

# FlowTuner 1.0

Users Guide

# Table of Content

Introduction.....	3
What is FlowTuner.....	3
Fonts Conventions.....	3
Installation.....	5
System Requirements.....	5
VPN Basics.....	5
FlowTuner Installation.....	7
Networking Setup.....	8
VPN At Client Side.....	10
Operators Guide.....	11
How To Log In.....	11
FlowTuner Basics.....	11
First Steps.....	13
Administrators Management.....	13
Users Management.....	13
Options.....	14
If your are in trouble.....	16

# INTRODUCTION

---

Welcome to FlowTuner 1.0 Users Guide! In this introduction you can learn general information about FlowTuner, read about fonts conventions and how to read this guid.

## WHAT IS FLOWTUNER

FlowTuner is employee Internet activities management software. Features of FlowTuner 1.0 includes:

- Ability of setting Internet access quotas for individual employees and whole departments
- Automatical termination of Internet connection after quota exhausting
- Employees can view their Internet usage statistics in real time
- Easy to use web Interface
- Internet usage reports
- All calculations made in real time mode
- Support for Linux и FreeBSD operation systems
- Ability of inspection WWW sites visited by employees
- VPN technology support

You can read description of every FlowTuner feature in this manual.

## FONTS CONVENTIONS

To make reading easy all new terms printed in *italic* font. Code examples printed in dark background, for example:

```
#!/bin/sh
echo 'script example'
```

File names, paths, and programs names printed in courier font, for example /opt/flowtuner.

Some times text contains important notes. They are marked by exclamation sign at margins. Read such notes carefully, it can save to you a lot of time in the future.



Most of the text is operation system independ, but there is few exceptions. There are blue signs at margins with operation system names. You can skip that paragraphs if you have no plans to install FlowTuner on that OS.



# INSTALLATION

---

This part intended for system administrators willing to install FlowTuner software. Remember that you can ask Flowix engineers install FlowTuner remotely. If you aren't going to install FlowTuner yourself you can skip reading of this part.

## SYSTEM REQUIREMENTS

In order to use FlowTuner you need Pentium II class computer (or better) and 128Mb or more system memory.

FlowTuner supports following operation systems:

- Linux c kernels 2.4.x, 2.6.x or newer
- FreeBSD 5.3 or newer

To view report you need setup Java Runtime Environment (JRE) on client side. It is recommended to user JRE 5.0 Update 4 or newer. You can download JRE for free from <http://www.java.com>



Warning! Do not use JRE 1.4.2p6 for FreeBSD because it contains bug prevents normal database operation. It is recommended to use Linux JRE 1.4.2 in Linux compatibility mode. If you have strong reasons to use JRE 1.4.2p6, contact Flowix personnel for additional instructions.

To install FlowTuner you need operational gcc compiler, system headers files, `make` and `patch` utilities. Make sure your system has no working pptp server because it will conflict with pptp servers supplied with FlowTuner.

## VPN BASICS

FlowTuner employees Virtual Private Network (VPN) technology for secure Internet access. VPN has number of advantages over direct Internet access:

- Reliable users authentication
- Protection from IP- and MAC-addresses spoofing
- Simple deployment
- Users can access Internet from any computer in corporate network or from notebooks
- Reliable traffic accounting

VPN supported by every operation systems, including all version of Microsoft Windows, Linux and FreeBSD.

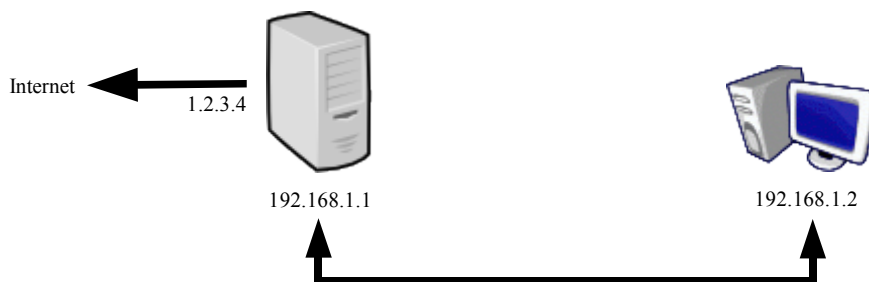
There is number of VPN protocols. As for now most popular is Point to Point Tunnelling Protocol (PPTP). VPN-connection is tunnel with two endings: one at client side and another one at server side. Both endings has own IP addresses.

Usually at server side IP address assigned by PPTP daemon, and client side IP address assigned by FlowTuner.

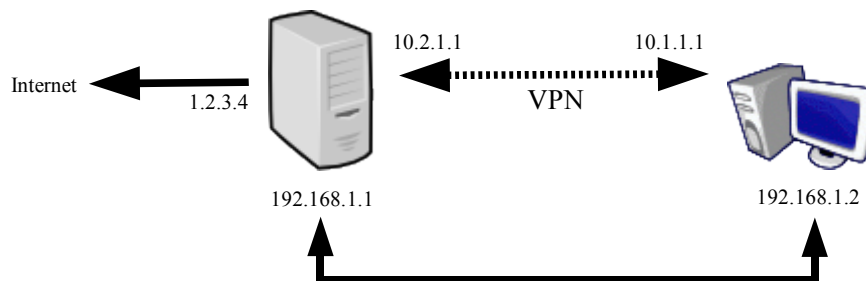
During VPN connection negotiation FlowTuner authenticates users with strong cryptographic algorithms, that's why nobody can decode password by using network sniffers software. After connection established operation system sends all traffic doesn't belongs to local network via VPN tunnel. VPN server do accounting of every single byte passing through tunnel and sends counters values to FlowTuner in specified time frame. FlowTuner receives counters values, calculate statistics and can terminate connection if user is out of quota.

pptpd daemon listens for VPN connections requests and calls pppd daemon when connection arrives. From technical point of view FlowTuner is RADIUS server. ppp daemon makes users authentication and sends request to RADIUS server to check users passwords. FlowTuner also contains pdsd daemon for connections termination purpose.

Let's imagine Internet access server and small corporate network. Server has two network interfaces: one for Internet connectivity, with 1.2.3.4 IP address. Another network interface connected to local network and has IP address 192.168.1.1. Employees workstations has IP addresses starting from 192.168.1.2:



After VPN connection established it looks like virtual network tunnel with additional IP addresses at client and server side:



Operation system at employee computer will automatically route all network traffic doesn't belongs to 192.168.1. network via VPN tunnel. Every packet routed via VPN tunnel will have source IP address 10.1.1.1, because it was assigned to client side of tunnel during connection negotiation. Now it is necessary to make possible reach

Internet for packet from private 10.1.1. network.

There is two ways to allow Internet access from private IP addresses (to get best results use both ways simultaneously):

1. Enable Network Address Translation (NAT)
2. Install transparent proxy server

NAT can dynamically substitute private IP address of client side VPN tunnel with server IP address. In this example 10.1.1.1 address will be substituted with 1.2.3.4 address and employee computer will gain Internet access.

By using transparent proxy server every HTTP traffic will be redirected to proxy server with Internet connectivity.

Both NAT and transparent proxy doesn't require any changes at client side. It is always smart idea to use both simultaneously because proxy server can cache traffic, FlowTuner can get site visits statistics from proxy and every protocols (not only http) will working because of NAT.

## FLOWTUNER INSTALLATION

To install FlowTuner just unpack FlowTuner archive, go to FlowTuner directory and run install script:

```
./install
```

It took some time to complete installation. There will be few warnings on screen during pptpd compilation. After installation complete you can see addresses you can type in browser to access FlowTuner administration web interface.

If you are using Squid proxy server you need to specify location of access\_log file. To do it edit /opt/flowtuner/etc/sqscan.conf file.

To use Linux JAVA in FreeBSD make sure Linux compatibility layer is enabled in kernel and mount Linux /proc file system. To mount /proc just add following line to /etc/fstab file:

```
linprocfs /compat/linux/proc linprocfs rw 0 0
```

After that to mount Linux /proc just run following command:

```
mount /compat/linux/proc
```

If you are using FreeBSD 5.x or newer you need to install FreeBSD 4.x compability libraries (compat-4.x). You can do it with /stand/sysinstall utility.

To run FlowTuner use following command:

```
/opt/flowtuner/bin/startft start
```

You can stop FlowTuner in the same way:

```
/opt/flowtuner/bin/startft stop
```

As for now FlowTuner is successfully installed, but it is recommended to check http.conf and create your own keystore secret key.



http.conf file contains FlowTuner embedded web server options. It is already configured by installer, but it is possible to do some tuning. Open http.conf and look at <listeners> section. It contains options for HTTP and secure HTTPS protocols.

HTTP protocol properties allows you to set TCP port for built in WEB server.

HTTPS protocol is secure version of HTTP. It makes guarantee that nobody can intercept and decode information transmitted over HTTPS connection. To encrypt network traffic HTTPS needs keys stored in special keys storage. Keys may be protected with password and storage itself may have password too. Keys must be signed by authorized organization, but it is possible to generate so called «self signed» keys.

To generate self signed key type following command (in one line):

```
keytool -genkey -keyalg RSA -keystore <keystore_file>
-storepass <keystore_password> -alias myself
```

Replace <keystore\_file> with desired name of key storage file and replace <keystore\_password> with desired password. Keytool will ask some questions about your organization and your personality. After generation complete copy generated file to /opt/flowtuner/etc directory and set key storage file name, key storage file password and key password in http.conf.

Now you can login to FlowTuner administration web interface. Run FlowTuner and type in address bar of your browser something like

```
http://localhost:8080/cc.cgi
```

where localhost is address of server with FlowTuner installed, 8080 – HTTP port number from http.conf file, cc.cgi is the name of administrative program. Besides of cc.cgi there is stat.cgi application used by employees to view their own statistics.

All FlowTuner web programs is also available via secure HTTPS protocol. To use it just replace 'http' with 'https' and correct port number. For example:

```
https://localhost:8090/cc.cgi
```

By default you can login to FlowTuner web interface with 'admin' login name and 'admin' password. You must change password immediately after FlowTuner setup.

## NETWORKING SETUP

There is two ways to allow Internet access through VPN connections: use NAT or proxy server. In any case, first of all you need to go to «Options» -> «Addresses» menu in administration web interface and set IP address range for client side VPN tunnels. Feel free to use any unused private IP address range, for example 10.1.1.1 – 10.1.1.254.

If you are Linux user you need to add one rule to iptables to enable NAT (write it in one line):



```
iptables -t nat -A POSTROUTING -s 10.1.1.0/24 -o eth0 -j SNAT --to-source 1.2.3.4
```

where eth0 is network interface connected to Internet, 1.2.3.4 – IP-address of server used for Internet access, 10.1.1.0/24 – subnet used at client side of VPN tunnels.



To enable NAT in FreeBSD you need to specify name of interface used for Internet access and enable firewall. Add following lines to /etc/rc.conf file:

```
natd_enable="YES"
natd_interface="fxp0"
firewall_enable="YES"
firewall_script="/etc/rc.ipfw"
```

After that add rule following rule to firewall script /etc/rc.ipfw (write it in one line):

```
${fwcmd} add divert natd ip from 10.1.1.0/24 to not 10.1.1.0/24
```

where 10.1.1.0/24 is subnet used at client side of VPN tunnel. Changes in rc.conf and rc.ipfw will take effect after reboot.

Now it is time to configure transparent proxy server. It is recommended to use Squid proxy server. Find squid.conf configuration file and set following parameters::

```
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

Now find access control parameters in squid.conf and allow VPN clients access to proxy server:

```
acl vpnnet src 10.1.1.0/255.255.255.0
http_access allow vpnnet
```

where 10.1.1.0/24 is subnet used at client side of VPN tunnels. Make sure you have added access rules before «deny all» rule (http\_access deny all). All changes will take effect after restart of squid server.



The only thing to do for now is transparent redirection HTTP connections to proxy server. In Linux add following rule to iptables firewall (write it in one line):

```
iptables -t nat -A PREROUTING -s 10.1.1.0/24 -p tcp --dport 80 -j REDIRECT --to-ports 3128
```

where 10.1.1.0/24 is subnet used at client side of VPN tunnel, 3128 is a port listened by proxy server.



If you are using FreeBSD add following rule to /etc/rc.ipfw file (write it in one line):

```
${fwcmd} add fwd 127.0.0.1,3128 tcp from 10.1.1.0/24 to not me 80
```

where 10.1.1.0/24 is subnet used at client side of VPN tunnel, 3128 is a port listened by proxy server.

Congratulations! Now your system is properly configured for Internet connections.



For better security it is recommended to configure firewall to reject traffic from IP addresses used at client side of VPN tunnels passing via physical network interfaces. Also make sure that nobody besides IP addresses used at client side of VPN tunnels can use proxy server (by default squid is configured to do that).

## **VPN AT CLIENT SIDE**

At client side everything you need is to configure VPN connection. As for now every OS has built-in VPN support, including all versions of Window with exception of Windows 95 (VPN support for Windows 95 available free of charge at [microsoft.com](http://microsoft.com) website).



Do not forget to disable traffic encryption in VPN connection settings. It is not supported in FlowTuner because it request to much processor power to encrypt all traffic at descent speed.

# OPERATORS GUIDE

---

This part describes FlowTuner web interface. To learn lessons well read it near computer with open FlowTuner web interface. Try all described features yourself and you will become familiar with FlowTuner in no more than one hour.

## HOW TO LOG IN

To log into FlowTuner administration web interface open your favourite web browser and type in address bar one of following lines:

```
http://myserver.com:8080/cc.cgi  
https://myserver.com:8090/cc.cgi
```

Replace myserver.com with real address of your server with installed FlowTuner software. Look at previous part if you is not sure which address to use.

It is always recommended to use https connection instead of http because it is more secure.

Users can access special web interface to view their statistics by typing something like

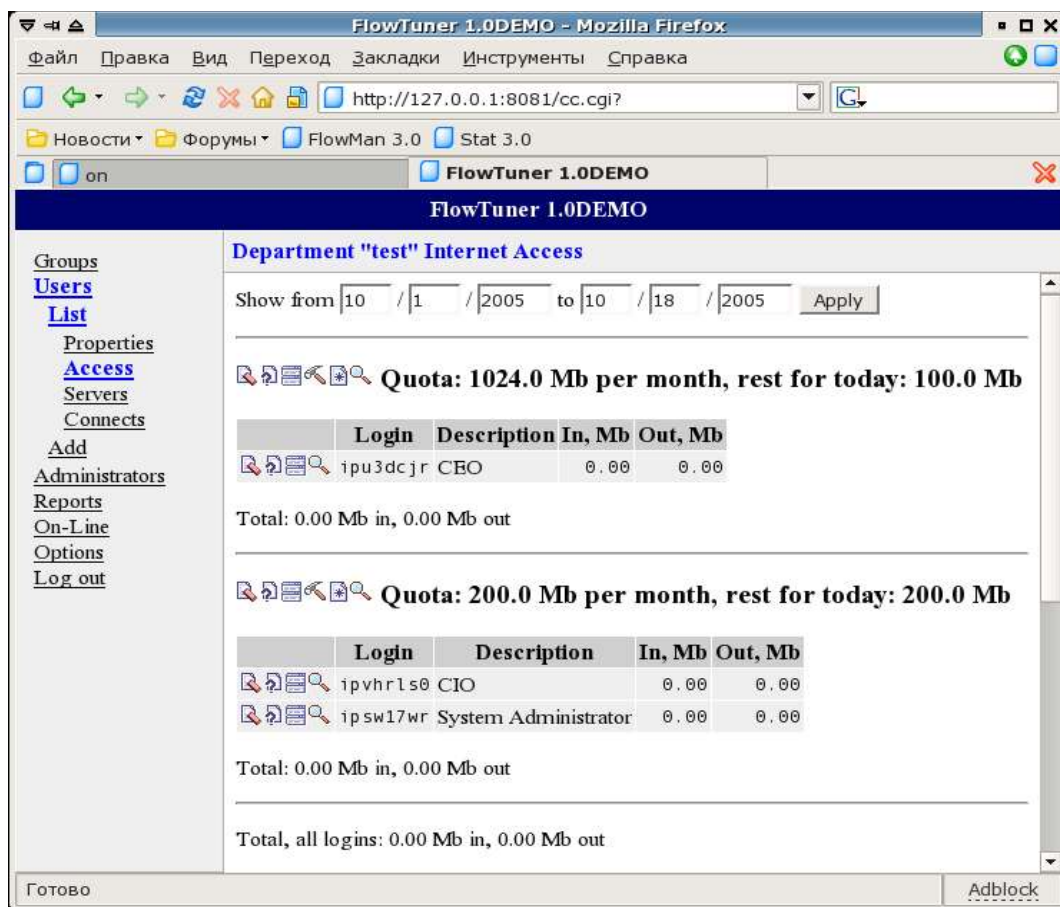
```
http://myserver.com:8080/stat.cgi  
https://myserver.com:8090/stat.cgi
```

It is good idea to save this addresses in browser bookmarks to save typing.

By default there is administrator with login «admin» and password «admin».

## FLOWTUNER BASICS

Look at FlowTuner shot:



There is main menu at the left side. After you select item of menu submenu items appeared. Always look carefully at the menu side during interface learning.



Never use «Back» browser button in web-interface. It can cause unnecessary duplication of last actions or other undesired effects.

Almost all tables in FlowTuner web interface has icons set at the leftmost columns. Use that icons to edit data. Here is list of most used icons:

<i>Icon</i>	<i>Meaning</i>
	Delete row
	Edit row
	Correct quota reminder
	View visited web servers list
	View connections list

If unsure place mouse over icon and wait a little. Small button description will pop up soon.

## FIRST STEPS

First task to do is administrator password change. Click at the «Administrators» menu item and click at administrator properties icon at administrators tables. After that administrator properties sheet must be shown. Erase all asterisks at password field, enter new password and press «Save» button. Read more details about administrators management at next chapter.

The next step is to create users group. It is impossible to add new users unless at least one group is exists. Go to «Groups» menu, enter name of new group and press enter. New group will be shown immediately in the groups list.

Now it is possible to add new departments and users

## ADMINISTRATORS MANAGEMENT

*Administration* is users with rights to access to FlowTuner administration web interface. You can view list of administrators by clicking at «Administrators» menu item. Right after FlowTuner installation there is one default administrator.

To add new administrator fill the form below administrators list and press «Add administrator» button. Status field can be used to disable administrator access to web-interface quickly. You can change administrator information by clicking «Properties» icon at administrators table.

## USERS MANAGEMENT

To manage users go to «Users» menu. You can't add new users if there is no groups exists.

«Users» menu has hierarchical nature. There is groups at the top level of hierarchy. Groups consists of departments. Each department can have any number of quotas, which contains actual users.

There is several types of quotas. It is possible set quota for month, week, day or special «manual» quota. In manual mode one must add traffic to quota manually. Every quota has «remainder» field. When reminder become zero all users in quota will be disabled.

To add new department click at «Users» menu item and click at «Add department» link at the bottom of departments list. Fill in form, select appropriate group and press «Add» button. Now you can set first quota for department.

Select limit type. When you choose quota type «Monthly», it means that every 1<sup>st</sup> day of every month reminder will set to quota value. For example, if quota equals to 1000 megabytes than at 1<sup>st</sup> date reminder will automatically set to 1000 megabytes.

If quota type is «manual» then you must add some traffic to this quota by hands. When quota is over quota will be disabled and wouldn't automatically enabled.

To add quota one need select quota type, quota value in megabytes, optional quota description and set auto disable and auto enable fields. If auto disable is off then logins wouldn't be turned off when reminder goes negative. If auto enabled if off than logins wouldn't be turned on when reminder goes positive. After quota was added you will be prompted to create login in that quota.

Each quota has number of icons at the left side. By clicking that icons one can delete quota, edit quota properties, add or remove extra traffic («Operations» menu), view visited web sites or add new logins to quota.

To correct quota reminder use «Operations» menu. Depending on values of «auto disable» and «auto enable» fields users will be automatically enabled or disabled when reminder goes positive or negative. «Source» field will contains login name of administrator changed reminder.

Each login has several fields: user name, login name, password, IP address pool and maximum number of simultaneous connections. IP address pool tells what IP address will be assigned to client side of VPN tunnel. User will be limited with specified number of simultaneous VPN connections (use zero value to eliminate restrictions).

To view who is on line go to «On-line» menu item. It is possible to hang up users manually. Click to «Hangup» icon and select hangup method. Normally always use first hang up method. But if you have troubles (for example if user ppp daemon was accidentally killed) you can just remove user record from online list. It is possible to store removed connection in connections list and subtract it from users remainder or just eliminate it without reminder update.

To build and print reports use «Reports» menu item. Remember to install latest JRE at your computers, or reports menu wouldn't work.

## OPTIONS

There is number of preferences in «Options» menu. Normally you needn't modify any of them with exception of RADIUS update interval and IP address pools. «Options» menu has several sub menus.

«General» sub menu allows to set maximum number of records to display at one page. Too many records can cause browser each too many memory and slow operations.

«Addresses» item used for IP pools setup. Each pool has own name and to IP addresses: first and last address in the pool. It is possible to have several address pools for different users.

«RAS» menu item contains options for automatically generated login names and passwords.

«RADIUS» menu item consists of two sub items: «RADIUS Properties» and «RADIUS Devices».

«RADIUS Properties» menu allows change properties of built in RADIUS server. The most important option is «interim update interval». Smaller interval cause better

quotas precision, but can increase server load. For small sites 3 seconds is optimal value. RADIUS packets log can make debugging simpler if something goes wrong.

«RADIUS Devices» menu usually filled automatically by installer. You needn't change anything there unless you really knows what you do.

## **IF YOUR ARE IN TROUBLE**

---

If something goes wrong just contact FlowTuner support team. Every FlowTuner comes with half year of free support. Go to <http://www.flowix.com> web site and drop a letter about your problem. Don't forget that Flowix support includes free remote installation. Ask for remote installation and save your time.

Thank you for choosing Flowix product!