





Установка TraffPro.

TraffPro (Traffic & Protection).

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

Оглавление

Цель разработки и область применения.	3
Термины и сокращения.....	6
I. Установка Traffpro.....	7
II. Просмотр статистики посещений сайтов пользователями:	12
III. Настройка связи TraffPro + NetFlows v9 v5	15
IV. Описание настройки DHCP сервера.....	16
Дополнительная информация.	20
Пример использования TraffPro совместно со	20
squid версии (2.6 или 3.0):	20

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

Цель разработки и область применения.

Система TraffPro, призвана решить круг задач, связанных с расчётом используемого трафика в офисе, домашних или корпоративных сетях, установки контроля доступа к защищенным ресурсам и сетям. Продукт разработан с учетом облегчения процесса установки и обслуживания, с минимальными требованиями к уровню подготовленности обслуживающего персонала.

Затраты на установку, обслуживание и оборудование:

☞ Система, по своей структуре, создана для уменьшения затрат как на обслуживание шлюзов и серверов, так и на снижение требований к квалификации сотрудников, её обслуживающих, что влечёт за собой двойное снижение затрат на отделы ИТ и поддержку оборудования.

☞ Мощность оборудования, используемого для работы системы прямо пропорциональна количеству сотрудников организации, подключённых к сети Internet, через данное шлюзовое оборудование, что соответственно не требует дополнительных затрат на мощные дорогостоящие серверы.


☞ Модульность системы позволяет оптимально подобрать необходимые модули для Ваших задач, без лишних расходов на совершенно не нужный Вам функционал.

☞ Дополнительная терминальная административная консоль позволяет с лёгкостью управлять системой даже с мобильного телефона (через низкоскоростные каналы связи, такие как GPRS), что делает систему гибкой и лёгкой в обслуживании.

☞ Система устанавливается на свободную операционную систему GNU/Linux, что уменьшает затраты на покупку дорогостоящих операционных систем.

☞ Операционная система Linux, на данном этапе её развития, считается надёжнейшей системой, из имеющихся систем в мировом сообществе. Что само по себе, влечёт повышение безопасности ваших сетей, уменьшение затрат на аварийные ситуации и непредвиденные простои по причине сбоев и неполадок.

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жиляева Анна	стр. 3 из 23
--------------	---------------------------------	-----------------------------------	--------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business


Комплекс позволяет:

1. Контролировать потребление трафика внешней сети пользователями внутренней сети
2. Защитить ресурсы внутренней сети и самого сервера
3. Получать отчётность по использованию трафика внешней сети.
4. Получать отчёты по действиям сотрудников.

Дополнительные характеристики системы.


- ☒ Возможность использования неограниченного количества внешних и внутренних интерфейсов
- ☒ Распределённое вычисление трафика (использование нескольких шлюзов доступа в Internet при одной БД и единой административной консоли)
- ☒ Использовать систему совместно с DHCP сервером (упрощает настройку рабочих станций и позволяет работать нескольким пользователям с одной рабочей станции)
- ☒ Возможность использовать систему совместно с прокси-сервером Squid (как обычным, так и прозрачным), что способствует как повышению безопасности, так и установлению более жёсткого контроля над посещением ресурсов, и удаления нежелательных элементов web - страниц.
- ☒ Возможность использования как внутреннего парсера логов Squid (автоматическое занесение данных напрямую в БД TraffPro), так и программного обеспечения сторонних разработчиков. Так же допускается одновременное использование обоих видов контроля.
- ☒ Гибкая система прав административных консолей позволяет не нарушать структуру вашей организации и назначать права управления системой, в соответствии с занимаемой должностью сотрудника.
- ☒ Автоматическая настройка NAT или маскардинга, в зависимости от предпочтений администратора
- ☒ Удобная система обновления продукта до актуальных версий (без утомительных последовательных обновлений от версии к версии), позволяет пропускать несколько предыдущих версий и в любой момент актуализировать вашу систему.
- ☒ Модульность системы позволяет оптимально подобрать модули, необходимые для решения задач именно вашей организации.
- ☒ Система с лёгкостью справляется с каналами во внешнюю сеть 100 мегабит и более.

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жиляева Анна	стр. 4 из 23
--------------	---------------------------------	-----------------------------------	--------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business


- ☞ Система имеет многоязычный интерфейс, может быть (самостоятельно или по запросу) переведена на ваш родной язык.
- ☞ Для большей надёжности, вы можете использовать защищённые соединения в информерах пользователей (клиентов) и административных консолей.
 - ☞ Дополнительные параметры и конфигурационные файлы системы позволяют специалисту Linux-систем самостоятельно настроить параметры среды Linux для оптимизации в каждом конкретном случае.
 - ☞ Распределение нагрузки канала между пользователями и создание ограничений на скорость на различных тарифных планах. Скорость в системе может регулироваться плавно в широких пределах, а не скачкообразно, как во многих подобных системах учёта.

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жилиева Анна	стр. 5 из 23
--------------	---------------------------------	-----------------------------------	--------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

Термины и сокращения.

Термины и сокращения	Определения
TraffPro	Система учёта и контроля Internet-трафика (Traffic and Protection)
БД	База данных MYSQL
Демон	Бинарный исполняемый файл (программа), запущенная как сервис, работающий в фоновом режиме

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

I. Установка Traffpro.

Перед началом установки Traffpro, вы должны убедиться в том, что у вас установлены следующие пакеты:

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

Перечень пакетов приведен для дистрибутивов: Fedora, Redhat, CentOS.

Если вы планируете использовать связку Squid + Traffpro, то уберите из автозагрузки Squid, иначе будут конфликты. При старте Traffpro сам запустит Squid.

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

Перед началом установки, выключите **selinux**. Для этого, приведите конфигурационный файл /etc/selinux/config вот к такому виду:

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

Рекомендуется перезагрузить сервер.

#установка необходимых пакетов:

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

#запуск необходимых служб:

```
service mysqld start
```


```
service httpd start
```

```
#####
```

```
##Установка пароля root для доступа к MySQL:
```

```
#!/usr/bin/mysqladmin -u root password 'новый пароль'
```

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жилиева Анна	стр. 7 из 23
--------------	---------------------------------	-----------------------------------	--------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

**#Смену пароля пользователя root рекомендуется делать после установки
#Траффпро, или нужно сменить скрипт запуска установки базы mysql. Это
#затруднительно для большинства.**

```
#
#Перезапуск MySQL:
#service mysqld restart
#####
```

#распаковка архива установочного пакета системы Traffpro:
tar -zxvf traffpro.X.X.X-XX.tar.gz -C /tmp

```
#Переход во временную директорию и запуск установки:
cd /tmp/traffpro.X.X.X-XX
./install.sh
```

Дальше все интуитивно понятно, процесс установки производится в стиле вопрос-ответ.

После окончания установки, проверяем конфигурационные файлы TraffPro:

Содержимое файлов может отличаться, в зависимости от выбранных вами ответов во время установки системы.

Пример :

```
/etc/traffpro/traffpro.cfg:
# определение, в каком режиме будет запущено приложение - true
# запускается в режиме демона, false
# запускается в режиме обычного консольного приложения
daemon=true
# адрес базы данных
# Возможные значения (localhost, 127.0.0.1, 10.10.0.1)
# Обычно значение отличное от localhost используется для
# распределенной схемы учета трафика.
db_url=localhost
# Порт подключения к MySQL.
Порт необходимо указывать в том случае, если вы сменили порт в конфигурационном
файле /etc/my.cnf
# Параметр по умолчанию 3306
db_port=3306
# имя пользователя базы данных mysql, под чьими правами будет подключаться система
# по умолчанию это root и пустой пароль.
# Более подробно смотрите на сайте http://traffpro.ru
db_usr=root
# пароль на доступ к системе для пользователя db_usr
db_passwd=
# имя базы данных, к которой подключается система
# В старых версиях имя было office, в новой traffpro.
```

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жилиева Анна	стр. 8 из 23
--------------	---------------------------------	-----------------------------------	--------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

db_name=office

*# время ожидания перед отправкой данных в базу данных
чем меньше этот параметр тем больше и быстрее растет база данных.*

time_out=720

*# Влияет на время авторизации, рекомендуемое значение 10.
Чем больше значение, тем реже демон обращается к БД за проверкой изменений.*

time_in=10

*# Включение/отключение контроля MAC адресов для клиентов true/false.
Рекомендуемое значение - true.*

control_eth_addr=true

Номер шлюза сети (применяется при распределённом учёте трафика, при единственном шлюзе устанавливается в ноль 0)

net_number=0

Детализация по портам - в случае false ограничение по портам сохраняется, но лог ведётся обобщенно по всем портам, т.е. в отчетах не будет деления по портам.

ports_detail=true

*# Включение защиты, сервера и учета трафика самого сервера.
При включении этого параметра, добавляем сервер в web админке.
WEB-админка -> Система -> Серверы - Добавить Сервер.
При добавлении указываем внешний IP.*

ss_enabled=true

*# Указываем карточку с внешним интерфейсом.
Узнать можно ifconfig -a*

eth_out=eth3

*# Детализация www страниц.
Возможные значения true/false.
С версии 1.2-XX и выше, сквид больше не нужен для ведения логов посещений ресурсов.
Теперь при значении true демон ведет учет посещений своими ресурсами.
При параметре false возможно использование squid для работы с Траффпро, но учет посещений будет идти только по портам идущих через прокси сервер.*

url_detail=true

*# Внимание демон сам подстраивает буфер но не советуем делать размер пакетов больше 200 так как это около 12 мегобайт и большой размер буфера при форс мажоре замедлит работу демона, а не ускорит
Размер очереди пакетов*

ip_queue_maxlen=2048

Если параметр указан то поднимается NAT а если не указан то MASQUERADE

out_ip=192.168.1.200

*# Включение монитора, если параметр стоит в false то ниже два параметра выключены, если в true
то нижнее два параметра не забываем.*


monitor_on=true

Адрес прослушивания для монитора (если не указывать параметр то по умолчанию 127.0.0.1)

listen_addr=192.168.1.200

Порт прослушивания для монитора (если не указывать параметр то по умолчанию 9999)

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жилыева Анна	стр. 9 из 23
--------------	---------------------------------	-----------------------------------	--------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

listen_port=9999

Упразднен с версии 1.3.3-9X, для запуска создан отдельный скрипт /etc/init.d/tp-scheduler

Запускать таймер true, не запускать false

Выполнение SQL запросов или sh скриптов. Данные для запросов берутся из админки.

timer=false

Путь установки. Тут содержаться все рабочие файлы Траффпро.

to_install_dir=/opt/traffpro

Использовать squid для учета посетителей ресурсов сети пользователями.

При значении true - прокси сервер нужно убрать из авто загрузки и тогда

прокси сервер будет запускаться через скрипт запуска Траффпро.

Для правильной работы нужно внести следующие данные в конфигурационный файл squid.conf

Данные параметры нужно внести в конфиг squid, согласно структуре конфигурационного

файла squid, так как он чувствителен к расположению параметров.

#squid_connect=true

Данный параметр указывает местоположение файла, который будет

использоваться для передачи файлов в базу данных mysql.

Владелец файла станет root, если вы решите отменить данный параметр,

смените потом владельца файла (chown squid.squid access.log)

#squid_log_file=/var/log/squid/access.log

Блокировка сайтов демоном. Т.е. при использовании данного параметра,

не нужно для блокировки ресурсов использовать

стороние сервисы, такие как squid, squidGuard, iptables.

url_block=true

Данный параметр отвечает за учет icstr запросов и др. отличных от udr и tcr,

т.е. без этого параметра в мониторе активности системы

не будут отображаться. Если true параметр активен, если false выключен.

not_udptcp_control=true

Максимально количество запросов на соединение за время time_in от клиента

antiflood=500

Отключение обратного определения ip -> domain для отчётов о посещениях

not_resolv_dn=true

Брать данные о маршрутах, и поднятия NAT из базы данных.

Данные нужно вносить через web-админку.

nat_data_in_db=true

Вести учёт по шлюзам, т.е. сколько трафика с какого шлюза.

log_route=true

для плагина PPPD- говорит плагину, что если не нашёл в базе traffpro

пускай ещё и секрет файлы проверит, если true, т.е. файлы где хранятся логин и пароли.

secret_files=false

Агрегация таблицы посетителей ресурсов клиентами. Значение по умолчанию включено true.

Для отключения установите в false


url_agregate=false

Тип шейпера. true - линейный одна очередь на всех клиентов системы.

false - распределённый каждый клиент имеет свою очередь (по умолчанию)

shaper_type_linear=false

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жилиева Анна	стр. 10 из 23
--------------	---------------------------------	-----------------------------------	---------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

```
# Включение/выключение, учета трафика демоном с вашей железки (Cisco).
# Возможные значения этого параметра on, off, comb.
# Включено on (учёт только по netflows) off (отключено)
# comb (учёт и методами ядра линукс и netflows одновременно)
enable_netflow_type=on
# Настройки netflow. Предназначен для сбора информации об IP-трафике внутри сети.
# Для подсчета трафика с Cisco.
# Адрес, по которому прослушиваются пакеты netflow с отправляемые с вашей железки
netflow_addr=192.168.0.237
# Порт, по которому прослушиваются пакеты netflow с отправляемые с вашей железки
netflow_port=8818
```

Пример

/etc/traffpro/traffpro_rule.cfg:

```
#Позволит не потерять контроль над сервером
#при включённой защите сервера.
iptables -A INPUT -m tcp -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -m tcp -p tcp --sport 22 -j ACCEPT
```

#Проверьте доступ к данным файлам:

ls -l /etc/traffpro/

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

#Проверьте, создалась ли база:

mysqlshow - покажет все базы данных, если вы не меняли название базы, то должна появиться БД TraffPro.

#Если все в порядке, запускаем Traffpro:

service traffpro start

#Проверим, запустилась ли система учета трафика:

ps x | grep traffpro | grep -v "grep"


Должно отобразиться следующее:

```
2621 ? Ssl 1:34 /opt/traffpro/billing-daemon/bin/billing daemon=true
```

#Если все работает, проверяем, будут ли запускаться сервисы при старте системы, и, при необходимости, добавляем необходимые сервисы в автозагрузку:

```
chkconfig --levels 345 mysqld on
chkconfig --levels 345 httpd on
chkconfig --levels 345 traffpro on
```

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жилиева Анна	стр. 11 из 23
--------------	---------------------------------	-----------------------------------	---------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

II. Просмотр статистики посещений сайтов пользователями:

Первый способ:

Включить нужный параметр в конфигурационном файле (/etc/traffpro/traffpro.cfg):
url_detail=true

Внимание! Если вы используете эту функцию, установка кеширующего DNS сервера, обязательна!

Этот параметр включает возможность просмотра посещений пользователей, без учета количества скачанного с каждого ресурса.

Второй способ:


(использование Traffpro+Squid):

1. Установка squid.
yum install squid
1. Настройка squid
vi/etc/squid/squid.conf

Пример конфигурационного файла squid (/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
http_access deny all
```

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жиляева Анна	стр. 12 из 23
--------------	---------------------------------	-----------------------------------	---------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

```

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

# Обязательно, если в качестве приёмника логов используется
TraffPro
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

```

Обратите внимание на то, что пользователь, от имени которого вы запускаете **squid**, должен иметь права на чтение/запись файлов кэша и логов squid. Также укажите DNS сервера - **dns_nameservers**.

3. Включение следующих параметров в конфигурационный файл (/etc/traffpro/traffpro.cfg):

```

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

```


4. Настройка MySQL
vi /etc/my.cnf

```

[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

```

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жилиева Анна	стр. 13 из 23
--------------	---------------------------------	-----------------------------------	---------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

```

table_cache=2048
sort_buffer=64M
record_buffer=256M
max_connect_errors=100
connect_timeout=300

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

```

Исправления связаны с предоставлением больших ресурсов mysql, чем в стандартных настройках.

Так же рекомендуется подправить стандартный конфигурационный файл **apache** сервера.

Особенно обратить внимание на следующие параметры:

```

<Directory />
  Options FollowSymLinks
  AllowOverride None
</Directory>

```


Options Indexes FollowSymLinks

AddDefaultCharset

DirectoryIndex index.php index.html index.html.var

Более подробно о назначении этих параметров читайте на <http://apache.org/>

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жиляева Анна	стр. 14 из 23
--------------	---------------------------------	-----------------------------------	---------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

III. Настройка связи TraffPro + NetFlows v9 v5

Для настройки системы требуется изменить конфигурационный файл и добавить или отредактировать параметры:

Адрес, по которому коллектор будет принимать входящие данные от систем, генерирующих NetFlows

`netflow_addr=192.168.0.237`

Порт, по которому коллектор будет принимать входящие данные от систем, генерирующих NetFlows


`netflow_port=8818`

Режим работы модуля NetFlows

Может принимать 2 значения on/off

`enable_netflow_type=on`

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жиляева Анна	стр. 15 из 23
--------------	---------------------------------	-----------------------------------	---------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

IV. Описание настройки DHCP сервера.

TraffPro имеет возможность задавать для клиентов статические адреса и сохранять данные в конфигурационный файл dhcp. В целях безопасности, не рекомендуется сохранять данные в основной конфигурационный файл.

Рекомендации и последовательность действий.


Установим пакеты:

```
yum install dhcp или apt-get install dhcp3-server
```

Перейдем к редактированию конфигурационных файлов.

```
#
# DHCP Server Configuration file.
# see /usr/share/doc/dhcp*/dhcpd.conf.sample
#
# оставляем без изменения
# имя-сервера; (в кавычках)
server-name "router";
# Сервера синхронизации времени, список IP-адресов – через запятую;
(приоритетный - вперед)
option ntp-servers 192.168.10.1;
option time-servers 192.168.10.1;
Изменение времени года. Зима, Лето.
# 1440 - летнее, 10800 - зимнее
option time-offset 14400;
# Доменное имя
option domain-name "rumyancevo.local, kursakovo.local, rosinka.local";
#
option domain-name-servers rumyancevo.local;
# DNS сервера
option domain-name-servers 192.168.10.1;
# Netbios сервер.
option netbios-name-servers 192.168.10.1;
option netbios-dd-server 192.168.10.1;
# Если используется самба, то используем этот параметр.
option netbios-node-type 8;
# Шлюзы, если несколько, то через запятую.
option routers 192.168.10.1;
#option dhcp-renewal-time 3000;
# Маска подсети
option subnet-mask 255.255.255.0;
# Широковещательный адрес
```

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жилыева Анна	стр. 16 из 23
--------------	---------------------------------	-----------------------------------	---------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business


```

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;
#оставляем без изменения ведение лога
log-facility local7;
# Порт, который слушается dhcp сервером.
Local-port 67;
# использовать DNS для определения по IP-адресу значения опции hostname
get-lease-hostnames true;
deny duplicates;
Основная подсеть.
subnet 192.168.10.0 netmask 255.255.255.0 {
interface eth1;
#Временные клиенты.
pool {
range 192.168.10.250 192.168.10.254;
allow unknown-clients;
}
# Курсаково.
pool {
include "/etc/dhcp/dhcp-rumyancevo.conf";
range 192.168.10.10 192.168.10.249;
deny unknown-clients;
}
}
#Второй vlan, интерфейс eth1:1.
subnet 192.168.12.0 netmask 255.255.255.0 {
interface "eth1:1";
# Временные клиенты.
pool {
range 192.168.12.250 192.168.12.254;
allow unknown-clients;
}
}
# Румянцево.
pool {

```

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жилиева Анна	стр. 17 из 23
--------------	---------------------------------	-----------------------------------	---------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

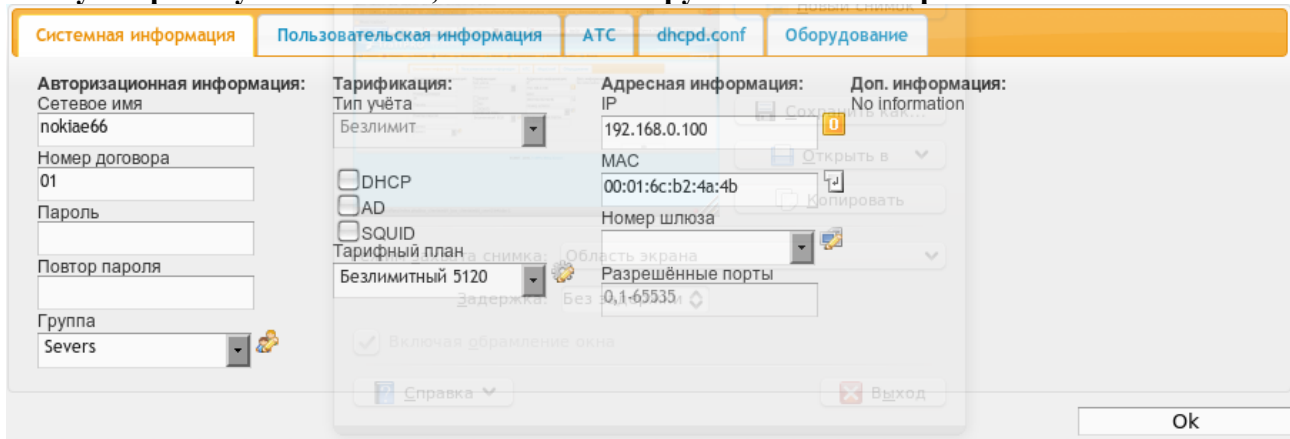
```
include "/etc/dhcp/dhcp-kursakovo.conf";
range 192.168.12.10 192.168.12.199;
deny unknown-clients;
}
pool {
include "/opt/traffpro/from_traffpro.conf";
range 192.168.12.200 192.168.12.249;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.10.255;
option domain-name-servers 192.168.10.1;
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;
}
}
```

Нас интересует кусок выделенный красным именно, его мы добавим в админке, и туда же будут сохраняться данные **/opt/traffpro/from_traffpro.conf**.




Дальше перейдем к созданию нового пользователя.

Галку **dhcp** не нужно ставить, если мы планируем запись в **dhcp.conf**



Создадим пользователя и нажмем «ОК». Откроем нового пользователя и перейдем на вкладку **dhcpd.conf**

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

Местоположение в dhcpd.conf

root

Сохраняем «ОК»

Перейдем сразу после этого в «Система» - «Сервис» - «dhcpd.conf»

dhcpd.conf

До

```

После
host nokiae66 {
  hardware ethernet 00:01:6c:b2:4a:4b;
  fixed-address 192.168.0.100;
  option host-name "nokiae66";
  ddns-hostname "nokiae66";
}

```

Сохранить изменения

И проделаем следующие

dhcpd.conf

До

```

После
host nokiae66 {
  hardware ethernet 00:01:6c:b2:4a:4b;
  fixed-address 192.168.0.100;
  option host-name "nokiae66";
  ddns-hostname "nokiae66";
}

```

Сохранить изменения

Нажмем «Отослать»

dhcpd.conf

Сохранить изменения

Данные успешно записаны в /opt/traffpro/from_traffpro.conf

До

```

После
host nokiae66 {
  hardware ethernet 00:01:6c:b2:4a:4b;
  fixed-address 192.168.0.100;
  option host-name "nokiae66";
  ddns-hostname "nokiae66";
}

```


Сохранить изменения

Проверим записались данные или нет.

`cat /opt/traffpro/from_traffpro.conf`

И перезапустим `service dhcpd restart` или `/etc/init.d/dhcp3-server restart`

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жилиева Анна	стр. 19 из 23
--------------	---------------------------------	-----------------------------------	---------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

Дополнительная информация.

- <http://prov.traffpro.ru/> - официальный сайт проекта
- <http://traffpro.ru/forum/> - официальный форум проекта

Пример использования TraffPro совместно со

squid версии (2.6 или 3.0):

На момент написания используются связки traffpro+squid, squid двух веток 2.6 и 3.0. Пример основан на версии squid 3.0

В конфигурационном файле, есть параметры, отвечающие за логирования посещений сайтов, т.е. кто, куда ходил.


1. **url_detail=true**
2. **squid_connect=true**
3. **squid_log_file=/var/log/squid/traffpro.log**

Если вы используете первый **url_detail=true**, то у вас будет в отчете отображаться только IP/HOST и количество подключений на него, но не будет отображаться количества скачанного.

Если вы используете 1, 2, 3 параметра вместе, то у вас отображается и количество скачанного по портам, идущим через прокси - сервер, количество скачанного с определенного ресурса, плюс вы можете увидеть посещение по портам, идущим мимо прокси, но количество скачанного отображаться не будет.

Использование сразу трех параметров увеличивает нагрузку на сервер, так что если вы чувствуете притормаживание, лучше использовать какой-то один параметр, или увеличить

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жилыева Анна	стр. 20 из 23
--------------	---------------------------------	-----------------------------------	---------------


	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

ресурсы для нужного сервиса.

Вот пример с реально работающего сервера, со связкой \

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

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жилиева Анна	стр. 21 из 23
--------------	---------------------------------	-----------------------------------	---------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business


```

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
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
#####
После старта в директории логов squid, должен появиться файл
prw-rw-rw- 1 root root      0 2009-02-09 21:51 traffpro.log

```

Также выполните команду

Исполнитель:	Галеев Рустам Синяев Валерий	Кононенко Николай Жилиева Анна	стр. 22 из 23
--------------	---------------------------------	-----------------------------------	---------------

	Проект: Электронный документ	
	Документ	TraffPro (Traffic & Protection). Установка TraffPro.
	Дата:	20.02.2010
	Версия:	1.3.4 business

chkconfig --levels 2345 squid off

Можно перезапустить squid.