




# TraffPro Installation Guide.

**TraffPro (Traffic & Protection).**


(Russian - English Translation and additions to English manual By Harsh Vadgama and Alexei Pletneov.)

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

## Table of Contents

Purpose, Design And Scope.....	3
Software Objectives.....	3
Terms and abbreviations.....	6
I. Installing TraffPRO.....	6
II. Viewing URL surfing reports.....	13
The First Method.....	13
The Second Method (using Traffpro+Squid ).....	13
III. Setting up a connection of TraffPro + NetFlows v9 v5 15.....	17
IV. DHCP Server setting configuration.....	18
Additonal Information.....	25
Example of setting up TraffPro with squid version (2.6 or 3.0).....	26

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 2 of 28
----------	------------------------------------	----------------------------------	--------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

## Purpose, Design And Scope


### Software Objectives

TraffPro has been designed to solve tasks related to calculating the amount of network traffic being utilized in an office, home or corporate network. It accounts and reports this traffic, protects Networks via access control protocols and secures resources within the network . This product has been designed to make installation and administration easier without requiring a large knowledge base. Support personel is what we consider a minimum requirement to maintain and manage the system.

### Cost of Installing , Maintaining And Buying Equipment:

- ◆ The system in its own structure has been designed to reduce the cost of maintaining servers and gateways as well as lowering the IT staff qualifications (i.e. you don't need a highly qualified linux or windows admin to run the system). This leads to a dual cost reduction to both to the IT department and Hardware to be used.
- ◆ Hardware used in the system is directly-proportional to number of employees connected to the Internet by adding multiple gateways (via NICS) in a single server, which accordingly does not require additional expenses as would be the case for large expensive servers.
- ◆ Modular system allows greater flexibility in terms of choosing what suits your organization best. You can choose which modules you need without buying the whole system thus being cost effective.
- ◆ Additional terminal administrative consoles (SSH) makes it easy manage the system, even from your mobile phone (via low-speed channels connection such as GPRS), which makes the system flexible and easy to maintain.
- ◆ The system is installed on a free operating system GNU / Linux, that reduces the cost of buying expensive operating systems.
- ◆ Linux Operating System , at this stage of its development, is now considered to be reliable system in the world of IT, which itself increases the security of your network, reducing the cost of emergency situations and unforeseen downtime failures and malfunctions.

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 3 of 28
----------	------------------------------------	----------------------------------	--------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business


### The Software provides:

1. Ability to control traffic flowing from an external network to the internal network (e.g. LAN/ISP network etc) and vice versa
2. Ability to use more than one ISP and route them to your network.
3. Protect your resources within your Internal Network/LAN and the Server itself.
4. Receive reports on consumed traffic within the internal network.
5. Receive reports on what users do within you network.

### Additional Features


- ◆ Use unlimited number of external and internal interfaces
- ◆ Automatically routes traffic from your network (through one or multiple NICS) to the internet. No need to do it manually (NAT/masquaring) .
- ◆ Monitor and control Bandwidth Consumption in a network
- ◆ Use a distributed traffic computing (via use of multiple gateway servers to access the internet with a single server which acts as a database)
- ◆ Restrict users from unauthorized access to the Internet (controlled by IP, MAC, User Name's and Passwords)
- ◆ Can be used as simple traffic consumption and traffic reporting system without User Authorization except by IP or IP+MAC
- ◆ Web Based Interface for users, who can use it to gain authorization for access the Internet.
- ◆ Protect the server From external Intrusion / hackers via an inbuilt firewall
- ◆ Control server bandwidth and trafficCan be used with a DHCP server.
- ◆ Can be used with a proxy server
- ◆ Can be used with ppp servers (vpn, pptp, pppoe)
- ◆ Restrict users to websites using a 2 way policy: Either allow users to access URLs or block them. (Restriction is done via all IP protocols (tcp, udp etc)
- ◆ Get statistics on websites visited and amount of traffic downloaded by users via all protocols and ports.
- ◆ Control traffic across multiple servers (i.e many servers with traffpro but without a database connected to different networks can access the Internet via a single server with traffpro which has database and a administrative console)

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 4 of 28
----------	------------------------------------	----------------------------------	--------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

- ◆ Connect Unlimited number of users without any restriction.
- ◆ Connect more then 1000 users without sorting them out in different networks (i.e. connect all in one server!)
- ◆ Reports on total amount of traffic used by users.
- ◆ Receive reports from users on the total traffic consumed on weekdays
- ◆ Receive reports from users on amount of traffic used based on ports
- ◆ Receive reports from users on amount of traffic used based on ports and days
- ◆ Receive reports from users on amount of traffic used based on number of connections to a resource (by ip + port, and or by domain)
- ◆ Equalize speeds to give priority to all users without the bandwidth being used up by one user.

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 5 of 28
----------	------------------------------------	----------------------------------	--------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

## Terms and abbreviations

Terms and abbreviations	Definition
TraffPRO	TraffPRO (Traffic & Protection) A Network Security, Reporting and Billing System
DB	The MySQL Database
Daemon	Computer program that runs in the background rather than under the direct control of a user;

## I. Installing TraffPRO

Before you install Traffpro, make sure that you have installed the following packages:

```
iptables, iptables-devel
mysql mysql-server, mysql-devel, mysql-libs
httpd
php, php-mysql
gcc, gcc-c++
```

The packages specified apply to the following distributions: Fedora, Redhat, CentOS. For other OS read the forums.


If you plan to use Squid with TraffPro then disable squid auto-start service otherwise there shall be a conflict when Traffpro starts. Traffpro will automatically start the squid service.

```
chkconfig --levels 345 squid off
```

Before installing Traffpro, disable **selinux**. To do edit the file */etc/selinux/config* using nano or vi and make it look like this

```
# This file controls the state of SELinux on the system.
```

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 6 of 28
----------	------------------------------------	----------------------------------	--------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

```
# SELINUX= can take one of these three values:
# enforcing - SELinux security policy is enforced.
# permissive - SELinux prints warnings instead of enforcing.
# disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
# targeted - Targeted processes are protected,
# mls - Multi Level Security protection.
SELINUXTYPE=targeted
# SETLOCALDEFS= Check local definition changes
SETLOCALDEFS=0
```

We recommend you reboot the server after making the changes

# Install the necessary packages

```
yum install httpd mysql-devel iptables-devel gcc php php-mysql mysql-server gcc-c++ libstdc++-devel
```

Start the necessary services

```
service mysqld start
```

```
service httpd start
```

```
#####
```

```
##Installing the root passowrd for MySQL access:
```

```
#!/usr/bin/mysqladmin -u root password 'new passowrd'
```

```
#It is recommended you change the root password after installing
```

```
#TraffPRO, or change the start up script installing the mysql databas.
```

```
#This can be difficult for many users.
```


```
#
```

```
#Restart MySQL service:
```

```
#service mysqld restart
```

```
#####
```

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 7 of 28
----------	------------------------------------	----------------------------------	--------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

Uncompress the archive

```
tar -zxvf traffpro.X.X.X-XX.tar.gz -C /tmp
```

Change to the directory where you uncompressed the file and run the script

```
cd /tmp/traffpro.X.X.X-XX
```

```
./install.sh
```

Further on installation is relatively simple as the script is executed in a question and answer type basis.

After the installation is complete, review your traffpro configuration file.

**/traffpro.cfg** is the main configuration file. If you choose to configure your system later during the install process or you decide to make changes after you installed TraffPro you can adjust it.

**Configuration File contents can vary, depending on your choice of answers during installation.**

Example of the traffpro.cfg file **/etc/traffpro/traffpro.cfg**:

```
# Define which mode to run in. Two values true or false.
```

```
# true - runs in daemon mode
```

```
# false - runs in console mode (debug mode)
```

```
daemon=true
```

```
# Database address
```

```
# Can have values like (localhost, 127.0.0.1, 10.10.0.1)
```

```
# If using traffpro as a central server with other sub-servers then another value is used apart from local #host where the address in sub-servers will have the central servers IP.
```

```
db_url=localhost
```

```
# Port connecting to MySQL.
```

```
#The port value must be specified in case you changed the port in the configuration file
```

```
# /etc/my.cnf
```

```
# Default value is 3306
```

```
db_port=3306
```

```
# MySQL Database user name , under whose rights the system will connect to and run.
```

```
# The default is root and blank password.
```

```
# For more information please visit http://en.traffpro.ru
```


```
db_usr=root
```

```
# User password to access the MySQL database .
```

```
db_passwd=
```

```
# Database name to connect to the system
```

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 8 of 28
----------	------------------------------------	----------------------------------	--------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

# For older versions the name was office and in the new version its traffpro.

**db\_name=office**

# Waiting time before sending data to the database (in seconds)

# The less the value the faster information is sent and the size of the db becomes large fast too

**time\_out=720**

# Affects authorization time, the recommended value of 10.

# The higher the value, the less the demon looks into the database for verification of changes.

**time\_in=10**

# Enable/Disable MAC address control for users. Can be true/##false

# Recommended value - true

**control\_eth\_addr=true**

# Gateway number (used when traffic is distributed to more than one gateway to

# sub-servers. If you have only one gateway, default is set to 0)

**net\_number=0**

# Enable detailed port logging (in case it is set to false, logging will continue but

# Individual ports will not be logged. Only a summary of on all ports will be

# logged)

**ports\_detail=true**

# Enable firewall for the server and billing system.

# If you enable this setting, add the server using the web admin panel.

# WEB-Admin -> System -> Servers - Add Server.

# When adding indicate the external IP facing the internet.

**ss\_enabled=true**

# State the external interface

# Can be known using ifconfig -a

**eth\_out=eth3**

# Details of users URL surfing reports.

# Possible values are true / false.


# As of version 1.2-XX and above, squid is no longer needed for logging surfing histories

# Now, if true, the daemon keeps a record of visits to their resources.

# When set to false, Squid can be used squid to work with Traffpro for the histories, but accounting

# of surfing histories visits will be logged via ports going through the proxy server.

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 9 of 28
----------	------------------------------------	----------------------------------	--------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

**url\_detail=true**

# Note that the daemon itself will adjust the buffer automatically but we do not suggest you adjust the size of packets to more than 200 because a buffer size of 12 megabytes and larger under force majeure slow down the demon, but does not accelerate the size of packet queue

**ip\_queue\_maxlen=2048000**

# If stated then NAT will be used, if left blank then MASQUERADE is used.

**out\_ip=192.168.1.200**

# Enable the monitor. If set to true then then two parameters below it should not be left out.

**monitor\_on=true**

# Address the monitor listens on (default 127.0.0.1)

**listen\_addr=192.168.1.200**

# Port the monitor listens on (default 9999)

**listen\_port=9999**

# Removed from version 1.3.3-9X, and a new script has been made in its place /etc/init.d/tp-scheduler  
# True=loads timer, false=does not load timer

# Execute SQL queries or sh scripts. Data requests are taken from the admin area.

**timer=false**

# Path where traffpro should install to

**to\_install\_dir=/opt/traffpro**

#Allow traffpro to use SQUID logging user surfing histories . If set to true the proxy server should be removed as a autostartup script which will then be run using traffpro.

# To work properly you need to add the following data in the squid.conf configuration file

**#squid\_connect=true**

# This option specifies the location of the file, which will

# Used to transfer files to the MYSQL database.

# Then change the files (chown squid.squid access.log)

**#squid\_log\_file=/var/log/squid/access.log**

# Blocks sites. Using this parameter,

# you do not need to block resources using


# services like squid, squidGuard, iptables.

**url\_block=true**

# This parameter is responsible for accounting icmp requests other

# than the udp and tcp, i.e. without this parameter, the system

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 10 of 28
----------	------------------------------------	----------------------------------	---------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

# activity monitor will not be displayed. If set to true the true the #parameter is active, false if off.  
 Display the status on the monitor of packages that do not belong to the TCP and UDP

**not\_udptcp\_control=true**

# Maximum number of connection requests during time\_in from the client

**antiflood=500**

# Disable reverse domain name look up to enable url surfing histories to be caught.

**not\_resolv\_dn=true**

# Allows daemon to route data, and raise the NAT using values from the database.

#Data is input through the web-admin panel.

**nat\_data\_in\_db=true**

# Shows how much traffic and load is being taken up by a gateway.

**log\_route=true**

# For the PPPD plugin – informs the plug-in that if file is not found in the traffpro database, it should

# also check the secret files if value is set to true. i.e. file where the login and passwords are stored.

**secret\_files=false**

# Aggregate clients url-surfing resources. Value is set to true by default.

# To disable set to false

**url\_agregate=false**

# Shaper Type. If set to true – All clients are queued in one line.

# False – Each client has his own queue (default)

**shaper\_type\_linear=false**

# Turn on / off, traffic accounting daemon with your router (Cisco).

# Possible values are on, off, comb.

# Turn on (accounting only for netflows) off (off)

# Comb (accounting and methods of the Linux kernel and netflows simultaneously)

**enable\_netflow\_type=on**

# Netflow configuration. Designed to collect information on the IP-traffic within the network.

# Address on which tapped packages are sent using netflow to the cisco from your server

**netflow\_addr=192.168.0.237**


# Port on which to listen to netflow packages flowing from your server

**netflow\_port=8818**

**The second configuration file /etc/traffpro/traffpro\_rule.cfg**

This configuration file is used to add your own iptables' rules.

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 11 of 28
----------	------------------------------------	----------------------------------	---------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

**For, example, putting these strings into your traffpro\_rule.cfg file will enable** SSH access to your server. (Which will be done automatically if you choose that option during installation)

```
iptables -A INPUT -m tcp -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -m tcp -p tcp --sport 22 -j ACCEPT
```

#Check your file permissions:  
ls -l /etc/traffpro/

```
-rw-r--r-- 1 root root 339 Nov 19 17:43 traffpro.cfg
-rw----- 1 root root 493 Nov 20 22:11 traffpro_rule.cfg
```

#check if the database was created:  
**mysqlshow** — will show all the databases and if you did not change the database name during installation you should see «traffpro».

#If everything is okay start the traffpro service if you did not do it:  
**service traffpro start**


#Check if the traffpro system is running:  
**ps x | grep traffpro | grep -v "grep"**

you should see:  
**2621 ? Ssl 1:34 /opt/traffpro/billing-daemon/bin/billing daemon=true**

#If everythings is working, then configure the necessary services to auto-start on reboot.  
# Note no need to do this if you already choose the option to auto-start everything during the  
# initial script installation

```
chkconfig --levels 345 mysqld on
chkconfig --levels 345 httpd on
chkconfig --levels 345 traffpro on
chkconfig --levels 345 tp-router on
chkconfig --levels 345 tp-atsloger on
```

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 12 of 28
----------	------------------------------------	----------------------------------	---------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

## II. Viewing URL surfing reports

### The First Method

Enable the url\_detail line in the configuration file / etc / traffpro / traffpro.cfg:

**url\_detail = true**

**(Note! Make sure you have installed # a caching nameserver for this feature to work.)**

This option enables the administrator view what urls users visited.

Will allow you to view downloaded traffic without installing a squid proxy server.

### The Second Method (using Traffpro+Squid )

1. Install squid  
**yum install squid**
  
2. **Configure Squid**  
nano /etc/squid/squid.conf


Example of the squid configuration file (**/etc/squid/squid.conf**):

```

acl manager proto cache_object
acl all src 0.0.0.0/0
acl localhost src 127.0.0.1
acl ip src 192.168.1.0/24 192.168.3.0/24
acl SSL_ports port 443 563 15781
acl CONNECT method CONNECT
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access allow manager
http_access allow ip
http_access deny !Safe_ports

```

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 13 of 28
----------	------------------------------------	----------------------------------	---------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

```

http_access deny all
icp_access allow all
http_port 192.168.1.200:3128 transparent
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin ?
cache deny QUERY

# Use TraffPro for logs in case you are set it to parsing
logformat traffpro %>a %<A %lp %st %ru
access_log /var/log/squid/access.log traffpro

request_body_max_size 10240 KB
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern . 0 20% 4320
acl apache rep_header Server ^Apache
broken_vary_encoding allow apache
cache_mgr admin@z-tec.ru
cache_effective_user nobody
dns_nameservers 192.168.1.200 217.150.34.129 80.79.64.210
coredump_dir /var/spool/squid

```

Please note that the user who is running squid on your behalf must have the rights to read/write cache files and squid logs. Also specify the DNS server **dns\_nameservers**.

3. Enable squid parameters settings in the configuration file (/ etc / traffpro / traffpro.cfg):


```

squid_connect = true
squid_log_file = / var / log / squid / access.log

```

4. Reconfigure MySQL  
vi /etc/my.cfg

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 14 of 28
----------	------------------------------------	----------------------------------	---------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

```
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
user=mysql
# Default to using old password format for compatibility with mysql 3.x
# clients (those using the mysqlclient10 compatibility package).
old_passwords=1
long_query_time=10
key_buffer=256M
table_cache=2048
sort_buffer=64M
record_buffer=256M
max_connect_errors=100
connect_timeout=300

[mysqld_safe]
log-error=/var/log/mysql.log
pid-file=/var/run/mysqld/mysqld.pid
```


Editing it provides more MySQL resources than the standard configuration.

Similarly it is recommended to re-configure the **apache** configuration file.  
Pay attention to changes in the following settings

```
<Directory />
Options FollowSymLinks # this setting.
AllowOverride None
</ Directory>


Options Indexes FollowSymLinks # this setting.
AddDefaultCharset # this setting.
DirectoryIndex index.php index.html index.html.var # this setting.
```

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 15 of 28
----------	------------------------------------	----------------------------------	---------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

Further details about this settings can be found at the official Apache site  
<http://apache.org/>

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 16 of 28
----------	------------------------------------	----------------------------------	---------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

### III. Setting up a connection of TraffPro + NetFlows v9 v5 15

You need to add or edit three parameters to your `/etc/traffpro/traffpro.cfg`

Address to which the collector will accept incoming data from the systems generating NetFlows

**netflow\_addr=192.168.0.237**

The port on which the collector will accept incoming data from the systems generating NetFlows


**netflow\_port=9996**

Enable NetFlows funtion

**enable\_netflow\_type=on**

**Note:** The IP's on which the accounting takes place must be present in the traffpro client database or client must be authorized to access the internet via the standard authorization methods (client based web interface)

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 17 of 28
----------	------------------------------------	----------------------------------	---------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

## IV. DHCP Server setting configuration

TraffPro has a function that can give clients static IP addresses and store the data in the dhcp configuration file. For security purposes, you should not store data in main configuration file.

Recommended settings:

Install packets:

```

yum install dhcp
    or
apt-get install dhcp3-server

```


Now we edit the dhcpd.conf file for example

```

#
# DHCP Server Configuration file.
# see /usr/share/doc/dhcp*/dhcpd.conf.sample
#
# leave unchanged
# Server-name; (in quotes)
server-name "router";
# Server time synchronization, the list of IP-addresses - separated by commas;
#(Prioritized – placed first)
option ntp-servers 192.168.10.1;
option time-servers 192.168.10.1;
#Change Time zones. Winter, Summer.
# 1440 - Summer, 10800 - Winter
option time-offset 14400;
# Domain Name
option domain-name "rumyancevo.local, kursakovo.local, rosinka.local";
#
option domain-name-servers rumyancevo.local;
# DNS сервера

```

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 18 of 28
----------	------------------------------------	----------------------------------	---------------


	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

```

option domain-name-servers 192.168.10.1;
# Netbios Server.
option netbios-name-servers 192.168.10.1;
option netbios-dd-server 192.168.10.1;
# If you are using Samba, then use this option.
option netbios-node-type 8;
# Gateways, if more then one then separate using comma
option routers 192.168.10.1;
#option dhcp-renewal-time 3000;
# Network mask
option subnet-mask 255.255.255.0;
# Broadcast address
option broadcast-address 192.168.10.255;
#
ddns-updates on;
#
ddns-update-style interim;
#
default-lease-time 116000;
#
max-lease-time 142000;
#
one-lease-per-client true;
#
authoritative;
#leave unchanged logging
log-facility local7;
# Port, on which DHCP server will listen on
Local-port 67;
# Use DNS for determining by IP-address hostname value option
get-lease-hostnames true;
deny duplicates;
#Main subnet

```

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 19 of 28
----------	------------------------------------	----------------------------------	---------------


	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

```

subnet 192.168.10.0 netmask 255.255.255.0 {
interface eth1;
#Temporary clients.
pool {
range 192.168.10.250 192.168.10.254;
allow unknown-clients;
}
# rumyancevo.
pool {
include "/etc/dhcp/dhcp-rumyancevo.conf";
range 192.168.10.10 192.168.10.249;
deny unknown-clients;
}
}
#Second vlan, interface eth1:1.
subnet 192.168.12.0 netmask 255.255.255.0 {
interface "eth1:1";
#Temporary clients.
pool {
range 192.168.12.250 192.168.12.254;
allow unknown-clients;
}
# kursakovo.
pool {
include "/etc/dhcp/dhcp-kursakovo.conf";
range 192.168.12.10 192.168.12.199;
deny unknown-clients;
}
pool {
include "/opt/traffpro/from_traffpro.conf";
range 192.168.12.200 192.168.12.249;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.10.255;

```

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 20 of 28
----------	------------------------------------	----------------------------------	---------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

```

option domain-name-servers 192.168.10.1;
option netbios-name-servers 192.168.10.1;
option netbios-dd-server 192.168.10.1;
option routers 192.168.12.1;
deny unknown-clients;
}
}

```

We are interested in the lines marked in red, which we shall add to the admin area, and there is where the clients data will be saved.

**/opt/traffpro/from\_traffpro.conf**

Make sure the file has write properties using the command. If you notice that the file is still giving problems with permissions you can simply move it to the /etc/dhcp directory

**chmod 666 from\_traffpro.conf**


Next go to **System --> Settings** and look for a setting named **dhcpcd\_conf\_path**

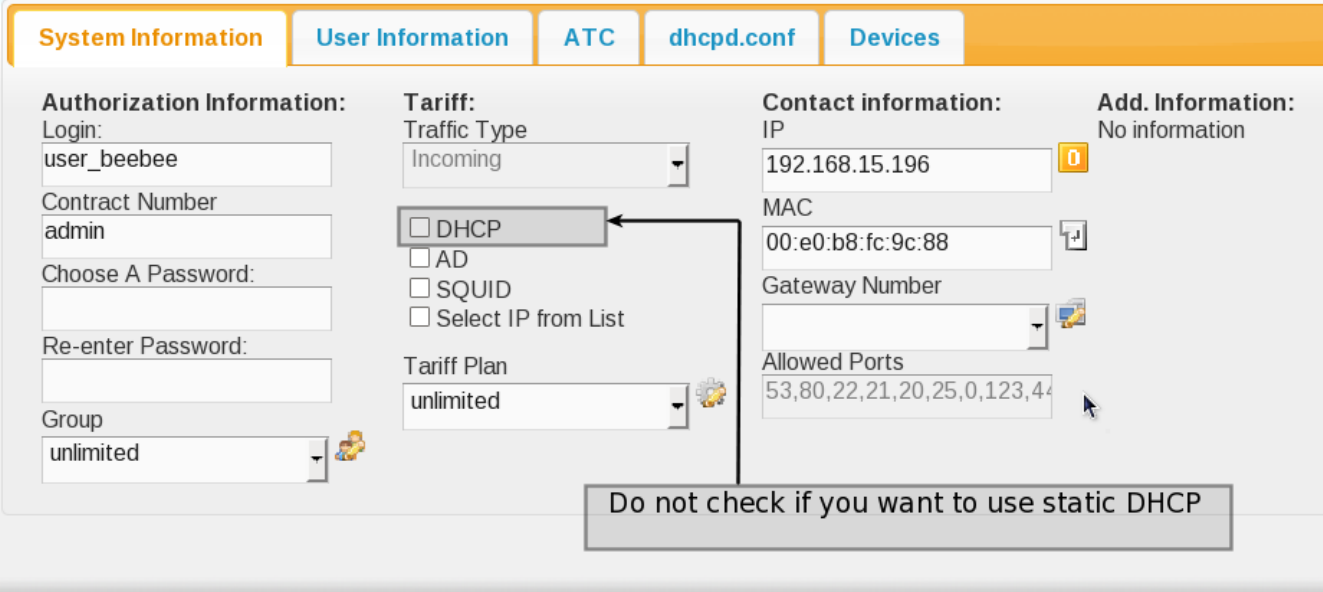
The path is set as **/etc/dhcp.conf** but since this file cannot be edited, you need to change its path and point it to where our **from\_traffpro.conf** file. In my case i changed it from **/etc/dhcp.conf** to **/etc/dhcp3/from\_traffpro.conf**

Next we create a new user.

The dhcp check-box should be left blank, if we plan to record this client in dhcp.conf

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 21 of 28
----------	------------------------------------	----------------------------------	---------------


	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

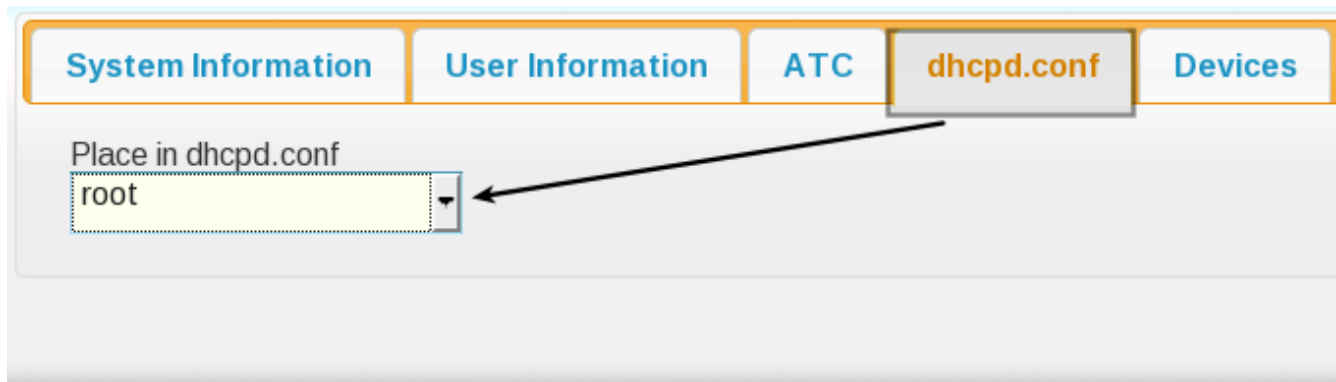


The screenshot shows the 'dhcpd.conf' configuration page. It includes sections for 'Authorization Information', 'Tariff', 'Contact information', and 'Add. Information'. The 'DHCP' checkbox is highlighted with a callout box that says 'Do not check if you want to use static DHCP'.

Create user and click "Apply". Now edit this new user and click on the dhcpd.conf tab.

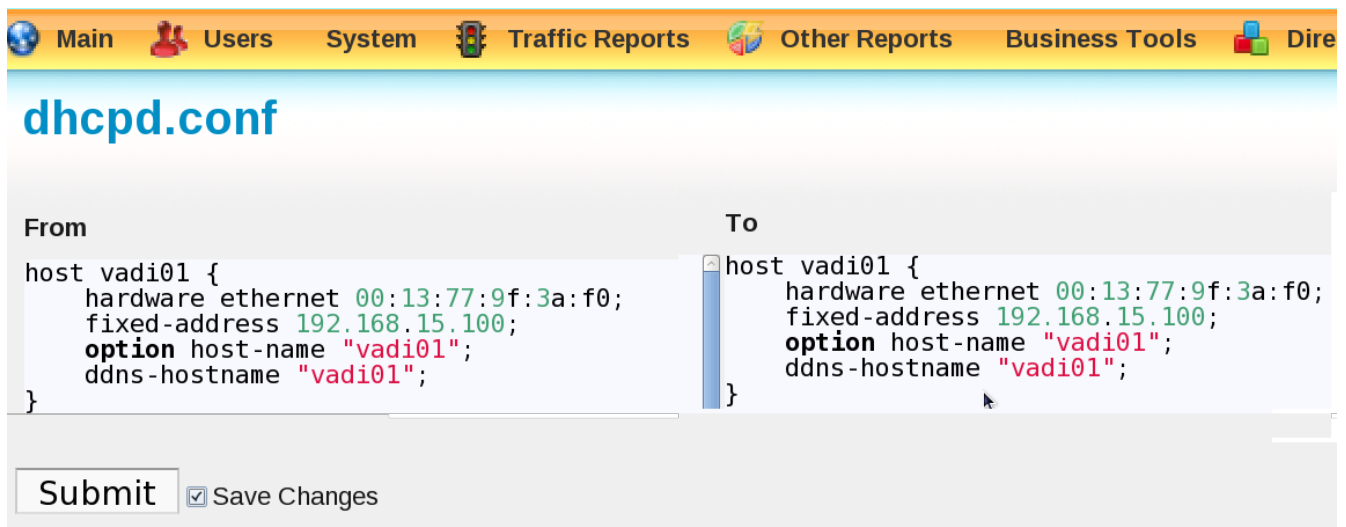
Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 22 of 28
----------	------------------------------------	----------------------------------	---------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business




Choose root and then click “Apply”.

Next we choose from the menu bar System --> Service --> **dhcpd.conf**



There are 2 sides you will see.

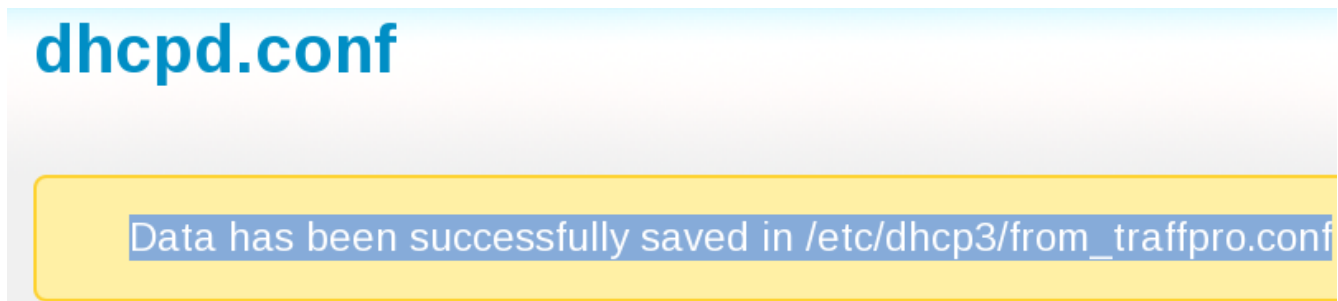
Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 23 of 28
----------	------------------------------------	----------------------------------	---------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

FROM --> shows you the old from\_traffpro.conf file  
TO --> shows you the new edited file with new user.

If all seems okay, check the box “**Save Changes**” and click on **Submit**

If the changes are successful then you will see message




You can verify if the changes were written or not using the following command

**cat /opt/traffpro/from\_traffpro.conf**

Then restart the dhcp server. It needs to be restarted everytime a change is made to our from\_traffpro.cfg file.

**service dhcpd restart** or **/etc/init.d/dhcp3-server restart**

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 24 of 28
----------	------------------------------------	----------------------------------	---------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

## Additional Information


Can be found at

<http://prov.traffpro.ru> - Official Site in Russian

<http://traffpro.ru/forum> - Official Forum in Russian

<http://en.traffpro.ru/> - Official English Site with forum

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 25 of 28
----------	------------------------------------	----------------------------------	---------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

## Example of setting up TraffPro with squid version (2.6 or 3.0)

Below is an example of how you can use TraffPro with Squid (Version 2.6 or 3.0)

Example is based on squid version 3.0

In the configuration file (traffpro.cfg) the following values will be present. (Squid values will automatically be there is you enabled squid access during installation.

1. **url\_detail=true**
2. **squid\_connect=true**
3. **squid\_log\_file=/var/log/squid/traffpro.log**

If you enabled **url\_detail=true** , this means that in your reports only the ip of the user will be present but you the amount of traffic used will be shown as 0.

If you use the first **url\_detail = true**, then your report will state only **IP / HOST** but will not the amount downloaded via that **IP/HOST**.


If you use all 1, 2, 3 variants together, then the ports will also be shown which the proxy server allows number + downloaded resources plus you can see which ports were visited by proxy, but the amount downloaded will not be displayed.

Using all three parameters increases the load on the server so you can omit a parameter, or increase resources for the desired service.

Below is an example of a real server with using squid.

```
#####
to_install_dir="/opt/traffpro"
daemon=true
db_url=localhost
db_usr=admin
db_passwd=admin
db_name=office
time_in=10
```

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 26 of 28
----------	------------------------------------	----------------------------------	---------------


	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

```

time_out=180
control_eth_addr=true
net_number=0
ports_detail=true
ss_enabled=true
eth_out=eth1
url_detail=true
out_ip=192.168.2.101
listen_addr=127.0.0.1
listen_port=9999
ip_queue_maxlen=2048
squid_connect=true
squid_log_file=/var/log/squid/traffpro.log
timer=false
#####
squid configuration file
#####
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8
acl stim src 192.168.2.0/24
acl SSL_ports port 443 10000 15781
acl CONNECT method CONNECT
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow stim
http_access allow stim
http_access deny all
icp_access allow stim
icp_access deny all
htcp_access allow stim

```

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 27 of 28
----------	------------------------------------	----------------------------------	---------------

	Project: Electronic Document	
	Document:	TraffPro (Traffic & Protection). Installation Guide
	Date:	10 <sup>th</sup> March 2010
	Version:	1.3.4 Business

```

htcp_access deny all
http_port 192.168.2.101:3128 transparent
hierarchy_stoplist cgi-bin ?
logformat traffpro %>a %<A %lp %st %ru
access_log /var/log/squid/access.log squid
access_log /var/log/squid/traffpro.log traffpro
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern (cgi-bin|\\?) 0 0% 0
refresh_pattern . 0 20% 4320
cache_mgr vsinyaev@voler.ru
visible_hostname voler.ru
icp_port 3130
dns_nameservers 192.168.2.101 91.192.21.3 217.150.34.129 80.79.64.210
coredump_dir /var/spool/squid
#####

```

After starting the service, you will find the following file in the squid logs directory.

```
prw-rw-rw- 1 root root 0 2009-02-09 21:51 traffpro.log
```

also run the command

```
chkconfig --levels 2345 squid off
```

Authors:	Galeev Rustam Kononenko Nikolai	Zhinyaeva Anna Sinyaev Valery	Page 28 of 28
----------	------------------------------------	----------------------------------	---------------