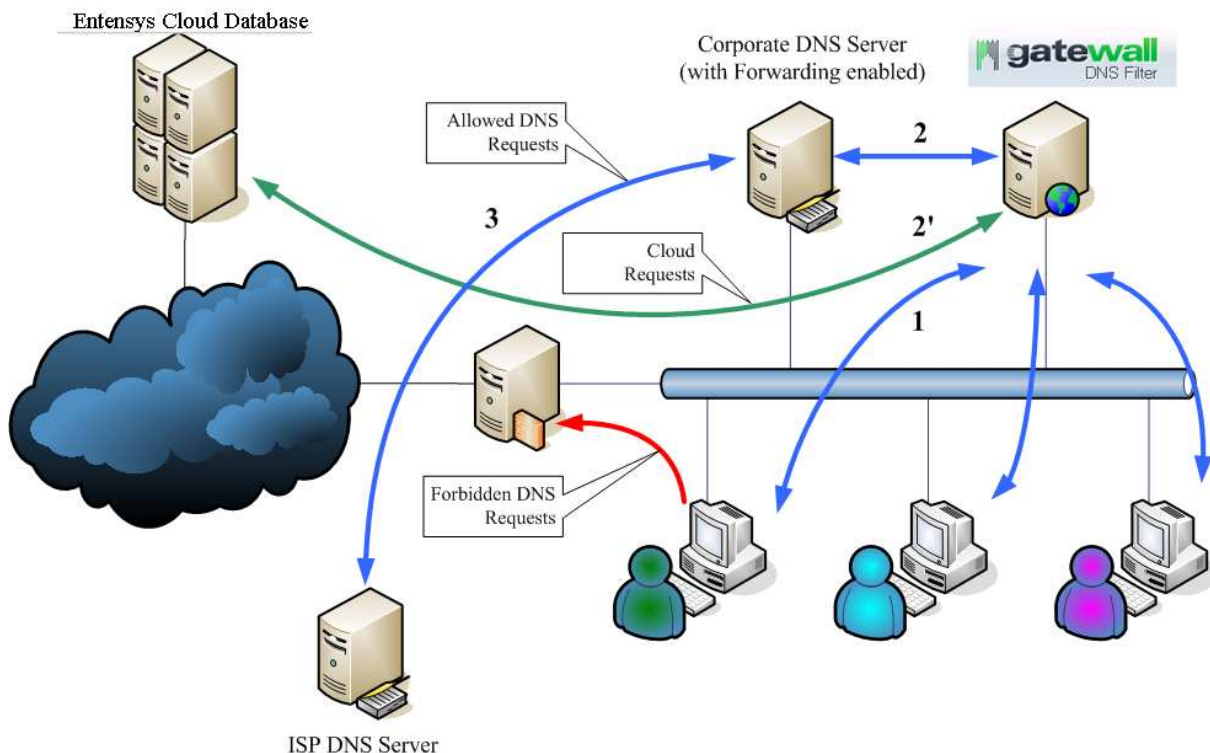
If host access is denied, the user will be forwarded to address 127.0.0.1 or GateWall DNS Filter's own address. Forwarding to GateWall DNS Filter's own IP address will occur when the "Forward to local IP address" option is enabled in DNS Settings – Forwarding Blocked Requests menu. If so, any user requesting a forbidden resource through a browser will be forwarded to a special reference page containing a notice of denied access.

GateWall DNS Filter Deployment Options

In corporate networks, GateWall DNS Filter may be deployed in two different ways. The first option is to locate GateWall DNS Filter upstream of the corporate DNS server. With this option, the corporate DNS server allows forwarding DNS requests to the ISP's DNS server(s). Create LAN users with IP authorization using DNS Filter administrator console. Specify corporate domain name in `exclude_domains` parameter of the `<Entensys URL Filter />` section of the server settings file. DNS settings should confirm that DNS requests will be sent to the internal corporate DNS server. Internet access must be allowed on a client PC with GateWall DNS Filter via HTTPS and BCAP (Entensys URL Filter Control Application Protocol, TCP port 2316) protocols. This option of GateWall DNS Filter deployment allows generating detailed statistics for all LAN users (client machines).



The second option is to install GateWall DNS Filter immediately downstream of the corporate DNS server. With this option, corporate DNS server settings need to specify GateWall DNS Filter as the server forwarding requests (Forwarder). Create just one user in DNS Filter settings with the IP address of the corresponding corporate DNS server. In DNS Filter settings, specify ISP's DNS server(s) as the forwarding DNS servers. This option allows reduction of GateWall DNS Filter load due to additional caching on the corporate DNS server. However, this will make LAN users' request statistics unavailable.



Important! While GateWall DNS Filter is not a gate solution, DNS requests sent directly by users into the Internet must be blocked in either deployment option.

Displaying Additional Debug Information

An administrator may create special *.sem files in DNS Filter's root folder to collect additional information about GateWall DNS Filter's operation. A SEM file is an empty *.sem file with a definite name. The following file names are used for certain functions: dnslog.sem – detailed information about DNS name resolution; bclg.sem – detailed information about requests to Entensys URL Filter; and dblog.sem – information about database activity. DNS Filter server must be restarted after any of these SEM files has been created. All debug information will be registered in %DNSFilter%\Logging\dnsfilter.log.

Application's logging parameters can be set in the <logs /> section of the server settings file. The maximum log size is set in max_size parameter; the default maximum size is 20 Kb. If the log file size exceeds the maximum setting, DNS Filter server will create a new dnsfilter.log log file and add a date to the name of the old file. There are no limitations as to the number of log files that can be created.

Important! Using SEM files in high-load systems will cause a quick propagation of log files and result in higher CPU loads.