UserGate Proxy & Firewall v.6

User guide

www.entensys.com

Table of Contents

Introduction

A proxy server is a program system that functions as an intermediary between a user's workstation and other network services.

The solution transmits all of the user's requests to the Internet, receives an answer and sends it back. If there is a cache function available, the proxy server remembers the workstations' requests to external resources, and in case there is a repeat request, it returns the resource from its own memory, significantly reducing the request time.

In some situations, the proxy server can modify or block the client's request or a server’s response for specific purposes, for example, to protect workstations from a virus.

About the program

UserGate Proxy & Firewall is a comprehensive solution for connecting users to the Internet, making sound traffic calculations, restricting access and protecting your network with its own built-in instruments.

UserGate enables the tariffing of user Internet access, both by traffic amounts and by time spent online. An administrator can add various billing plans, dynamically switch them, automate funds crediting and withdrawal, and control access to Internet resources. The built-in Firewall and Antivirus module protects the UserGate server and scans the traffic passing through it for malicious code. To ensure safe Internet access for your business, you can use the built-in VPN Server & Client.

UserGate consists of several parts: the server, the Administration Console (UserGate Administrator) and several additional modules. UserGate server (the process *usergate.exe*) is the main part of the proxy server where all of its functional capabilities are embodied.

UserGate server provides Internet access, calculates traffic, tracks users’ online statistics, and carries out many other tasks.

UserGate Administration Console is a program designed to control UserGate server. The UserGate Administration Console communicates with the server module through a special protected protocol above TCP/IP, enabling server remote administration.

There are also three additional modules included in UserGate: Web Statistics, UserGate Authorization Client and Application Control.

System requirements

It is recommended to install UserGate server on a computer with the Windows XP/2003/7/8/2008/2008R2/2012 operating system, connected to the Internet via a modem or any other type of connection. Server hardware requirements are as follows:

Network configuration	Minimum requirements	Recommended requirements
Small LAN: 5-20 users	Intel Pentium 1 GHz, 1 Gb RAM, Microsoft Windows 7, DSL	Intel Pentium/Atom 1,7 GHz, 2 Gb RAM, Microsoft Windows 2008/7, DSL
Medium LAN: Over 20 users	Intel Pentium 2 GHz, 2 Gb RAM, Windows 7, DSL	Intel Core 2 GHz, 2 Gb RAM, Microsoft Windows 2008/2012, Ethernet
Large LAN: Over 150 users	Intel Core Duo 2 GHz, 4 Gb RAM, Microsoft Windows 2008, ISDN or Ethernet	Intel Core Duo 3 GHz, 8 Gb RAM, Microsoft Windows 2008/2012, Ethernet

UserGate Proxy & Firewall installation

To install UserGate, simply run the installation file and specify the Installation Wizard options. When installing the software for the first time, you can leave the default options. When the installation is finished, restart the computer.

Registration

To register the program, start UserGate server, connect the Administration Console to the server, choose “**Help**” from the menu and then “**Register Product**". The first time the Administration Console is connected, a registration dialog box will appear offering two options: request a trial key or request a full license key. The request is carried out online (HTTP protocol) via the entensys.com website.

When requesting a full license key, you must enter a special PIN code that is issued when you buy UserGate Proxy & Firewall or by the Support Service for a trial period. When registering, you also need to enter additional personal information (user name, e-mail address, country and region). Personal data is used exclusively for issuing a user license and is not shared with anyone. After receiving a full license key or trial key, UserGet server will automatically restart.

Important note! The trial version of UserGate Proxy & Firewall will work for 30 days. When contacting Entensys, you can request a special PIN code for an extended trial. For example, you may request a trial key for three months. You cannot receive a repeat trial license without entering a special extended PIN code.

Important note! While using UserGate Proxy & Firewall, the registration key status is periodically verified. To ensure proper UserGate operation, Internet access via HTTPS must be allowed. This is required for performing an online test of the key status. If the key verification fails three times, the proxy server license will be reset and a program registration dialog will appear. The program has a counter for the maximum number of activations, which is 7 times. Once this limit is exceeded, you can activate the product with your key only after contacting the Support Service at http://entensys.com/support.

Update and removal

The new UserGate Proxy & Firewall v.6 may be installed over previous v.5 versions. In this case, the Installation Wizard will offer to save or overwrite the server settings file *config.cfg* and the statistics file *og.mdb*. Both files are located in the directory where UserGate is installed (hereafter *%UserGate%).* UserGate server v.6 supports the UserGate v.4,5 settings format. Therefore, the first time you run the server, all settings will be converted into the new format automatically. Settings of earlier versions are incompatible with the new version.

Important note! For the statistics files, the program only supports current user balances transfer. The traffic statistics will not be transferred. The database was changed due to problems with the old version and its size limits. The new Firebird version does not have these drawbacks.

Removal of UserGate server is accomplished through the removal option in the “**Start – Programs**” menu or through "**Add or remove Programs**" (**Programs and Features in Windows 7/2008**) in the Windows Control Panel. After removing UserGate, some files remain in the program's installation directory unless the **Remove All** option was enabled.

UserGate Proxy & Firewall licensing policy

UserGate server is designed to provide Internet access to local area network users. The maximum number of users that may be simultaneously connected to the Internet via UserGate is called number of "sessions" and is defined by the registration key. UserGate v.6 uses a unique registration key that does not support previous UserGate versions. The trial version of the program will work for 30 days and is restricted to 5 sessions. The "session" concept should not be confused with the number of user-launched Internet applications or connections. A user may connect any number of times, unless there is a special limit applied to the user.

UserGate's integrated antivirus modules (from Kaspersky Lab, Panda Security and Avira), as well as the Entensys URL Filtering module, require independent licensing. The integrated modules will work for 30 days in the trial version of UserGate.

The Entensys URL Filtering module, designed for site categorizing, also works for 30 days in the trial version. When you buy UserGate Proxy & Firewall with the filtering module, the Entensys URL Filtering license is valid for one year. After the license period expires, filtering through the module becomes unavailable.

Administration Console

The Administration Console is an application designed to control a local or remote UserGate server. To use the Administration Console, start UserGate server by selecting **Start UserGate server** in the UserGate Agent context menu (● icon in the System Tray, and then **Agent**). You can also start the Administration Console through the Agent's context menu or by using **Start – Programs** if the Administration Console is installed on another computer. To modify your settings, you must connect the Administration Console to the server.

Data exchange between the Administration Console and UserGate server is carried out via SSL protocol. When initializing the connection (SSL Handshake), authentication is carried out by UserGate server transferring its certificate, located in **%UserGate%\ssl** directory, to the Administration Console. No certificate or password is required from the Administration Console's end in order to connect.

Connection settings

The first time the Administration Console launches, it displays the **Connections** page, where only one connection is specified with **localhost** as the server and **Administrator** as the user. There is no connection password. To connect the Administration Console to the server, double-click on the **localhost-administrator** line or press the **Connect** button on the Control Panel. You can create several connections in the UserGate Administration Console. You must specify the following parameters in the connection settings:

- **Server name** – this is the connection name
- **User name** – login to connect to server
- **Server address** – domain name or UserGate server IP address
- **Port** – TCP port used to connect to the server (port 2345 is the default)
- **Password** – the connection password
- **Always ask for password** – this option asks for your login and password whenever you connect to the server
- **Automatically connect to this server** – the Administration Console automatically connects to this server when it starts.

The Administration Console settings are stored in the *console.xml* file, located in the **%UserGate%\Administrator\** directory. On the UserGate server side, the user name and md5 hash connection passwords are stored in the **config.cfg** file, located in the **%UserGate_data** directory where **%UserGate_data%** is the folder for Windows XP (C:\Documents and Settings\All Users\Application Data\Entensys\UserGate6), and for Windows 7/2008 the folder – (C:\Documents and Settings\All Users\Entensys\UserGate6)

Setting a connection password

You can create a login name and password for connecting to UserGate server through the "**Administrator Settings**" section on the "**General Settings**" page. In this section you can also specify a TCP port for connecting to the server. In order for the new settings to take effect, you must restart UserGate server (using the "**Restart UserGate Server**" option in the Agent menu). After restarting the server, you should also specify new settings in the Administration Console connection settings. Otherwise, the Administrator will not be able to connect to the server.

Important note! To avoid problems with UserGate Administration Console operation, it is not recommended to change these settings!

UserGate administrator authentication

In order for the Administration Console to connect to UserGate server successfully, the administrator must go through an authentication procedure on the server side. The administrator authentication is carried out after setting up the Administration Console SSL connection to UserGate server. The Console transmits the login and administrator password md5 hash to the server. UserGate server compares the received data with the data specified in the settings file *config.cfg*. Authentication is successful if the data received from the Administration Console is the same as the data specified in the server settings. If the authentication fails, UserGate server breaks the SSL connection with the Administration Console. The result of the authentication procedure is registered in the **usergate.log** file, located in the **%UserGate_data%\logging\** directory.

Setting a UserGate statistics database password

A user's statistics, such as traffic, resources visited and etc. is logged by UserGate server in a special database. The database may be accessed directly (for the integrated Firebird database) or through ODBC driver, which allows for the use of different database formats (MSAccess, MSSQL and MySQL). The Firebird database - **%UserGate_data%\usergate.fdb** is used by default. The login and password to access the database is SYSDBA\masterkey. You can set a different password through the **General settings** → **Database settings** option in the Administration Console.

NAT (Network Address Translation) common settings

The **NAT Common Settings** option allows you to specify the timeout value for NAT connections through TCP, UDP, or ICMP protocols. The timeout value defines a user’s connection time through NAT after data transfer over the connection is finished. The **Print Debug Log** option is used for debugging and allows you to turn on the extended logging mode of the UserGate NAT driver if needed.

Attack detector is a special feature allowing you to activate an internal mechanism that tracks and blocks a port scanner or attempts to occupy all of the server ports. This module works in automatic mode and the events are logged in the **%UserGate_data%\logging\fw.log** file.

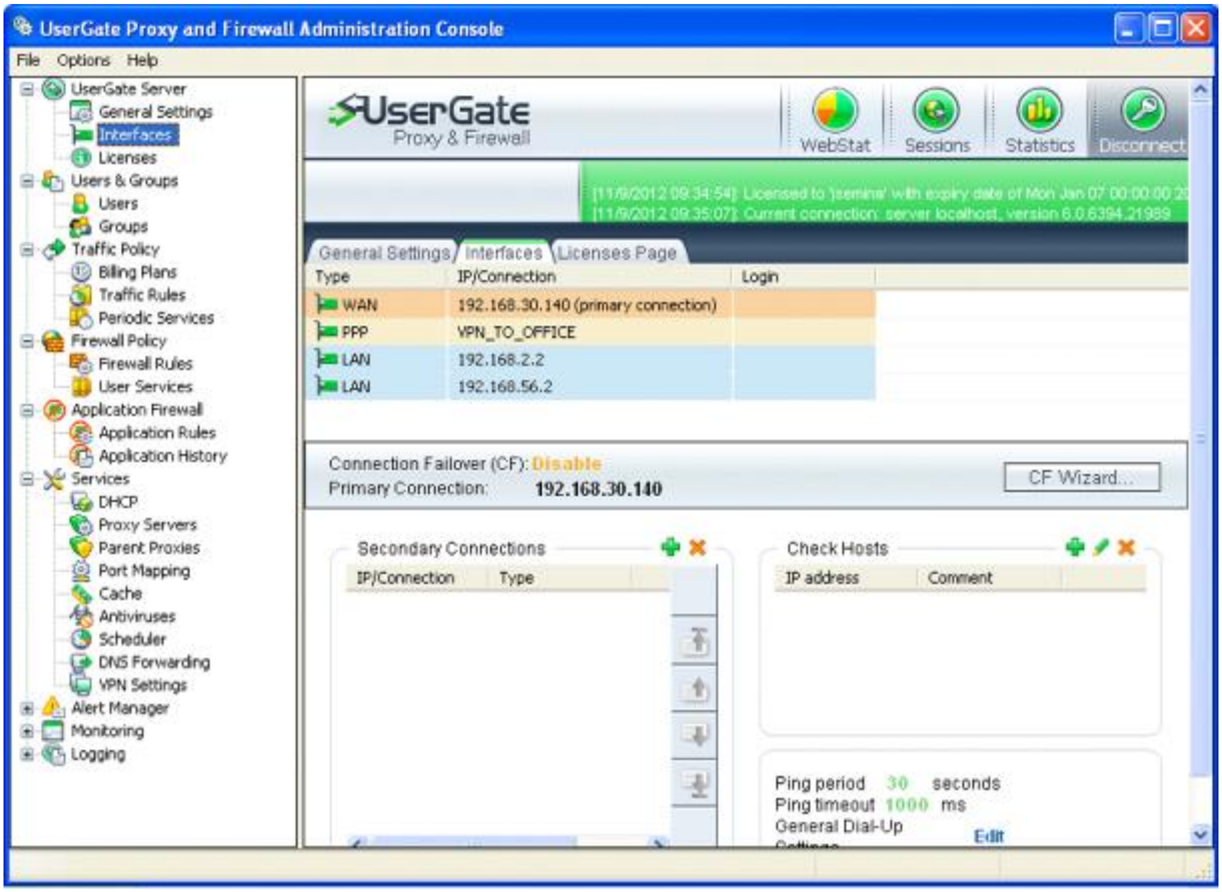
Important note! This module's settings can be changed through the **Options** section of the **config.cfg** configuration file.

General settings

Block by browser line is a list of the User-Agent’s browsers that may be blocked by the proxy server. For example, you can block old browsers, such as IE 6.0 or Firefox 3.x, from accessing the Internet.

Interface Settings

The **Interfaces** page (Fig. 1) is the most important of the UserGate server settings because it defines such important features as traffic count accuracy, Firewall rules creation, Internet channel bandwidth restrictions for specific types of traffic, relationships among networks, and the order of request processing by the UserGate NAT (Network Address Translation) drive.



[11/9/2012 09:34:54]: Licensed to 'semina' with expiry date of Mon Jan 07 00:00:00 2
[11/9/2012 09:35:07]: Current connection: server localhost, version 6.0.6394.21989

Type	IP/Connection	Login
WAN	192.168.30.140 (primary connection)	
PPP	VPN_TO_OFFICE	
LAN	192.168.2.2	
LAN	192.168.56.2	

Connection Failover (CF): Disable
Primary Connection: 192.168.30.140

IP/Connection	Type

IP address	Comment

Ping period 30 seconds
Ping timeout 1000 ms
General Dial-Up Settings

Figure 1. Server interface settings

The "**Interfaces**" page lists all of the available network interfaces on the server where UserGate is installed, including Dial-Up (VPN and PPPoE) connections. The UserGate administrator must define the connection type for each network adapter. Thus, for an adapter connected to the Internet, you should select the WAN type, while for an adapter connected to a local area network, the LAN type should be selected. Dial-Up (VPN, PPPoE) type connections cannot be changed. For these connections, UserGate server automatically sets **PPP interface** as the type. For Dial-Up and VPN connections, you can enter a user name and password by double-clicking on the corresponding interface. The interface located at the top of the list is used as the default Internet connection.

Traffic calculation in UserGate

Traffic passing through UserGate server is assigned either to the user from the local area network that initiates the connection, or to UserGate server itself if it initiates the connection. For UserGate server traffic there is a special predefined user, *UserGate Server*, specified in the statistics database. *UserGate Server* traffic includes Kaspersky Lab, Avira and Panda Security, as well as DNS name resolution through DNS forwarding. All traffic is accounted for, along with control headers.

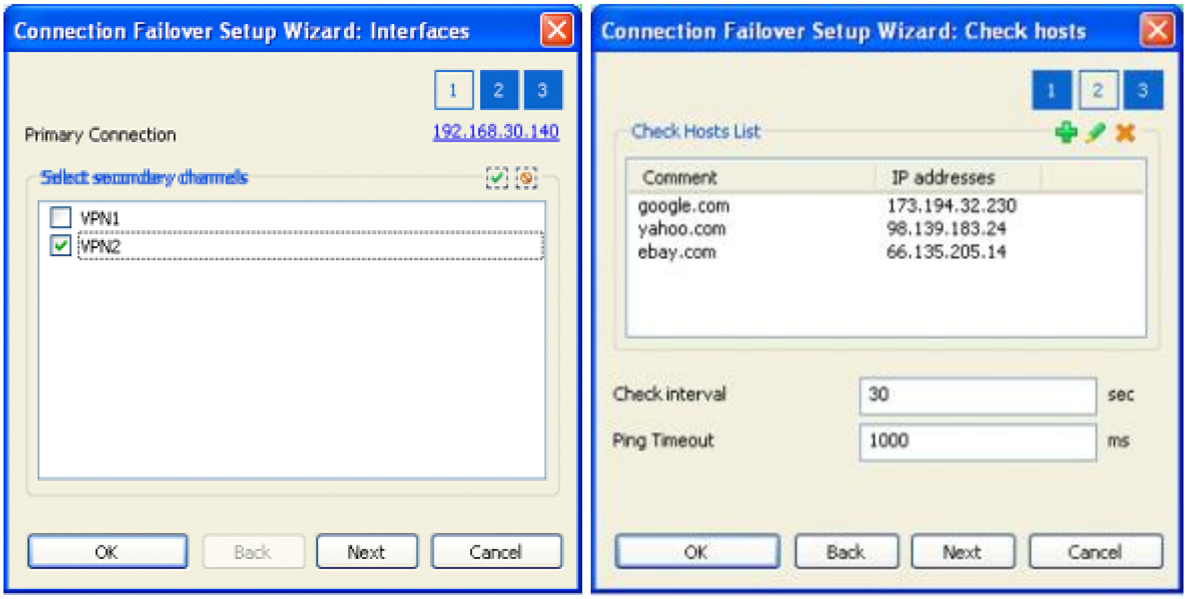
There is also an added feature that accounts for Ethernet headers.

When all server network adapters types (LAN or WAN) are specified correctly, traffic in the direction of “local network – UserGate server” (for example, accessing shared network resources on the server) is not taken into account.

Important note! Using third party Firewall or antivirus products for the purpose of traffic checking may seriously affect the accuracy of UserGate traffic calculation. It is not recommended to set up and use any third party network software on a computer where UserGate server is installed!

Connection Failover

Connection Failover Setup is available on the “Interfaces” page. By clicking on the **Setup Wizard**, you can select the interface that will be used as a reserve channel. The second page provides a selection of hosts to be checked by the proxy server for Internet connection availability. The program will check these hosts' availability at the specified frequency by sending ICMP **Echo-requests** to the specified channels. If at least one of the specified hosts responds, the connection is interpreted as active. A lack of response from all specified hosts will be interpreted as primary Internet connection failure and the system's main gateway server will be switched to the reserve channel gateway. If NAT rules were created with special **Masquerade** interface specified as the external interface, these rules will be recreated according to the current routing table. The created NAT rules will begin working through the reserve channel.



Connection Failover Setup Wizard: Interfaces

Primary Connection 192.168.30.140

Select secondary channels

□ VPN1
☑ VPN2

Connection Failover Setup Wizard: Check hosts

Check Hosts List

Comment	IP addresses
google.com	173.194.32.230
yahoo.com	98.139.183.24
ebay.com	66.135.205.14

Check interval 30 sec

Ping Timeout 1000 ms

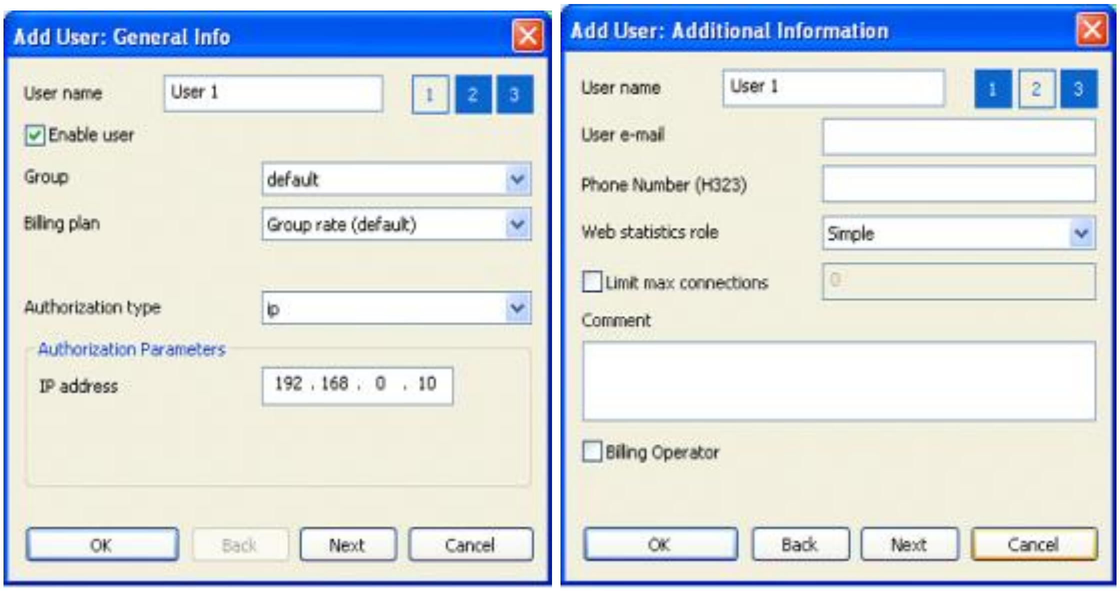
Figure 2. Connection Failover Setup Wizard

As a reserve connection, UserGate server can use either an Ethernet connection (dedicated channel, WAN interface) or a Dial-Up connection (VPN or PPPoE connection, PPP interface). After switching to the reserve Internet connection, UserGate server regularly checks the primary channel's availability. If the primary Internet connection becomes available, the program switches users back to it.

Users and Groups

To provide Internet access, it is necessary to create users' accounts in UserGate. To simplify administration, users can be grouped by location or by access level. The most logical way to combine users into groups is by access level since it makes traffic management much easier. Initially, there is only one group available in UserGate: the *default group*.

To create a new user, choose the "**Add new user**" option or press the "**Add**" button on the Control Panel on the "**Users and Groups**" page. Another way to add users is by scanning the network with ARP requests. Click on an empty space in the Administration Console on the **Users** page and choose the **Scan local area network** option. Next, enter the local area network details and wait for the scan results. You will then see a list of users who can be added to UserGate. As shown in Fig. 3, the required fields for the user are: Name, Authorization type, Authorization parameters (IP address, login and password, etc.), Group and Billing plan. By default, all users belong to the *default* group. Each UserGate user must have a unique name. You can also specify the user's access level to the web statistics, define an internal H323 phone number, restrict the number of connections for the user, and enable NAT rules, traffic-management rules and/or Application Firewall module rules.



Add User: General Info

User name: User 1

☑ Enable user

Group: default

Billing plan: Group rate (default)

Authorization type: ip

Authorization Parameters

IP address: 192 . 168 . 0 . 10

Add User: Additional Information

User name: User 1

User e-mail:

Phone Number (H323):

Web statistics role: Simple

□ Limit max connections 0

Comment

□ Billing Operator

Figure 3. UserGate user profile

Each UserGate user inherits all the settings of the group to which he belongs, besides the billing plan, which can be redefined. The billing plan specified in each user's profile is used for tariffing all of the user's connections. If the Internet connection is not subject to a tariff, you may use a blank tariff called "default."

Synchronization with Active Directory

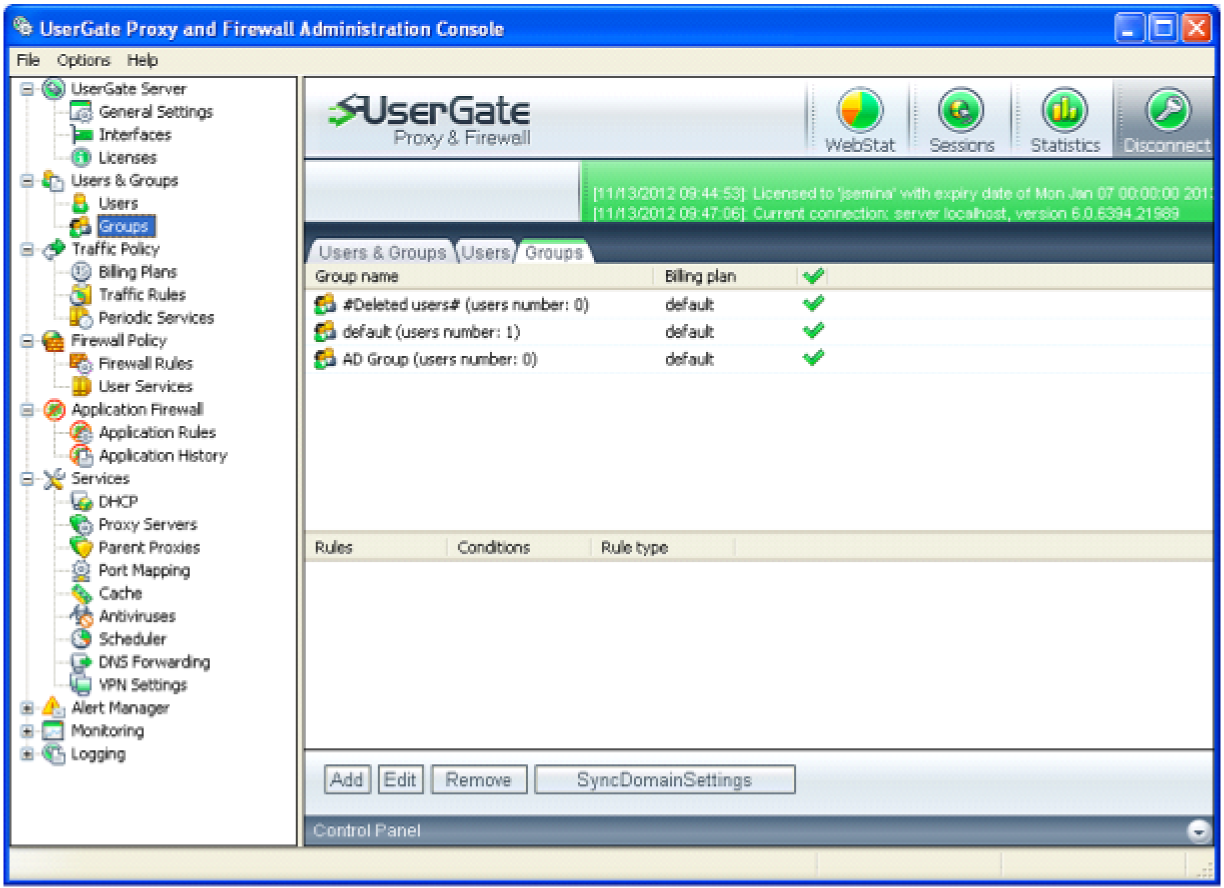
UserGate user groups can be synchronized with Active Directory groups. To use synchronization with Active Directory, the computer with UserGate Proxy & Firewall does not necessarily have to be in the domain.

The synchronization setup is a two-step process. The first step is to go to the UserGate Administration Console's Group page, as shown in Fig. 4, select the "**Synchronization with AD**" option and set the following parameters:

- domain name
- domain controller IP-address
- Active Directory user name and password (the user name can be entered in UPN (User Principal Name) format)
- polling interval (in seconds)

The second step is to open the UserGate user group properties (after waiting for the polling interval), choose the "**Enable Synchronization with AD**" option and choose one or several groups from Active Directory.

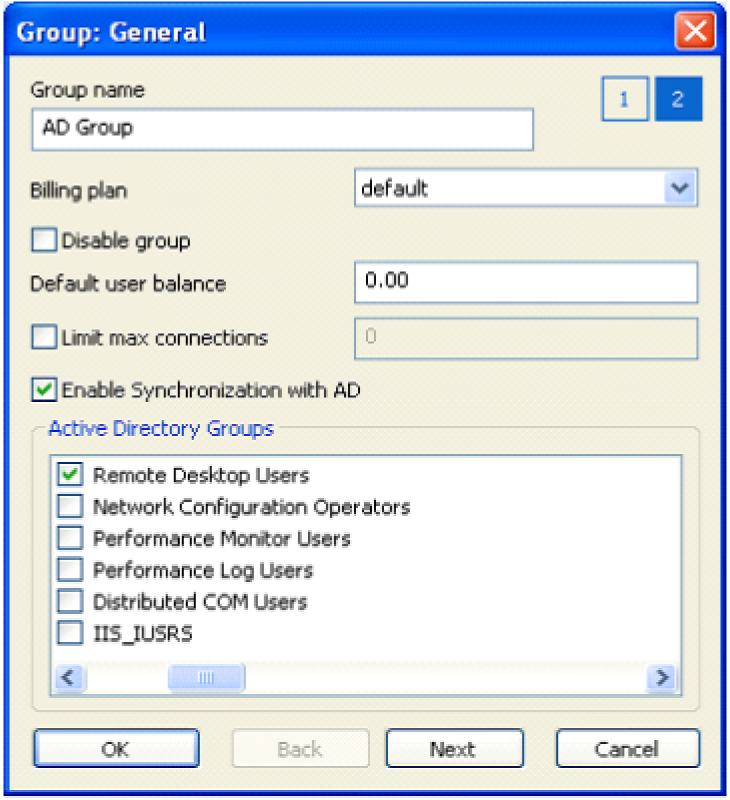
During the synchronization, users from the selected Active Directory groups will be automatically added to the corresponding UserGate groups. Authorization type for the imported users will be set to “HTTP (NTLM) authorization.” The imported user's status (on/off) is controlled by the status of the corresponding account in the Active Directory domain.



[11/13/2012 09:44:53]: Licensed to 'jsemina' with expiry date of Mon Jan 07 00:00:00 201
[11/13/2012 09:47:06]: Current connection: server localhost, version 6.0.6394.21989

Group name	Billing plan	✓
#Deleted users# (users number: 0)	default	✓
default (users number: 1)	default	✓
AD Group (users number: 0)	default	✓

Rules	Conditions	Rule type



Group name: AD Group

Billing plan: default

□ Disable group

Default user balance: 0.00

□ Limit max connections: 0

☑ Enable Synchronization with AD

Active Directory Groups

☑ Remote Desktop Users
□ Network Configuration Operators
□ Performance Monitor Users
□ Performance Log Users
□ Distributed COM Users
□ IIS_IUSRS

Figure 4. Active Directory synchronization settings

Important note! To carry out the synchronization, LDAP protocol must be able to pass between UserGate server and the domain controller.

User personal statistics page

Every UserGate user can view his statistics page. Access to the personal statistics page can be obtained at the following address: http://192.168.0.1:8080/statistics.html where, for example, 192.168.0.1 is the local address of UserGate server and 8080 is the port on which the UserGate HTTP proxy server is running. The user can view his personal advanced statistics by logging in through http://192.168.0.1:8081.

Important note! It is not recommended to change the standard port for web-statistics from 8081 to any other.

Important note! The 6.x version has an added 127.0.0.1:8080 listening interface, which is necessary for the web-statistics to function when the UserGate HTTP proxy server is disconnected. Because of this, port 8080 on interface 127.0.0.1 will always be working on UserGate Proxy & Firewall as long as **usergate.exe** is running.

User Authorization Methods

Internet access is provided only for users who successfully pass authorization on UserGate server. The program supports the following user authorization methods:

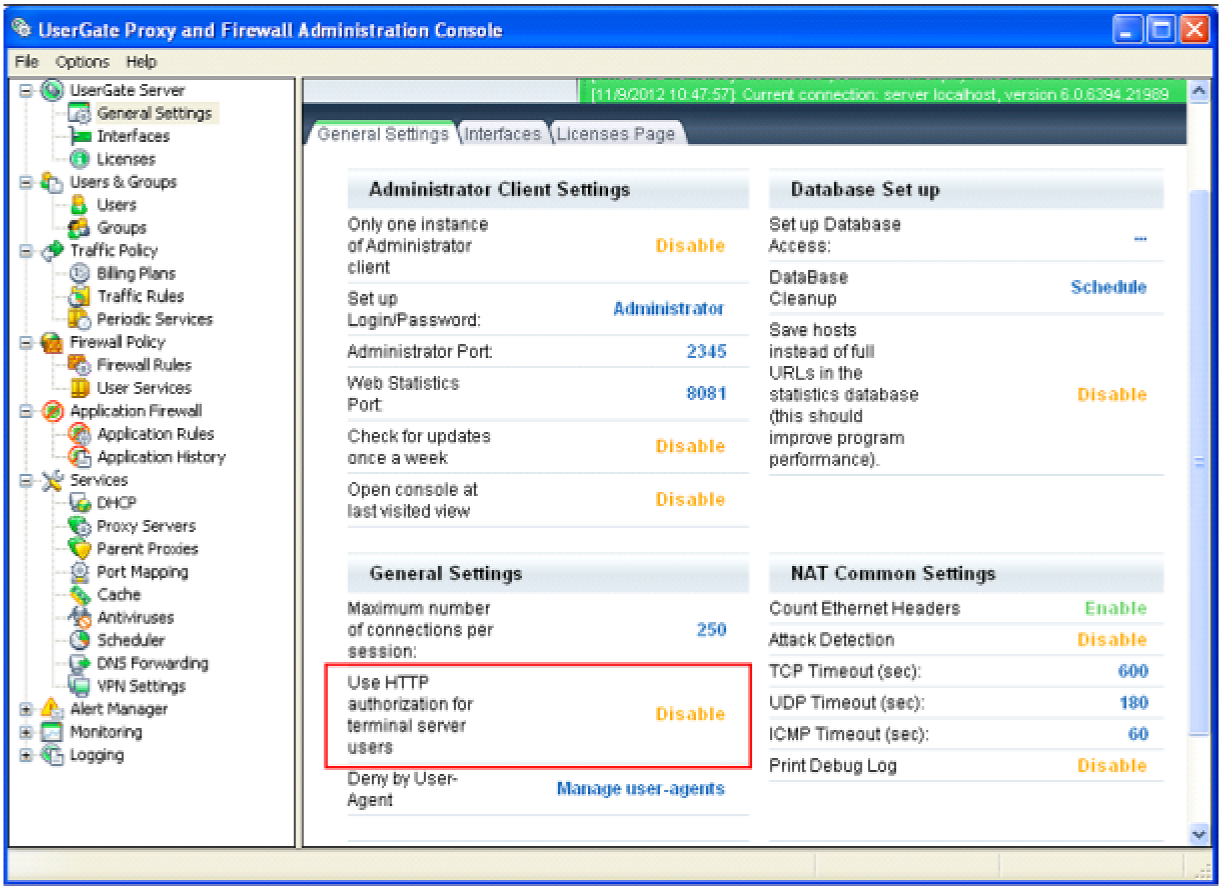
- by IP address
- by IP address range
- by a combination of IP and MAC addresses
- by MAC address
- by means of HTTP (HTTP-basic, NTLM)
- authorization through user name and password (Authorization Client)
- simplified version of Active Directory authorization

For the last three authorization methods, you must install a special application on the user's workstation - the UserGate Authorization Client. The corresponding MSI package (**AuthClientInstall.msi**) can be found in the "**%userGate%\tools**" directory and can be installed automatically through Active Directory group policy tools. The "**%userGate%\tools**" directory also contains the administrative template to install Authorization Client through Active Directory group policy tools.

If UserGate server is installed on a computer not included in an Active Directory domain, it is recommended to use the simplified version of Active Directory authorization. In this case, UserGate server will compare the login and domain name received from the Authorization Client with the corresponding fields specified in the user profile without requesting the domain controller.

Terminal user support

Along with classic (basic) HTTP authorization, UserGate server also supports HTTP authorization for terminal users. You can enable this option on the "**General Settings**" page in the Administration Console (Fig. 5). This authorization method allows terminal users to connect to the Internet using their individual UserGate accounts by means of authorization data (user name and password) for each new connection.



[11/9/2012 10:47:57]: Current connection: server localhost, version 6.0.6394.21989

Administrator Client Settings

Only one instance of Administrator client	Disable
Set up Login/Password:	Administrator
Administrator Port:	2345
Web Statistics Port:	8081
Check for updates once a week	Disable
Open console at last visited view	Disable

Database Set up

Set up Database Access:	...
DataBase Cleanup	Schedule
Save hosts instead of full URLs in the statistics database (this should improve program performance).	Disable

General Settings

Maximum number of connections per session:	250
Use HTTP authorization for terminal server users	Disable
Deny by User-Agent	Manage user-agents

NAT Common Settings

Count Ethernet Headers	Enable
Attack Detection	Disable
TCP Timeout (sec):	600
UDP Timeout (sec):	180
ICMP Timeout (sec):	60
Print Debug Log	Disable

Figure 5. Terminal user support

The “**HTTP authorization for terminal server users**” mode is useful if you need to ensure that several network applications are running from a single computer under different UserGate accounts. In this case, enter the address and port of the appropriate UserGate proxy (HTTP, Socks 5) and authorization parameters (user name and password) for each network application.

Using HTTP authorization with transparent proxy

UserGate v.6 has the added feature of HTTP authorization for a proxy server working in transparent mode. If the workstation's browser is not set to use a proxy server and the UserGate HTTP proxy transparent mode is enabled, all requests from unauthorized users will be forwarded to an authorization page where you have to specify your user name and password.

After authorization, you do not have to close this page. The authorization page refreshes regularly by means of a special script to keep the user’s session active. This mode makes all UserGate services, including NAT, available for an authorized user. To end the session, press the **Logout** button on the Authorization page or simply close the tab with the authorization; 30-60 seconds later, authorization on the proxy server will disappear.

Important note! This authorization method does not work for terminal server users.

NTLM authorization

UserGate Proxy & Firewall HTTP-proxy supports NTLM authorization. To use this authorization method, you must set the Active Directory synchronization parameters and complete the following:

- allow NetBIOSNameRequest (UDP:137) packages to pass between UserGate server and the domain controller
- provide for NetBIOSSessionRequest (TCP:139) packages to pass between UserGate server and the domain controller
- register the UserGate HTTP proxy address and port in the user's workstation browser

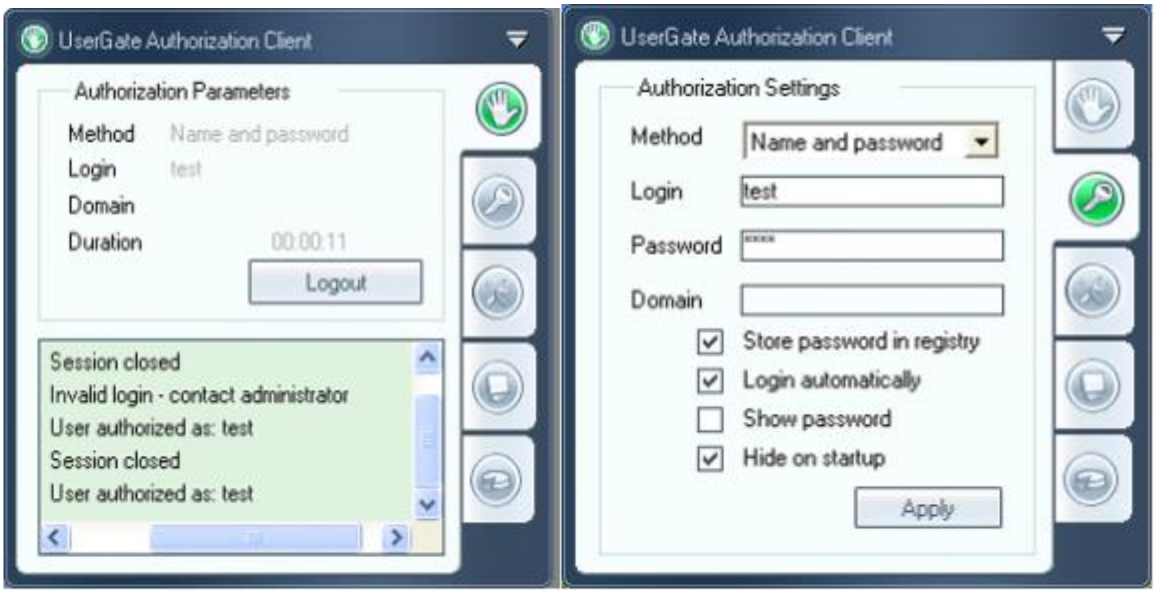
Important note! To use NTLM authorization, the workstation where UserGate is installed does not have to be in the Active Directory domain.

Using Authorization Client

The UserGate Authorization Client is a network application that works at the Winsock level, which connects to UserGate server using a predefined UDP port (port 5456 is used by default) and sends user authorization parameters: the authorization type, user name, password, and etc.

In the Authorization Client settings, you should specify the UserGate server IP address and port, and the authorization method and parameters (user name/password) as specified in the user's UserGate profile.

The first time it is launched, the UserGate Authorization Client monitors the **HKCU\Software\Policies\Entensys\Authclient** registry key to find settings obtained through the Active Directory group policy. If these settings are not found in the system registry, you have to specify the UserGate server address manually in the third tab from the top in the Authorization Client. After the server address is defined, press the “**Apply**” button and go to the second tab. On this page, enter the user's authorization parameters. The specified Authorization Client settings are stored in the **HKCU\Software\Entensys\Authclient** registry key. The Authorization Client log is saved in the **Documents and Settings\%USER%\Application data\UserGate Client** folder.



Method Name and password
Login test
Domain
Duration 00:00:11

Session closed
Invalid login - contact administrator
User authorized as: test
Session closed
User authorized as: test

Method Name and password
Login test
Password ****
Domain

☑ Store password in registry
☑ Login automatically
□ Show password
☑ Hide on startup

Figure 6. Authorization Client settings

UserGate Authorization Client shows statistics on bytes sent/received, time spent online, and its cost. Additionally, there is a link available in the Authorization Client to the user's personal statistics page. You can change the Authorization Client's skin by editing the appropriate template, in the form of an ***.xml** file, located in the client's parent folder.

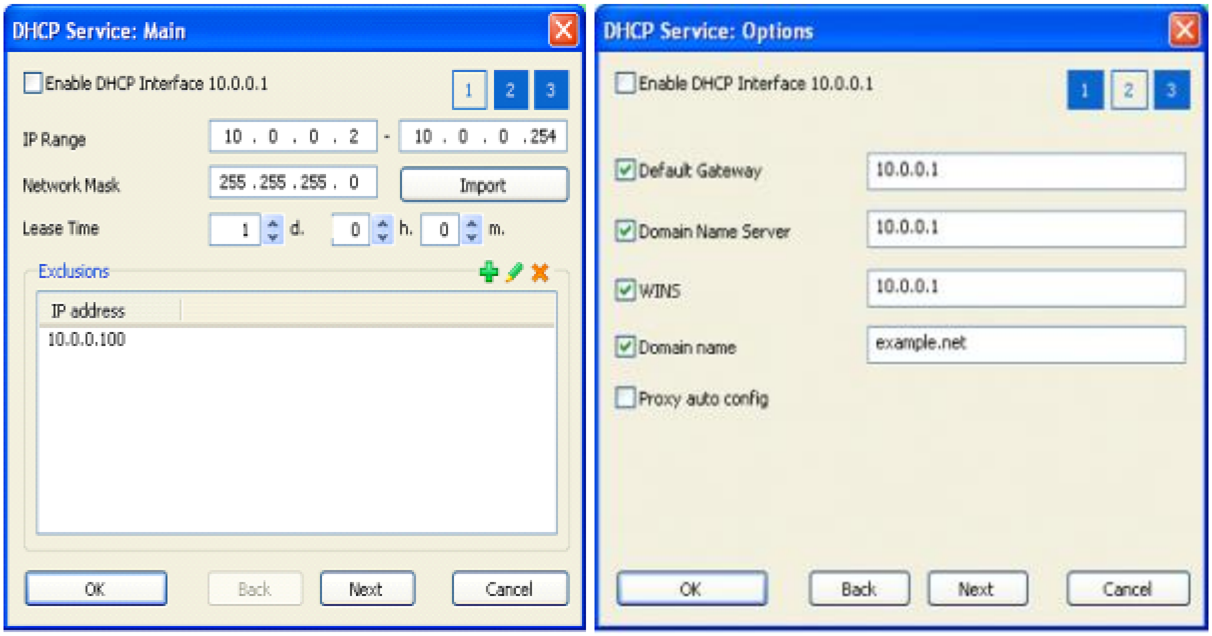
Important note! The Authorization Client is not supported for terminal server users.

UserGate Services settings

DHCP settings

DHCP (Dynamic Host Configuration Protocol) service automates the process of configuring network settings for local area network clients. With DHCP server, you can dynamically assign the IP address, gateway address, DNS, WINS-server and etc. for all network devices.

To enable the UserGate DHCP server, select the "**Services** → **DHCP Server** → **Add interface**" option in the UserGate Administration Console or press the "**Add**" button in the Control Panel. In the displayed dialog box, select the network interface where DHCP server will run. For the minimum DHCP server configuration, it is sufficient to set the following parameters: IP address range (address pool)—the range of addresses available to local area network clients from the server, the network mask, and the lease time. The maximum pool size in UserGate is 4000 addresses. If necessary, you can exclude one or several IP addresses from the chosen address pool by using the "**Exclusion**" button. You can also attach a permanent IP address to a particular network device by creating a corresponding reservation in the **Reservations** page. An IP address stays permanent when a lease is extended or obtained by making a **Reservation** for the network device's MAC address. To create a reservation, enter the IP address of the device only; the MAC address will be defined automatically when you press the corresponding button.



DHCP Service: Main

□ Enable DHCP Interface 10.0.0.1

IP Range 10 . 0 . 0 . 2 - 10 . 0 . 0 . 254

Network Mask 255 . 255 . 255 . 0

Lease Time 1 d. 0 h. 0 m.

Exclusions

IP address
10.0.0.100

DHCP Service: Options

□ Enable DHCP Interface 10.0.0.1

☑ Default Gateway 10.0.0.1

☑ Domain Name Server 10.0.0.1

☑ WINS 10.0.0.1

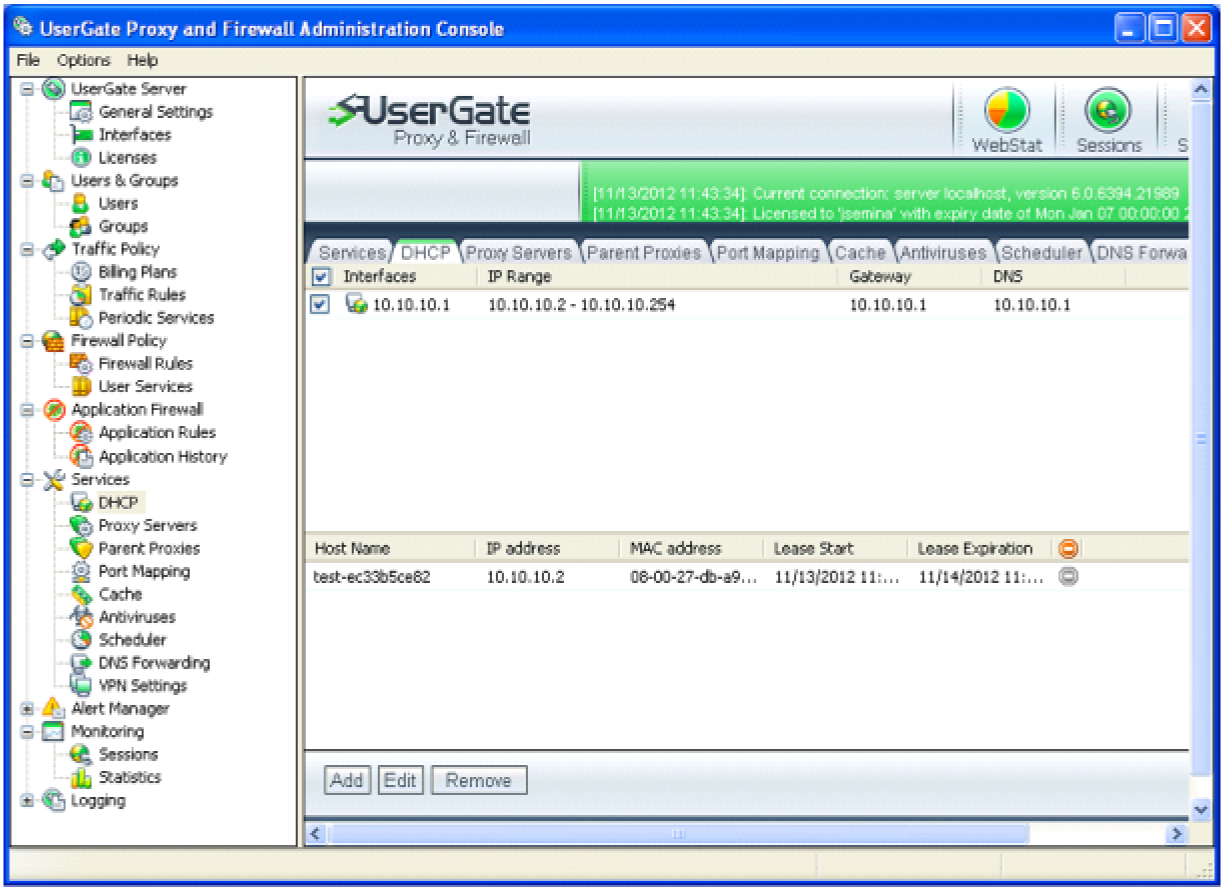
☑ Domain name example.net

□ Proxy auto config

Figure 7. UserGate DHCP server settings

UserGate DHCP server supports the import of Windows DHCP server settings. In order to use this feature, you must first save the Windows DHCP settings to a file. To do so, launch the command prompt (**Start → Run** , enter “**cmd**” and press **<Enter>**) on the server where Windows DHCP is installed, and type the following command in the window that appears: **netsh dhcp server IP dump>file_name**, where **IP** is your DHCP server’s IP address. The import of settings from the file is performed through the corresponding button on the first page of the DHCP server setup wizard.

The delivered IP addresses are shown in the lower part of the Administration Console page (Fig. 8) along with the client information (workstation name, MAC address) and lease start and end time values. By selecting a previously delivered IP address, you can add a user to UserGate, create MAC address reservations, or remove the given IP address.



```
[11/13/2012 11:43:34]: Current connection: server localhost, version 6.0.6394.21989
[11/13/2012 11:43:34]: Licensed to 'jsemina' with expiry date of Mon Jan 07 00:00:00 2
```

☑ Interfaces	IP Range	Gateway	DNS
☑ 10.10.10.1	10.10.10.2 - 10.10.10.254	10.10.10.1	10.10.10.1

Host Name	IP address	MAC address	Lease Start	Lease Expiration	⊖
test-ec33b5ce82	10.10.10.2	08-00-27-db-a9...	11/13/2012 11:...	11/14/2012 11:...	⊖

Figure 8. Removing issued addresses

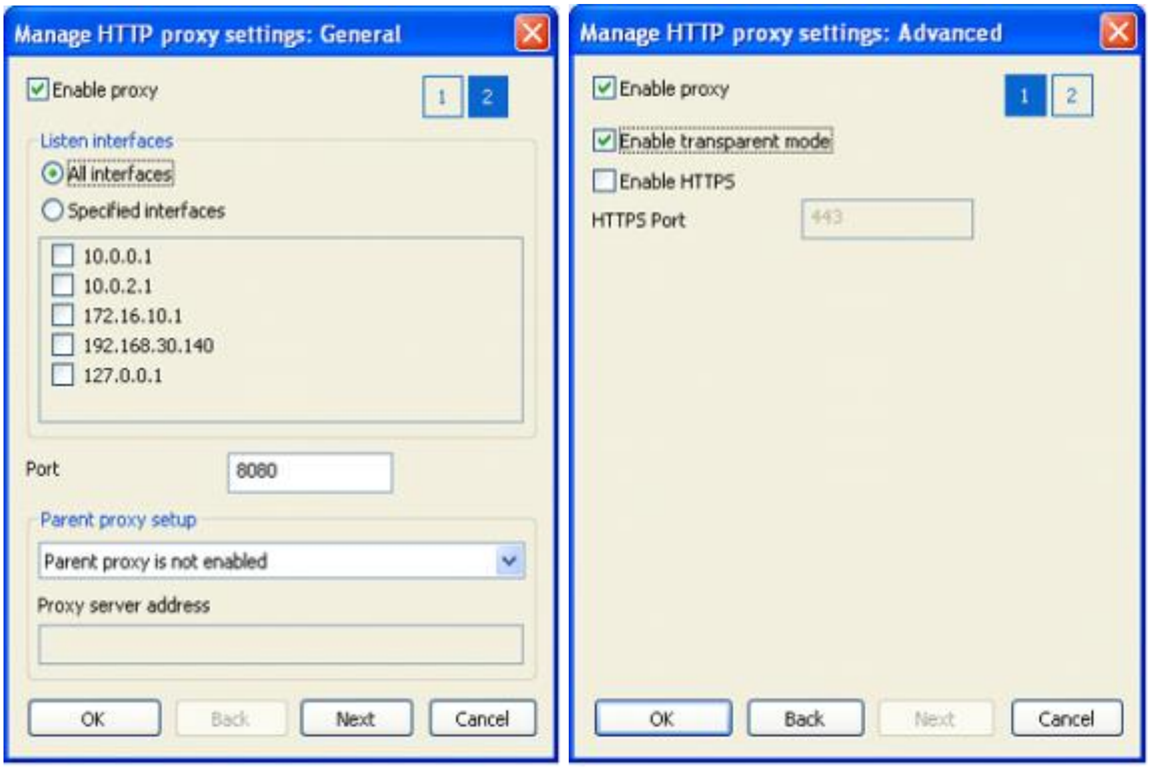
The removed IP address will be placed into the pool of free DHCP server addresses after a certain period of time. The option of removing an IP address becomes useful if a workstation that received an address from UserGate DHCP server is later taken offline, or if its MAC address was changed.

DHCP server can answer client requests when requesting the "**wpad.dat**" file. This method of receiving proxy server settings is carried out by sending a template file, available in the **C:\program files\entensys\usergate6\wwwroot\wpad.dat** folder.

For more information on this method of receiving proxy server settings, see the Wikipedia article.

UserGate Proxy service settings

The following proxy servers are integrated in UserGate server: HTTP (supports "FTP over HTTP" and HTTPS modes - the Connect method), FTP, SOCKS4, SOCKS5, POP3 and SMTP, SIP and H323. Proxy server settings are located in the "**Services → Proxy settings**" page in the Administration Console. The main settings are the interface (Fig. 9) and the port number where the proxy is running.



Manage HTTP proxy settings: General

☑ Enable proxy

Listen interfaces

● All interfaces
○ Specified interfaces

□ 10.0.0.1
□ 10.0.2.1
□ 172.16.10.1
□ 192.168.30.140
□ 127.0.0.1

Port 8080

Parent proxy setup

Parent proxy is not enabled

Proxy server address

Manage HTTP proxy settings: Advanced

☑ Enable proxy
☑ Enable transparent mode
□ Enable HTTPS

HTTPS Port 443

Figure 9. Proxy server primary settings

By default, only HTTP proxy is enabled in UserGate, which listens to the 8080 TCP port on all of the server's available network interfaces.

To assign the client browser to work through the proxy server, simply specify the proxy address and port in the corresponding settings field. In Internet Explorer, proxy settings are set in the "**Tools – Internet options – Connection – LAN settings**" menu. When working though HTTP proxy, you do not need to specify the gateway and DNS in the TCP/IP settings of the user workstation's network connection because the HTTP proxy is responsible for name resolution.

Each proxy server has access to the mode of cascading inclusion into an upstream proxy-server.

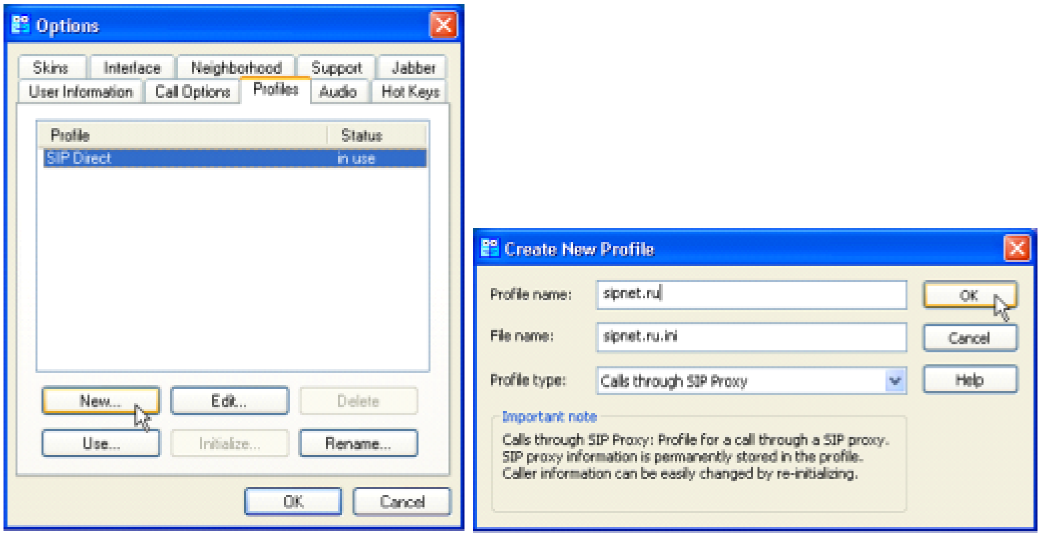
Important note! The port specified in the proxy server settings is opened automatically in the UserGate Firewall. Therefore, to ensure higher security, it is recommended to specify only local network server interfaces in the proxy settings.

IP telephony (SIP, H323) protocol support

UserGate can function as an SIP proxy that controls SIP Registrar connection status (stateful proxy). The SIP proxy can be enabled in the **Services → Proxy Settings** page and always works in transparent mode, listening to ports 5060 TCP and 5060 UDP. When using SIP proxy, information about the current connection state (registration, calling, waiting, etc.), as well as information about the user's name (number), call duration and amount of bytes sent/received is shown on the **Sessions** page in the Administration Console. This information is also saved in the UserGate statistics database.

In order use UserGate SIP proxy, you should specify the UserGate server IP as the default gateway in the TCP/IP settings on the user's workstation. Also, you must specify a DNS server address.

Let us illustrate the client side settings using the example of the SJPhone software phone and Sipnet provider. Start the SJPhone, choose **Options** in the context menu, and create a new profile. Enter the profile name (Fig. 10), for example **sipnet.ru**, and specify **Call through SIP Proxy** as the profile type.



Profile	Status
SIP Direct	in use

Profile name: sipnet.ru

File name: sipnet.ru.ini

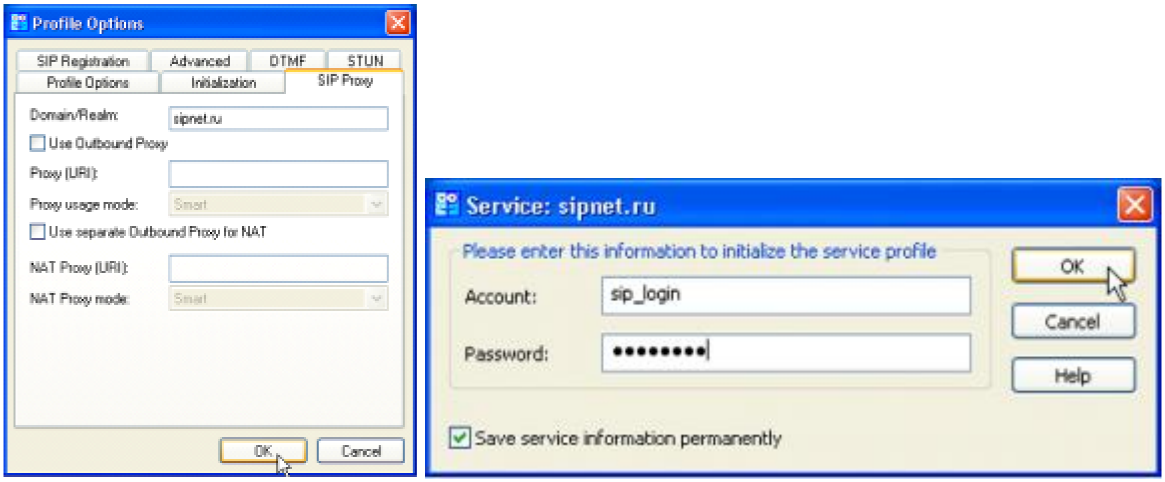
Profile type: Calls through SIP Proxy

Important note

Calls through SIP Proxy: Profile for a call through a SIP proxy.
SIP proxy information is permanently stored in the profile.
Caller information can be easily changed by re-initializing.

Figure 10. Creating a new profile in SJPhone

In the **Profile Options** dialog box, specify your VoIP provider proxy server address. When closing the dialog box, enter the server authorization data (user name and password) for the VoIP provider.



Domain/Realm: sipnet.ru

□ Use Outbound Proxy

Proxy (URI):

Proxy usage mode: Smart

□ Use separate Outbound Proxy for NAT

NAT Proxy (URI):

NAT Proxy mode: Smart

Please enter this information to initialize the service profile

Account: sip_login

Password: •••••••••

☑ Save service information permanently

Figure 11. SJPhone profile settings

Important note! If your voice traffic does not pass in either direction when enabling SIP proxy, you must either use STUN proxy server or let the traffic pass through NAT on all ports (ANY:FULL) for the required users. When enabling NAT rules on all ports, you have to disable SIP proxy server!

SIP Registrar mode support

The SIP registrar function lets you use UserGate as ATS (Automatic Telephone Station) software for a local area network. The SIP Registrar function works simultaneously with the SIP proxy function. In order to authenticate with the UserGate SIP Registrar, you should specify the following in SIP UAC (User Agent Client) settings:

- UserGate address as SIP server address
- UserGate user name (without spaces)
- Any password

H323 protocol support

H323 protocol support enables you to use UserGate server as a H323 Gatekeeper. In the H323 proxy settings, you need to specify the interface on which UserGate will be listening for client queries, port number, and an H323 gateway address and port. For authorization on UserGate Gatekeeper, the user should specify his user name (user name in UserGate), password (any password), and the phone number specified in the user's UserGate profile.

Important note! If UserGate GateKeeper receives a call to a H323 number that does not belong to any authorized UserGate user, the call will be forwarded to an H323 Gateway. Calls to an H323 Gateway are made in **CallModel: Direct** mode.

UserGate mail proxies

UserGate mail proxies are designed to support both POP3 and SMTP protocols, as well as to scan mail traffic for viruses. When UserGate POP3 and SMTP proxies are used in transparent mode, the mail client settings on a user's workstation are the same as if it were connected directly to the Internet.

If UserGate POP3 proxy is used in non-transparent mode, then in the mail client settings of the user's workstation you should specify the computer's UserGate IP address and the port that corresponds to the UserGate POP3 proxy. In addition, you need to specify a login for the remote POP3 server authorization in the following format: e-mail_address@PoP3_server_address. For example, if the user's e-mail is user@mail123.com, you should enter **user@mail123.com@pop.mail123.com** as the login for the UserGate POP3 proxy in the mail client. This format is necessary in order for UserGate server to detect the remote POP server address.

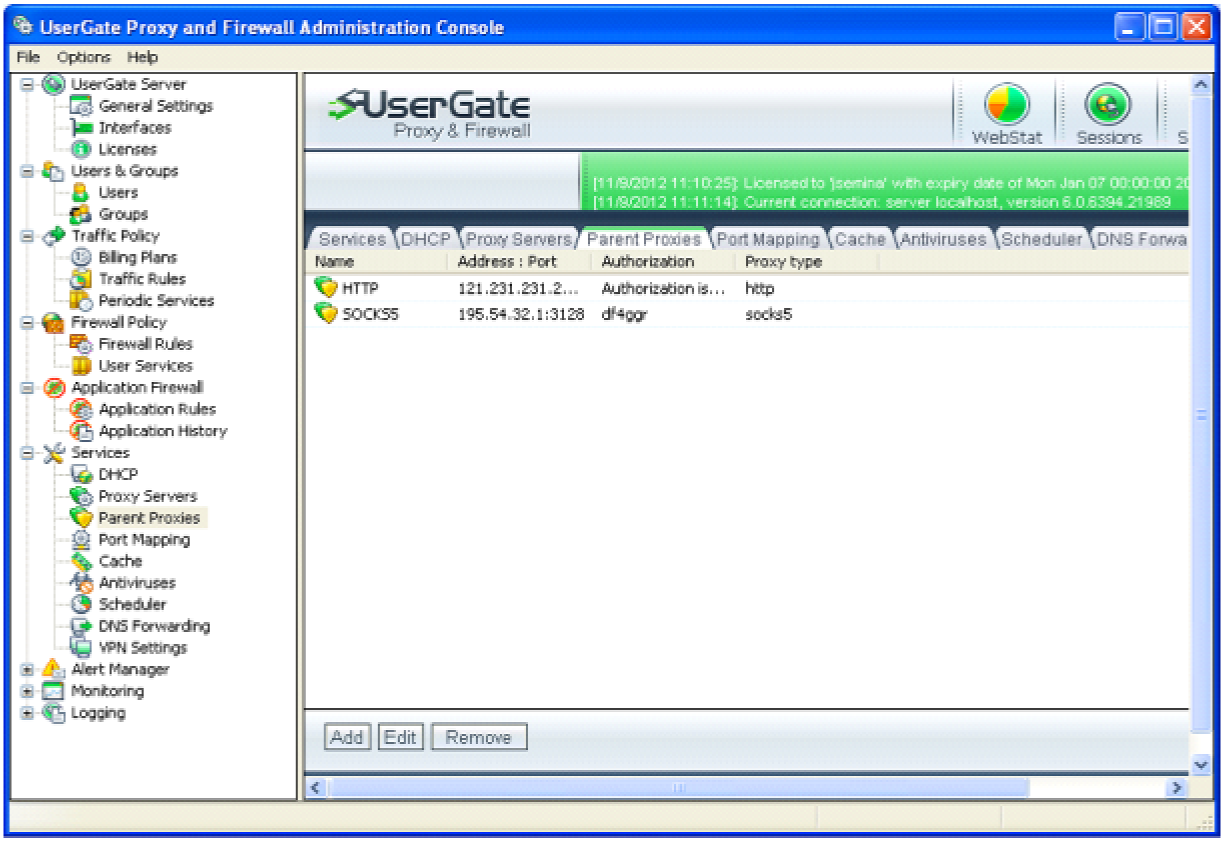
If UserGate SMTP proxy is used in non-transparent mode, then in the proxy settings section you need to specify the SMTP server IP address and port that UserGate will use to send mail. In this case, in the mail client settings of the user's workstation you need to enter the UserGate server IP address and port that correspond to the UserGate SMTP proxy as the SMTP server address. If authorization is needed for sending mail, then in the UserGate SMTP proxy settings you need to enter the username and password that correspond to the SMTP server shown in the UserGate SMTP proxy settings.

Transparent mode

The **Transparent mode** option in the proxy server settings is available if UserGate server is installed along with a NAT driver. In transparent mode, the UserGate NAT driver listens to the standard service ports: 80 TCP for HTTP, 21 TCP for FTP, 110 and 25 TCP for POP3 and SMTP on network interfaces of a workstation with UserGate. When users' requests come in, it sends them to the corresponding proxy server in UserGate. When using transparent mode, it is not necessary to specify the proxy server address and port in each network application, which considerably reduces the administrator's workload for providing LAN-to-Internet access. However, you need to specify UserGate server as the gateway and specify a DNS server address in each workstation's network settings.

Parent proxies

UserGate server can work either with a direct Internet connection or through upstream proxy servers. These proxies are grouped in UserGate on the **Services → Parent Proxies** page. UserGate supports the following parent proxy types: HTTP, HTTPS, Socks4, and Socks5. For each parent proxy, you should specify the standard parameters in the settings: address and port. If the upstream proxy supports authorization, you may specify the corresponding user name and password in the settings. All created parent proxies become available in the UserGate proxy server settings.



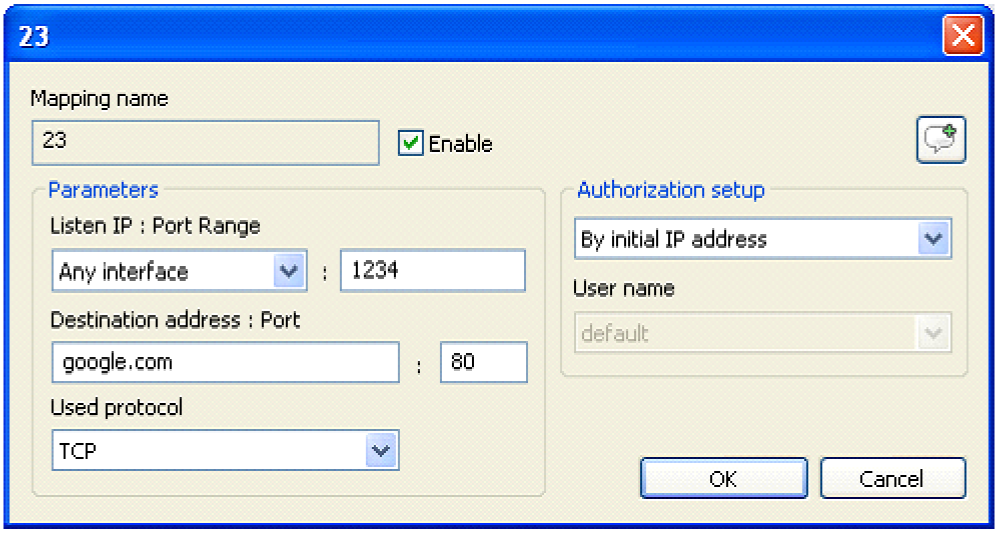
```
[11/9/2012 11:10:25]: Licensed to 'jsemina' with expiry date of Mon Jan 07 00:00:00 20
[11/9/2012 11:11:14]: Current connection: server localhost, version 6.0.6394.21989
```

Name	Address : Port	Authorization	Proxy type
HTTP	121.231.231.2...	Authorization is...	http
SOCKS5	195.54.32.1:3128	df4ggr	socks5

Figure 12. Parent proxy in UserGate

Port mapping

UserGate supports the **Port mapping** function. Port mapping rules allow UserGate server to redirect user requests from specific ports of a UserGate workstation network interface to other addresses and ports, for example, to another workstation in the local area network. The **Port mapping** option is available for TCP and UDP protocols.



23

Mapping name: 23

☑ Enable

Parameters

Listen IP : Port Range: Any interface : 1234

Destination address : Port: google.com : 80

Used protocol: TCP

Authorization setup: By initial IP address

User name: default

Figure 13. UserGate ports definition

Important note! If port mapping is used to provide access to company internal resources from the Internet, you should choose **Specified user** as the **Authorization** parameter. Otherwise the port will not be redirected.

Cache settings

An important purpose of a proxy server is network resource caching, which reduces the Internet connection load and greatly increases the access speed to commonly visited resources. UserGate proxy server implements both HTTP and FTP traffic caching. Cached documents are saved in the local **%UserGate_data%\Cache** folder. In the cache settings you may specify the following: cache size limit and the cached document storage lifetime. You can also enable the option of dynamic pages caching and traffic calculation from cache. With the **Calculate traffic from cache** option enabled, the UserGate user will be assigned not only external (Internet) traffic, but also traffic obtained from the UserGate cache.

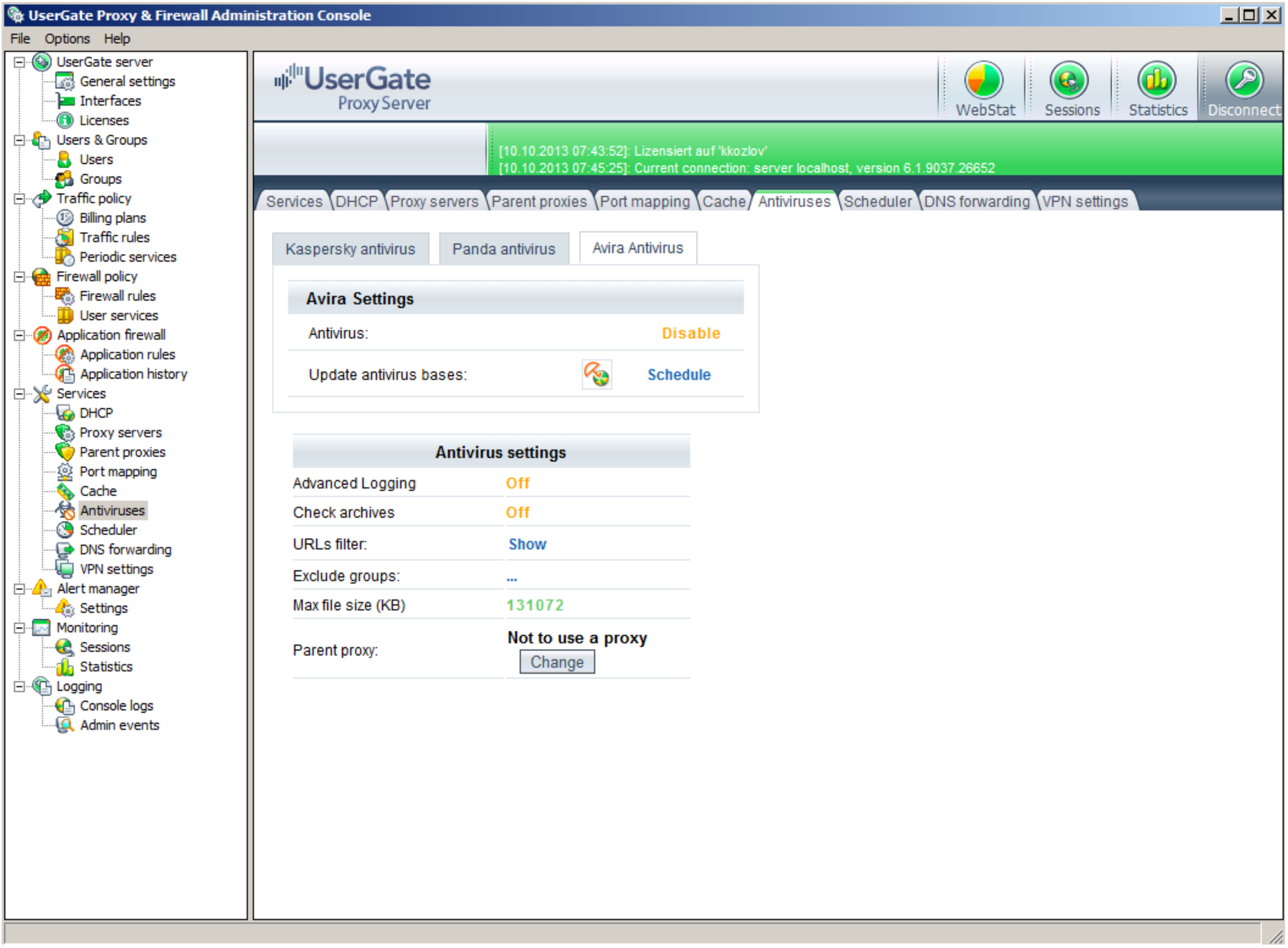
Important note! To view current cache records, you must launch a special tool for viewing cache databases. To do so, right-click on the UserGate Agent icon in the System Tray and choose the "Open cache view" option.

Important note! If you enabled cache but still don't have any resources in "Cache view," then you probably need to enable the transparent proxy server for HTTP protocol on the "Services - Proxy settings - HTTP" page.

Antivirus scanning

There are three antivirus modules integrated in UserGate server: Kaspersky Lab, Avira and Panda Security. All of antivirus modules are designed to scan incoming traffic through UserGate HTTP, FTP and mail proxy servers, as well as outgoing traffic through SMTP proxy.

Antivirus settings are available on the **Services** → **Antivirus** page in the Administration Console (Fig. 14). For each antivirus tool, you can specify which protocols to scan, setup the antivirus databases update frequency, and enter URLs that do not have to be checked (the **URLs Filter** option). In the settings, you can also specify a group of users whose traffic does not have to be scanned for viruses.



[10.10.2013 07:43:52]: Lizensiert auf 'kkozlov'
[10.10.2013 07:45:25]: Current connection: server localhost, version 6.1.9037.26652

Avira Settings

Antivirus:	Disable
Update antivirus bases:	Schedule

Antivirus settings

Advanced Logging	Off
Check archives	Off
URLs filter:	Show
Exclude groups:	...
Max file size (KB)	131072
Parent proxy:	Not to use a proxy Change

Figure 14. UserGate antivirus modules

Before running the antivirus modules, you need to start the antivirus database update and wait for it to complete. By default, the Kaspersky antivirus database updates are downloaded from the Kaspersky Lab site, whereas Avira nad Panda antivirus updates are taken from Entensys site.

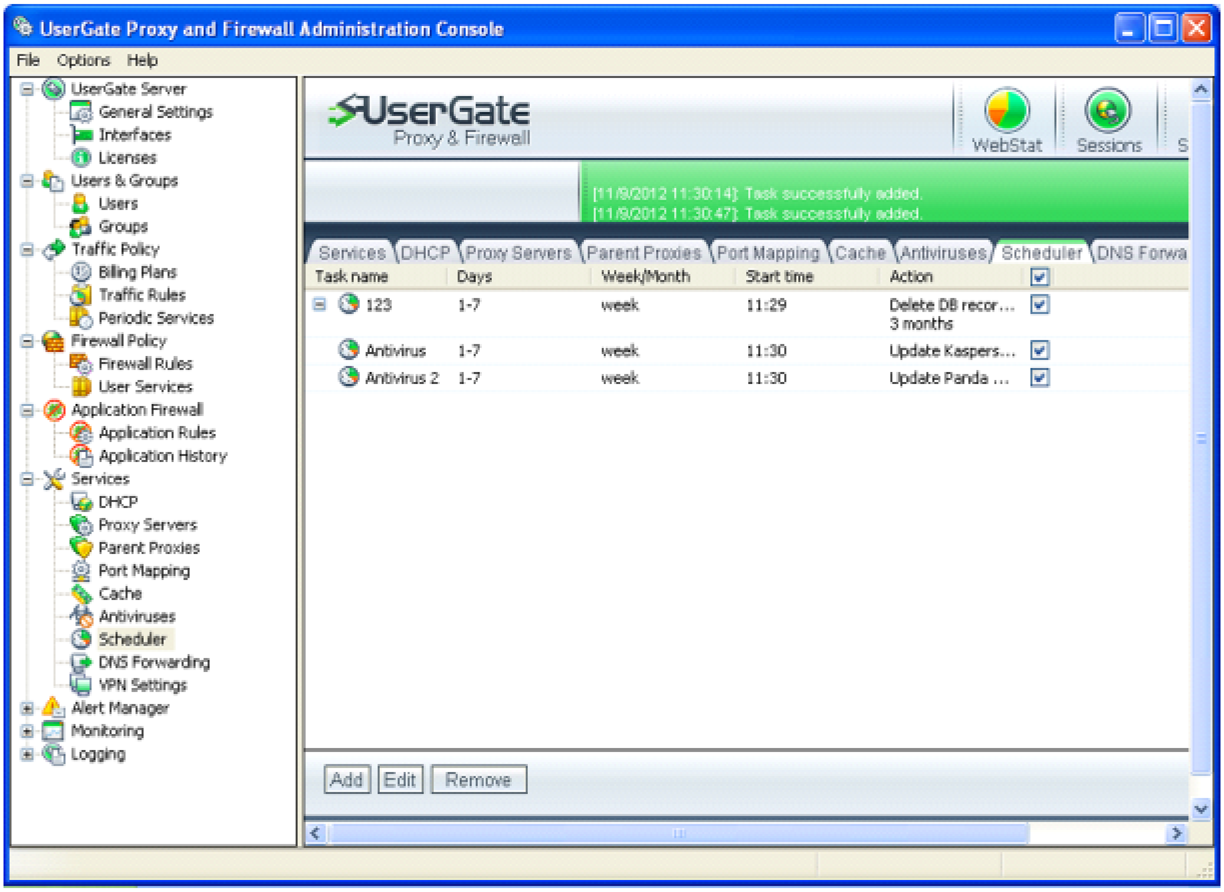
UserGate server supports simultaneous work of all antivirus engines. In this case, the

Kaspersky Antivirus will scan the traffic first.

Important note! When traffic scanning for viruses is enabled, UserGate server blocks HTTP and FTP multithreaded file downloads. Blocking partial file transfer through HTTP may cause problems with the Windows Update service.

UserGate scheduler

There is a task scheduler built into UserGate server that can be used to perform the following tasks: Dial-Up connection initialization and release, delivery of statistics to UserGate users, arbitrary task execution, antivirus database updates, statistics base purging, and checking database size.



[11/9/2012 11:30:14]: Task successfully added.
[11/9/2012 11:30:47]: Task successfully added.

Task name	Days	Week/Month	Start time	Action	☑
123	1-7	week	11:29	Delete DB recor... 3 months	☑
Antivirus	1-7	week	11:30	Update Kaspers...	☑
Antivirus 2	1-7	week	11:30	Update Panda ...	☑

Figure 15. Setting UserGate scheduler

The **Execute Program** option in the UserGate scheduler can be used to carry out a sequence of commands (scripts) from ***.bat** or ***.cmd** files.

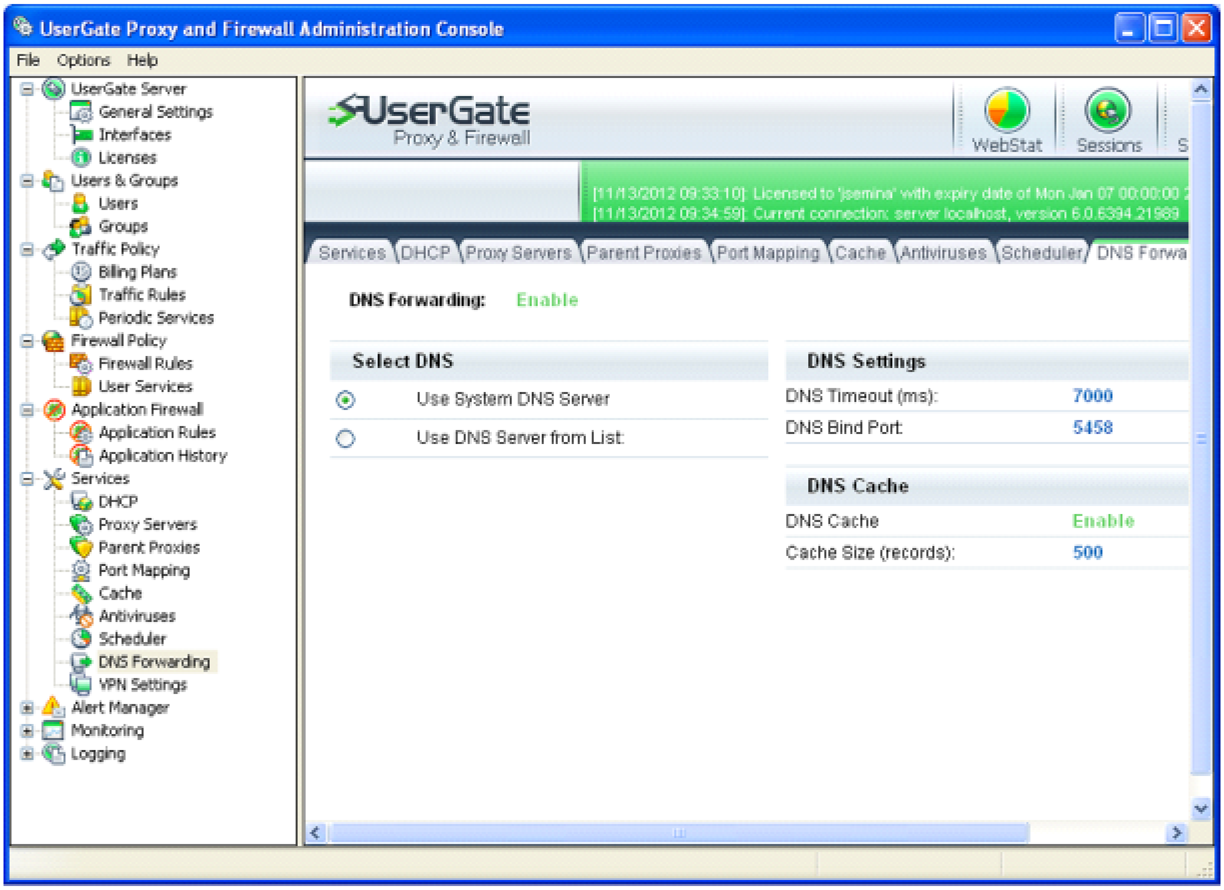
Important note! You cannot run an application with a graphics interface from the scheduler if UserGate was launched under the **System** account.

DNS settings

UserGate supports two methods for name resolution: DNS module and NAT rules. The DNS module is used with all UserGate services: proxy servers, Entensys URL Filtering, and antivirus tools. This module is designed to handle DNS queries of the following types: A, MX, and PTR, and it also supports non-recursive queries. Communication with UserGate services is performed on the Winsock level. By default, the DNS module uses the 5458 UDP port and DNS servers specified in the server network settings. If there are several DNS servers specified, UserGate calls to servers are based on the response time. If a particular DNS server doesn't provide a timely response, UserGate automatically calls all other servers. The first one to respond becomes primary for UserGate server calls.

For resolving user DNS queries, DNS forwarding mode is used. DNS forwarding settings are available in the **Services → DNS forwarding** section of the Administration Console. In forwarding mode, the DNS module listens to the 53 UDP port on the server's LAN adapters end. DNS queries coming from WAN adapters are ignored.

Responses to DNS queries are cached in the server memory, greatly improving the speed of repeat queries for name resolution. The DNS module also tracks changes in the **%WINDIR%\system32\drivers\etc\hosts** file, updating records in its own cache as needed. All records from the hosts file are stored in the DNS's own cache memory while the DNS is active.



```
[11/13/2012 09:33:10]: Licensed to 'jsemina' with expiry date of Mon Jan 07 00:00:00 2
[11/13/2012 09:34:59]: Current connection: server localhost, version 6.0.6394.21989
```

DNS Forwarding: Enable

Select DNS

● Use System DNS Server

○ Use DNS Server from List:

DNS Settings

DNS Timeout (ms):	7000
DNS Bind Port:	5458

DNS Cache

DNS Cache	Enable
Cache Size (records):	500

Figure 16. DNS settings

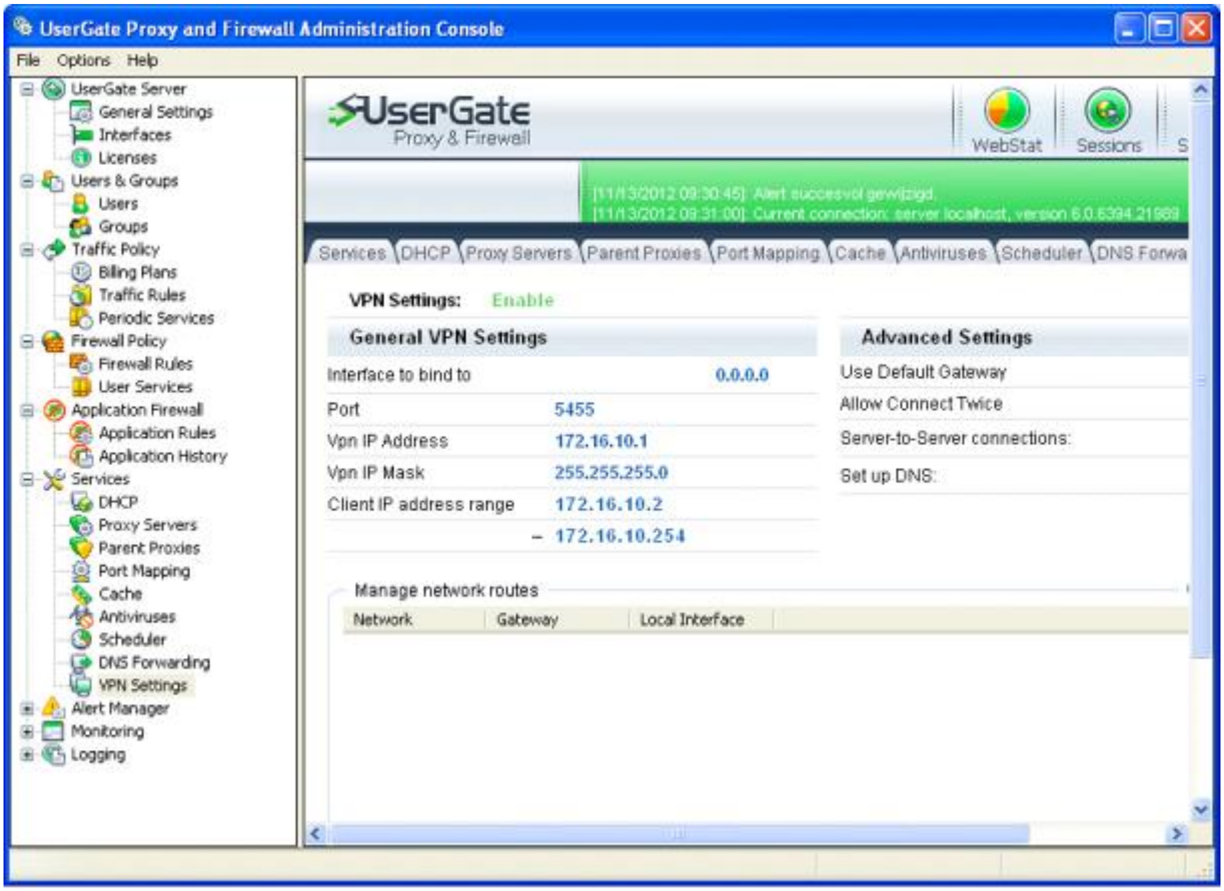
Setup through NAT is carried out by adding a NAT rule for the service under the name **DNS**, which can then be applied to all or some UserGate users. In this case, you should specify the Internet provider's DNS server IP address or any public DNS server as the DNS server on the network settings of the client workstation, for example - 8.8.8.8.

Important note! To reduce the load on the network and consume the least traffic, it is recommended to use DNS forwarding instead of specifying your provider's DNS server IP.

VPN server settings

A fully featured VPN server has been added to version 6.x, with support for **Client - Server** and **Server - Server** connections. The VPN server and client base is a network driver that is installed in the system. The VPN adapter is disabled until VPN server is enabled in the **Services → VPN settings** of the UserGate Administration Console. In the client part, the VPN adapter becomes active when connecting to VPN server.

The VPN server setup is carried out by specifying several parameters: the interface where VPN server will receive incoming connections, VPN server IP address, virtual network IP address range that can be distributed to VPN clients, and other parameters. Figure 17 shows a typical example of VPN server settings.



[11/13/2012 09:30:45]: Alert succesvol gewijzigd.
[11/13/2012 09:31:00]: Current connection: server localhost, version 6.0.6394.21989

VPN Settings: Enable

General VPN Settings

Interface to bind to 0.0.0.0
Port 5455
Vpn IP Address 172.16.10.1
Vpn IP Mask 255.255.255.0
Client IP address range 172.16.10.2 – 172.16.10.254

Advanced Settings

Use Default Gateway
Allow Connect Twice
Server-to-Server connections:
Set up DNS:

Manage network routes

Network	Gateway	Local Interface

Figure 17. VPN server settings

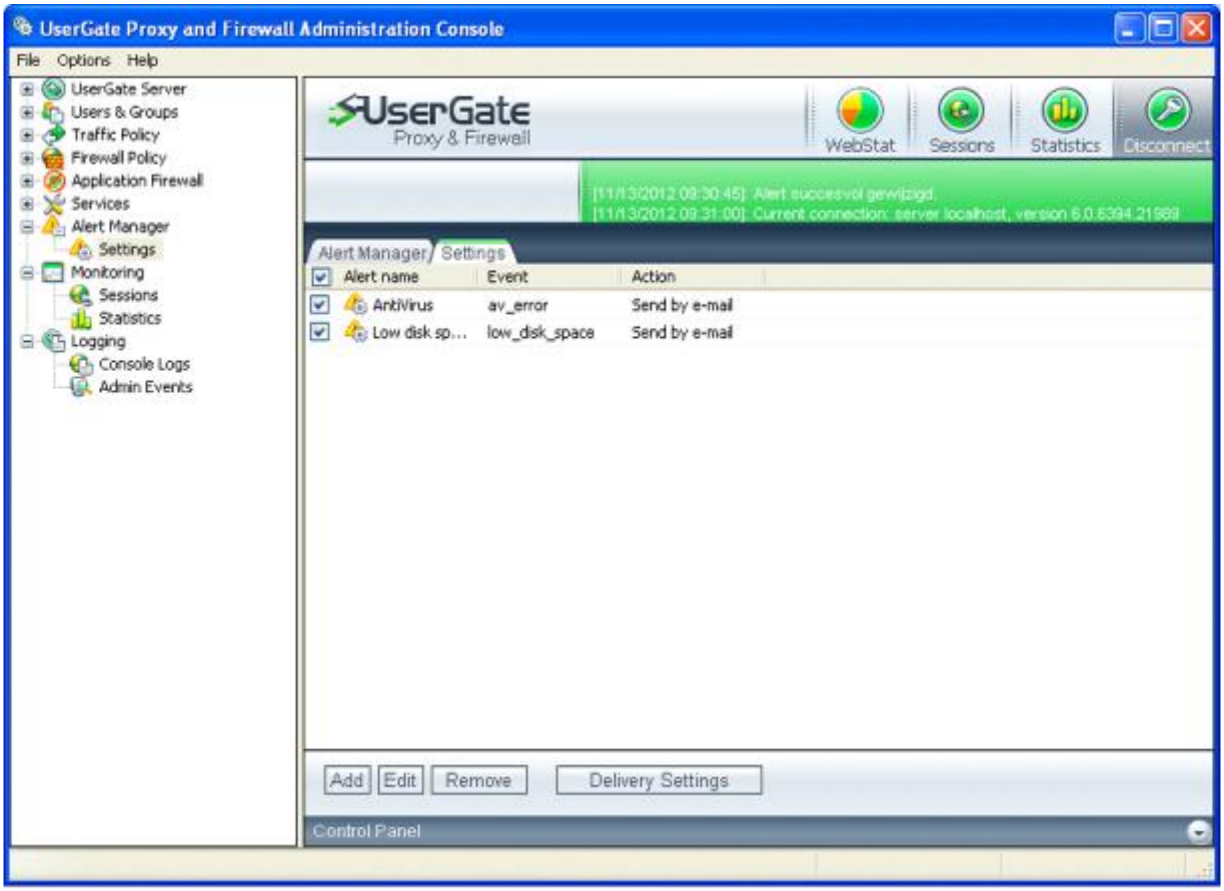
Initially the VPN server IP address is interpreted by UserGate software as a regular LAN interface; accordingly, this interface can be used either for mapping rules between the local area network and the VPN network, or for creating NAT rules between the VPN network and the Internet network.

An important feature of VPN server is the option of route transfer to VPN clients. There are two options for this:

1. If remote clients will use the UserGate VPN server as the main gateway, e.g. all Internet use will enter through UserGate server (a corporate network), then the **Use as main gateway** option should be enabled in the VPN server options. In this case, both corporate local network resources and the Internet will work for VPN clients.
2. If VPN clients will use only local area network resources when connecting to the UserGate VPN server, then VPN clients need to specify routes in the **Controlling network routes** section to access the corporate network, similar to routes that are set by the "**Route add"** command in OC Windows. In this case, the **Use as main gateway** option should be disabled.

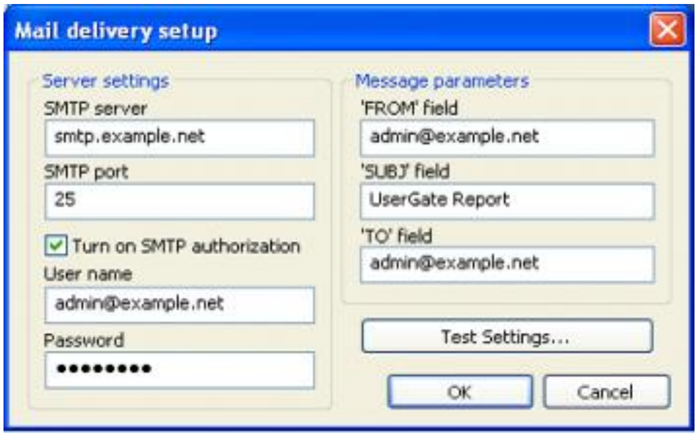
Alert manager

The purpose of the “Alert manager” module is to inform a UserGate system administrator of certain types of events that occur to UserGate server. For example, you can create a virus detection alert when scanning traffic, an antivirus module error alert, or a “license expired” alert for an antivirus tool. There is also a "low disk space" alert, as well as alerts about changes in the network interface parameters. The alert will be delivered by e-mail through the SMTP server specified in the **Delivery Settings**, available in the Control Panel.



[11/13/2012 09:30:45]: Alert succesvol gewijzigd.
[11/13/2012 09:31:00]: Current connection: server localhost, version 6.0.6394.21989

☑	Alert name	Event	Action
☑	AntiVirus	av_error	Send by e-mail
☑	Low disk sp...	low_disk_space	Send by e-mail



Server settings

SMTP server: smtp.example.net

SMTP port: 25

☑ Turn on SMTP authorization

User name: admin@example.net

Password: ●●●●●●●●●

Message parameters

'FROM' field: admin@example.net

'SUBJ' field: UserGate Report

'TO' field: admin@example.net

Figure 18. Delivery settings

UserGate Firewall

Principle of operation

The built-in Firewall, being an integral part of UserGate's NAT driver, is designed to handle network traffic according to predefined rule sets. When creating a Firewall rule, you must specify the following: source and destination addresses, service (protocol-port pair) and action: **Allow/Block**. The Firewall rule type is defined automatically according to specified parameters. Firewall supports the following rule types: network translation (NAT) rule, Routing rule, and Firewall (FW) rule.

By default, only one rule is present in UserGate Firewall - the **#NONUSER#** rule, which allows or blocks all incoming traffic coming to the server from the Internet or from the local area network. If you enable **Block** mode for the **#NONUSER#** rule, then UserGate Firewall will block all incoming and outgoing network packets except transit (NAT) packets from the local area network into the Internet and back. This is the best setting if UserGate server is installed on a standalone PC that's connected directly to the Internet.

If UserGate server is installed on a PC that is also used as a workstation needing access to specific Internet services, then you should create the appropriate permissive rules in the Firewall settings. These rules will always be placed above the **#NONUSER#** rule in the rules list. Firewall rules are viewed in a prioritized sequence where the higher priority rules are located higher in the list and are handled first. Rules can be moved to a different place in the list, thus changing their priority.

Services used in UserGate, such as proxy server or port mapping, automatically generate permissive Firewall rules. For example, when you turn on the proxy server, the Firewall automatically creates a rule allowing queries to pass to the proxy server port. Automatic rules can be removed only by disabling the corresponding service. The UserGate administrator can block a permissive automatic rule by creating an appropriate prohibitive rule and placing it at the top of the rules list.

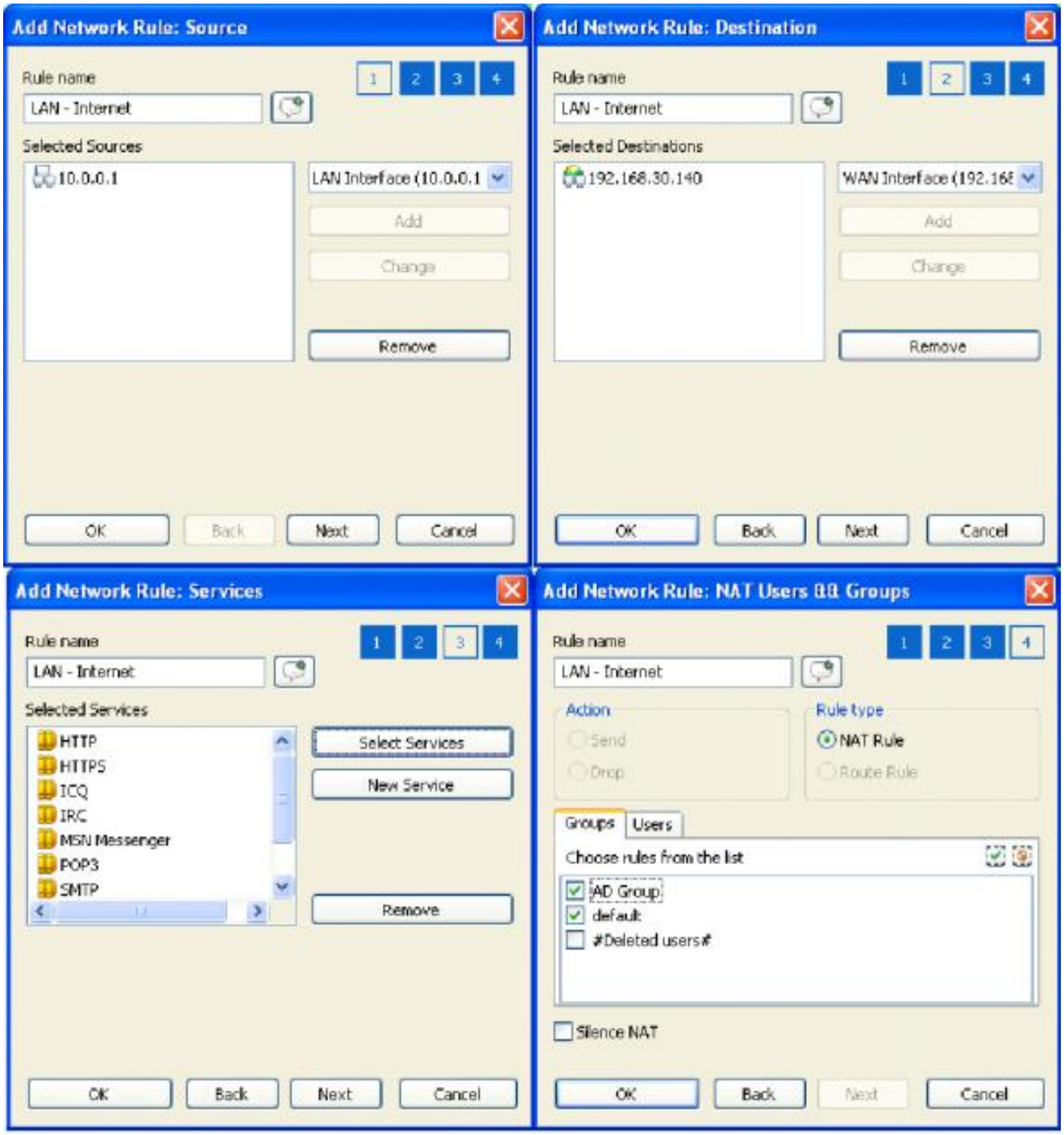
Firewall events log

The UserGate Firewall can log events related to FW operation, including system booting and shutdown, Firewall start and shutdown, and the administrator's login and logout from the system. The notifications are logged in special files, located in the **%UserGate_data%\logging** directory and in separate UserGate statistics databases tables. UserGate Firewall can generate an audit record for the following events:

- all queries to proxy services, blocked by filtration rules. The table titled **RULES_EVENTS** in the **firebird.fdb** database;
- traffic sent/received by authorized users, broken by protocols and other parameters. The table titled **CONNECTIONS** in the **firebird.fdb** database;
- traffic of the server where UserGate is installed that is not generated by any of the clients (its own traffic), including time, volume, IP addresses and ports. The table titled **CONNECTIONS** in the **firebird.fdb** database;
- detection of an infected file by an antivirus tool. The table titled **ANTIVIRUS_EVENTS** in the **firebird.fdb** database ;
- start and shutdown of any applications on the system where the software is running. The server log file **%UserGate_data%\logging\application.log**;
- the administrator's login and logout of the sytem. The server log file **%UserGate_data%\logging\usergate.log**;
- critical and noncritical errors in the system and surrounding OS. The server log file **%UserGate_data%\logging\usergate.log**;
- information on diverted and sent IP packets. The server log file **%UserGate_data%\logging\fw.log** when the appropriate options are enabled in the Firewall rules.

Network address translation rules (NAT)

To create a translation rule (Fig. 19), select the LAN adapter as a source and a UserGate server WAN adapter as a destination, and specify one or several services. Also, choose which users or groups are allowed to use this rule.


Add Network Rule: Source
1
2
3
4
Add
Change
Remove
OK
Back
Next
Cancel
Add Network Rule: Destination
Add Network Rule: Services
Select Services
New Service
Add Network Rule: NAT Users && Groups
Action
Rule type
Groups
Users
Choose rules from the list

Add Network Rule: Source

Rule name: LAN - Internet

Selected Sources: 10.0.0.1

LAN Interface (10.0.0.1

Add Network Rule: Destination

Rule name: LAN - Internet

Selected Destinations: 192.168.30.140

WAN Interface (192.16ε

Add Network Rule: Services

Rule name: LAN - Internet

Selected Services:
- HTTP
- HTTPS
- ICQ
- IRC
- MSN Messenger
- POP3
- SMTP

Add Network Rule: NAT Users && Groups

Rule name: LAN - Internet

Action: ○ Send ○ Drop

Rule type: ● NAT Rule ○ Route Rule

☑ AD Group
☑ default
□ #Deleted users#

□ Silence NAT

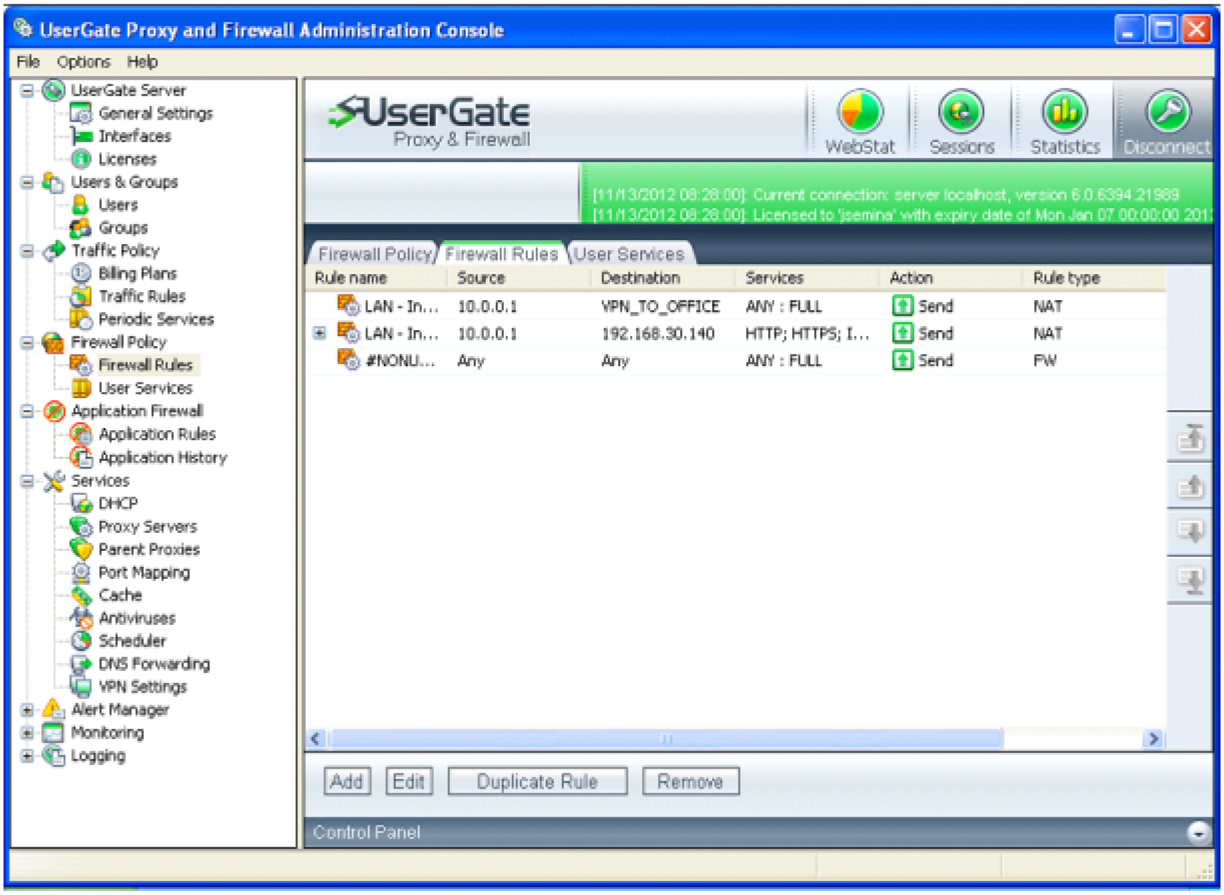
Figure 19. Translation (NAT) rule creation

In order for the translation rules to work, specify the gateway - the local UserGate server IP address and DNS server, in the workstation's TCP/IP network settings because when working with NAT, domain names resolution is not performed locally, e.g. on a user's workstation. If a required service (protocol/port pair) is absent in the predefined services list, you can add it in the dialog for creating Firewall rules or through the **Services** page in the Administration Console.

Important note! UserGate v. 6 has a very important added option in NAT UserGate driver to account for the local mapping table when sending a packet to the Internet. Thus, if the mapping rules registered in the system's local mapping table did not work for you, this problem has now been solved.

Working with multiple providers

The UserGate NAT driver supports work with several simultaneous Internet connections (the simplest non-automatic load balancer). For this purpose, the UserGate administrator can create several NAT rule sets which differ only by their external interfaces (WAN or PPP) (Fig. 20). This feature of the UserGate NAT driver makes it possible to provide Internet access through one provider for a certain group of users, and through a different provider for another group. It is not recommended to apply two translation rule sets simultaneously for different interfaces, the same user or group of users.



[11/13/2012 08:28:00]: Current connection: server localhost, version 6.0.6394.21989
[11/13/2012 08:28:00]: Licensed to 'jsemina' with expiry date of Mon Jan 07 00:00:00 201

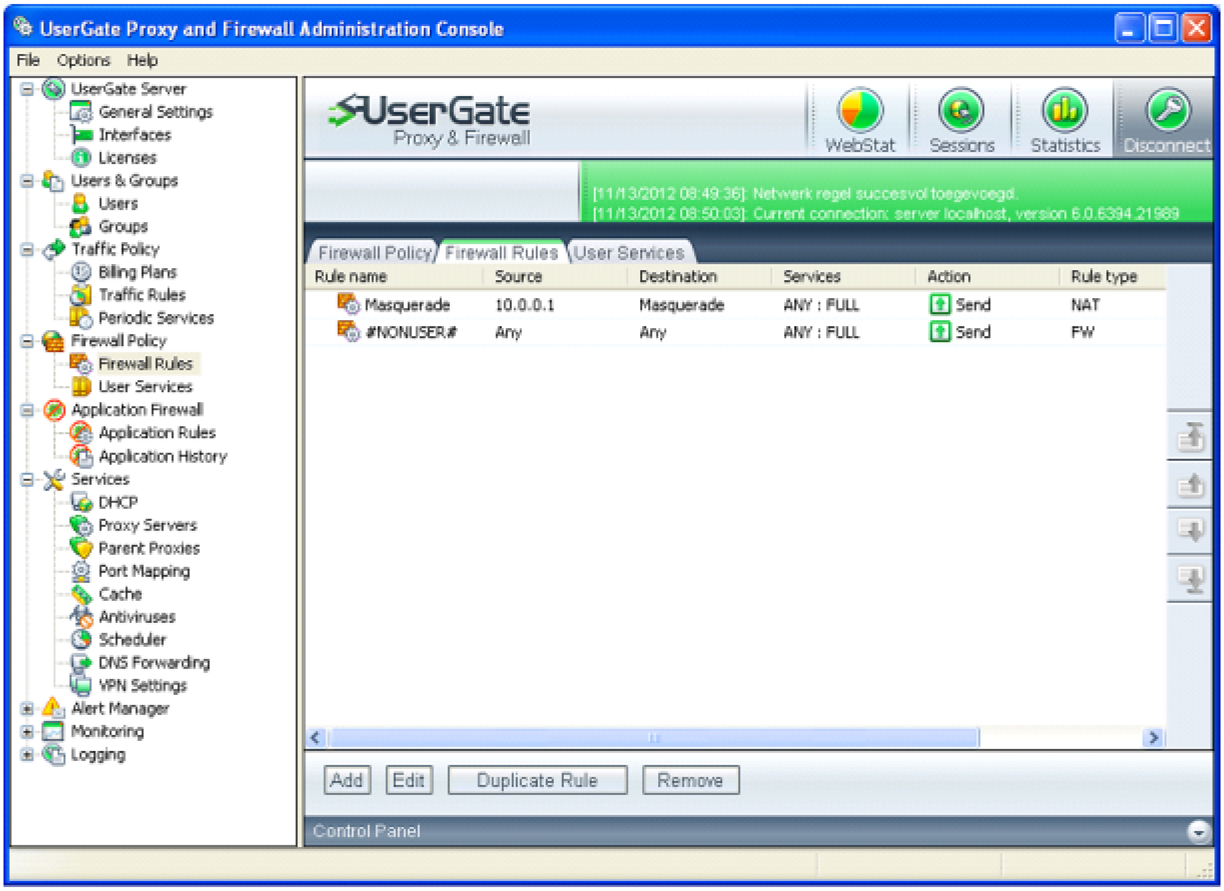
Rule name	Source	Destination	Services	Action	Rule type
LAN - In...	10.0.0.1	VPN_TO_OFFICE	ANY : FULL	Send	NAT
LAN - In...	10.0.0.1	192.168.30.140	HTTP; HTTPS; I...	Send	NAT
#NONU...	Any	Any	ANY : FULL	Send	FW

Figure 20. Working with multiple providers

Important note! This option is incompatible with the Connection failover and Automatic choice of the outgoing interface functions! Thus, if you are balancing through NAT rules, you can't enable and properly setup all of the local services using the reserve channel logic. NAT rules will always work, with the exception of transparent proxy servers, which have higher priority for handling packets than NAT rules.

Automatic choice of the outgoing interface

In the presence of several external interfaces (WAN or PPP) on a workstation with UserGate server, you may choose **Masquerade** as an outgoing interface in the NAT rules. The **Masquerade** function is used when the server's outgoing network interface used for package transfer is not known beforehand (for example, if a reserve channel is enabled). In this case, the interface will be defined dynamically by comparing the destination host network address with the network address of all UserGate server WAN adapters. If the network address of a destination host does not match any WAN adapters (PPP adapters), the package will be sent through the primary Internet channel. The **Masquerade** function must be used in order for NAT to work with a reserve channel.



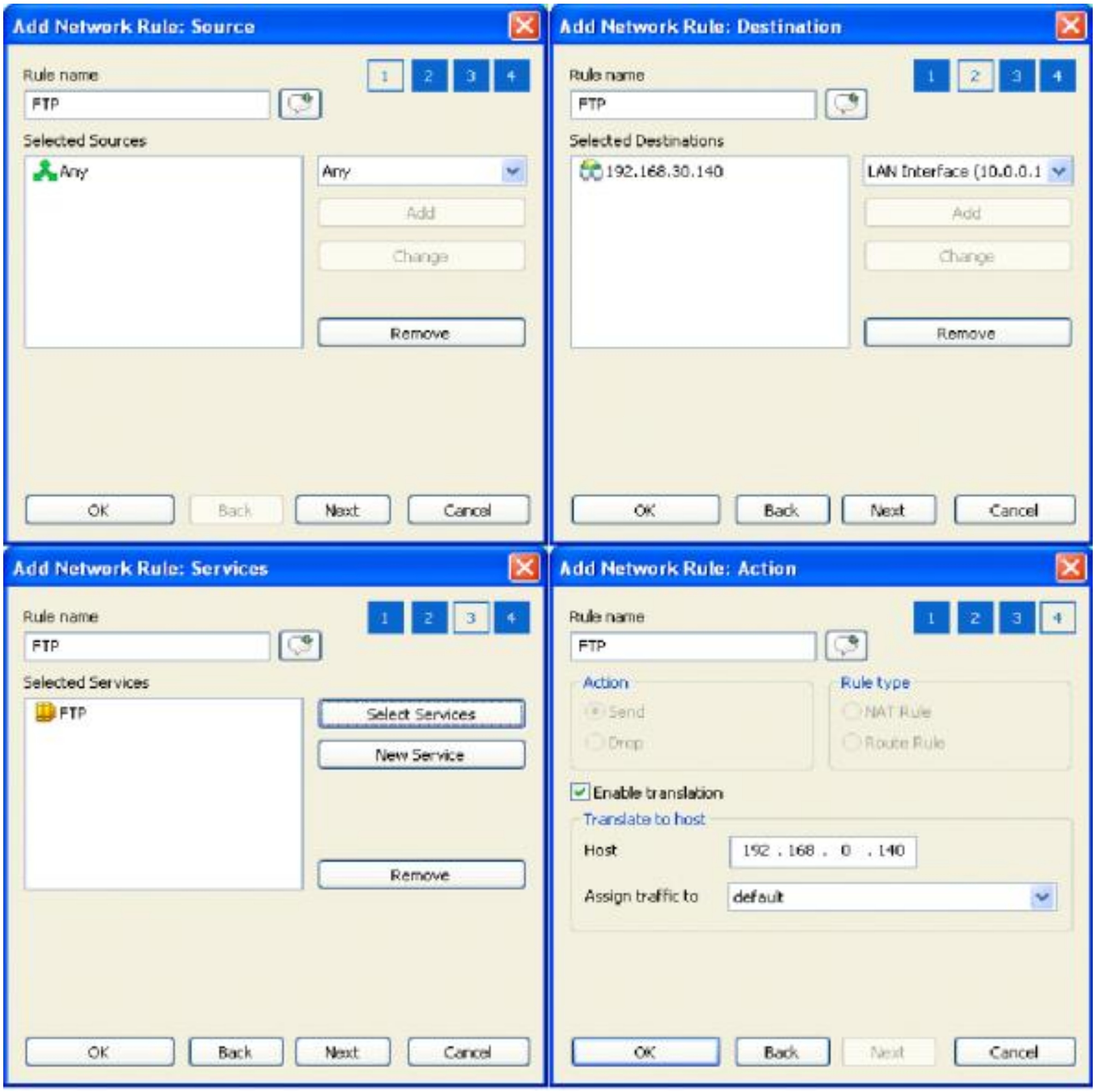
[11/13/2012 08:49:36]: Netwerk regel succesvol toegevoegd.
[11/13/2012 08:50:03]: Current connection: server localhost, version 6.0.6394.21989

Rule name	Source	Destination	Services	Action	Rule type
Masquerade	10.0.0.1	Masquerade	ANY : FULL	Send	NAT
#NONUSER#	Any	Any	ANY : FULL	Send	FW

Figure 21. Automatic choice of the outgoing adapter in the NAT rules

Network resources publishing

With UserGate Firewall, you can open access to your company's internal network resources from the Internet; for example, to a Web, FTP, VPN or mail server. In this case, all requests to a certain port of the UserGate server’s external IP address will be redirected to the internal server according to the rule. Access to a company's internal resources can be provided for all (source - **Any**) or for specified Internet hosts only. In order to create resource publishing, you need to specify one or several services on the Firewall rule (Fig. 22). If several services are specified, you need to register "**0**" as the destination port. Thus, the source port will be the destination port when translating packages from the Internet to the local area network.



Add Network Rule: Source

Rule name: FTP

Selected Sources: Any

Any

Add Network Rule: Destination

Rule name: FTP

Selected Destinations: 192.168.30.140

LAN Interface (10.0.0.1

Add Network Rule: Services

Rule name: FTP

Selected Services: FTP

Add Network Rule: Action

Rule name: FTP

Action: ● Send ○ Drop

Rule type: ○ NAT Rule ○ Route Rule

☑ Enable translation

Translate to host

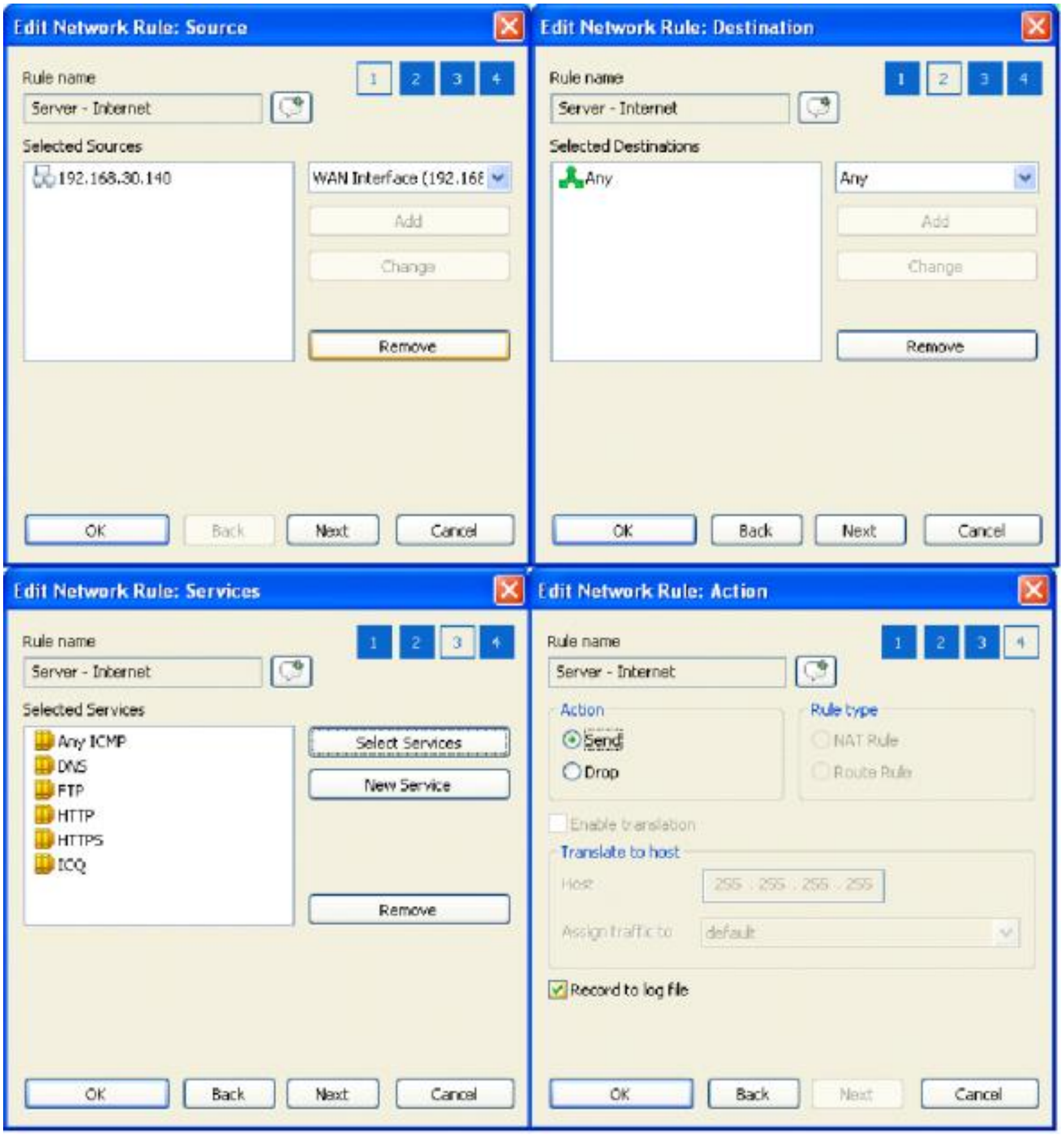
Host: 192 . 168 . 0 . 140

Assign traffic to: default

Figure 22. FTP server publishing

Filtration rules settings

It is common for UserGate to be installed on a PC used both as a workstation and a file server in a small local area network at the same time. If the #NONUSER# rule is working in **Block** mode, it is necessary to create several special permissive Firewall rules. These rules should permit outgoing requests to the Internet for such basic services as HTTP, HTTPS, FTP, POP3 and SMTP. An example of such rules is shown in Figure 23.



Edit Network Rule: Source

Rule name: Server - Internet

Selected Sources: 192.168.30.140

WAN Interface (192.168

Edit Network Rule: Destination

Rule name: Server - Internet

Selected Destinations: Any

Any

Edit Network Rule: Services

Rule name: Server - Internet

Selected Services:
Any ICMP
DNS
FTP
HTTP
HTTPS
ICQ

Edit Network Rule: Action

Rule name: Server - Internet

Action
● Send
○ Drop

Rule type
○ NAT Rule
○ Route Rule

☐ Enable translation

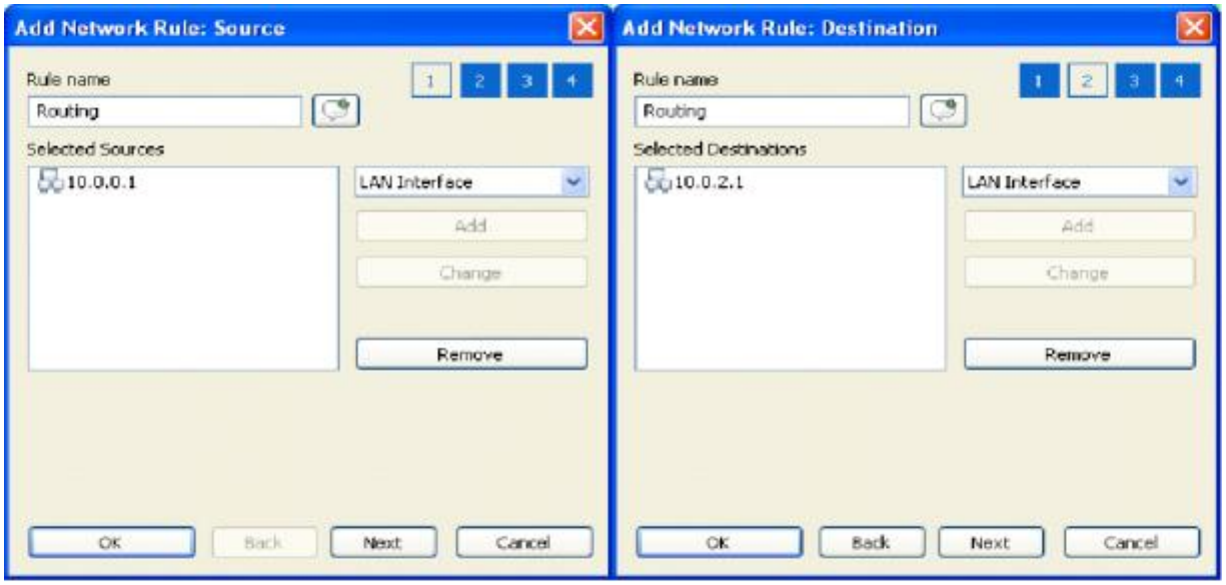
Translate to host
Host: 255 . 255 . 255 . 255
Assign traffic to: default

☑ Record to log file

Figure 23. UserGate server rules

Routing support

If UserGate server is installed on a PC connected to several local area networks, then UserGate server can be set up to act as a router providing transparent bidirectional connections among networks. Routing rules can be set up between any pair of LAN interfaces (Fig. 24).



Add Network Rule: Source

Rule name: Routing

Selected Sources: 10.0.0.1

LAN Interface

Add Network Rule: Destination

Rule name: Routing

Selected Destinations: 10.0.2.1

LAN Interface

Figure 24. UserGate routing

Important note! UserGate user authorization is not required for routing, and traffic count is not monitored.

Important note! Routing should not be confused with NAT rules, for which a local routing table is used. If you want the routing rules you create to continue operating after UserGate is installed through Windows, you need to add the routing rules as described above.

UserGate Speed Limitations

UserGate supports a speed limitation method using a NAT driver. The limit can be set either though a tariff applied to a user or through a traffic control rule (**Speed → Set up speed**). Speed limitation works for traffic through UserGate proxy services and translation (NAT) rules.

Application Firewall

Internet access management policy is logically continued by the Application Firewall module. A UserGate administrator can permit or block Internet access for both users and network applications on a client workstation. To do so, it is necessary to install the special **App.FirewallService** application on the user's workstation. The package installation can be performed either through an executable file or through the appropriate MSI package (**AuthFwInstall.msi**), located in the **%Usergate%\tools** directory.

Network application management is performed on the basis of the administrator-defined rules. Application rules must be applied to a UserGate user or group of users. There are two types of rules: default rules and users' rules. Any workstation where the **Application Firewall Service** is running can receive default rules under the following conditions:

- The service detects the UserGate server,
- A set of default rules was created in UserGate.

All **Application Firewall** rules must belong to a certain rules group. A special group, **DEFAULT_RULES** is assigned to store the default rules in UserGate. A UserGate administrator can also create his own groups for user rules.

Initially, UserGate has only one default rule which allows any user network application to access any IP address using any protocols. It is recommended to use this rule at the initial stage of the **Application Firewall** module setup for gathering network application usage statistics.

Application Firewall Service on the user's workstation obtains the user rules set only after user authorization on UserGate server. A user can be authorized either with the UserGate Authorization Client or without it through an IP or MAC address. User rules can supplement or override the default rules. When the UserGate Client is used for user authorization, the **Application Firewall** module creates a link between the Windows account for which the Authorization Client is running and the UserGate user profile. Thus, changing the Windows account when the Authorization Client is running will disable all user rules. The module does not support HTTP user authorization.

The Application Firewall policy with default settings (the first run) is defined as the following:

- If UserGate server is unavailable, all network applications are allowed.
- If UserGate server is available, only local queries of network applications and services are allowed.

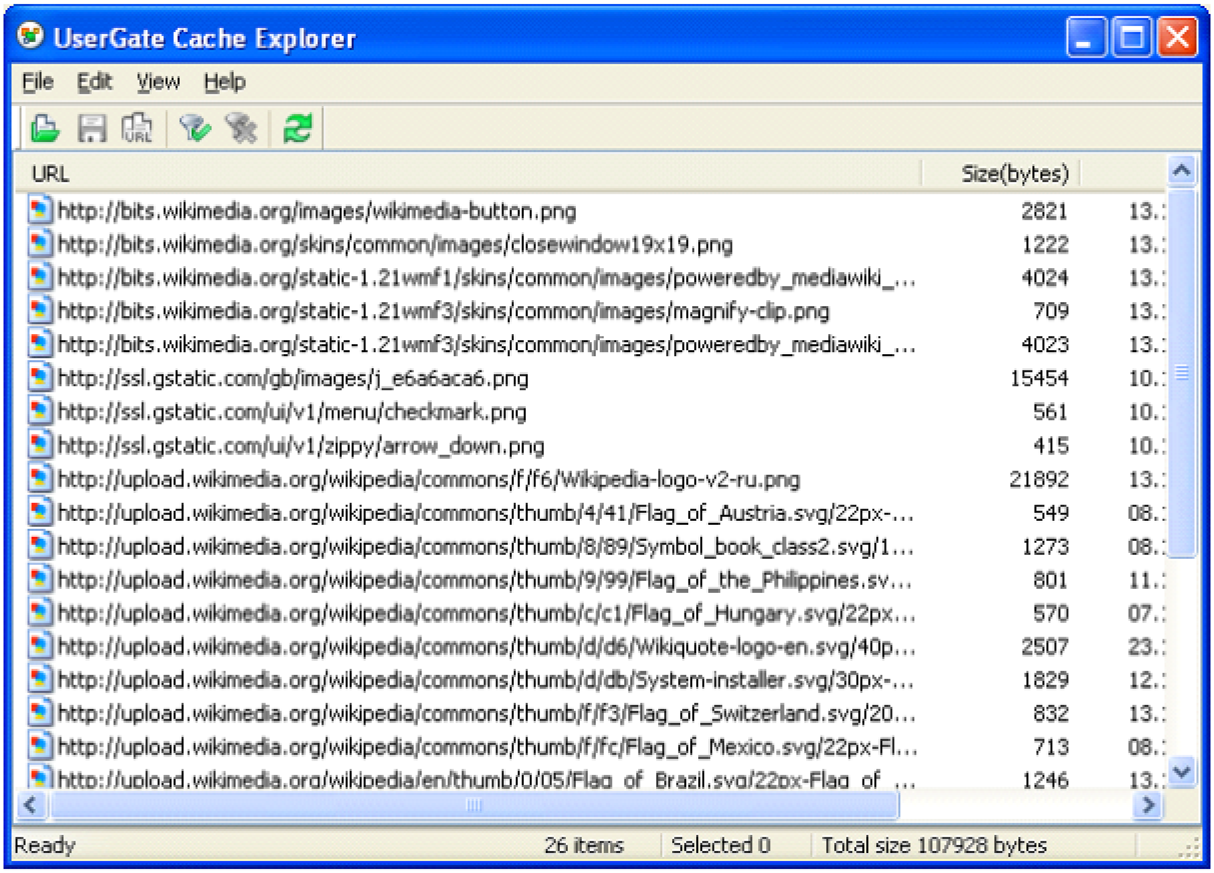
Application Firewall Service stores the network application statistics in the workstation's local folder **%ProgramFiles%\Entensys\ApplicationFirewall\Cache** and sends them periodically, at a 10 minute interval, to UserGate server. The sending frequency is defined by the **Send Statistics** parameter of the **HKLM\Software\Policies\Entensys\ApplicationFirewall** system registry. Also, unique caching rules are embedded in the **Application Firewall** module. If UserGate server is unavailable for any reason, the **Application Firewall** service continues to work according to rules stored in the local cache while waiting for the next update time (**Rules Life Time** registry parameter). By default, the rules are updated every 5 minutes.

User application statistics are available on the **Application Firewall – Statistics** page. The table shows user and workstation information, as well as network application information.

By double-clicking on the corresponding line in the statistics, a dialog box appears which the UserGate administrator can use to create an application rule.

UserGate Cache Explorer

The Cache Explorer module (Fig. 25) allows you to view the cache database content in UserGate. To start the Cache Explorer, use the **Run Cache Explorer** option in the UserGate Agent menu in the System Tray or the corresponding item in the Start - Programs menu. When starting the Cache Explorer, you need to specify the location of the **cache.dat** file (the UserGate cache database). The Explorer interface lets you search, sort, and filter the cached content. Finally, you can save any or all selected cached documents to a folder of your choice.



URL	Size(bytes)	
http://bits.wikimedia.org/images/wikimedia-button.png	2821	13.:
http://bits.wikimedia.org/skins/common/images/closewindow19x19.png	1222	13.:
http://bits.wikimedia.org/static-1.21wmf1/skins/common/images/poweredby_mediawiki_...	4024	13.:
http://bits.wikimedia.org/static-1.21wmf3/skins/common/images/magnify-clip.png	709	13.:
http://bits.wikimedia.org/static-1.21wmf3/skins/common/images/poweredby_mediawiki_...	4023	13.:
http://ssl.gstatic.com/gb/images/j_e6a6aca6.png	15454	10.:
http://ssl.gstatic.com/ui/v1/menu/checkmark.png	561	10.:
http://ssl.gstatic.com/ui/v1/zippy/arrow_down.png	415	10.:
http://upload.wikimedia.org/wikipedia/commons/f/f6/Wikipedia-logo-v2-ru.png	21892	13.:
http://upload.wikimedia.org/wikipedia/commons/thumb/4/41/Flag_of_Austria.svg/22px-...	549	08.:
http://upload.wikimedia.org/wikipedia/commons/thumb/8/89/Symbol_book_class2.svg/1...	1273	08.:
http://upload.wikimedia.org/wikipedia/commons/thumb/9/99/Flag_of_the_Philippines.sv...	801	11.:
http://upload.wikimedia.org/wikipedia/commons/thumb/c/c1/Flag_of_Hungary.svg/22px...	570	07.:
http://upload.wikimedia.org/wikipedia/commons/thumb/d/d6/Wikiquote-logo-en.svg/40p...	2507	23.:
http://upload.wikimedia.org/wikipedia/commons/thumb/d/db/System-installer.svg/30px-...	1829	12.:
http://upload.wikimedia.org/wikipedia/commons/thumb/f/f3/Flag_of_Switzerland.svg/20...	832	13.:
http://upload.wikimedia.org/wikipedia/commons/thumb/f/fc/Flag_of_Mexico.svg/22px-Fl...	713	08.:
http://upload.wikimedia.org/wikipedia/en/thumb/0/05/Flag_of_Brazil.svg/22px-Flag_of_...	1246	13.:

Ready | 26 items | Selected 0 | Total size 107928 bytes

Figure 25. Cache Explorer

UserGate traffic management

Traffic management rules

UserGate server enables you to manage users' Internet access by using traffic management rules. These rules can deny user access to certain network resources, set up traffic consumption limits, create Internet scheduling for users' work, and track user accounts status. Traffic management rules affect a certain object, causing an action to be performed in relation to it. There are 4 object-action pairs defined in UserGate: **Connection → Close**, **Traffic → Don’t count**, **Tariff → Change**, and **Speed → Set up**. For a traffic management rule to execute, you need to define the rule’s conditions, such as the time, day of the week, URLs (IP), traffic limit (per day, week or month), and etc. Defined conditions may be combined using logical **AND/OR** operators, giving the UserGate administrator greater flexibility when creating rules. Rules can be applied to UserGate users or user groups.

Internet access restriction

Internet access restriction is a typical task of a proxy server. For this purpose, there are **Connection → Close** rules in UserGate. When working with the proxy server (HTTP, FTP), you may specify the resource domain name (URL) and IP address in the traffic management rule. UserGate server can implement filtering by any URL fragment.

The following options are available for providing an IP address: **IP source address**, **IP destination address**, as well as the **Inverse** option, which means all IP addresses except the specified ones. Note that for NAT traffic, you should specify only the IP address as the condition since UserGate NAT driver does not work with domain names.

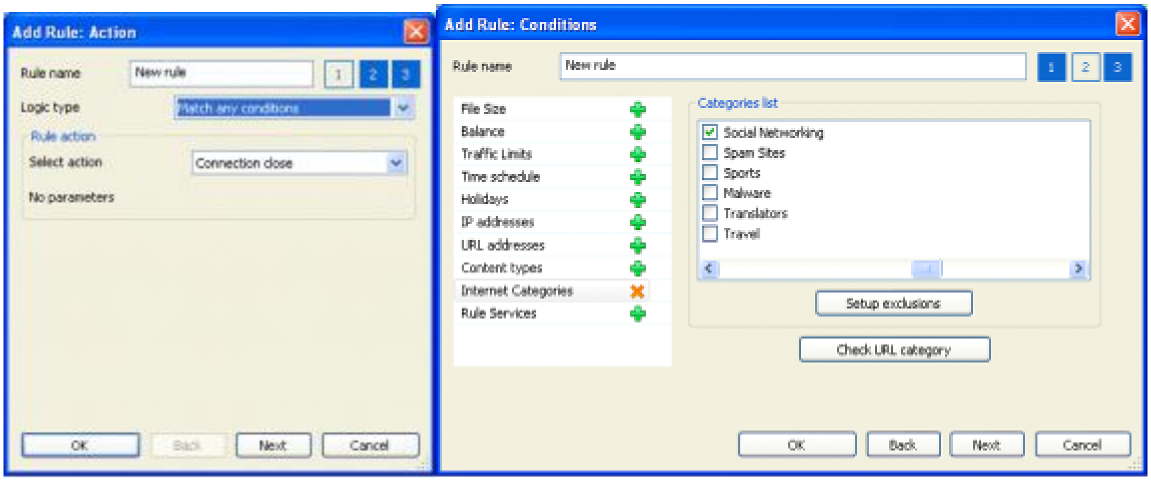
Entensys URL Filtering

UserGate Proxy & Firewall supports Entensys URL Filtering 2.0 technology, which lets you deny access to sites having certain content without specifying those sites’ names. Using site categories allows for a more flexible and simple policy of Internet access management.

Categorized filtering is available for UserGate proxy services and for NAT traffic, working in both transparent and non-transparent modes. For NAT traffic, categorized filtering will be available only if a user’s DNS requests go through the DNS forwarding module in UserGate.

To deny access to sites with particular content (Fig. 26), open the **Traffic policy → Traffic rules** page, create a **Connection → Close** rule, and specify the unwanted category on the second page of the rule creation dialog.

Here you may also add exceptions to the filtering rules by site categories.



Rule name: New rule
Logic type: Match any conditions
Select action: Connection close
No parameters

Rule name: New rule

- File Size ✚
- Balance ✚
- Traffic Limits ✚
- Time schedule ✚
- Holidays ✚
- IP addresses ✚
- URL addresses ✚
- Content types ✚
- Internet Categories ✖
- Rule Services ✚

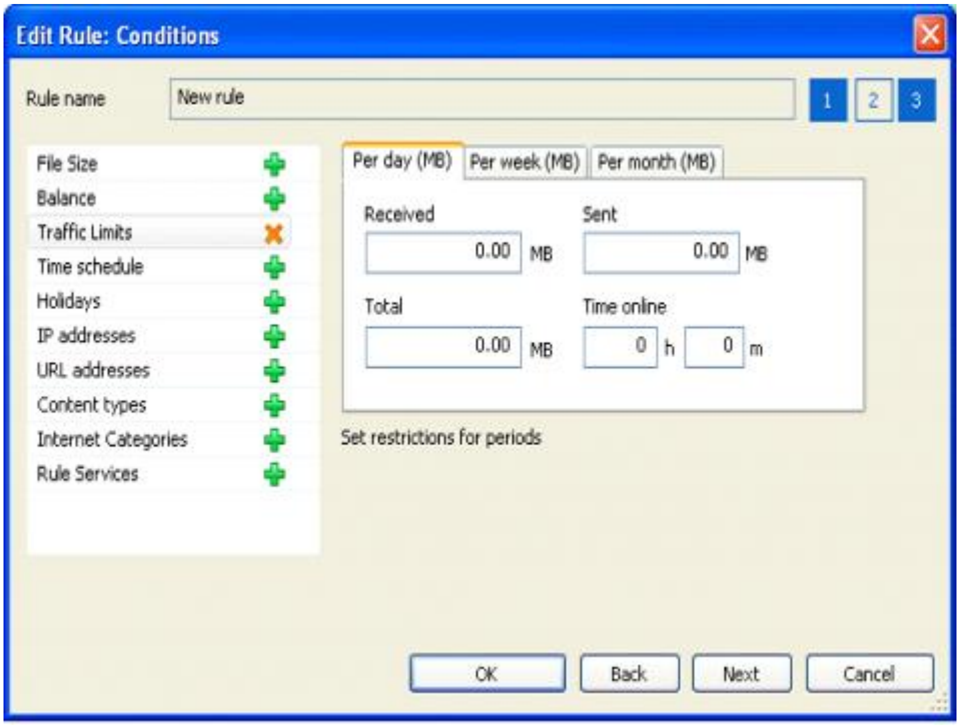
☑ Social Networking
☐ Spam Sites
☐ Sports
☐ Malware
☐ Translators
☐ Travel

Figure 26. Categorized filtering

Important note! Site categories specified in version 5.4 will have a completely different correspondence to site categories in the new version, UserGate 6.x as the URL filtering provider has changed. For more information, contact the Entensys Support Service. Later versions will include a feature for automatic conversion of old rules settings to new ones where the categorized filtering rules will be saved.

Setting traffic consumption limits

You may apply the **Connection → Close** traffic management rules not only to prohibit access to certain Internet resources, but also to limit traffic consumption. In this case, you may specify a maximum value of incoming/outgoing or total traffic per day, week, or month as the condition (Fig. 27).



Edit Rule: Conditions

Rule name: New rule

Received: 0.00 MB
Sent: 0.00 MB
Total: 0.00 MB
Time online: 0 h 0 m

Set restrictions for periods

Figure 27. Traffic limit

If a traffic consumption limit is applied to a UserGate user, then as soon as the limit is exceeded, their Internet access will be blocked completely or partially depending on additional parameters, such as Firewall services to which the rule applies.

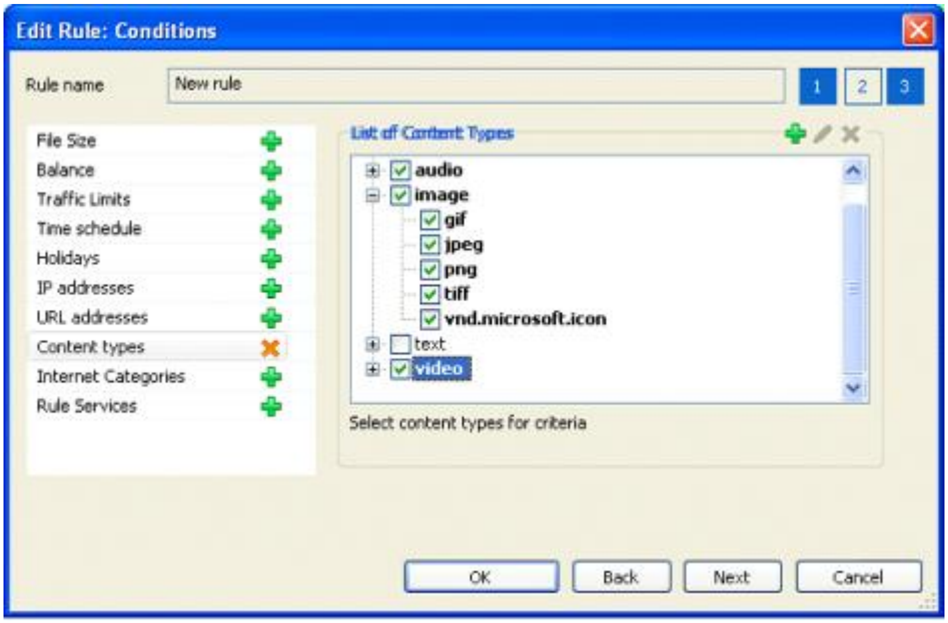
Important note! Setting a traffic consumption limit for a UserGate user group is the same as setting this limit for all members of the group. Thus, the group's total traffic is not limited.

File size restriction

UserGate traffic management rules let you restrict the maximum size of downloaded files. This option is available for the rule with the **OR** logical type and can be applied only to traffic through HTTP or FTP proxy.

Content-type filtering

For traffic through UserGate HTTP proxy, there is an option of **Content-type** filtering, which is included in the header of a web-server response to a user request. The Content-type specifies the nature of the data in a web-server response: audio (and its format), video (and its format), image (jpg, png), document type (MS Word, MS Excel) and etc. The Content-type field is analyzed by UserGate and depending on the traffic rules, the content can be either blocked or allowed. Filtering by Content-type can be used to block access to certain formats of video or audio files, disable Javascript, or prevent documents of a specific extension from being transferred over the network. This option works only for HTTP protocol.



Edit Rule: Conditions

Rule name: New rule

List of Content Types

- ☑ audio
- ☑ image
  - ☑ gif
  - ☑ jpeg
  - ☑ png
  - ☑ tiff
  - ☑ vnd.microsoft.icon
- □ text
- ☑ video

Select content types for criteria

Figure 28. HTTP filtering by Content-type

The content-types list is stored in a special ***.xml** file, located in the **%UserGate5%\Administrator** folder. A UserGate administrator can add new **content-types** to this file or through the Administration Console. The link to iana.org is included for this purpose.

Billing system

Internet access tariffing

In addition to direct traffic registration, UserGate server can also be used to calculate Internet connection expenditures. This feature is provided by UserGate's integrated billing system. Underlying the billing system is the notion of an **Internet access billing plan**. By default, UserGate settings contain only one billing plan with zero values for incoming, outgoing, and temporal traffic costs. The UserGate administrator can create any number of billing plans according to Internet provider cost policies or according to his own preferences in case UserGate is used to provide paid Internet access.

UserGate access billing plans can be applied both to users and/or user groups. By default, the Internet connections of all users belonging to the same group are rated according to the group’s specified billing plan. Nevertheless, an administrator can redefine billing plans in the users' attributes.

In the billing plan fields, you can specify how to handle a user who has passed the threshold of 0 CU in his account. The user's access can be blocked or the speed can be limited for his account.

The billing plan includes the most widely used parameters: the amount of prepaid traffic, the amount of free traffic, and the accounting period for these payments (daily, weekly, monthly).

Billing plan modifiers are available on the second page of the billing plan attributes. Modifiers are special actions or triggers that cause the billing plan's parameters to change. Modifiers may include Internet use time, holidays and the amount of traffic that the user may download, beyond which the billing plan parameters must be changed.

Regular events

These are events that always occur within each specified period and cause certain actions to take place with the user's balance.

For example, to reduce a user's balance daily by 1 CU, create a new service, enter 1 CU as the "Withdraw amount," enter "Daily" as the period, and apply this regular service to the required user or user group. On the second page of the regular events service you may specify a list of resources to which the user will have non-billable (free) access. You can also check the "Public resources" field, in which case all specified IP addresses will be non-billable. If this field is unchecked, then access to the specified resources will be blocked for everyone except users to whom this regular events service applies. Thus, in disabled mode, you can provide a paid service that will be blocked for all users by default, but users to whom this regular event applies can login to the IP address specified on the second page.

Dynamic billing plans switching

UserGate traffic management rules can be used to switch among dynamic billing plans. The most common task related to a Dial-Up connection is switching billing plans by time of day (day and night). Another task arises when different billing plans are used for access to an Internet service provider’s internal network and for the Internet. Both tasks are accomplished via the **Tariff** → **Change** rule.

UserGate remote administration

Remote connection settings

The UserGate Administration module can be used to control a remote server. To do so, specify the domain name or IP address of the remote computer where UserGate server is running in the **Server address** parameter in the connection settings.

To use the Administration module from a remote computer, simply install the Administration Console from the UserGate installation media. You can select the corresponding option in the program's installer parameters.

UserGate server remote restart

The UserGate server remote restart function has been added into the Administration Console. Using the Administration Console, you can connect to the remote UserGate server and choose **File** – **Restart server** in the menu.

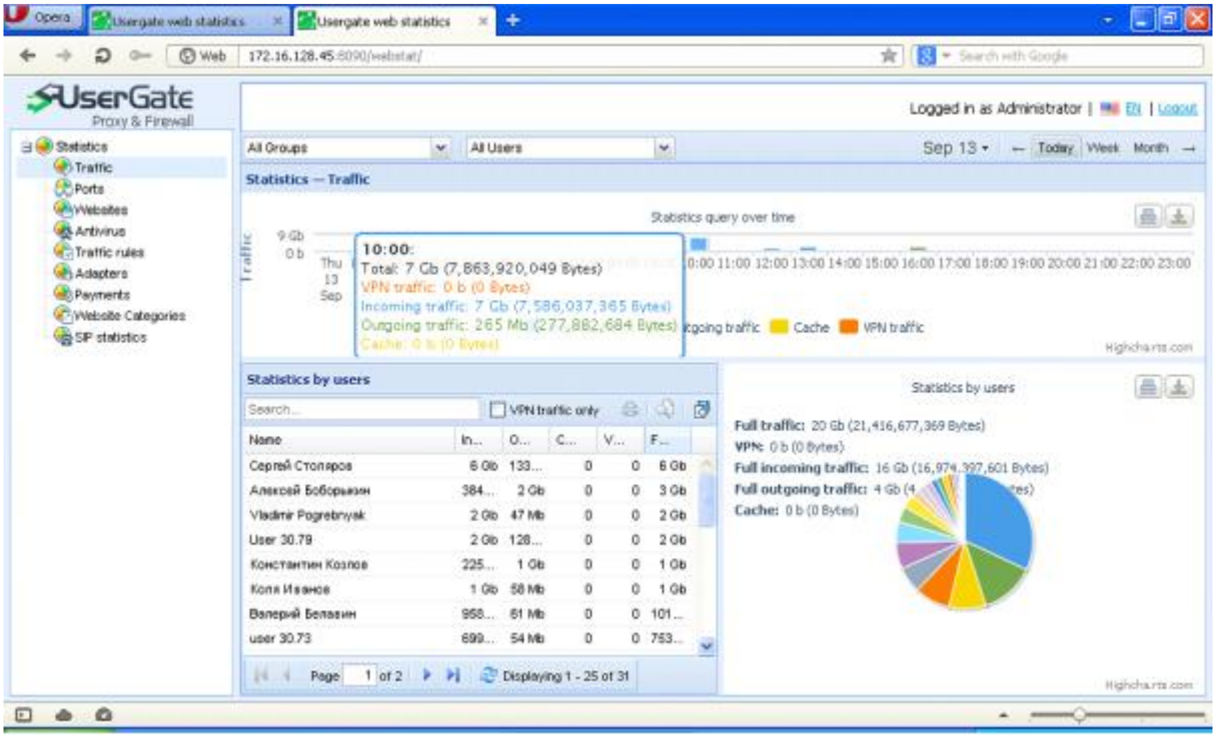
Checking for the new version

In the **General Settings** section of the UserGate Administration Console, there is a **Check for new version** option. If this option is enabled, the server generates a query to the developer's site, requesting the latest avalabile version number. If the vendor's resource offers a newer version, the Administration Console displays the corresponding message. In this case, the administrator can download the new version from the site and install it.

Checking for the new version does not cause automatic UserGate reinstallation.

UserGate Web statistics

UserGate server stores users' traffic statistics information in its own database. By default, the Firebird format is used as the database. The database is the **usergate.fdb** file, located in the program's installation directory, **%UserGate_data%\usergate6**. Brief information about the total traffic of users and groups is available in the **Monitoring - Statistics** section of the UserGate Administration Console. Detailed statistics can be accessed through a special **UserGateWebStatistics** module, being a web-application that's designed to work with the UserGate statistics database (Fig. 29).



10:00:
Total: 7 Gb (7,863,920,049 Bytes)
VPN traffic: 0 b (0 Bytes)
Incoming traffic: 7 Gb (7,586,037,365 Bytes)
Outgoing traffic: 265 Mb (277,882,684 Bytes)
Cache: 0 b (0 Bytes)

Name	In...	O...	C...	V...	F...
Сергей Столяров	6 Gb	133...	0	0	6 Gb
Алексей Боборыкин	384...	2 Gb	0	0	3 Gb
Vladimir Pogrebnyak	2 Gb	47 Mb	0	0	2 Gb
User 30.79	2 Gb	128...	0	0	2 Gb
Константин Козлов	225...	1 Gb	0	0	1 Gb
Коля Иванов	1 Gb	58 Mb	0	0	1 Gb
Валерий Белавин	958...	61 Mb	0	0	101...
user 30.73	699...	54 Mb	0	0	753...

Page 1 of 2 Displaying 1 - 25 of 31

Full traffic: 20 Gb (21,416,677,369 Bytes)
VPN: 0 b (0 Bytes)
Full incoming traffic: 16 Gb (16,974,397,601 Bytes)
Full outgoing traffic: 4 Gb (4
Cache: 0 b (0 Bytes)

Figure 29. Web-statistics home page

Every UserGate user can be assigned a certain access level to the web statistics. Thus, an ordinary user may check only his own statistics, while an administrator is authorized to see all UserGate user statistics.

Statistical information is represented not only in table form, but also as graphs and diagrams, making the reports much easier to understand and providing a visual representation of them.

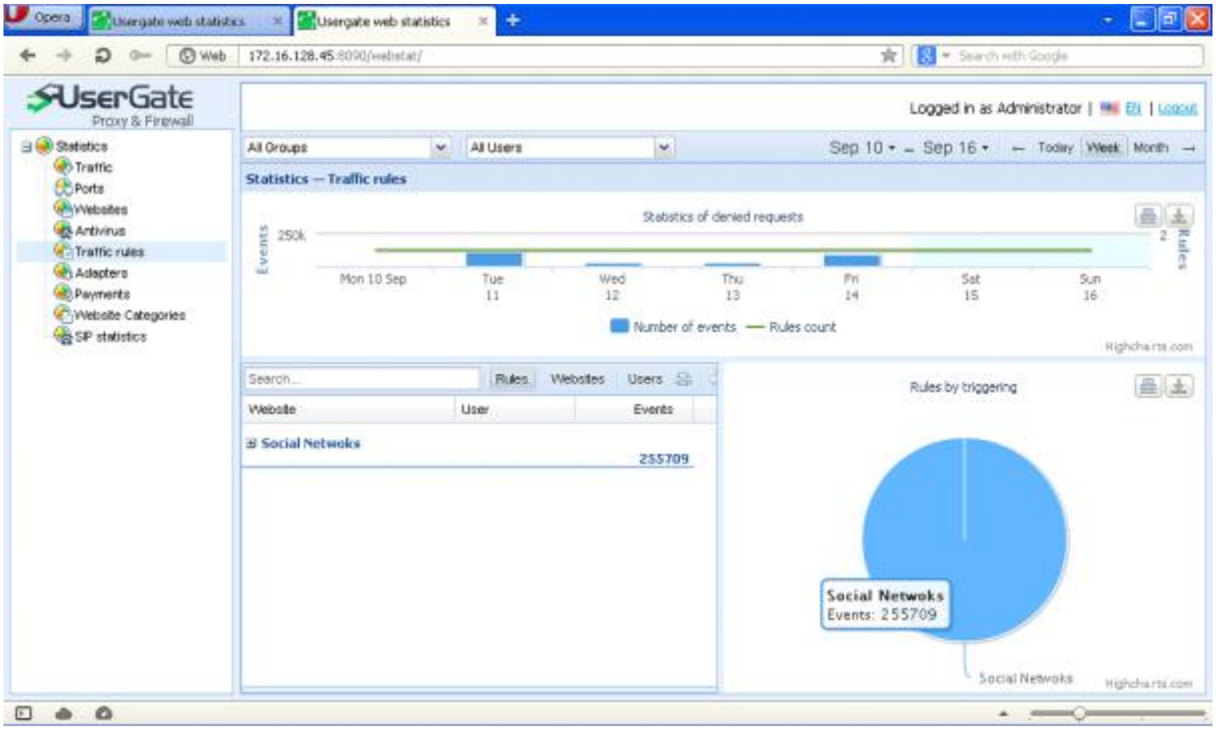
You can access the web statistics by visiting the link https://192.168.0.1:8081 where, as an example, 192.168.0.1 is the UserGate server address.

There is also a link to the web statistics available on the last tab of UserGate Authorization

Client.

Traffic management rules efficiency rating

To manage Internet access, the UserGate administrator can create traffic management rules and apply them to a user or group of users.



Website	User	Events
⊞ Social Netwoks		
		255709

Figure 30. Traffic management rules efficiency statistics

To estimate a rule's efficiency, there is a section called **Rules events log** on the web-statistics page. These statistics only include information about **Connection** → **Close** rules efficiency. Users with **Administrator** or **Director** privileges have access to additional statistics, allowing them to obtain the "weight" of each URL in total rule efficiency numbers.

Antivirus efficiency rating

Antivirus tools allow the exclusion of some UserGate groups from being scanned for viruses. Web statistics lets you obtain a report about the amount of antivirus events per user. The statistics are available in the **Antivirus events log** section. For users with **Administrator** or **Director** access levels, there is an additional statistic available, **Antivirus event statistics,** showing each UserGate user's "weight" in the number of total antivirus events.

SIP usage statistics

UserGate web statistics lets you see statistics on how SIP is used. The **Director Charts → SIP Statistics** section shows a list of users who use SIP in UserGate. The table contains the call's source address, the destination address, and the call duration.

Supplement

UserGate integrity control

Each binary file included in the program is signed by a digital certificate issued by Entensys. The signature guarantees the file's integrity and the code's soundness. You can make sure the signature is present by opening the file's attributes and going to the **Digital Signature** tab. The main executable file **usergate.exe** was also processed by a protection tool that, among other functions, tracks the hash sum. If the file is damaged or modified, the application will not start.

Launch success verification

UserGate launch success can be tracked using the **usergate.log** file, located in the **%UserGate_data%\usergate6\logging** directory. When the launch is successful, the log file does not contain any error messages. The **usergate.log** file stores data on the launch of all UserGate modules: proxy servers (specifying the listened interface and port number), DNS module, Entensys URL Filtering, antivirus and etc.

Messages in the main **usergate.log** log beginning with the "!" symbol signify errors in the program's operation or configuration. Informative messages start with the "star" symbol.

Debugging data output

A UserGate administrator may receive additional debugging information about UserGate operation. There is a special semaphore (*.sem) files mechanism designed to deduct debugging data. To enable debug logs output, launch the Administrator Console and in the **Options - Expanded logs** menu, choose the required debug logs. All debugging data is stored in its own file in the **%UserGate_data%\logging** folder. The below table shows where different debug logs store their information:

Name	Events description	Log file
authlog	UserGate user authorization	Usergate.log

socketlog	Proxy server operation	Usergate.log
socketadvlog	Proxy server work with query detailization	Usergate.log
rulelog	Traffic management rules operation	Usergate.log
kavlog	Integrated antivirus tools (KAV, Avira, Panda) operation	Usergate.log
natlog	NAT rules operation	debug.log
fwlog	Firewall operation	Fw.log
dblog	Work with statistics database	Usergate.log
diallog	Reserve channel operation and work with PPP connections	Usergate.log
cachelog	UserGate cache operation	Usergate.log, cache.log
dnslog	DNS module operation	Usergate.log
siplog	SIP proxy operation	Usergate.log
h323log	H323 proxy operation	Usergate.log
rtplog	RTP traffic processing in SIP and H323	Usergate.log

Technical Support

The Technical Support section on the http://entensys.com/support site has additional information on setting up UserGate Proxy & Firewall. Here you can also submit a request to solve any problems you may have.