1) **Monitor Bandwidth and Limit Internet Speed in Forefront TMG 2010**

**Features:**

- New: It is possible to setup multiple traffic quotas that apply to the same client
- Full integration with Forefront TMG/ISA Server and its management console (remote control being possible as well)
- Forefront TMG/ISA Server arrays with multiple servers are supported (Bandwidth Splitter synchronizes its activity between all array members, so that limits are applied to entire array as a whole and not per server)
- Managing the traffic of all HTTP, HTTPS and FTP connections (for web proxy clients) and TCP/UDP connections (for FWC and SNAT clients). It is also capable to manage all TCP/UDP traffic of DMZ servers and all others that use Forefront TMG/ISA Server as NAT or router (but not in ISA Server 2000).
- Managing the traffic of published servers
- Setting up the allowable bandwidth for individual users (by AD accounts) and hosts (by IP addresses) and groups of users and hosts
- Transparency for users: you do not need to install any software on client computers
- Real time monitoring of all users and hosts that access Internet through Forefront TMG/ISA Server with detailed information on all their connections, including bandwidth usage graphs for individual users and connections
- Bandwidth usage reports
- Web statistics for users
- Flexible allocation of bandwidth depending on the time of the day or the day of the week (Schedules) and requested server addresses (Destinations)
- Even bandwidth distribution for users inside groups (in case bandwidth is allocated to a group of users)
- Even distribution of bandwidth for the active connections of each user
- It is possible to set speed limits and quotas separately for incoming and/or outgoing, or total (incoming + outgoing) traffic
- Limiting the number of simultaneous connections from individual users and hosts
- For some types of web pages, you can set the download speed higher than the standard speed not to let the restrictions slow down the normal work of users (HTTP Boost)
- Setting traffic quotas for users, hosts, groups of users and groups of hosts per day, week, month or without any time limitations along with a possibility to automatically reallocate the unused traffic to the next period
- It is possible not to take the traffic to specified destinations or at specified time into account in traffic usage counters (this is useful if there is a high-speed connection with some networks and there is no need to limit that traffic, or if you need uninterruptable access to some servers to which quota should not apply)
✓ It is possible to not just block users’ access to Internet when their traffic quota has been exceeded, but instead to use a different shaping rule (probably with a stricter speed limit), without blocking access to Internet
✓ It is possible to customize web pages that users see when their quota exceeded
✓ Bandwidth Splitter is permanently tested and observed in environment with thousands of users. This helps us to ensure product stability and performance.
✓ Free if used with up to 10 clients

You can request your feature or support ideas proposed by other users by following this link, or by using the button in bottom-right corner of this web page.

**Connections Serviced**

Bandwidth Splitter is built into Forefront TMG/ISA Server using web and application filters to control most traffic going through Forefront TMG/ISA Server.

Bandwidth Splitter has power to control:

✓ Outgoing web proxy connections (HTTP, HTTPS and FTP)
✓ Connections of Firewall clients (all TCP/UDP connections)
✓ Connections of SecureNAT clients (all TCP/UDP connections)
✓ Connections of published servers
✓ Connections established through application filters (the built-in SOCKS4 filter or third-party SOCKS5 filters)
✓ Connections of the Scheduled Content Download/Job Scheduler service
✓ All routed TCP/UDP connections passed through Forefront TMG/ISA Server (from DMZ servers, etc) (not possible in ISA Server 2000)

Bandwidth Splitter do not control:

✓ Low-level, non TCP/UDP based protocol connections (e.g. ICMP)
✓ Connections between the Local Host network and any internal network (any except External). It is done intentionally because these connections are especially critical, and generally they do not need any bandwidth control.
✓ In version for ISA 2000 only: Routed IP packets (set up in IP Packet Filters) including all data going from/to the DMZ area

**How it works?**

Unlike numerous other tools for Forefront TMG/ISA Server that just count traffic by analyzing log files, Bandwidth Splitter deeply integrates into Forefront TMG/ISA Server to control most of the traffic. However it does not install any network drivers. Bandwidth Splitter operates using web filter to control web traffic (HTTP, HTTPS and outbound FTP), and application filter to control all other TCP/UDP traffic. These filters extend Forefront TMG/ISA Server functionality
allowing you to count and shape traffic. This means that Bandwidth Splitter is just an add-on for Forefront TMG/ISA Server for traffic/bandwidth management. It does not brake or replace Forefront TMG/ISA Server security or functionality.

Because of that integration with Forefront TMG/ISA Server, Bandwidth Splitter can shape traffic based on user accounts (not only by IP addresses) regardless which workstations are used by clients.

Forefront TMG allows you to create scheduled rules that grant or deny access to a system or user. The problem is that this is a binary ‘off or on’ option. It also has a limitation in that it will not close any active sessions. For example, a large download will not be stopped once the schedule becomes active.

**Using Bandwidth Splitter**

Bandwidth Splitter is a very good and cost effective tool for implementing more flexible bandwidth control in Forefront TMG. It is also very capable and supports arrays.

One really nice feature is that allows you to not only limit the user’s available bandwidth but you can also set usage caps. What makes it even better is that you can specify a soft cap after which the bandwidth is further throttled or shaped. Bandwidth Splitter has the ability to do this for authenticated users based on their AD username, as well as for IPs. Check the Bandwidth Splitter site for more information.

This guide will step you through using Bandwidth Splitter for the following use cases:

- Ensure no user has more than x amount of bandwidth available
- Set a soft cap after 100MB of data usage the resets daily
- Throttle a user to a very low bandwidth once the cap is reached

**Creating The Shaping Rules**

1. **Limit the maximum bandwidth per user**

This first rule will limit the maximum bandwidth available for each user in your ‘Internal’ network.

   1. Open the Forefront TMG Management console
   2. Expand the **Bandwidth Splitter** Section
   3. Right click **Shaping Rules** and select **New | Rule**
   4. Name the rule ‘Pre-cap shaping’
   5. Select **IP address sets specified below**
   6. Click **Add | Networks | Internal**
   7. Click **Next**
8. On the Destinations page click Add | Networks | External and click Next

9. On the Schedule page, select Always then click Next
10. On the Shaping page select ‘Shape incoming and outgoing traffic’
11. Specify the Maximum available incoming and outgoing bandwidth values Note: this is in kbits/s and not KB/s
12. Click Next

13. Do not limit the number of concurrent connection. Click Next
14. On the Shaping Type page select ‘Assign bandwidth individually to each applicable user/address’
15. Click Next
16. On the Extra Parameters page do not check any boxes. Click Next
17. Click Finish to create the rule.

2. Throttle bandwidth once the usage cap is reached

We now need to create another rule to limit the maximum bandwidth available once the usage cap is reached.

Follow the same process above but with the following changes:

1. Name the shaping rule ‘Post-Cap Shaping’
2. On the Shaping page select a smaller kbits/s value

3. On the Extra Parameters page check Apply this rule only when traffic quota is exceeded
Reorder the rules and apply changes

You should now have two rules in the Rules list. You need to reorder the Post-Cap shaping rule above the Pre-Cap Rule. To do this:

1. Right click the ‘Post-Cap rule’ and select Move Up
2. To apply these changes to Forefront TMG you need to click the green check button in the toolbar.

Creating the Bandwidth Cap / Quota Rule

The following rule will set the limit for “high bandwidth” usage. After this amount of data has been used the “lower bandwidth” limit is enforced.

1. Open the Forefront TMG Management console
2. Expand the Bandwidth Splitter Section
3. Right-click Quota Rules | New | Rule
4. Name the rule ‘Soft Data Cap’
5. Select ‘IP address sets’ specified below
6. Click Add | Networks | Internal
7. Click Next
8. On the Traffic Quota page select ‘Limit total traffic (incoming+outgoing)’
9. Specify the Total MB value you want to allow
10. Select the Reset period to ‘Daily’. Click Next
11. On the **Quota Type** page select ‘Assign quota individually to each applicable user/address’
12. Click **Next** and click **Finish**
13. Apply the rule to the Forefront TMG configuration with the green check button in the toolbar.

**Testing the configuration**

Since the data caps and available bandwidth is not visible to the user during normal usage it is a little trick to test the effectiveness of your rules. To test the configuration yourself, set a low quota so that you can easily hit the soft cap. You can watch the usage graphs in the bandwidth manager console but a more graphic way of doing is as follows:

1. Use a speed benchmark tool like [http://speedtest.net](http://speedtest.net)
2. Run a benchmark test before you consume any of your cap data. This would give you an indication of what your maximum throughput is.
3. Generate enough data to use up your cap (Google Earth does this very quickly)
4. Once things start to slow down, run the speed test again. You should now see the data rate being pegged to your low limit.

That’s all there is to it. This is a basic example for some common use cases, and should hopefully give you a good indication to the bandwidth management potential using Bandwidth Splitter.
2) **New Rule:**

Right click on Shaping Rules>New>Rules. Follow the wizard and select as appropriate.

---

Your ads will be inserted here by

**Easy Ads.**

Please go to the plugin admin page to paste your ad code.
Welcome to the New Shaping Rule Wizard

This wizard helps you create a new shaping rule. Shaping rules determine where, when and how much bandwidth specified users allowed to use.

Note: Be sure to create new rule elements required by the rule before you use this wizard.

©2011 MicrosoftGURU.com.au

Shaping rule name:
Shape 1

To continue, click Next.

New Shaping Rule Wizard...

Applies To
Specify client type and clients to which this rule applies.

This rule applies to traffic from these sources:
- IP address sets specified below
- User sets specified below

Applies to requests coming from:

User Sets
- All Authenticated Users

Note: If rule is applied to user sets, those users should be authenticated. For that they should be allowed in generic Firewall Policy rules as authenticated users, that is at Users tab you should specify something other than All Users.
New Shaping Rule Wizard...

Shaping Type
Specify one of two possible methods how shaping rule should be applied.

- Assign bandwidth individually to each applicable user/address
- Distribute bandwidth between all applicable usersaddresses
- Static bandwidth distribution

©2011 MicrosoftGURU.com.au

< Back  Next >  Cancel  Help

New Shaping Rule Wizard...

Extra Parameters
Specify additional parameters for this rule.

Apply this rule only when client's traffic quota has been exceeded.
Internet access will not be blocked in this case.
(By default this option is unchecked, which means that this rule will be applied in any case. And if client's traffic quota is exceeded, access will be blocked.)

©2011 MicrosoftGURU.com.au

< Back  Next >  Cancel  Help
To create quota for a group, right click on quota rule>New>rule.

Follow the wizard and select as appropriate for your infrastructure.

Once finished. Apply changes.
3) Creating rules with Bandwidth Splitter

You can create two types of rules with Bandwidth Splitter:

- Shaping rules, which control which users can access which resources at what speeds, at what times.
- Quota rules, which control the overall usage allowed per day, week or month, or without time limits.

You really have a lot of flexibility, as you can set schedules so that a particular user (or group or computer) is limited to a specified speed during one timeframe, but a different speed at a different time. You can even configure different speed limits and quotas for incoming and outgoing traffic. Another nice option is to let users’ or hosts’ bandwidth allocations “roll over” to the next time if they don’t use their entire allocations. I also like that you can exclude the traffic to some specific destinations or during specific times from the usage counters while limiting the traffic to other destinations or during other times.

Creating a rule is simple. Just right click the appropriate node in the left pane of the TMG management console (Shaping Rules or Quota Rules) and click New, and then Rule. This invokes the wizard, with which you can choose to apply the rule to IP address sets or user sets, as shown in Figure 2, where we are creating a new shaping rule that applies to the computer named SEVEN-RC.

![Figure 2: You can apply rules to IP address sets or user sets](image-url)
Next, you select the destinations to which the rule applies. Thus you can control that computer’s or user’s traffic to a particular network, network set or computer. At first I was unsure if you are able to specify times granularly, but with some help, I found that you can select any schedule defined in the array. To do this, you need to create them in the Firewall Policy>Toolbox>Schedules folder. You will then be able to choose them in the shaping rules. The same applies to all rule elements you want to use in shaping or quota rules (user sets, computer sets, etc.).

The next dialog box is where you determine how this rule will function. First you select whether to do no shaping, shape total traffic (incoming + outgoing), shape incoming and outgoing traffic separately; shape incoming traffic only or shape outgoing traffic only. Then you can set the bandwidth limits in kilobits per second (kbits/s), as shown in Figure 3.

![New Shaping Rule Wizard](image)

**Figure 3:** Setting bandwidth limits on incoming and/or outgoing traffic is called shaping

HTTP boost lets you set the bandwidth speed higher than normal for downloads from certain types of web pages, so that users who have been inactive for a specified minimum amount of time can work at higher speed, and you can also control the duration of the boost as well as the inactivity period. You set the types of content for which HTTP boost will be used in the Advanced tab of Bandwidth Splitter’s General options.

The next page lets you limit the number of concurrent connections from this user or computer. If you’ve applied the rule to a set of users or IP addresses, you can select whether to assign bandwidth individually to each applicable user/address, or distribute the allocated bandwidth between all of the users/addresses. Finally, you can choose to apply the shaping rule only when
the client’s quota has been exceeded. That makes it possible for you to drop the client’s bandwidth speeds, instead of denying Internet access altogether when the quota is reached.

And that’s all there is to it; just click Finish to close the wizard, as shown in Figure 4.

Figure 4: After you complete the wizard, you can review a summary of the rule

Creating a quota rule is similar; in this case, you can set limits in the same way (on total traffic, incoming and outgoing separately, incoming only or outgoing only), specifying the amount of bandwidth in megabytes for a daily, weekly or monthly period (or selecting “Never” for no time limit). You can also select not to count cached web pages if you’re limiting incoming traffic, and you can select to transfer the remainder of the allocation to the next time period if it isn’t all used, as shown in Figure 5.
Figure 5: Configuring quota rules is just as easy as creating shaping rules.

Again, if this rule applies to a set of users or computers, you can assign quotas individually or share the quota between the members of the set.

Once you’ve created your rules, they show up in the right pane, as shown in Figure 6.

Figure 6: Your rules are displayed in the right pane of the TMG management console.
Quota Counters, Monitoring and Advanced Options

The quota counters node in the TMG management console gives you information about the objects (users, groups, computers) that are subject to traffic quota rules. It shows you the quota rule(s) applied to the object, how much of the allocated bandwidth is remaining and the quota reset period. A nice touch is that the administrator can manually change the counter of remaining traffic in the object’s properties.

The monitoring node is nice, too (Figure 7). It allows you to see, in real time, the activity of all clients that are accessing the Internet through TMG, along with the shaping and quota rules that are applied to each. You see the IP address, user name, quota allocation remaining and bandwidth speeds. Unfortunately, you can’t disconnect users through this interface.

![Figure 7: Monitoring allows you to see all active users and their connections in real-time](image)

If you want to collect bandwidth usage statistics, you enable that by right clicking the top Bandwidth Splitter node in the TMG console’s left pane, selecting Properties and then the Database tab. Check the box to enable collecting of bandwidth usage statistics, as shown in Figure 8. Note that before you can configure the connection settings for collecting statistics, you need to have the second database and tables set up. Check the documentation for info on how to do that.
Figure 8: You can enable collection of bandwidth usage statistics but you’ll need a second database set up first.

When you enable logging of usage statistics, you can create nice reports that can show usage by individual users or IP addresses, filtered by day, week, month, hour, day of the week and so forth. You can generate a report manually or schedule them to be run at specified times, and you can have them automatically sent to you via email.

Figure 9: Sample bandwidth usage report.
On the Advanced tab of that same dialog box, you’ll find a number of miscellaneous options that you can configure. For example, you can get a more exact appraisal of header packet size for UDP connections by checking the box to count packet headers. Unfortunately, this isn’t available for TCP connections. This tab is also where HTTP Boost is enabled or disabled (it’s enabled by default) and you can choose whether to treat connections from the External network as accepted/inbound. You can also choose here to deny connections when no quota or shaping rules exist (this is turned off by default and probably should stay that way in most situations, but it’s nice to have the option).

An important factor with any essential software is the ability to get back up and running if something happens to your system, and Bandwidth Splitter lets you save its configuration to a file so you can easily restore it. Quota counter values aren’t exported, but the general settings, shaping and quota rules and rule details such as user sets, network objects and schedules are.

**Conclusion**

Bandwidth Splitter is all about options. It seems the makers of Bandwidth Splitter have thought of every contingency, so that you can make exceptions when necessary without jumping through a lot of hoops. I like the simplicity with which you can set up sophisticated rules that give you fine tuned control over bandwidth usage, and a graphical interface that is integrated into TMG and does exactly what a GUI should do: makes most tasks so intuitive that you don’t even need to consult the documentation.

It’s not often you find a program that combines such simplicity of use with such complexity of function. If you’ve been wishing ISA/TMG allowed you to go beyond security and provide more control over Internet usage, Bandwidth Splitter fits the bill. I had no trouble at all giving this product the Gold award.
4) Only Screenshots:
### Network Monitoring

<table>
<thead>
<tr>
<th>Service</th>
<th>Type</th>
<th>Dir.</th>
<th>State</th>
<th>Auth.</th>
<th>Method</th>
<th>Remote Name</th>
<th>Remote Address</th>
<th>Local Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>TCP</td>
<td>Out</td>
<td>Established</td>
<td>SNAT</td>
<td>GET</td>
<td>g0628.upc-g.chubb.nl</td>
<td>85.87.40.28</td>
<td>2046</td>
</tr>
<tr>
<td>Firewall</td>
<td>TCP</td>
<td>Out</td>
<td>Established</td>
<td>SNAT</td>
<td>GET</td>
<td>d130-251-166-62.add-versa...</td>
<td>62.146.251.133</td>
<td>2038</td>
</tr>
<tr>
<td>Web</td>
<td>TCP</td>
<td>Out</td>
<td>Connected</td>
<td>Basic</td>
<td>GET</td>
<td>64.16.163.132</td>
<td>64.12.165.132</td>
<td>60</td>
</tr>
<tr>
<td>Firewall</td>
<td>TCP</td>
<td>Out</td>
<td>Connected</td>
<td>SNAT</td>
<td>GET</td>
<td>dyan-09-145-13-24-app.dyn...</td>
<td>63.154.143.25</td>
<td>1375</td>
</tr>
<tr>
<td>Firewall</td>
<td>TCP</td>
<td>Out</td>
<td>Connected</td>
<td>SNAT</td>
<td>GET</td>
<td>freely2kolab.com</td>
<td>64.92.167.102</td>
<td>2041</td>
</tr>
<tr>
<td>Firewall</td>
<td>TCP</td>
<td>Out</td>
<td>Connected</td>
<td>SNAT</td>
<td>GET</td>
<td>db-kolab4-rebel100-115.dyn...</td>
<td>60.223.190.116</td>
<td>2496</td>
</tr>
<tr>
<td>Firewall</td>
<td>TCP</td>
<td>Out</td>
<td>Closed</td>
<td>SNAT</td>
<td>GET</td>
<td>d8833.dpopool.de</td>
<td>60.144.131.237</td>
<td>1214</td>
</tr>
<tr>
<td>Firewall</td>
<td>TCP</td>
<td>Out</td>
<td>Closed</td>
<td>SNAT</td>
<td>GET</td>
<td>d8833.dpopool.de</td>
<td>60.144.131.237</td>
<td>1214</td>
</tr>
</tbody>
</table>
# Report "Test" for period 01.05.2009 - 31.05.2009

<table>
<thead>
<tr>
<th>No</th>
<th>Client IP</th>
<th>User Name</th>
<th>General In</th>
<th>General In Graph</th>
<th>General Out</th>
<th>General Out Graph</th>
<th>General Total -</th>
<th>General Total Graph</th>
<th>Cache In</th>
<th>Cache In Graph</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>28.211</td>
<td>31 495-766 814</td>
<td>6 850 320 281</td>
<td>36 323 115 595</td>
<td>2 156 576 532</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>28.11</td>
<td>8 325-607 473</td>
<td>187 000 117</td>
<td>6 493 009 587</td>
<td>287 512 944</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>28.49</td>
<td>3 233-161 792</td>
<td>6 979 392 594</td>
<td>3 157 290 293</td>
<td>542 232 265</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>28.2</td>
<td>5 423 759 740</td>
<td>5 930 050 189</td>
<td>6 559 550 047</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>28.215</td>
<td>3 669 171 592</td>
<td>297 165 014</td>
<td>3 076 256 516</td>
<td>78 500 057</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>28.267</td>
<td>3 727 564 586</td>
<td>189 730 782</td>
<td>3 823 043 313</td>
<td>147 749 322</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>28.162</td>
<td>3 827 050 034</td>
<td>216 677 687</td>
<td>3 787 037 721</td>
<td>778 278 317</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>28.10</td>
<td>3 893 508 134</td>
<td>239 510 854</td>
<td>3 864 018 038</td>
<td>307 670 876</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>28.4</td>
<td>3 722 645 475</td>
<td>6 103 154</td>
<td>3 897 079 833</td>
<td>4 402 082</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>28.41</td>
<td>2 589 228 740</td>
<td>231 449 947</td>
<td>3 149 707 073</td>
<td>2 977 542</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>28.149</td>
<td>2 318 456 342</td>
<td>247 547 125</td>
<td>2 866 343 467</td>
<td>13 773 189</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>28.158</td>
<td>2 350 488 685</td>
<td>183 023 381</td>
<td>2 563 304 996</td>
<td>359 720 631</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>28.212</td>
<td>2 202 253 089</td>
<td>154 904 086</td>
<td>2 396 237 522</td>
<td>196 327 325</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>28.9</td>
<td>2 059 406 611</td>
<td>323 012 639</td>
<td>2 362 620 539</td>
<td>134 627 002</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>28.05</td>
<td>1 995 695 992</td>
<td>101 697 588</td>
<td>2 056 972 330</td>
<td>42 400 209</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>28.201</td>
<td>1 912 540 671</td>
<td>2 036 070 433</td>
<td>73 975 096</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>28.70</td>
<td>1 757 542</td>
<td>1 910 045 569</td>
<td>154 650 616</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>28.09</td>
<td>1 127 229 550</td>
<td>1 925 565</td>
<td>4 490 622 664</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>28.36</td>
<td>1 705 564 032</td>
<td>1 725 982 518</td>
<td>215 817 476</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>28.165</td>
<td>1 734 284 411</td>
<td>1 867 712</td>
<td>4 490 557</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Others**

| Total | 191 030 538 093 | 19 876 400 889 | 216 906 939 782 | 15 688 742 734 |

**Bandwidth usage stats** (Min, Max rates) are calculated over time intervals equal to 2 hour(s), 26 minute(s), 24 second(s).

### Bandwidth Graphs:
- Min Total Rate: 2 kbit/s
- Max Total Rate: 2580 kbit/s
- Avg Total Rate: 557 kbit/s
<table>
<thead>
<tr>
<th>Quota Description</th>
<th>In Quota Left</th>
<th>Out Quota Left</th>
<th>Total Quota Left</th>
</tr>
</thead>
<tbody>
<tr>
<td>Some quota description text visible to users</td>
<td>15.5 MB (15%)</td>
<td>≈3.2 MB (86%)</td>
<td>-</td>
</tr>
</tbody>
</table>