



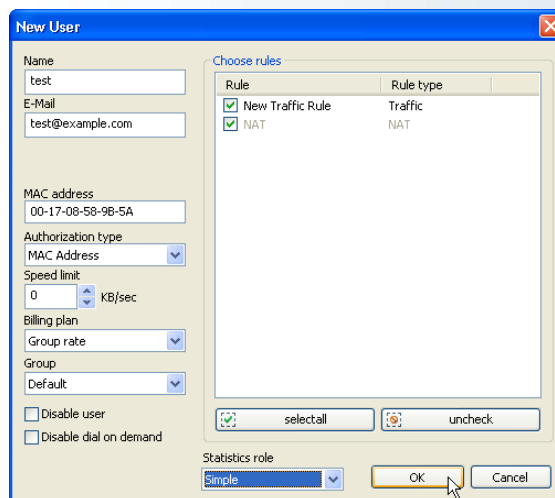
## Introduction

**UserGate Proxy & Firewall 5.0** is a complex solution designed to distribute Internet Access across an enterprise LAN, provide complete antivirus control, detect and prevent all external intrusions, as well as perform centralized management of all users' Internet activities, real-time downloads monitor and traffic control.

UserGate allows for the controlling of your employees' website browsing habits and the monitoring of downloads in real-time. Research by IDC reports that up to 40% of employee internet activity is non-work related. UserGate server can help boost employee productivity by giving you total control over what your employees can browse and what files they can download in real-time. Complete Internet access control is achieved through web categorization and web filtering techniques. BrightCloud tools are included, which is a 100% human-reviewed site categorization database. This gives you total control over what sites your users can browse and lets you block access to websites by particular categories, such as adult, online gaming, personal email, P2P and travel websites. UserGate also lets you monitor user downloads in real-time, and lets you block specific file-types such as mp3s. UserGate also scans all files for viruses, spyware and malware using multiple anti-virus engines. This significantly decreases the time for new virus signatures, thereby reducing the possibility of infection. Furthermore, UserGate lowers the risk of social engineering by blocking access to phishing websites through the use of an auto-updatable database of phishing URLs. UserGate version 5.0 offers major new features and provides fresh functional abilities to its customers.

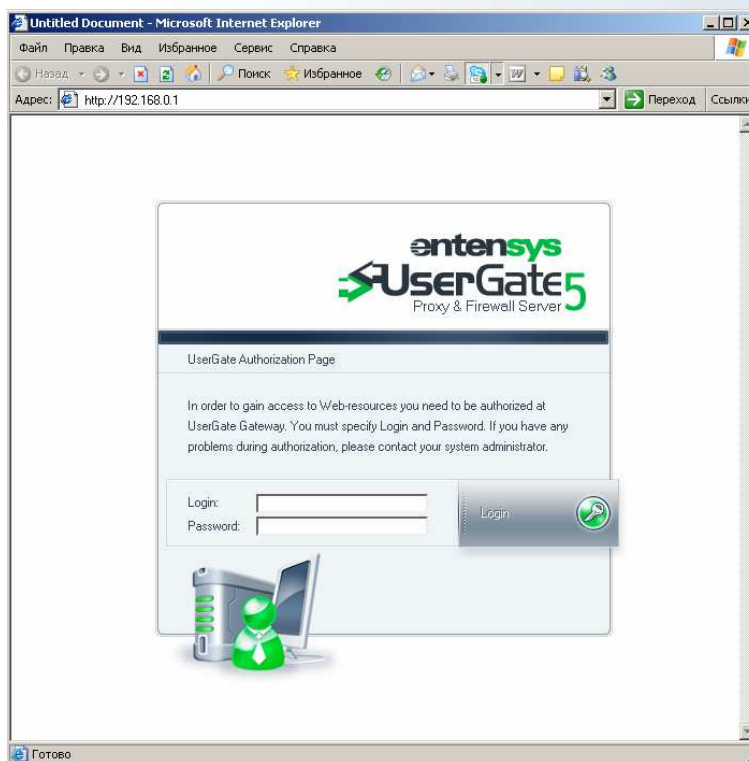
## New methods of user authorization

A new type of user authorization was added in UserGate 5.0 – authorization on MAC address (pic1)



Pic1 Creation of new user

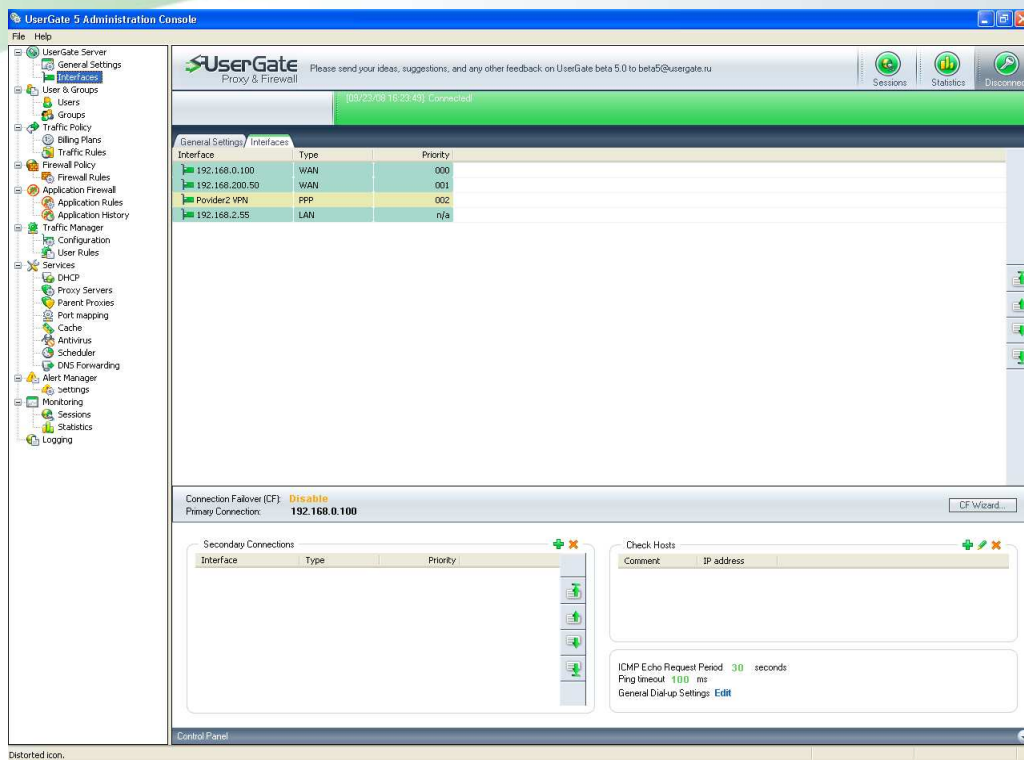
In addition, the algorithm for HTTP authorization was remade. Now, if an address and port are not specified in the browser settings at the client machine, and transparent proxy mode is enabled for HTTP proxy in UserGate, all requests from unauthorized users will be forwarded to an authorization page.



Pic2 UserGate authorization page

## Interfaces section

In the section “Interfaces” of the UserGate Administration Console, all available network server interfaces are listed. For precise traffic counts, as well as for relationship setting between networks (NAT, Touting) the UserGate administrator should specify the network adapter type (WAN or LAN), then set up a login and password for Dial-Up connections (PPP adapter). The sequence of WAN and PPP adapters in the interface list defines the sequence of requests processing by the UserGate NAT driver. The network interface at the top of this list is the primary Internet channel.



Pic 3 UserGate interfaces settings

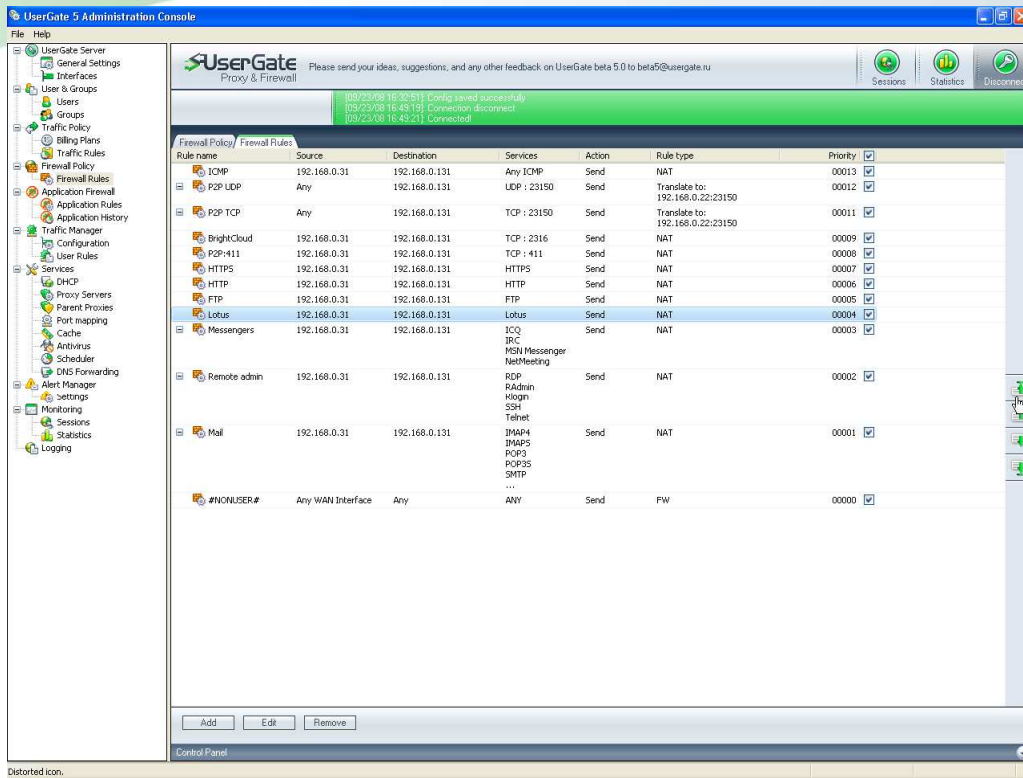
## NAT driver new functionality

The NAT driver functionality was greatly increased and enlarged in UserGate 5.0. In addition to the network address translation mode (SNAT) that is available in previous versions, the new driver supports automatic determination of outgoing interface (Masquerading) and works in Routing mode. Routing mode support allows the creation of several local subnets based on the UserGate server and the managing relations between networks.

## Firewall Policy

In this new version, Network resources publication, NAT rules and Firewall Policy are combined into one section of the Administration Console called "Firewall Policy".

The rule type (NAT, Firewall and Resources Publication) is automatically defined now based on parameters specified, such as the Source address and the Destination address, as well as the services available.

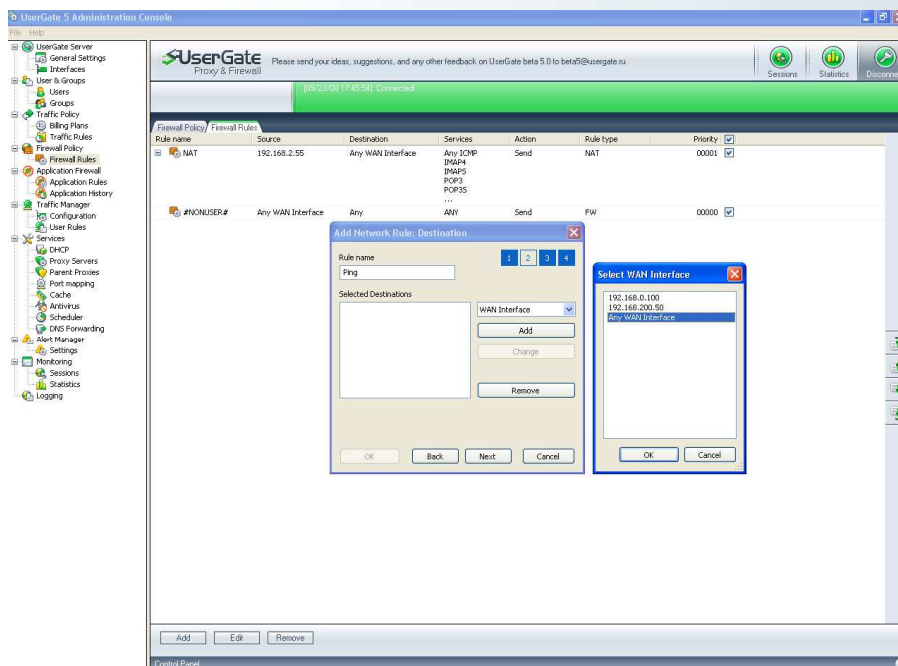


Pic. 4 Firewall Policy

NAT rules in UserGate can be created between any pair of LAN and WAN adapters. The Users and Groups that NAT rules are available for are specified on the last page of the rule creation dialog, which greatly simplifies the network administrator's work.

### Outgoing interface automatic choice (Masquerading)

In the presence of several WAN interfaces in NAT rules on a machine with UserGate, you may choose the item: "Any WAN interfaces" as an outgoing interface.



Pic5 Masquerading in Firewall Policy

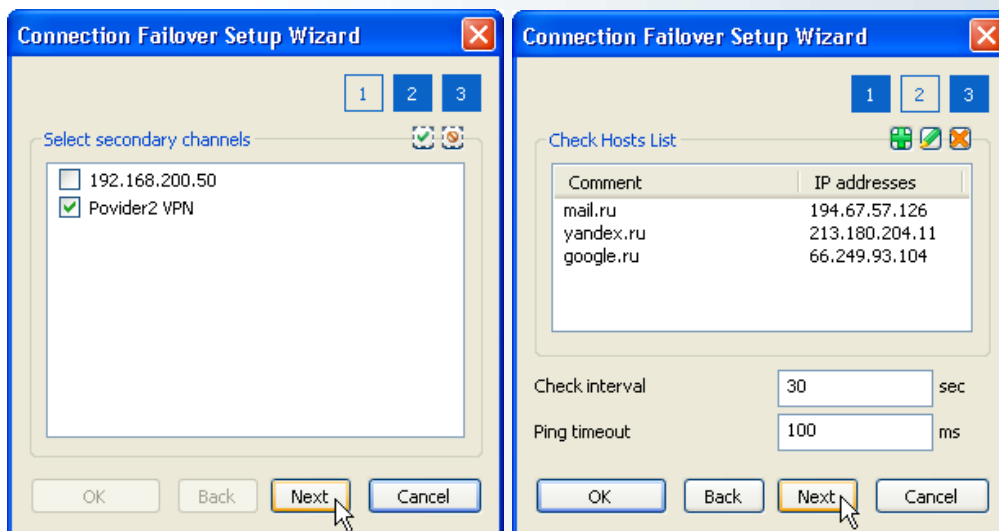
This choice means that an outgoing interface will be defined dynamically by comparison of the network destination host address with the network part of all UserGate WAN adapters. If the network part of the destination host does not match any WAN adapter, the packet will be sent through the Primary Internet channel.

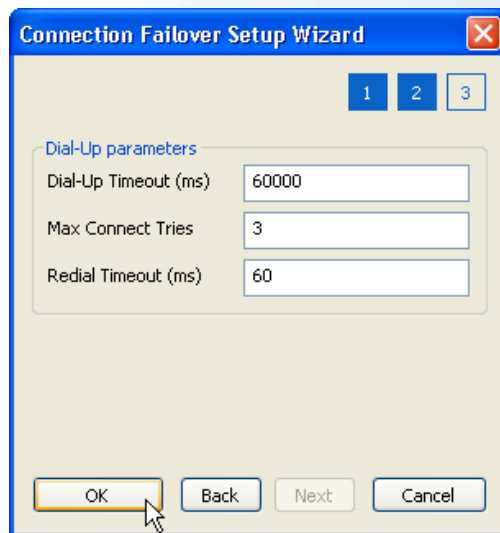
### Routing support

If a machine with UserGate is connected to several local networks, UserGate server can be set up as a Router providing a transparent bidirectional connection between networks. Routing rules can be set up between any pair of LAN interfaces. User authorization in UserGate is not required for routing, and traffic count is not executed.

### Connection Failover

If there are several Internet connections on a UserGate server, the option “Connection Failover” becomes available. To use Connection Failover, you should specify the following: the Primary Internet channel, one or several reserve channels, a list of control hosts’ IP addresses, and the control hosts’ check period. UserGate will carry out the check-up of control hosts availability using ICMP echo requests (pings). The UserGate administrator can specify several control hosts as well. In this case, the Primary channel inaccessibility is determined by a lack of response from all specified control hosts simultaneously. It is recommended that you specify as control hosts several of your most stable external hosts. Connection Failover settings are shown on pic6.





Connection Failover settings in UserGate.

As a Reserve channel in UserGate, you may use either an Ethernet connection (dedicated channel, WAN interface) or a Dial-Up connection (PPP interface). When the Primary channel is working, the function of automatic WAN interface choice is disabled.

Switching users to the reserve channel, UserGate server regularly checks the availability of the Primary channel and, if it's available, switches users back to the Primary channel.

### IP Telephony protocols support

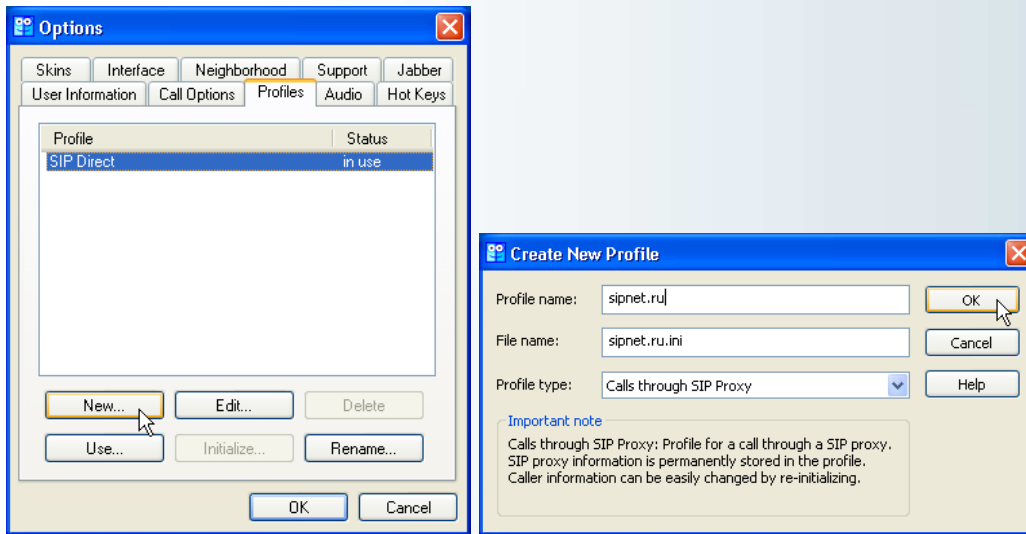
UserGate 5.0 supports protocols SIP and H.323, which allows the use of UserGate as a VoIP gateway for software IP phones, as well as for conventional IP phones.

SIP (Session Initiation Protocol) is a standard of initiation, changing and ending of user sessions, which includes multimedia elements, such as video and voice, instant messaging, online games and virtual reality. The popularity of this protocol can be explained by the low cost of Internet calls in comparison with phone and cellular providers. In UserGate 5.0, an SIP proxy function that checks connection statuses is released (state full proxy).

An SIP proxy can be enabled in the UserGate section: "Services-Proxy settings" and it always works in transparent mode, listening at ports: 5060 TCP and 5060 UDP. Using an SIP proxy for VoIP, the UserGate administrator can display full information about a connection state (registering, call, waiting, etc), information about a user's name (or his number), call duration and number of sent/received bytes. The same information will be written to the UserGate statistics database.

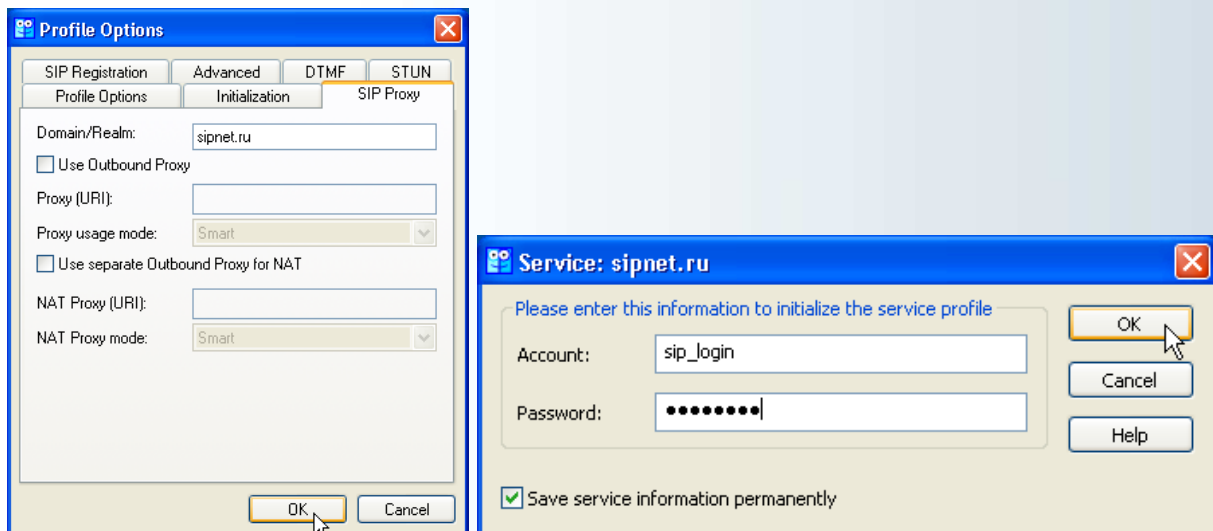
For SIP proxy usage you should specify on the client machine the IP address of UserGate as a gateway as the default, as well as specify the DNS server address.

The setup of the client side is illustrated by the sample of software phone SJPhone and Sipnet provider. Run SJPhone, choose the item: **Options** in the content menu and create a new profile (pic7)



Pic 7 SJPhone profile creation

Please, enter the name of the profile and, as a profile type, please specify, “Call through SIP Proxy”.



Pic 8 SJPhone profile settings

You should specify your VoIP provider proxy server address in the “Profile Options” dialog. When closing the dialog you should enter the data for authorization on your VoIP provider server (your user name and password).

Built-in H323 protocol support allows you to use UserGate server as a Gatekeeper. In H323 settings, you should specify the interface on which all client requests are listened – the port number as well as the H323 gateway address and port.

For authorization on UserGate Gatekeeper, the user should specify **login** (his user name in UserGate), **password** (his user machine's IP address) and **phone number** (found in the UserGate user settings).

## Bandwidth Manager

The algorithm used to manage bandwidth in UserGate is a combination of CBQ (Class Based Queue), WFQ (Weight Fair Queue) and PQ (Priority Queue) algorithms. The algorithm can be divided in three stages.

In the first stage (CBQ), classification for going through the NAT driver packets is accomplished by the user rules that are set. The classification is performed on the address part (source/destination address) and/or on the protocol part (protocol, source/destination port).

Packets that do not match any user rules will be processed using the default rule.

In the default rule, two parameters are specified: maximum bandwidth value allowed (kb/sec) and priority. The bandwidth value is specified in accordance with Internet connection parameters. The default bandwidth specified can be the same for both incoming and outgoing traffic.

If you are planning to use UserGate on networks with high-priority traffic (IP Telephony, Online conferences. etc), it is recommended that you set a default rule with the lowest absolute priority. In users' Bandwidth Manager rules, for high-priority traffic processing it is recommended that you set the highest absolute priority.

Speed limiting for certain traffic types is accomplished using users' Bandwidth Manager rules.

The following parameters are available in users' Bandwidth Manager rules:

- Priority
- Traffic direction (incoming/outcoming)
- maximum bandwidth value allowed (kb/sec or mb/sec)
- Packets delay (msec)
- Protocol (TCP/UDP/ICMP)
- Source IP address, Source port
- Destination IP address as IP/mask, destination port

- Adapter, traffic through which will be processed by Bandwidth Manager.

It's possible to specify both a certain host and an IP address range with 256 maximum elements as a source. You may specify a network IP address or a certain host (mask 32) as a destination.

Bandwidth Manager rule-priority defines in which FIFO (First In First Out) queue a packet will be put in after classification. There are 8 priority queues defined: 4 queues with absolute priority (HIGH, MEDIUM, NORMAL and LOW) and 4 queues with relative priority.

At the second stage of this algorithm (WFQ), packets from queues with relative priority pass through an interim FIFO buffer and are put into 4 outgoing queues with relative priority.

The presence of an interim buffer provides the sequence of packet processing that is needed and smoothes possible sudden speed changes. It's supposed, that in the current version of Bandwidth Manager all queues with the same relative priority have the same weight (equal to 1), i.e. in a general case with the same speed limits, traffic of the four types of relative priority will divide bandwidth into equal parts.

Manageable traffic speed limiting is provided in the last stage of the algorithm (PQ) but for queues with relative priority only. Depending on the set limit, a packet can be passed to the outgoing buffer, moved to the beginning of the queue (if the time delay parameter is set) or it can be rejected.

Queues with an absolute priority are intended for privileged traffic processing. If needed, such traffic can fill the full bandwidth of the dedicated Internet channel. The administrator can use only one parameter to affect privileged traffic processing; this parameter is ***absolute rule priority***.

When creating a Bandwidth Manager user rule set, please take into account the following:

- Bandwidth Manager is intended for traffic speed limiting for directions Server ↔ Internet and Local Network ↔ Internet.
- If a packet matches more than one limiting rule, then, when working with Bandwidth Manager, the first suitable rule will be applied.
- Bandwidth Manager's productivity is limited by the NAT driver's productivity, which is why it is not effective on high speeds.
- To achieve maximum capacity, please use unilateral rules.

### **Categorized URL filtering**

In the context of our technology partnership with BrightCloud we integrated the hosted BrightCloud Service and the BrightCloud Master Database into UserGate. A UserGate administrator can forbid access to certain content sites without specifying those sites' names.

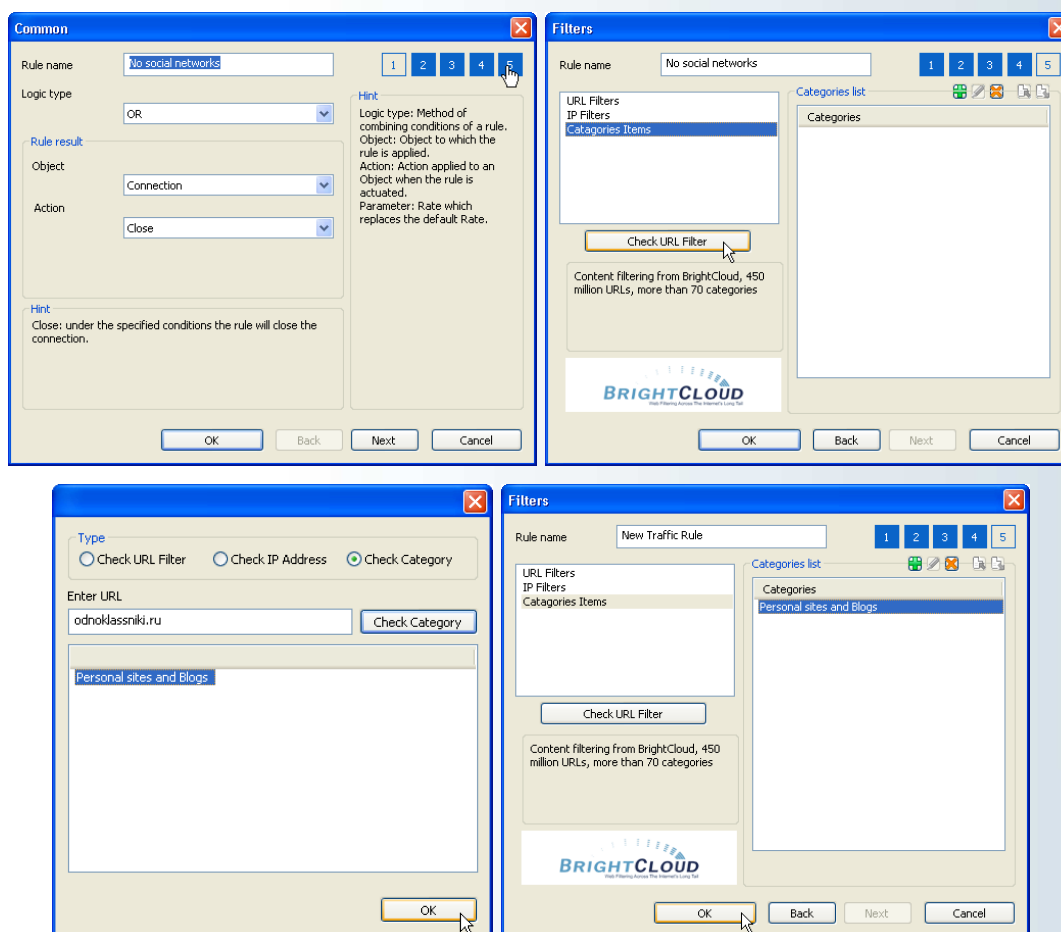
Additionally, it's possible to get a report from UserGate Statistics about the site categories visited, such as **Ads, Education, News**, etc.

Site categories usage allows for a more flexible policy of Internet access management.

Categorized filtering is available for UserGate proxy services working in both transparent and non-transparent modes.

If a browser on a client machine is not set for proxy use, categorized filtering will be available only when "DNS forwarding" is enabled in UserGate. The UserGate server IP address is specified as the DNS on a client machine. Categorized filtering is not released for NAT traffic.

To deny access to certain categories, open the section "Traffic Policy – Traffic Rules", choose "Connection" and "Close", then specify the unwanted Category on page five of the rule creation dialog.



Pic10 Categorized Filtering Rules.

## Application Firewall

Application Firewall is an integrated module that allows for the managing of Internet-based applications, and for the setting of restrictions on these applications usage per version/type/protocols or name. Now you can manage Internet access for both users and applications on a client machine.

For example, using Application Firewall, you can allow users that use only Internet Explorer of a particular version and deny all other browsers.

There are two types of rules in Application Firewall: default rules and users' rules. Default rules cannot be applied to a user, but any machine can get these rules if Application Firewall runs with the following conditions:

- Application Firewall service detects UserGate server
- A set of default rules was created.

For storing Default rules a special folder: **Default rules** is intended. The administrator can create groups for Users' rules. Initially, UserGate has only one default rule, which allows access of any user network applications to any IP addresses on all protocols. This rule is recommended to use at the beginning of Application Firewall setup for applications usage statistics gathering. Users' rules are applied only at the moment of user authorization on UserGate server. A user can be authorized using Authorization client or can be authorized without it just by using the address part (IP address, IP+ MAC, MAC address). Users' rules can add or forbid default rules. With user authorization through the Authorization Client, a bond "Windows account – UserGate account" is created in Application Firewall, i.e. switching of Windows account when Authorization Client is run cancels users' rules operating. Processing of users with HTTP authorization is not yet released.

Application Firewall policy with default settings (initial starting) is defined as the following:

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

The network applications statistic of Application Firewall is written in the local folder: %Program Files%\Entensys\Application Firewall\Cache and is sent periodically (each 10 minutes approximately) to UserGate server. The sending time span is assigned by the Registry parameter SendStatistics (HKLM\Software\Policies\Entensys\Application Firewall). Also, the proper Caching rules are embedded in the Application Firewall. If Usergate server is temporary unavailable, Application Firewall works during the updating time under the rules written in the local Cache (Update rules parameter). The rules updating period averages 5 minutes by default.

### **New authorization client**

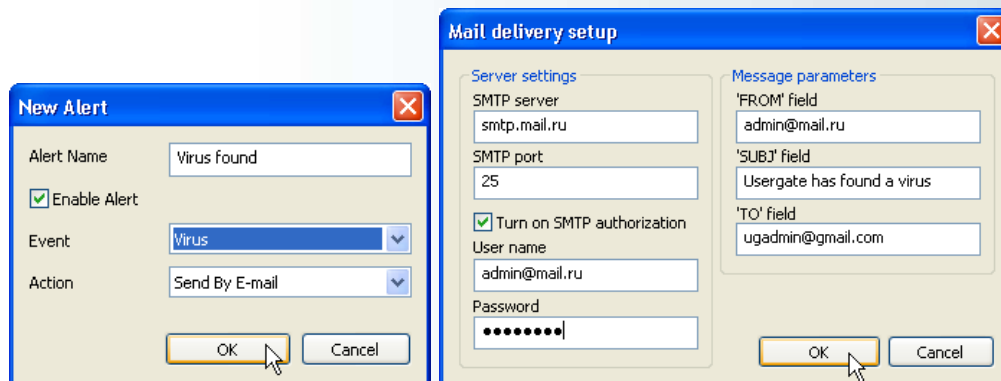
UserGate client authorization has been improved considerably. We have developed a new handy interface. A UserGate administrator can change the client authorization surface via

template editing in the \*.xml file form. A link on the user's personal page is added in the client authorization. When the network application is blocked, the client authorization displays the proper warning message. You can find the parameters of the client authorization settings in the "HKCU\Software\ Policies\Entesys\Auth client" branch of the Registry.

## Alert Manager

The Alert Manager Module was designed for the system administrator to be informed of some UserGate server events. For instance, in the Alert Manager Rules you can create the notification of a virus detection under traffic checking, about an antivirus module error or about a license key expiry.

You will get the alert message by e-mail via the SMTP server specified in the Delivery Settings.



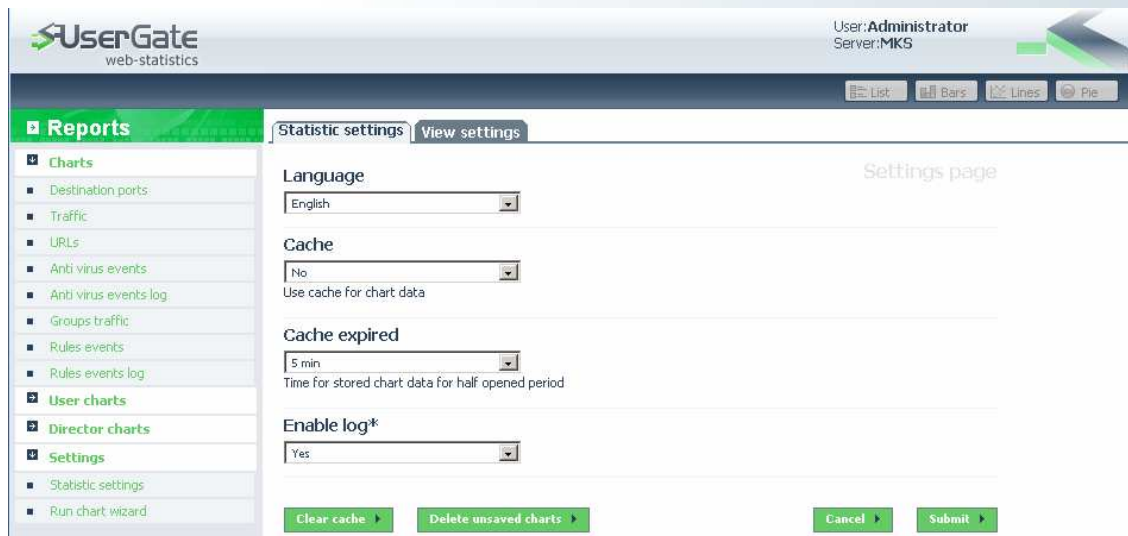
## Web Statistics

We have thoroughly upgraded the Statistics Module. UserGate Statistics is based on the web technology that makes it available over the whole world in the condition of the Internet connection and the web browser availability. Each UserGate user has a right to access UserGate Statistics. Thus, employees may check their own statistics, a chief could see the statistic of any user of his company's network and an administrator is authorized to create Statistic report templates.

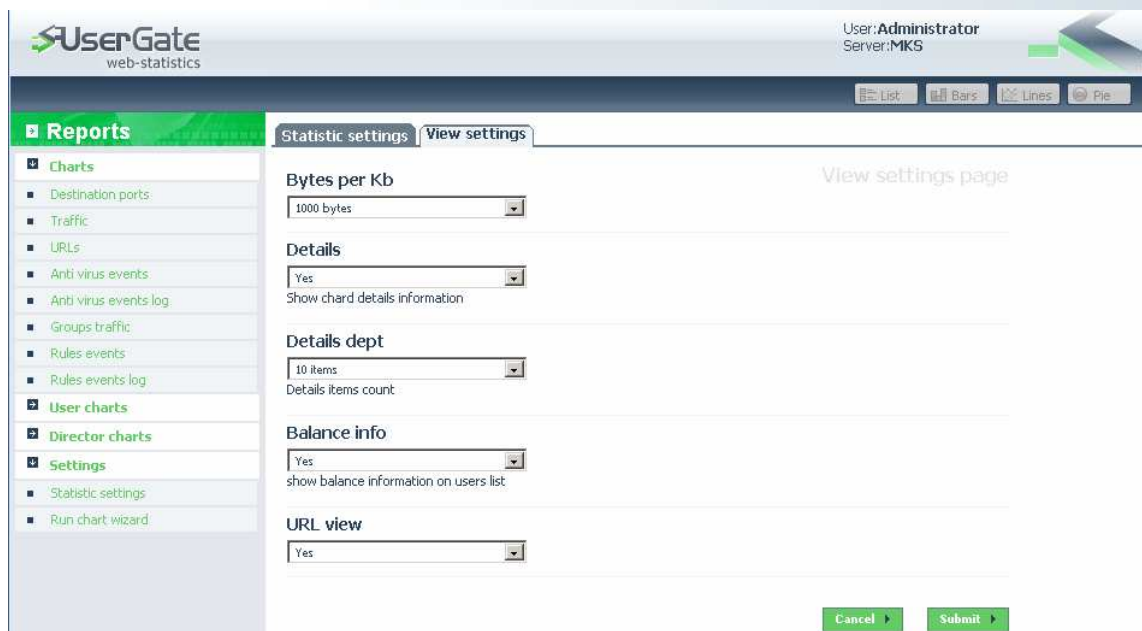
Statistic information is reflected now not only in the table (map) form, but also in the graphic shape (e.g. diagram) that makes the reports easier to view.

## Web Statistics possibilities

In the Statistics settings you can select a regional adjustment, the cache being used and keeping time, and the overhead information recording.



Statistic imaging allows for the setting of the number of bytes per kilobyte in much the same way a provider detects it; you can also indicate the information specification details and the URL addresses showing. In order to avoid excess loading of the Statistics screen it is possible to turn off a user's balance display (if you do not apply the Billing option).



## Opportunities for diagrams creation and editing:

- Three access levels to the information: User, Superior (Chief) and Administrator.
- Five diagram forms: linear, pie chart, bar chart, listing and grouping list.
- Option of data type, data grouping and data filtering.
- Option of few graphics exposure within the bounds of one diagram.

To create a diagram the Administrator should specify a name for the diagram, its visibility type, data grouping, and detect the users entitled to chart viewing. Then it is possible to create the necessary graphics.

The screenshot displays the 'UserGate web-statistics' interface. At the top right, it shows 'User: Administrator' and 'Server: MKS'. Below the navigation bar, there are tabs for 'Usergate', 'Events', and 'Antivirus'. The main content area is titled 'Usergate chart wizard page' and contains the following fields:

- Chart name:** A text input field containing 'New Chart'.
- Time interval:** A section with four radio buttons: 'Per day', 'Per week', 'Per month', and 'Custom interval'. A 'Selected interval' box shows 'from 23.09.2008 00:00 till 23.09.2008 23:59'.
- Chart type:** A dropdown menu currently set to 'Pie chart'.
- Data grouping:** A dropdown menu currently set to 'Group by type'.
- Chart visible:** A dropdown menu currently set to 'Common chart'.

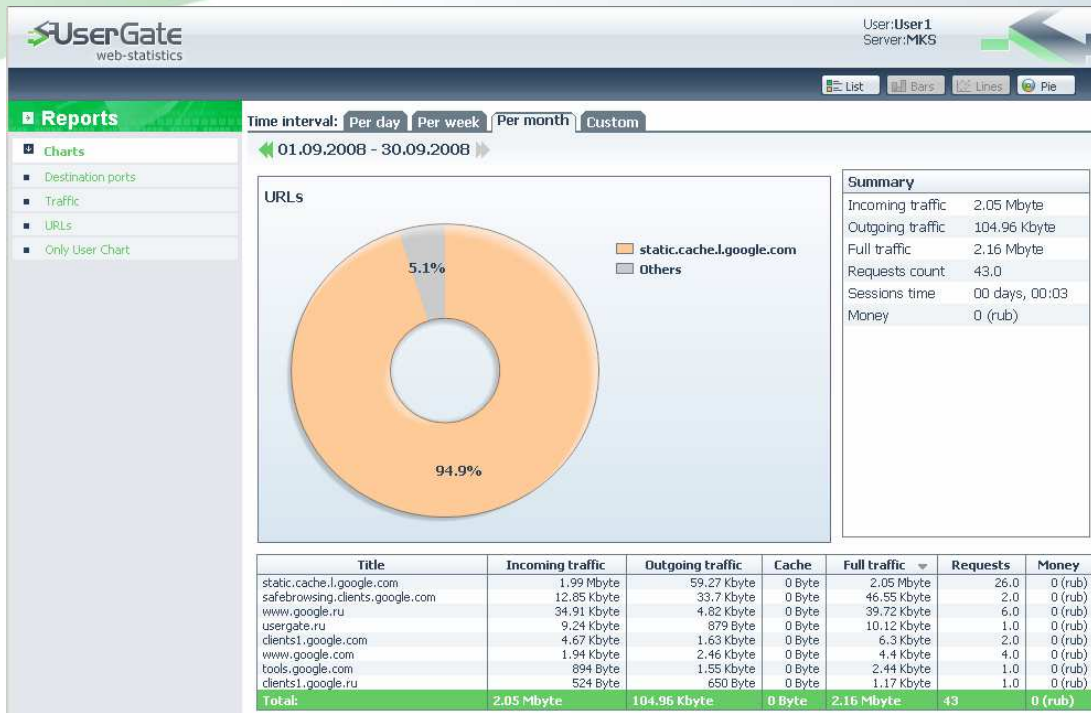
At the bottom of the form, there are three buttons: 'Edit graphic', 'Cancel', and 'Save'.

## Viewing Statistics possibilities:

- The reporting period (day, week, month, random period)
- A modification of the graphic view among the available ones
- Column grading (in the linear types).

## Possibilities of the 'User' level:

- Default browsing; view of the graphics created and assigned by the Administrator.
- User can see only those statistics concerning him.



### Possibilities of the 'Chief' level:

- Default browsing; view of the graphics created and assigned by the Administrator as well as the browsing of the graphics accessible to the 'User' category.
- A user at the 'Chief' level is entitled to see the common statistics over all users and also individual statistics per each user.



### Possibilities of the 'Administrator' level:

- Viewing, editing and creating of the all graphics types and Web Statistics displaying.

