



GateWall DNS Filter

Administrator Manual

CONTENTS	INTRODUCTION	3
GATEWALL DNS FILTER		3
SYSTEM REQUIREMENTS		3
GATEWALL DNS FILTER INSTALLATION		3
UPDATE AND UNINSTALL DNS FILTER		4
REGISTER GATEWALL DNS FILTER		4
GATEWALL DNS FILTER LICENSING POLICY		5
PROGRAM UPDATE		5
DNS FILTER ADMINISTRATION MODULE		5
CONNECTION SETUP		6
<i>Setting Connection Password</i>		6
MANAGING GATEWALL DNS FILTER STATISTICS DATABASE		7
<i>Using Third-Party Databases</i>		7
<i>Database Recovery</i>		8
USERS AND GROUPS		8
<i>User Authorization Methods</i>		9
DNS SETUP		9
TRAFFIC CONTROL RULES		10
ACCESS LOG AND REQUEST STATISTICS		10
EXCEPTION REQUESTS		11
BRIGHTCLOUD URL CATEGORY FILTERING		12
EXCEPTION LIST		13
REQUESTING URL CATEGORIES FROM BRIGHTCLOUD		14
GATEWALL DNS FILTER OPERATION		15
DECLINING DOMAIN NAME RESOLUTION REQUESTS		15
FORWARDING FORBIDDEN REQUESTS		16
GATEWALL DNS FILTER WEB STATISTICS		16
GATEWALL DNS FILTER DEPLOYMENT OPTIONS		17
DISPLAYING ADDITIONAL DEBUG INFORMATION		18

Introduction

GateWall DNS Filter is a DNS forwarder application with enhanced functionality. Its additional features include defining the requested host category, tracking and recording processed requests and managing traffic rules. 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

GateWall DNS Filter contains the following modules: a server, an administration console (DNS Filter Administrator) and a Web-server with HTTPS support and Web-statistics module.

DNS Filter server (DNSFilter.exe process) is a Windows system service. The server allows users' requests DNS resolution, filtering, and records requests' statistics.

DNS Filter administration console is used to control GateWall DNS Filter server. The console communicates with the server via a special protocol over TCP/IP, which allows administration of the server remotely. Brief statistics of DNS requests can be viewed from the administration console. More detailed statistics are available in the Web-statistics module.

An integrated Web-server is used to access the Web-statistics and can serve as a forwarder for users' HTTP requests. For example, when a user is trying to access a prohibited web site, a corresponding notification will appear on the screen.


System Requirements

GateWall DNS Filter server is supported by any Windows XP/2003/Vista/2008/Windows7 based PC with Internet connection. 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 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.

Two additional services will appear on the system services list: GateWall DNS Filter and GateWall DNS Filter DB Service. The first service is the DNS Filter itself (DNSFilter.exe process), and the other one is used to administer the integrated database (DB). The program uses FireBird as the integrated DB. Both services will start automatically after installation. The agent icon  will appear in the system tray for convenience. You may use the agent’s context menu to start the administration console, stop or restart DNS Filter server or access the log file.

Update and Uninstall DNS Filter

We recommend you uninstall 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. To uninstall DNS Filter, go to Start - Programs, find the application and select Uninstall or use the “Add/Remove Programs” in the Control Panel. A server settings file will not be deleted from %DNSFilter% folder during the uninstall process. If a third party statistics database was used, then it will not be deleted.

Register GateWall DNS Filter

When you start the administration console for the first time, a registration window will pop up requesting you to enter either your demo key or full license key. The key request is performed online (via HTTPS protocol), through a request to the usergate.ru website. When prompted to enter the full license key, you need to enter the special pin code provided to you when you purchased GateWall DNS Filter software. In addition, you will be additionally asked for personal data (user name, email, country, and region) during the registration process. The sole purpose of requesting your personal data is to link the license to the user. The personal information will not be disclosed. 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 work correctly, you must allow it to access the Internet via HTTPS protocol. It is a requirement for online status checks of the key.

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 BrightCloud categories will also be generated for maximum ten users.

GateWall DNS Filter's license includes the license for the BrightCloud module, which is a URL category filter. The BrightCloud license is a limited license, valid for one year. The online BrightCloud service will be unavailable when the license has expired.

Program Update

To check for updates, open the administration console and go to the Help menu. Then click on "Check for updates." DNS Filter will submit a request for the number of the latest software version to the vendor's website. If the current installed version is older than the version available on the website, a notification will appear in the administration console window. The administrator can download and install the latest version from the website. An update check will not cause an automatic reinstallation of GateWall DNS Filter.

DNS Filter Administration Module

Administration Module is an application designed to manage GateWall DNS Filter's local and remote servers. To use DNS Filter Administrator, you need to run DNS Filter service by clicking on "Start DNS Filter server" in the agent's menu. If the administration module is installed on another PC, you can launch DNS Filter Administrator from Start – Programs. Connect the administration module to the server to manage its settings.

Connection Setup

When you launch the administration console for the first time, it will open on the Connections page. The only connection displayed on this page is the connection with localhost server for the Administrator. By default, no password is assigned to connect to DNS Filter Service. To connect the administration console to the server, double-click on “localhost – Administrator” line or click “Connect” on the control panel. You may create several connections in the administration console. Connection settings include:

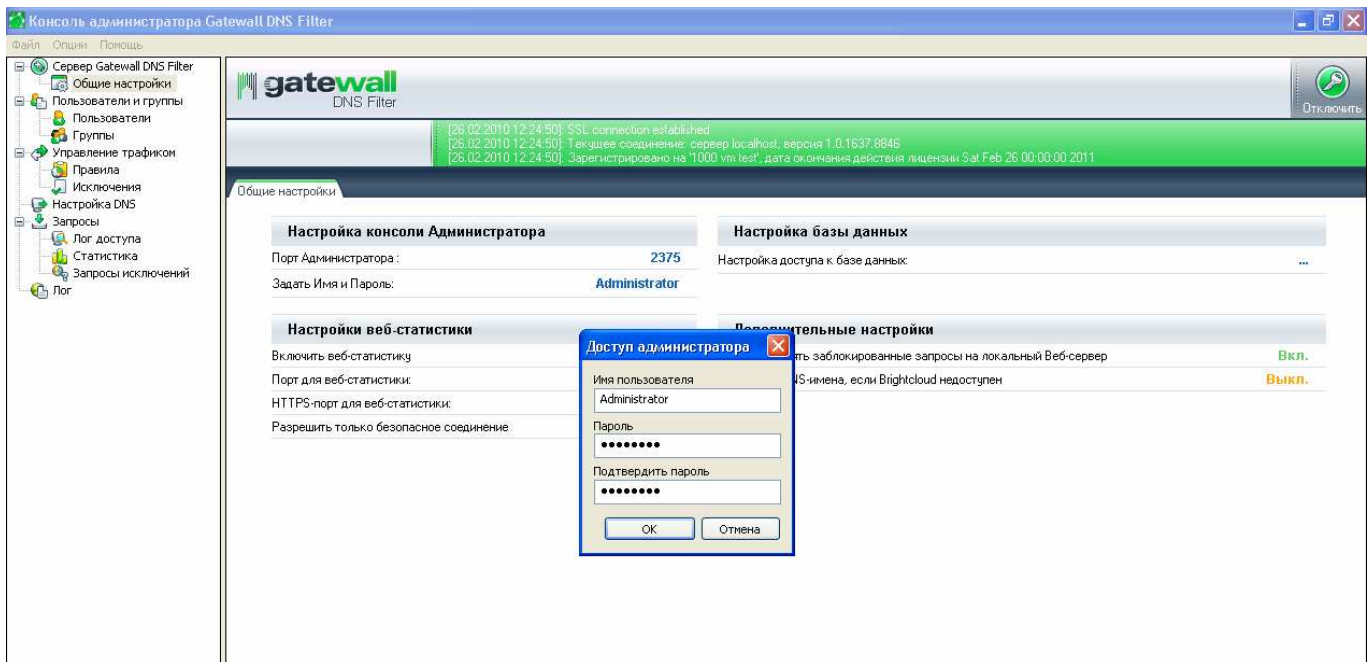
- Server name – name of the new connection
- User name – a login used to connect to the server
- Server address – DNS Filter server domain name or IP address
- Port – TCP port used to establish server connection (port 2375 is used by default)
- Password – a password for the new connection.

Select “Request password to establish connection” if you want the system to display a password dialog box when you are connecting to a server. Select “Connect automatically” if you want to connect to a given server automatically when you start the administration console.

Administration console settings are stored in file *console.xml*, which is located in folder %DNSFilter%\Administrator. On the server side, the username and password (hashed) are stored in file %DNSFilter%*dnsfilter.xml*.

Setting Connection Password

To assign login/password to a connection to DNS Filter server, open the General Settings page in the Administrator Console Settings window. You can also change the TCP port used to connect to the server in this window. Restart DNS Filter server for the changes to take effect (click “Restart DNS Filter server” in the agent’s menu). After you restart the server, enter the new settings in the connection parameters in administration console to enable the administrator to connect to the server.



Managing GateWall DNS Filter Statistics Database

DNS Filter 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 with 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 the password.

Using Third-Party Databases

Due to ODBC support, you can use almost any type of database (MS Access, MS SQL or MySQL). For MS SQL and MySQL format, GateWall DNS Filter’s installation package contains dumps of databases with the appropriate structures. These dumps are placed in folder “`%DNSFilter%\db_dumps.`”

If you need to setup 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 administration 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* parameter to 0 in *<database/>* section.
- Go to Windows “Administration – ODBC Sources” console and create a system DSN (Data Source Name) named DNSFilter that refers to the appropriate database (MySQL, MS SQL).
- Start GateWall DNSFilter service.

Note: DNSFilter 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.

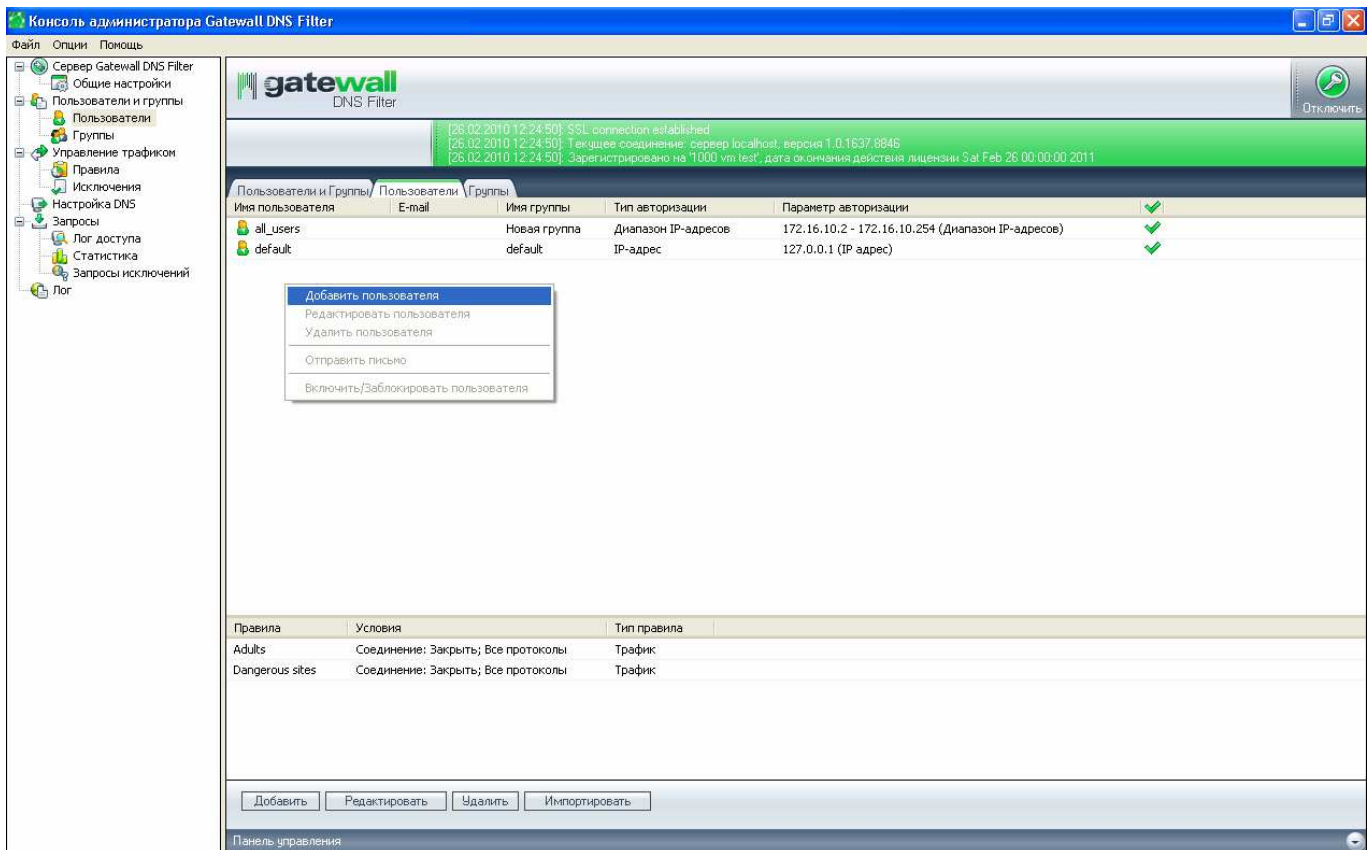
Database Recovery

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 join users to groups by their location or access rights for your convenience. Grouping users by their access rights is the most logical approach. This method will help you greatly simplify the traffic rules management. “Default” is the only group available in DNS Filter by default.



To create a new user, click “Add new user” or click the “Add” button on the control panel 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. You can also allow or block users’ access to the web statistics and assign traffic rules (DNS request filtering rules) on the user parameters page.

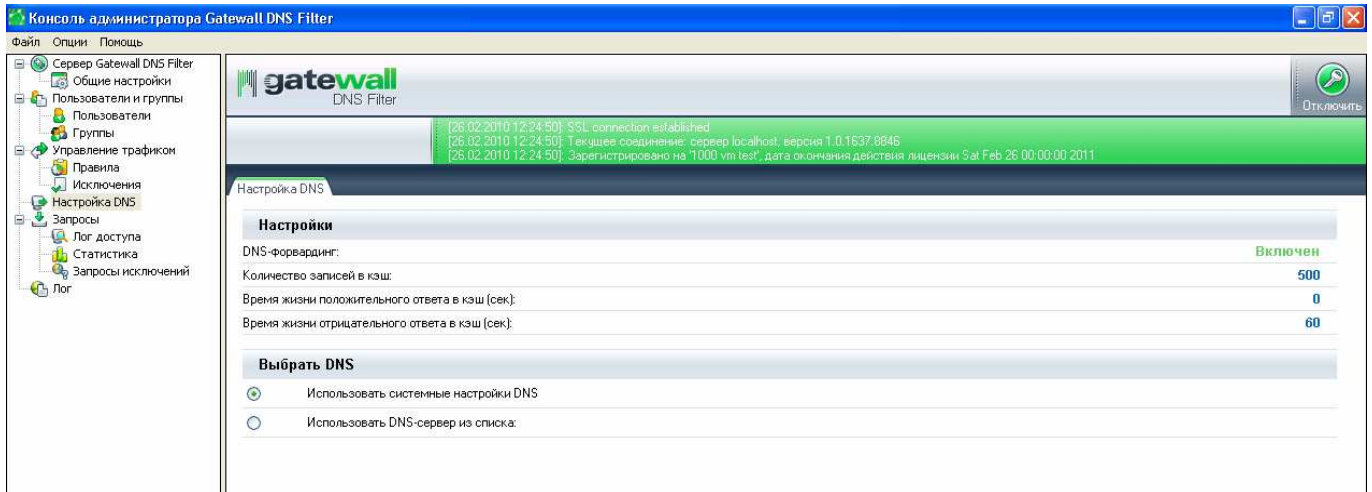
User Authorization Methods

DNS names resolution in GateWall DNS Filter server is available to all users on the LAN. The DNS request filtering will only apply to authorized users. 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 by 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 quantity of entries that can be stored in the program’s DNS cache is set

in `cache_size` parameter located in `<dns_forward />` section of the settings file. 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 (parameters `max_cache_pos_ttl` and `max_cache_neg_ttl`).



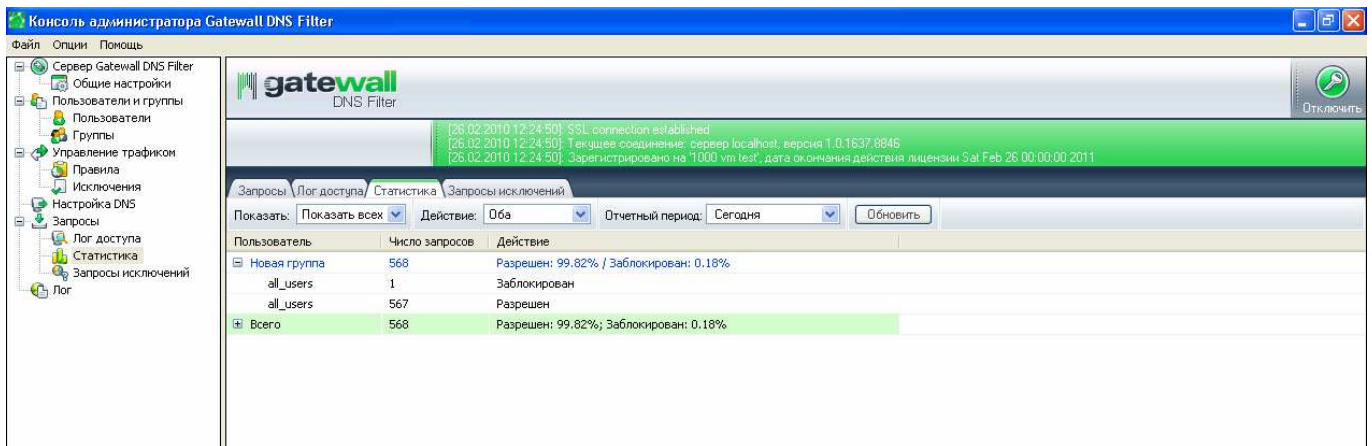
To configure DNS in the administration console, go to Services – DNS Setup. You may list one or more servers in the settings where DNS Filter will send client requests. By default, DNS Filter will use the DNS server listed in the network settings of the computer where the application is installed.

Traffic Control Rules

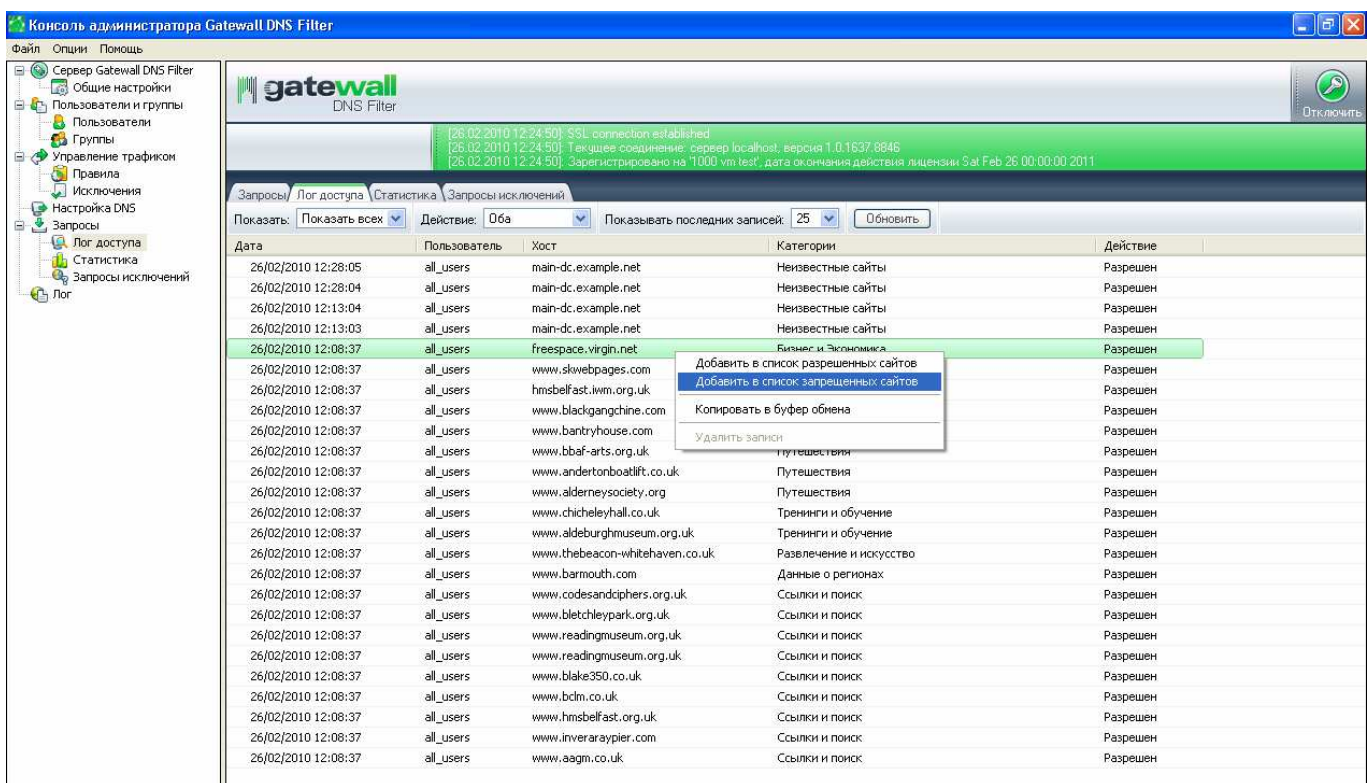
Traffic control rules are used to deny access to web sites of certain categories or in a given time of the day. These rules also enable URL filtering using blacklists and whitelists. Rule criteria may include time, day of the week or one or more URL categories. After you have created a traffic control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

Access Log and Request Statistics

The Requests section of the administration console contains statistics of requests processed by DNS Filter server. The Statistics page shows a statistics summary of all allowed and blocked requests. The statistics may be sorted by user, group or activity over a period of time.

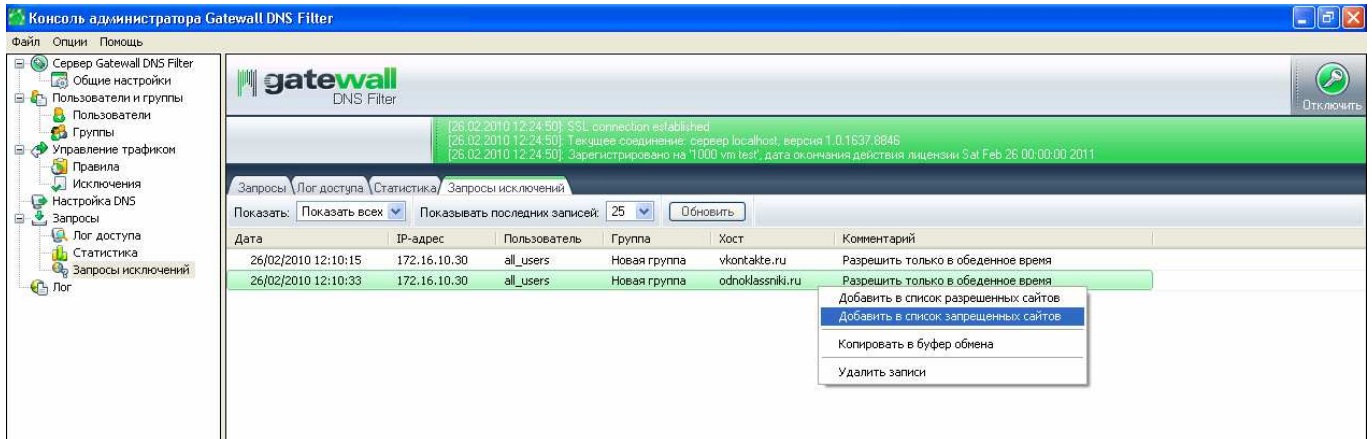


The Access Log page contains more detailed information about the latest name resolution requests, including the time of request and host name and category, as well as about the source of request (user/group). You may review statistics for the last 25, 50 or 100 requests.



Exception Requests

Users authorized to access GateWall DNS Filter's web statistics may create requests to add a domain name to the exception list. Such requests are registered in a special database table within GateWall DNS Filter.

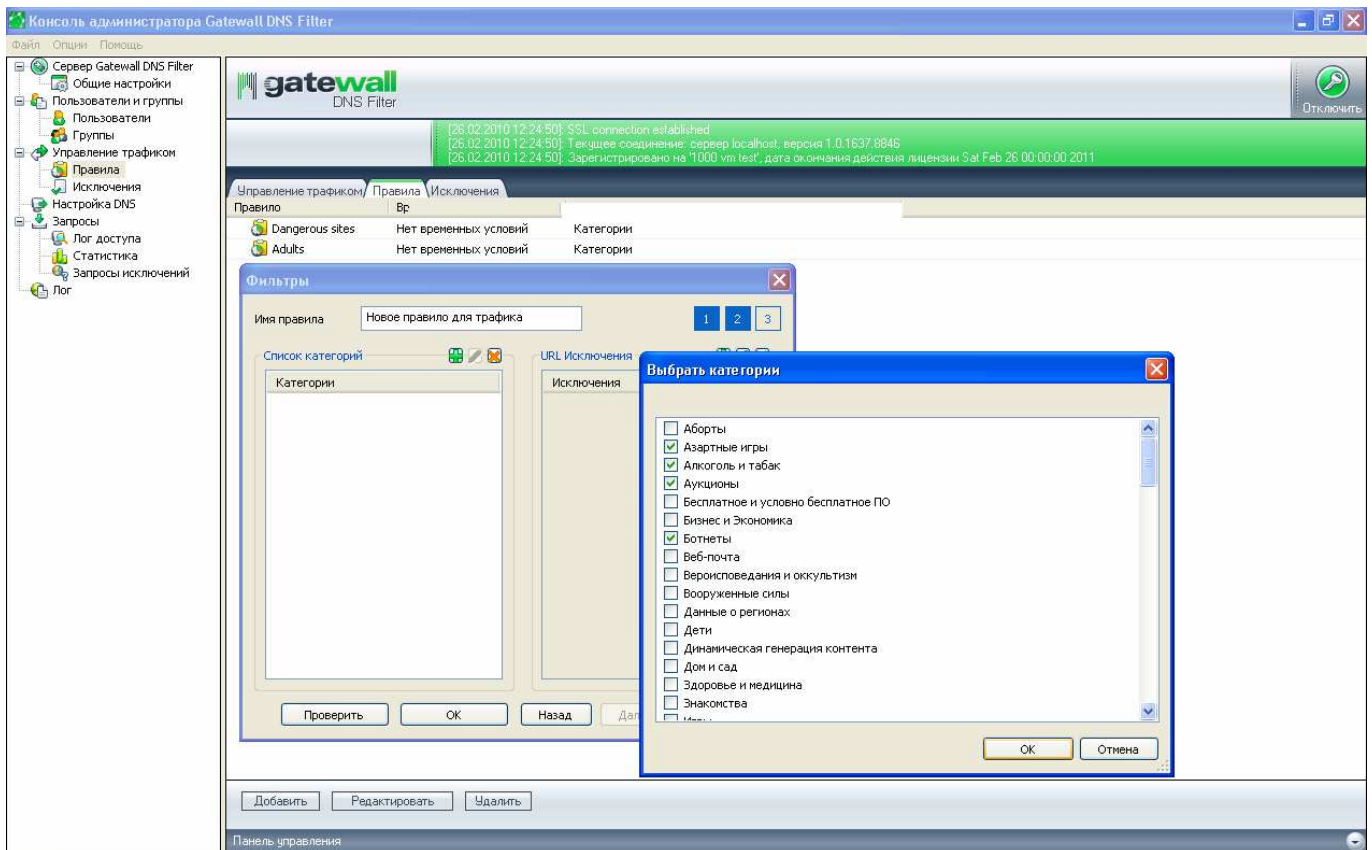


GateWall DNS Filter administrator may use the Exception Requests page to check the incoming requests, sort data by users and add requests on the exception list.

BrightCloud URL Category Filtering

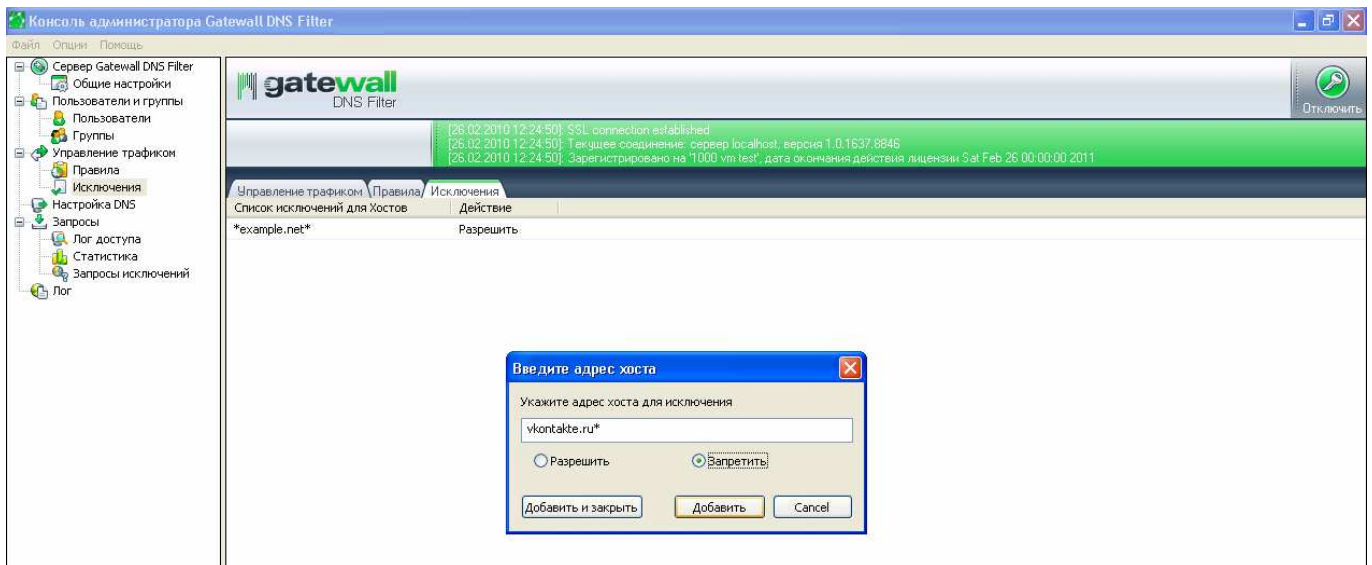
Through cooperation with BrightCloud Inc, GateWall DNS Filter includes integrated BrightCloud Service and BrightCloud Master Database tools. An administrator may deny clients access to web sites with certain types of content without having to name the sites. DNS Filter statistics module can generate a report of the categories of all visited web sites, such as advertising, education, news, etc. Filtering by URL categories allows a more flexible Internet access policy.

To deny access to a specific category of web sites, open Rules window in Traffic Control section, create a new rule and select one or more URL categories on the last page of the dialog box.



Exception List

You may add one or more hosts to your blacklist or whitelist using the exception list (see “Exceptions” in the settings tree). 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 resolved regardless of the applicable traffic control rules. The exception lists are global lists, i.e. they are applied to all users connected to GateWall DNS Filter.



Host names listed in the exception list are stored in `<white_list />` and `<black_list />` subsections of `<brightcloud />` section in the server settings file. You may specify incomplete host names in these subsections, replacing the omitted segment by a “*” symbol.

The settings file includes another section where you may specify whitelist hosts (“Allowed” option). Such hosts will be listed in `<exclude_domains>` subsection of `<brightcloud />` section. This list may only contain full domain host names.

Requesting URL Categories from BrightCloud

BrightCloud URL categories are requested from BrightCloud Master Database service. DNS Filter sends a request to the service, and the service’s address is specified in `server_name` parameter in the `<brightcloud />` section of the settings file.

Category resolution request is run asynchronously via the socket pool. The minimum and maximum numbers of sockets used for connection to BrightCloud service are set in `min_socket_number` and `max_socket_number` parameters in the `<brightcloud />` 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 internal BrightCloud cache to define the address and the 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 BrightCloud 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 parameter *max_transactions="50"* of the server settings. 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 routed 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 BrightCloud category, for example, if the service is unavailable.
- The request to BrightCloud is rejected due to license expiration.
- The number of sockets is insufficient to connect to BrightCloud service.

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

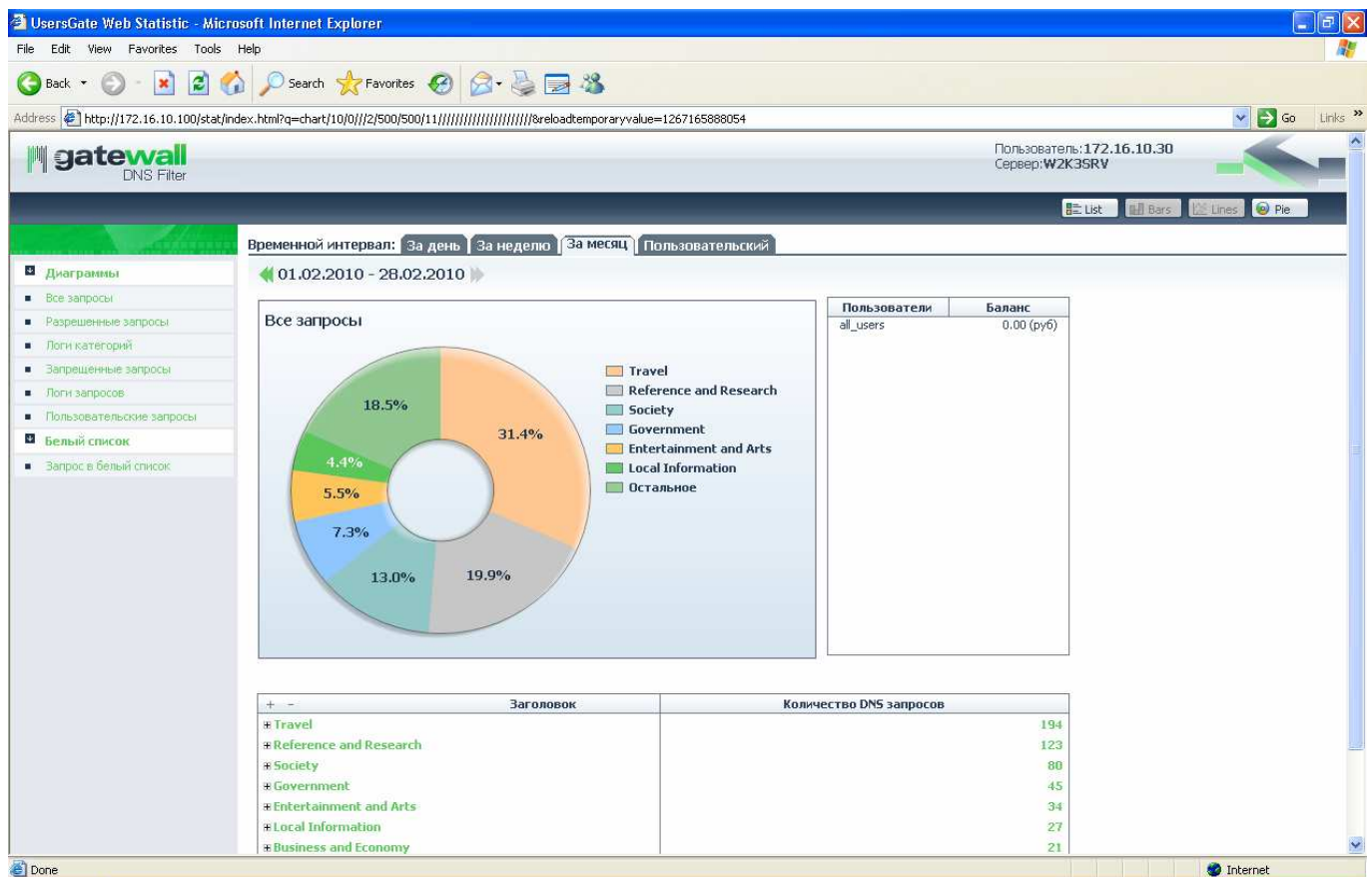
You can allow DNS name resolution when BrightCloud service is unavailable. This feature is enabled in the parameter "Allow DNS names if BrightCloud service is unavailable" of the general settings.

Forwarding Forbidden Requests

If host access is denied, the user will be routed to address 127.0.0.1 or GateWall DNS Filter’s own address. Routing to GateWall DNS Filter’s own IP address will occur when the option “Forward requests to internal Web server” is enabled. 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 Web Statistics

GateWall DNS Filter web statistics module provides detailed information about all the processed DNS requests by users, categories, time of day and result (“Allowed” or “Forbidden”). You may allow DNS Filter users access to web statistics. GateWall DNS Filter features two access modes: access to web statistics is allowed (default parameter) or blocked.



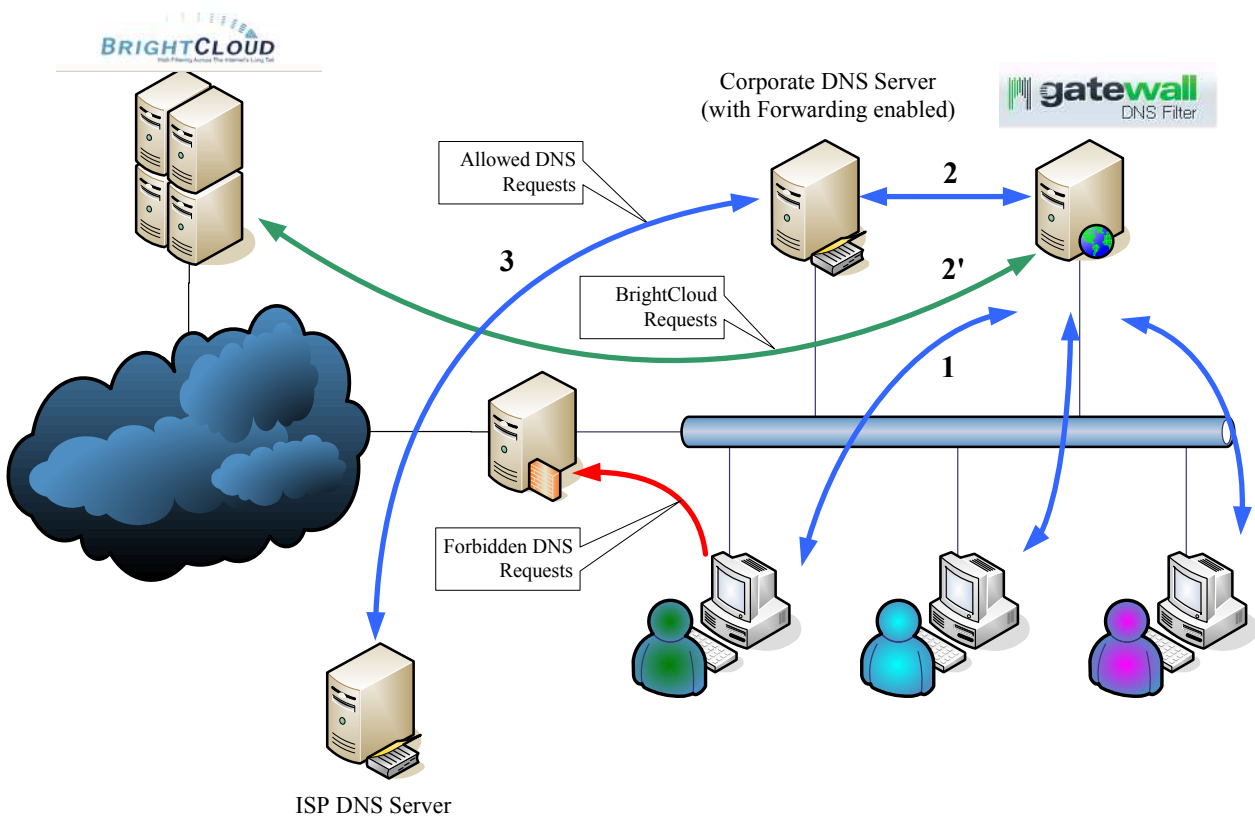
Web statistics can be reviewed at either of the following addresses: <http://192.168.0.1/stat/index.html> or <https://192.168.0.1/stat/index.html>, where 192.168.0.1 is DNS Filter

server's address. The specific port used for web statistics can be specified in "General Settings – Web Statistics Settings" section. Ports 80 and 443 are used by default.

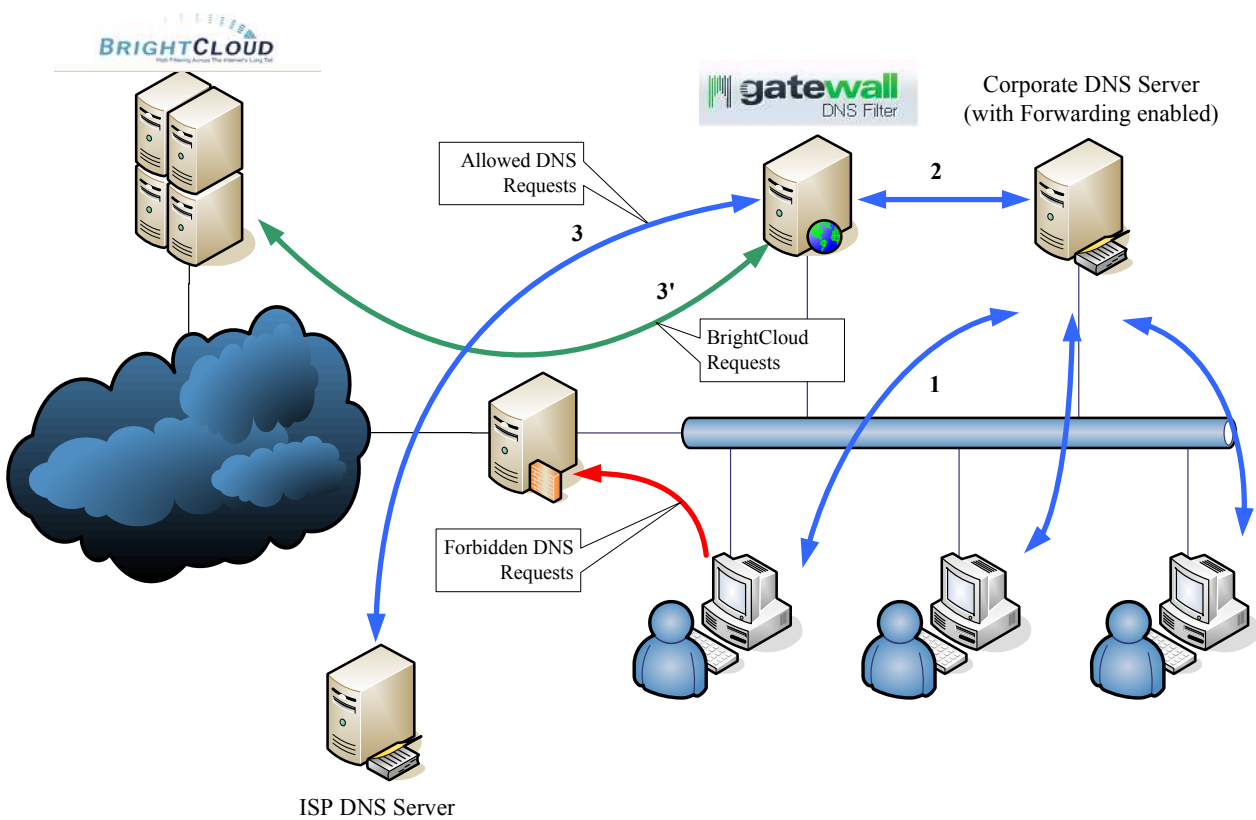
The web statistics module may be disabled on the General Settings page of GateWall DNS Filter's administration console.

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 `<brightcloud />` section of the server settings file. DNS settings should specify that DNS requests will be sent to the internal corporate DNS server. Internet access via HTTPS and BCAP (BrightCloud Control Application Protocol, TCP port 2316) protocols should be allowed on a PC with GateWall DNS Filter. 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 to forward 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! GateWall DNS Filter is not a gate solution, which means DNS requests sent directly by users to the Internet must be blocked.

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 file with a definite name and *.sem extension. The following names are used for certain functions: *dnslog.sem* – detailed information

about DNS name resolution; *bclog.sem* – detailed information about requests to BrightCloud; 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 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.