

Service Managed Gateway™

Managing User Limits on the Service Managed Gateway



Issue 1.1

Date 28 July 2010

| | | |
|------------|---|-----------|
| 1 | About this document | 3 |
| 1.1 | Scope | 3 |
| 1.2 | Readership | 3 |
| 1.3 | More information..... | 3 |
| 1.4 | Terminology | 3 |
| 2 | Introduction | 4 |
| 2.1 | How user limits work | 4 |
| 3 | Configuring the SMG..... | 5 |
| 3.1 | Enabling flow monitoring on the SMG..... | 5 |
| 3.2 | Configuring user limits on the SMG | 7 |
| 3.3 | Saving your configurations..... | 10 |
| 4 | Diagnostics..... | 12 |
| 4.1 | Monitoring user limits | 12 |
| 4.2 | Monitoring user limits with the firewall log | 13 |

© 2010 Virtual Access (Irl) Ltd. This material is protected by copyright. No part of this material may be reproduced, distributed, or altered without the written consent of Virtual Access. All rights reserved. All trademarks, service marks, registered trademarks and registered service marks are the property of their respective owners. Virtual Access is an ISO 9001 certified company.

1 About this document

1.1 Scope

This document explains:

- how the SMG enforces user limits,
- how to configure user limits, and
- how to diagnose problems with user limits.

1.2 Readership

This document is for engineers who have previous experience configuring and managing Service Managed Gateways (SMGs).

1.3 More information

For more information about managing the SMG, read the Service Managed Gateway documentation. The current documentation is available online at <http://virtualaccess.com/smgdocs/>

1.4 Terminology

| | |
|-------------------|--|
| IPAT (NAT) | IP Address Translation (Network Address Translation) |
| SMG | Service Managed Gateway |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |

2 Introduction

The GL6000 Service Managed Gateways (SMGs) have a limit of 5 simultaneous network users.

The GW series of SMGs has a user limits feature. You can configure the GW series user limit for a maximum of 999 users or fewer. Enabling user limits on the GW series also enables per-user flow statistics.

2.1 How user limits work

A network user is a local PC or other device that:

- establishes one or more TCP connections to a remote system, and
- routes packets for the connections through the SMG.

User limits places a limit on the number of different network users' access. However, there is no limit on the number of simultaneous Transmission Control Protocol (TCP) connections a network user can establish. User Datagram Protocol (UDP) and other non-TCP traffic are not limited. TCP connections connected directly to the SMG for management and configuration are not counted as active users.

To restrict the number of clients on a particular interface, this interface must have either IPAT (NAT) or flow monitoring enabled. If IPAT or flow monitoring are not enabled, then enabling user limits has no effect.

The SMG dynamically keeps track of active network users. If the maximum number of active users is not reached, the first TCP connection from a new user succeeds. But if the maximum number of active users is reached, a new user cannot create a TCP connection and the connection attempt fails.

By default, the user session is active until 30 minutes after their TCP connections close.

3 Configuring the SMG

The Service Managed Gateway (SMG) contains an internal web server that is used to configure the SMG. Before you can access the internal web server and start the SMG configuration, you must ensure that your PC has the correct networking set up.

When your Service Managed Gateway is correctly connected to your PC, type `fast.start` into the URL line of your browser to display the Start page.

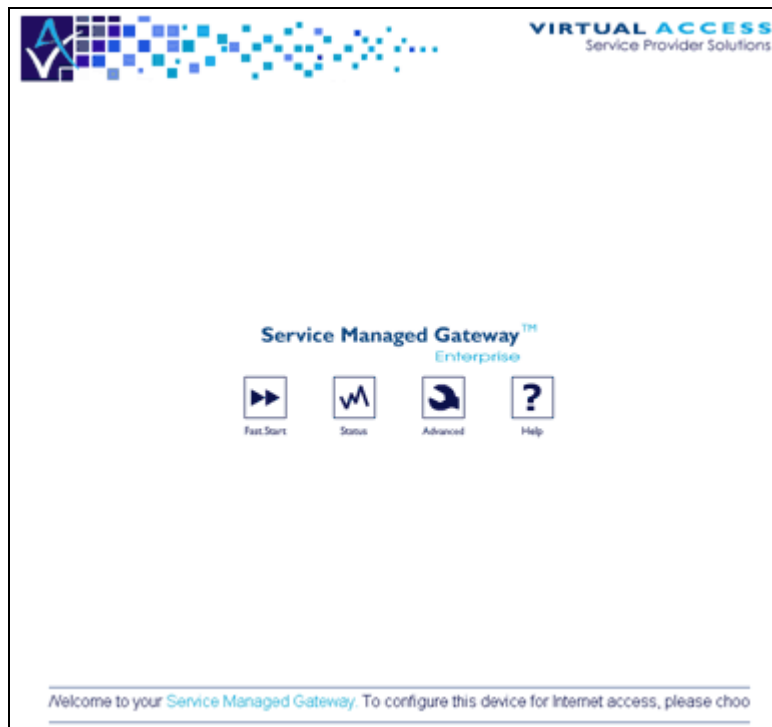


Figure 1: The SMG start page

If a login page appears type in the login password you received from your administrator.

If you have not received a password, contact the Virtual Access Support team.

Access the Fast Start Wizard by clicking the Fast.Start icon on the Start page of the embedded web.

The Fast Start Wizard will guide you through a series of forms that you must complete to configure your SMG.

3.1 Enabling flow monitoring on the SMG

If the interface that user limits is required to police does not have IPAT (NAT) enabled, you must enable flow monitoring on that interface.

To configure flow monitoring on the SMG, click **Advanced** on the SMG Start page. The Advanced menu appears.

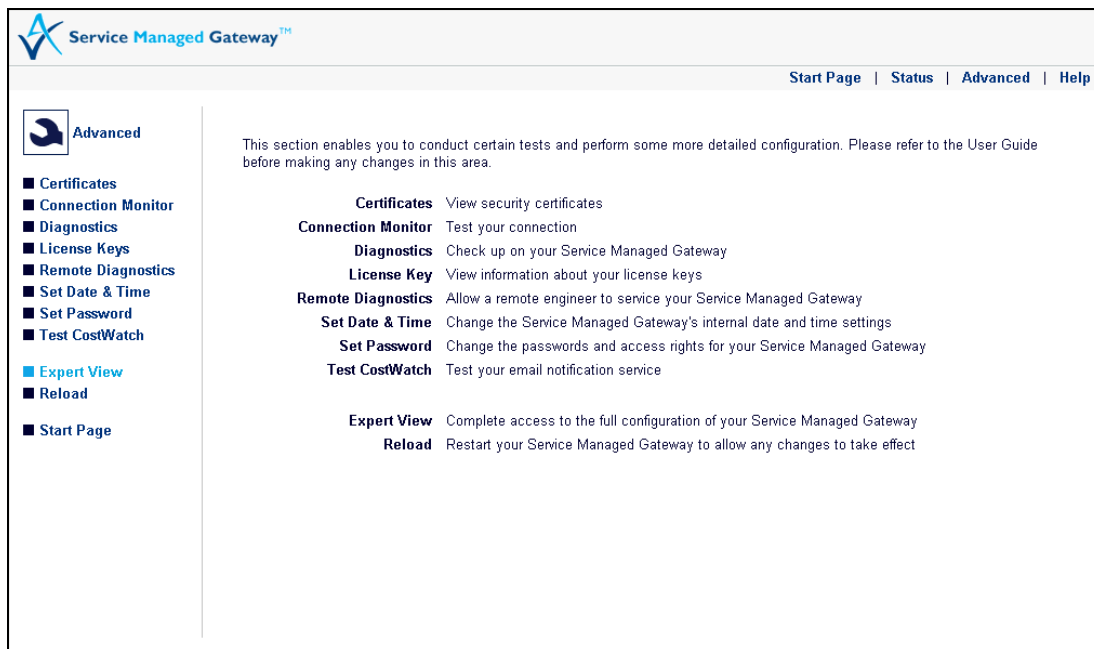


Figure 2: The advanced menu showing the expert view menu

In the left-hand menu, click **Expert View**

In the Expert View menu, select **interfaces -> interface-x -> ip -> ip**, where -x is the interface number. The following example shows how to enable flow monitoring on eth-1.

On the Interface page, click **Advanced** to view the advanced configuration options.

The screenshot shows the 'LAN IP Interface on eth-1' configuration page. The left-hand menu is expanded to 'ip', and the 'Flow Monitoring Enabled' option is highlighted with a red box. The configuration parameters are as follows:

| Parameter | Value |
|-------------------------------|---------------|
| Enabled | yes |
| IP Address | 0 0 0 0 |
| IP Address End | 0 0 0 0 |
| Mask | 255 255 0 0 |
| Metric | 1 |
| MTU | 1500 bytes |
| Maximum Reassembly Size | 65535 bytes |
| ICMP Mask Reply Enabled | yes |
| ICMP Mask Request Enabled | yes |
| ICMP Redirect Enabled | yes |
| Flow Monitoring Enabled | yes |
| Flow Monitoring Drop Unknown | no |
| Secondary IP Address Enabled | no |
| Secondary IP Address | 0 0 0 0 |
| Secondary IP Address Mask | 255 255 255 0 |
| TCP Largest MSS | 0 |
| Treat as Wan Interface | no |
| VPN Source Network | 0 0 0 0 |
| TCP Window Adjustment Enabled | no |
| TCP Window Size | 2048 |

Buttons at the bottom: Update, Delete, Standard

Figure 3: The advanced IP configuration on the interface on eth-1 page

On the interface on IP Interface page, set Flow Monitoring Enabled to **yes**. Leave all other parameters set as default.

Click **Update**. You can leave saving your configuration until you have made all the configuration changes you need to. For more information, read section 3.3, 'Saving your configurations'.

3.2 Configuring user limits on the SMG

To configure user limits on the SMG, click **Advanced** on the SMG Start page. The Advanced menu appears.

In the left-hand menu, click **Expert View**.

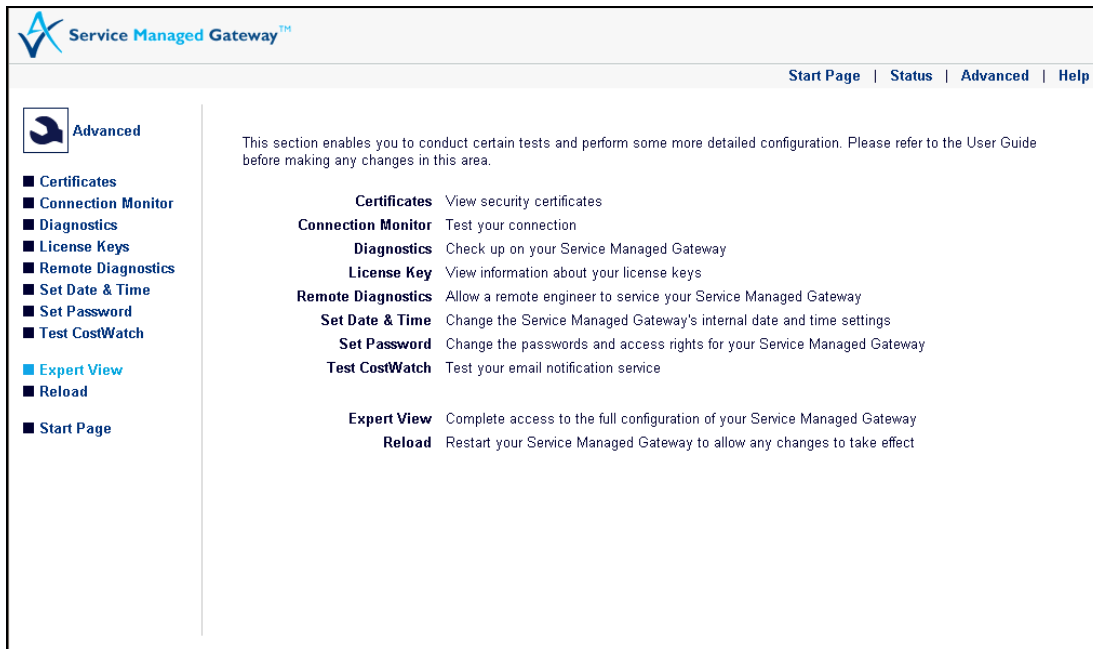


Figure 2: The advanced menu showing the expert view menu

In the Expert View menu, select **system -> security -> user limits**. The User Limits page appears.

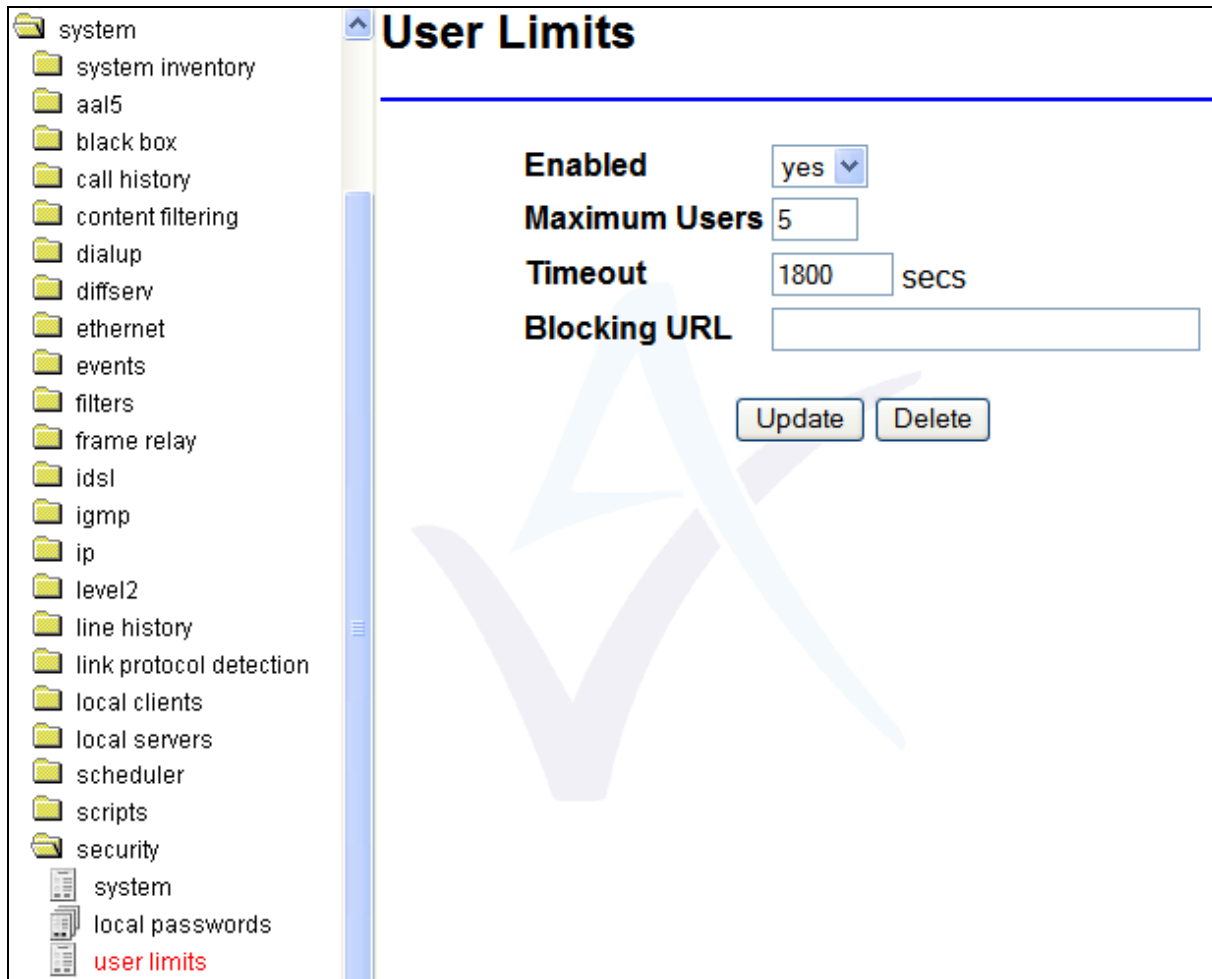


Figure 4: The user limits page

| Field | Description | Command Line | | |
|----------------------|---|---|------------|----------------------|
| Enabled | Enables or disables user limits. | Set IP Address translation user Limit enabled = | | |
| | <table border="1"> <tr> <td>yes</td> <td>Enables user limits.</td> </tr> <tr> <td>No</td> <td>Disables user limits.</td> </tr> </table> | | yes | Enables user limits. |
| yes | Enables user limits. | | | |
| No | Disables user limits. | | | |
| Maximum Users | Sets the maximum number of users that are allowed to use the Internet connection on the gateway simultaneously. | Set IP Address translation user Limit Count = | | |
| | Minimum Value | | 1 | |
| | Default Value | | 5 | |
| Maximum Value | 999 | | | |
| Timeout | Controls how many seconds the system will wait after a user closes their final connection, before freeing up a connection slot for another user to use. | Set IP Address translation user Limit timeout = | | |
| | Minimum Value | | 1 | |
| | Default Value | | 1800 | |
| Maximum Value | 999999 | | | |
| Blocking URL | Defines an optional URL to be used when a client tries to access a web page on port 80, | Set IP Address translation user | | |

| | | |
|--|--|--------------------|
| | <p>but exceeds the number of allowed users. By default, this setting is empty which will cause the router's built-in page user limits web page to be displayed. This page displays an error message, and, for local clients, a summary of which clients are currently using the connection.</p> <p>The field may be set to a URL string.</p> | Limit Blocking URL |
|--|--|--------------------|

Table 1: Fields and values for user limits configuration

Click **Update**. The Configuration Update Result page appears.

3.3 Saving your configurations

Configuration Update Result

Status Configuration committed successfully

Errors None

Save Changes will be lost unless [saved to flash](#)

Reboot? The system must be [reloaded](#) before all changes will come into effect

[Return to previous page](#)

Figure 5: The configuration update result page

Click **saved to flash**. The Save Configuration to Flash page appears.

Save Configuration to Flash

The last flash configuration loaded was **config1**.
When the system is next rebooted, **config1** will be loaded.

Some of your [recent changes](#) have not yet been saved to flash.

Save Committed Changes To Config 1 ▼

Figure 6: The save configuration to flash page

Click **Save**. The Configuration Saved page appears.

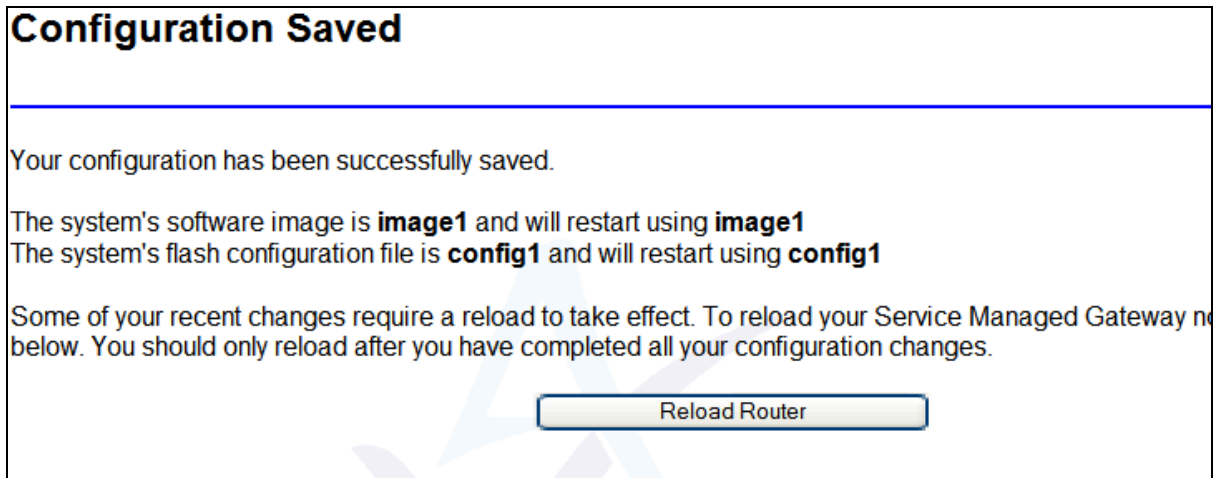


Figure 7: The configuration saved page

Click **Reload Router**.

The Reload Router button shows a progress timer and then the page returns to the Fast.Start page.

You can leave saving your configurations until you have made all the configuration changes you need to.

4 Diagnostics

The Service Managed Gateway supports extensive remote diagnostics, status and SLA monitoring capabilities.

The status and diagnostics tools are provided as a series of Java applets.

4.1 Monitoring user limits

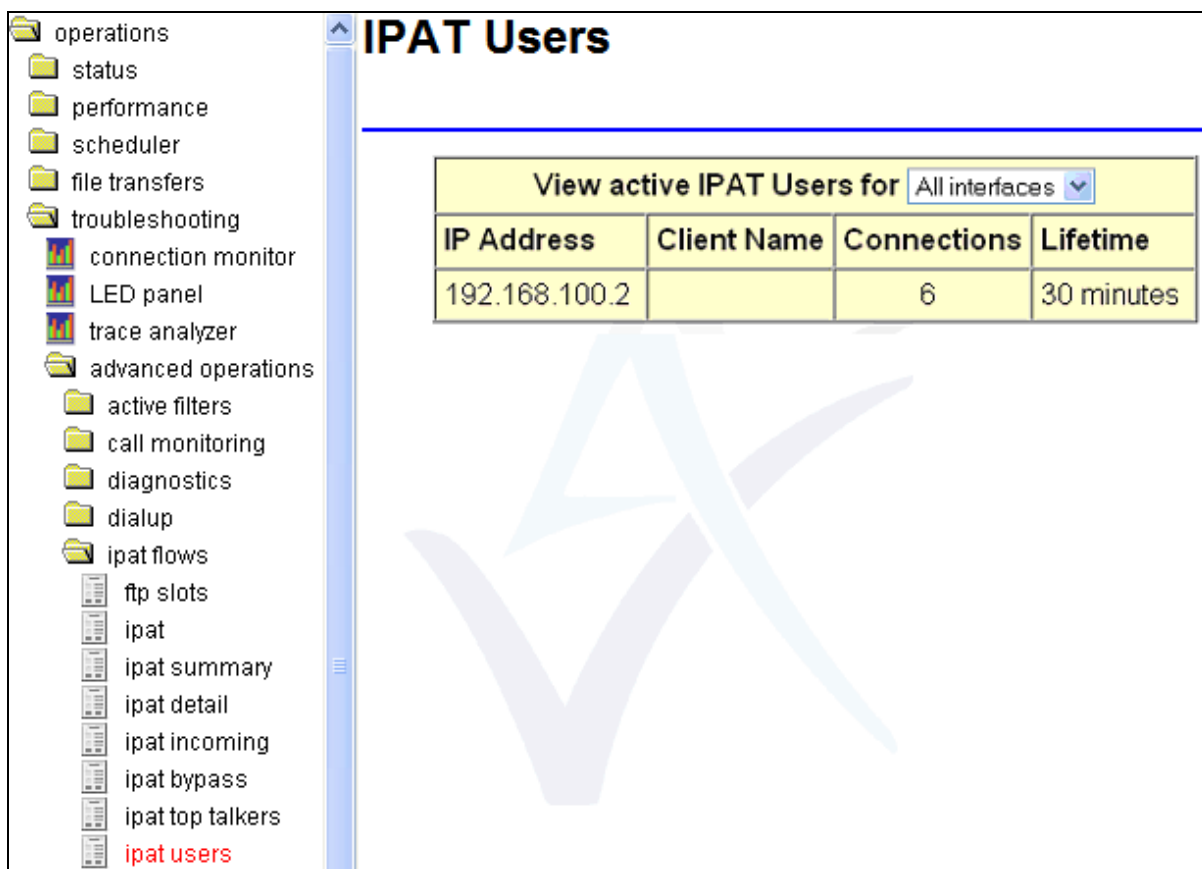
On the SMG Start page, click **Advanced**.

In the Advanced menu, click **Expert View**.

In the Expert View page on the top menu, click **Operations**.

In the Operations menu, select **operations -> troubleshooting -> advanced operations -> ipat flows -> ipat users**. The IPAT Users page appears.

From the drop down menu select **All interfaces**.



The screenshot shows the 'IPAT Users' page in a web application. On the left is a navigation tree with folders like 'operations', 'status', 'performance', 'scheduler', 'file transfers', 'troubleshooting', 'connection monitor', 'LED panel', 'trace analyzer', 'advanced operations', and sub-items under 'ipat flows' including 'ftp slots', 'ipat', 'ipat summary', 'ipat detail', 'ipat incoming', 'ipat bypass', 'ipat top talkers', and 'ipat users' (highlighted in red). The main content area is titled 'IPAT Users' and contains a table titled 'View active IPAT Users for' with a dropdown menu set to 'All interfaces'. The table has four columns: 'IP Address', 'Client Name', 'Connections', and 'Lifetime'. One row is visible with the IP address '192.168.100.2', 6 connections, and a lifetime of 30 minutes.

| View active IPAT Users for All interfaces | | | |
|--|-------------|-------------|------------|
| IP Address | Client Name | Connections | Lifetime |
| 192.168.100.2 | | 6 | 30 minutes |

Table 3: The IPAT users' page showing active users

By default, if a client tries to access a web page on port 80 (HTTP) when the number of users is exceeded, the following web page is displayed in the client's browser. It displays an error message and for local clients, a summary of which clients are using the connection.

Maximum number of web users exceeded.

The limit of 5 simultaneous web users has been reached. Please wait until one of the other users has finished using the network.

| Client Name | IP Address | Connections | Lifetime |
|-------------|-----------------|-------------|------------|
| Saturn | 192.168.100.100 | 0 | 26 minutes |
| Jupiter | 192.168.100.101 | 5 | 30 minutes |
| Mars | 192.168.100.107 | 6 | 30 minutes |
| Venus | 192.168.100.109 | 0 | 14 minutes |
| Neptune | 192.168.100.102 | 0 | 3 minutes |

For more information, please contact your service provider.

Figure 4: The maximum number of users exceeded page

4.2 Monitoring user limits with the firewall log

To view information on flows going through the SMG, you must enable the firewall log. For detailed information on enabling a firewall log, read the user guide 'How to Configure Firewall Logging'.

To view the firewall log, in the Expert View menu, click **Operations** in the top menu.

In the Operations menu, click **operations -> troubleshooting -> firewall -> firewall log viewer**.

The screenshot shows the 'Firewall Log' interface. On the left is a navigation tree with 'firewall log viewer' selected. The main area displays a table of log entries. The entry at index 33105 is highlighted in red and contains the text: '33105 Apr-30-2009 11:15:41 R eth-2 Px00 !User Flow 82.195.146.64->192.168.102.100'. Other entries show various TCP and UDP flows.

Figure 5: The firewall log page

When you exceed user limits, **!User Flow** is displayed on the firewall log list.