

FlowTuner 1.0

Руководство пользователя

Оглавление

Введение.....	3
Что такое FlowTuner.....	3
Типографские соглашения.....	3
Установка.....	5
Требования к системе.....	5
Теория работы FlowTuner.....	5
Установка FlowTuner.....	7
Настройка NAT.....	9
Настройка VPN на стороне клиента.....	10
Руководство оператора.....	11
Вход в программу.....	11
Основные понятия.....	11
Первые шаги.....	13
Работа с администраторами.....	13
Работа с пользователями.....	13
Настройки.....	15

ВВЕДЕНИЕ

В Ваших руках находится руководство пользователя FlowTuner 1.0. Во введении обсуждаются типографские соглашения, принятые в этом документе, дается инструкция по использованию руководства и краткое описание системы.

ЧТО ТАКОЕ FLOWTUNER

FlowTuner это автоматизированная система учета использования Internet. FlowTuner 1.0 обладает следующими возможностями:

- Возможность задания лимитов на использование Internet как для отдельных сотрудников, так и для целых отделов.
- Автоматическое отключение при исчерпании лимита.
- Просмотр статистики пользователями. Пользователь может зайти на специальную страничку и посмотреть статистику своих соединений при помощи обычного браузера.
- Удобный Web интерфейс администратора. Администрировать программу можно прямо из браузера через систему интуитивно-понятных меню.
- Возможность построения отчета по использованию Internet и его экспорта в другие системы.
- Все расчеты ведутся в режиме реального времени.
- Поддерживают операционные системы Linux и FreeBSD.

Все возможности FlowTuner подробно описываются в данном руководстве.

ТИПОГРАФСКИЕ СОГЛАШЕНИЯ

Для облегчения понимания материала руководства все вводимые определения обозначаются *курсивом*. Примеры кода выделены в темные блоки текста:

```
#!/bin/sh
echo 'пример скрипта'
```

Все имена файлов, пути, названия программ печатаются моноширным шрифтом, например, /opt/flowtuner.



Иногда в тексте встречаются важные замечания. Они помечены значком на полях, чтобы заострить внимание. Читайте замечания внимательно, в последствие это сможет сэкономить Вам много времени и сил.

Обычно текст руководства не зависит от используемой операционной системы, но некоторые замечания описывают особенности, связанные с работой FlowTuner под управлением какой-нибудь конкретной ОС. В таких случаях на полях рисуется значок с названием операционной системы. Если Вы используете иную



ОС, то можете смело пропускать такие абзацы.

УСТАНОВКА

Этот раздел предназначен для системных администраторов, которым необходимо установить FlowTuner 1.0. В отличие от всех остальных разделов, он разделен на части в которых описывается процедура установки в зависимости от типа операционной системы. Если читатель не собирается самостоятельно устанавливать FlowTuner, то этот раздел можно пропустить.

Если процесс установки покажется сложным, не отчаивайтесь: обратитесь на flowix.com и специалисты выполнят установку за вас.

ТРЕБОВАНИЯ К СИСТЕМЕ

Для работы FlowTuner необходим компьютер с процессором не ниже Pentium II (или аналогичным по быстродействию) и не менее 128Mb оперативной памяти.

Поддерживаются следующие операционные системы:

- Linux с ядрами 2.4.x, 2.6.x или новее
- FreeBSD 5.3 или новее

Для просмотра отчетов на стороне клиента необходимо установить Java Runtime Environment (JRE). Рекомендуется использовать версию 5.0 Update 4. JRE можно бесплатно скачать с сайта <http://www.java.com>



Внимание! Не используйте JRE 1.4.2р6 откомпилированную для FreeBSD, так как эта версия содержит ошибку, препятствующую работе базы данных. Рекомендуется использовать Linux JRE 1.4.2, для чего следует включить режим совместимости с Linux. Если Вы все же хотите использовать FreeBSD JRE 1.4.2р6, обратитесь в flowix.com за дополнительными инструкциями.

Для установки FlowTuner потребуется работающий компилятор gcc, заголовочные файлы, программы make и patch. В системе не должен работать демон rtpd, иначе FlowTuner не сможет нормально функционировать.

ТЕОРИЯ РАБОТЫ FLOWTUNER

Для доступа пользователей в Internet в FlowTuner используется технология Virtual Private Network (VPN). Данная технология обладает рядом преимуществ перед традиционным прямым подключением:

- Надежная аутентификация пользователей
- Защита от подмены ip- и mac-адресов
- Простота отключения пользователей
- Пользователи могут использовать Интернет с любого компьютера в сети
- Возможность надежного учета трафика

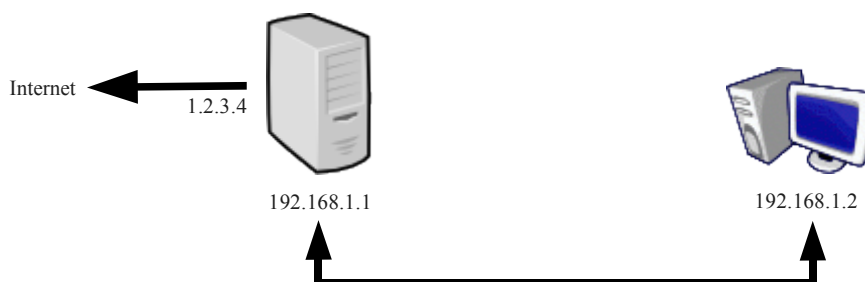
Технология VPN поддерживается всеми операционными системами, включая все версии Windows и не вызывает сложностей у пользователей, так как все диалоги привычны многочисленным пользователям Internet через модем.

Существуют разные технологии VPN. В последнее время наибольшее распространение получила технология на основе протокола PPTP (Point to Point Tunneling Protocol), поддерживаемая FlowTuner. VPN-соединение представляет собой туннель, имеющий два конца: один находится на стороне клиента, другой располагается на стороне сервера. Каждому концу туннеля присваивается IP-адрес. Обычно на стороне сервера этот адрес присваивается автоматически демоном PPTP, в то время, как на стороне клиента IP-адрес присваивается FlowTuner'ом.

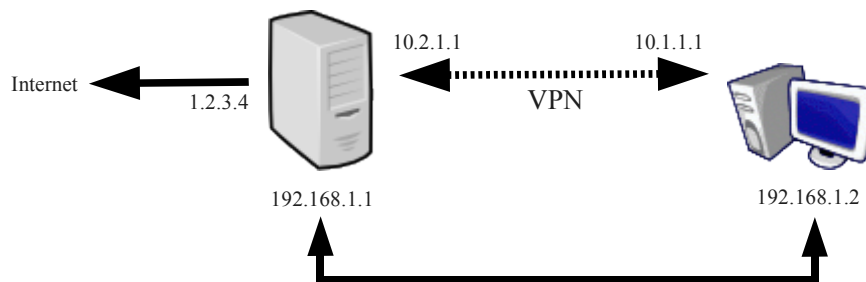
При установке VPN соединения FlowTuner проверяет имя и пароль пользователя, для чего используются надежные криптографические методы, что означает что злоумышленник не сможет “подсмотреть” чужой пароль с помощью программ мониторинга сети. После того, как соединение установлено, операционная система клиента начинает отправлять весь трафик через установившейся туннель, за исключением трафика относящегося к локальной сети клиентского компьютера, который посылается напрямую. Весь прошедший через VPN туннель трафик считается VPN сервером и, через указанные интервалы времени, передается FlowTuner'у. FlowTuner получает информацию о трафике, и, в случае необходимости, может принять решение о завершении соединения.

VPN соединения принимаются программой pptpd, которая в свою очередь запускает программу ppp, используемую для организации туннеля. Конструктивно FlowTuner представляет собой сервер RADIUS, к которому обращается ppp при установке, завершении или обновлении информации о сеансе связи. Для отключения пользователей используется демон pdsd.

Итак, представим себе ситуацию, когда имеется сервер, отвечающий за доступ в Internet и сеть состоящая из компьютеров пользователей. Сервер выходит в Интернет под IP-адресом 1.2.3.4, в локальной сети он виден под адресом 192.168.1.1. Пользовательские компьютеры имеют ip-адреса начиная с 192.168.1.2. Данная ситуация изображена на иллюстрации:



Теперь представим себе ситуацию когда все программы запущены, пользователь установил VPN соединение, образовался туннель с двумя адресами, один из которых находится на стороне клиента, а второй – на стороне сервера. Со стороны сервера туннелю был присвоен ip-адрес 10.2.1.1, со стороны клиента – 10.1.1.1.



Теперь весь трафик, не адресованный к сети 192.168.1. автоматически пойдет через VPN туннель и будет подсчитан FlowTuner'ом. Однако, для того, чтобы у пользовательского компьютера был доступ в Internet, необходимо обеспечить доступ в Internet с приватного IP-адреса 10.1.1.1.

Для обеспечения доступа в Internet можно применить два способа (а лучше комбинацию из обоих):

1. Использовать NAT
2. Использовать прозрачный прокси-сервер

NAT позволяет динамически заменять приватный IP-адрес клиентского конца VPN туннеля на IP-адрес сервера, т.е. в нашем примере адрес 10.1.1.1 будет автоматически заменяться на адрес 1.2.3.4, и клиентский компьютер получит доступ в Интернет.

При использовании прозрачного прокси-сервера все запросы идущие от пользователя к web-серверам будут перенаправляться на прокси-сервер, имеющий доступ в Internet.

Оба способа не требуют никаких настроек на стороне клиента. Имеет смысл использовать оба способа одновременно, что позволит сократить интернет-трафик за счет кеширования прокси-сервером и получить возможность проводить анализ того, на какие web-сервера ходят Ваши сотрудники.

Некоторые организации имеют несколько каналов подключения к Интернет. Иногда может потребоваться настроить FlowTuner так, чтобы разные пользователи выходили в Интернет через разные каналы (например, в учебном заведении может быть отдельный канал для студентов и отдельный канал для преподавателей). Для этого в FlowTuner можно сделать так что разным пользователям будут присваиваться IP-адреса из разных IP-подсетей (указать разные пулы IP-адресов), и настроить маршрутизацию и NAT на сервере таким образом, чтобы пакеты идущие из этих подсетей маршрутизировались через разные каналы.

УСТАНОВКА FLOWTUNER

Установка FlowTuner в UNIX-подобных операционных системах сводится к простому запуску программы инсталляции. Распакуйте дистрибутив, перейдите в образовавшийся каталог, запустите инсталляцию командой

```
./install
```

и подождите пока скрипт не закончит устанавливать программу. После окончания установки скрипт напишет адреса, при помощи которых можно попасть в web-интерфейс администрирования FlowTuner.

Сразу после установки следует указать FlowTuner расположение файла лога прокси-сервера (в случае, если планируется его использование). Для этого необходимо отредактировать файл `/opt/flowtuner/etc/sqscan.conf`.



При использовании JAVA из Linux в системе FreeBSD необходимо сначала смонтировать файловую систему `/proc`. Для этого добавьте следующую строчку в файл `/etc/fstab`:

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

Теперь для того чтобы смонтировать эту файловую систему достаточно написать команду

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



При использовании FreeBSD 5.x или старше следует установить пакет совместимости с FreeBSD 4.x (`compat-4.x`). Это можно сделать при помощи утилиты `/stand/sysinstall`.

Для запуска FlowTuner нужно использовать команду

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

Останавливать FlowTuner следует командой

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

На этом установку FlowTuner можно считать завершенной, однако рекомендуется заглянуть в файл конфигурации `http.conf` и создать свой секретный ключ `keystore`.

Файл `http.conf` содержит настройки, которые будут использованы FlowTuner для предоставления доступа к web-интерфейсу. В секции `<listeners>` задаются настройки протоколов HTTP и защищенного протокола HTTPS.

В свойствах протокола HTTP можно указать только порт по которому он будет доступен.

Протокол HTTPS защищен криптографически и позволяет исключить риск того, что кто-нибудь подсмотрит передаваемую через сеть информацию. HTTPS использует ключи которые хранятся в так называемом хранилище ключей. Ключ имеет пароль, кроме того само хранилище защищено паролем. Ключ должен быть подписан авторизованной организацией, однако возможна генерация "самоподписанных" ключей.

Для того, чтобы сгенерировать неподписанный ключ нужно набрать в командной строке следующую команду:

```
keytool -genkey -keyalg RSA -keystore <файл_keystore>  
-storepass <пароль_хранилища> -alias myself
```

и ответить на все вопросы. После этого полученный файл нужно скопировать в подкаталог `/opt/flowtuner/etc` и указать в файле `http.conf` имя файла

хранилища, пароль хранилища и пароль ключа.

Для проверки работы FlowTuner запустите его и обратитесь к web-интерфейсу администратора набрав в браузере в строке адреса

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

где localhost – адрес компьютера с FlowTuner, 8080 – номер порта для протокола HTTP из файла http.conf, cc.cgi – название программы администрирования. Кроме программы администрирования существует программы просмотра статистики stat.cgi.

Все эти программы доступны через протокол HTTPS. Для этого в браузере необходимо набрать в строке ввода адреса

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

Все поля имеют те же самые значения, что и для протокола HTTP, за исключением номера порта HTTPS.

По умолчанию в FlowTuner существует администратор с именем admin и паролем admin. Имя и пароль следует сменить сразу же после установки FlowTuner.

НАСТРОЙКА NAT

Для того, чтобы пользователи смогли выходить в интернет необходимо настроить преобразование адресов, выдаваемых клиентам в адреса, имеющие право выходить в Интернет. В первую очередь в интерфейсе администрирования следует зайти в меню “Настройки” -> “Адреса” и указать начальный и конечный IP-адреса, которые следует выделять клиентам. Далее в этом примере мы будем считать что клиентам присваиваются IP-адреса из подсети 10.1.1.0/255.255.255.0.



В Linux для включения NAT необходимо добавить в iptables правило NAT (пишется в одну строчку):

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

где eth0 – сетевая карта, через которую сервер выходит в Интернет, 1.2.3.4 – IP-адрес сервера, через который он выходит в Интернет, 10.1.1.0/24 – подсеть, используемая на клиентской стороне VPN туннеля.



В FreeBSD для настройки NAT в файле /etc/rc.conf необходимо включить демон natd и указать имя сетевой карты, которая будет использоваться для nat. Так же необходимо включить файрволл:

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

После этого в скрипте файрволла (обычно /etc/rc.ipfw) следует добавить правило, которое будет отправлять весь внешний трафик демону natd (пишется в одну строчку):

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

где 10.1.1.0/24 – подсеть, используемая на клиентской стороне VPN туннеля.

Далее следует настроить прозрачный прокси-сервер. Обычно в качестве прокси-сервера применяется squid. Для его настройки в качестве прозрачного прокси необходимо в файле конфигурации squid.conf найти и установить значения для следующих параметров:

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

В секции, отвечающей за настройку доступа нужно добавить подсеть VPN и разрешить ей доступ к прокси-серверу:

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

где 10.1.1.0/24 – подсеть, используемая на клиентской стороне VPN туннеля. Сделать это надо до правила, запрещающего доступ к прокси-серверу всем остальным пользователям (http_access deny all).

Для того, чтобы изменения вступили в силу, следует перезапустить squid.



Теперь остается только перенаправить трафик предназначенный для web-серверов на прозрачный прокси. В Linux для этих целей необходимо добавить следующее правило в файрволл (пишется в одну строку):

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

где 10.1.1.0/24 - подсеть, используемая на клиентской стороне VPN туннеля, 3128 – порт, на котором слушает squid.



В FreeBSD перенаправление на прокси-сервер так же делается в файрволе. Добавить в файл /etc/rc.ipfw следующую строку (пишется в одну строку):

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

где 10.1.1.0/24 – подсеть, используемая на клиентской стороне VPN туннеля.

После всех этих манипуляций система будет полностью настроена для использования FlowTuner.



Для улучшения безопасности рекомендуется запретить в файрволле трафик с адресов, используемых на клиентской стороне туннеля, проходящий через сетевые карты. Так же следует убедиться что никому кроме адресов, используемых на клиентской стороне туннеля, не позволено пользоваться squid (этому соответствуют настройки squid по умолчанию).

НАСТРОЙКА VPN НА СТОРОНЕ КЛИЕНТА

Настройка на стороне клиентский компьютеров сводится к настройке доступа через VPN. Во всех версиях Windows имеется встроенная поддержка VPN, за исключением Windows 95 для которой поддержку VPN надо скачивать отдельно с сайта microsoft.com.

При настройке доступа через VPN надо отключить шифрование трафика. Шифрование паролей рекомендуется включать, чтобы пароли не могли быть “подсмотрены” при передаче через сеть.

РУКОВОДСТВО ОПЕРАТОРА

Данный раздел описывает web-интерфейс FlowTuner. Освоить web-интерфейс будет значительно легче, если по мере чтения материала читатель будет заходить во все описываемые меню и выполнять все перечисленные в разделе действия.

ВХОД В ПРОГРАММУ

Для того, чтобы попасть в программу необходимо запустить браузер и написать в строке URL нечто похожее на

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

Рекомендуется работать по защищенному протоколу HTTPS (вторая строчка), чтобы предотвратить возможность утечки информации передаваемой через сеть.

Пользователи могут использовать для просмотра статистики примерно такой адрес:

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

О реальных названиях сервера и пути до программы пишет инсталлятор во время установки программы.

Для того, чтобы не набирать каждый раз длинный и плохо запоминающийся путь, сделайте закладку в браузере на странице ввода имени и пароля.

По умолчанию, есть только один пользователь с именем admin и паролем admin. Первое, что надо сделать при начале работы с FlowTuner – сменить пароль. Не желательно использовать в качестве паролей слова из естественных языков, имена, даты рождения и другие легко подбирающиеся слова. Для создания хороших легко запоминающихся паролей лучше использовать специальные программы – генераторы паролей.

ОСНОВНЫЕ ПОНЯТИЯ

Внешний вид интерфейса FlowTuner 1.0 показан на рисунке:

Слева располагается иерархическое меню, справа находится панель диалога. При выборе пункта меню и при нажатии на кнопки ввода и иконке в меню появляются дополнительные подпункты, поэтому первое время на панель меню надо обращать пристальное внимание.



При работе с web-интерфейсом никогда не пользуйтесь кнопкой браузера “Назад” (обычно изображается в виде стрелки влево). Ее использование в некоторых случаях может привести к нежелательному повторному вводу данных и другим неприятным эффектам.

Как правило таблицы показываемые в web-интерфейсе FlowTuner имеют слева колонку с набором иконок. Эти иконки используются для работы с данными таблицы. Наиболее часто встречаются следующие иконки:

<i>Иконка</i>	<i>Значение</i>
	Удалить строку
	Редактировать строку
	Экспортировать данные
	Напечатать данные
	Сохранить данные

При наведении указателя мыши на иконку появляется всплывающая подсказка которая объясняет значение иконки.

ПЕРВЫЕ ШАГИ

Первое, что надо сделать после установки FlowTuner – изменить пароль администратора. Для этого зайдите в пункт меню “Администраторы” и щелкните мышью на свойствах администратора. Появится диалог в котором вместо пароля будут показаны звездочки. Сотрите звездочки, введите новый пароль для администратора и нажмите на кнопку “Сохранить”. Более подробно о редактировании администраторов написано в следующем разделе.

Следующим шагом должно быть создание группы пользователей. Если не создано ни одной группы добавить клиентов будет невозможно. Для создания группы выберите меню “Группы”, введите желаемое имя группы (например, “Основная”) и нажмите кнопку “Добавить”. Новая группа немедленно появится в списке групп.

Теперь можно добавлять пользователей. Подробнее обо всех шагах читайте в следующих разделах руководства.

РАБОТА С АДМИНИСТРАТОРАМИ

Администраторами в FlowTuner 1.0 называются пользователи имеющие доступ к web-интерфейсу, то есть операторы системы биллинга.

Список администраторов можно просмотреть при помощи меню “Администраторы”. Сразу после установки системы в этом списке присутствует один администратор с правами “Администратор биллинга”.

Для добавления администраторов нужно использовать пункт меню “Администраторы”. При выборе этого меню внизу экрана появится форма, в которой имеется возможность задать имя входа, пароль и ФИО администратора. Поле доступ позволяет быстро включать и отключать доступ администратора. В случае, если доступ запрещен администратор не сможет войти в систему.

РАБОТА С ПОЛЬЗОВАТЕЛЯМИ

Пользователи управляются из меню “Пользователи”. Прежде, чем добавлять пользователей, надо создать хотя бы одну группу.

Пользователи располагаются иерархично. На верху иерархии расположены группы, которыми могут быть компании, факультеты, секции и т.п. Ниже по иерархии стоят отделы. Отделы имеют лимиты, в которые включаются пользователи.

Каждый отдел должен иметь хотя бы один лимит. Лимиты задаются на месяц, неделю или на день. Кроме того, есть специальный тип лимита, при котором ограничения задаются вручную. Для каждого лимита хранится остаток, выраженный в количестве мегабайт которые могут скачать пользователи. Когда остаток станет равным 0, все связанные с лимитом пользователи будут отключены.

Для создания подразделения выберите пункт меню “Пользователи”. Ссылка на диалог добавления подразделения будет находиться внизу страницы. Заполните данные о подразделении (Название, имя руководителя, комментарий, выберите группу) и нажмите на кнопку “Готово”. Теперь необходимо задать лимиты и связать с ними пароли на доступ в Internet.

Лимиты бывают разных типов. Можно установить лимит в день, неделю или месяц. Как правило используется лимит на месяц. Это означает, что каждого первого числа месяца остаток будет устанавливаться равным указанной в лимите сумме. Т.е. если лимит на месяц был равен 100 мегабайт, то первого числа месяца остаток на лимите будет приравнен к 100.

Специальный тип лимита “Вручную” означает, что никакие манипуляции с остатком не будут производиться автоматически. Такой режим обычно используется, когда пользователю выделяется трафик по требованию, например, после подписания соответствующей заявки.

При создании лимита нужно указать его тип, количество мегабайт доступных для скачивания по этому лимиту, описание лимита и указать, можно ли автоматически отключать и включать связанные с лимитом логины. Автоматическое отключение происходит когда остаток по данному лимиту становится равным 0. Отключенные логины могут автоматически включаться, когда остаток становится положительным.

Рядом с каждым лимитом есть набор иконок, которые позволяют удалить лимит, отредактировать его свойства, посмотреть соединения, изменить остаток, создать новый логин или посмотреть список www серверов, на которые ходили пользователи, включенные в этот лимит.

Изменение остатка называется “Операциями”. Оператор может вводить операции двух типов: приход (добавить трафик для скачивания) и расход (уменьшение остатка). При внесении операций с остатком в поле “Источник” записывается имя администратора.

При добавлении логина система автоматически генерирует имя входа и пароль пользователя, которые можно заменить на любые другие. Не допускается использование русских букв в именах входа и паролях. Пул адресов задает диапазон IP-адресов, которые будут присваиваться пользователю при установке соединения. Пользователь не сможет установить больше соединений, чем указано в поле “Одновременные подключения”.

Посмотреть, кто сейчас находится Online можно при помощи меню “На линии”. В этом меню можно сбрасывать пользователей с линии. Существует три способа отключения пользователей: первый способ подразумевает, что систем отправит серверу VPN запрос на отключение. Если по какой-то причине это не срабатывает (например, сервер VPN был аварийно перезагружен и “забыл” о таком пользователе), то можно удалить запись о том что пользователь был на линии и занести соединение в базу данных, либо удалить запись не учитывая соединение.

НАСТРОЙКИ

Меню “Настройки” позволяет редактировать различные опции используемые программой. Обычно в настройках требуется изменять только два параметра: IP-адреса и интервал обновления RADIUS. Меню состоит из нескольких подпунктов. В подпункте “RAS” задаются правила генерации имен входа и паролей, а так же устанавливается максимальная продолжительность сеанса связи (если она равна 00:00:00 то длительность не ограничена).

Меню “Адреса” позволяет создавать пулы IP-адресов, которые будут присваиваться пользователям при соединении.

Меню “RADIUS” содержит настройки встроенного в FlowTuner сервера RADIUS. Оно позволяет изменить номера портов сервера RADIUS и включить журнал записи пакетов (бывает полезно при настройке и решении проблем). Пункт “Интервал обновления” задает частоту, с которой FlowTuner будет получать информацию о состоянии соединений. Чем меньше это число, тем точнее будут отключаться пользователи.

В подпункте “RADIUS -> Серверы” задается список серверов доступа, с которыми будет работать FlowTuner. Обычно это будет сервер VPN на базе rrpdp, но возможно использовать и другие типы серверов доступа. Разные серверы доступа обладают разными возможностями. Для серверов на базе rrpdp всегда выбирайте одновременно возможности “Сервер удаленного доступа” и “POD” (это можно сделать при помощи щелчка мыши удерживая кнопку Ctrl). После добавления сервера доступа зайдите в его свойства, а оттуда в свойства возможности POD. Там задаются адрес, порт и пароль RADIUS которые будут использоваться для отправки запроса на отключение (Packet Of Disconnect). В случае, использования rrpdp за обработку POD отвечает pdsd, пароль и порт должны совпадать с теми, которые записаны в его файле конфигурации.