



# **D-Link DFL Traffic Counter**

**Система сбора и учета трафика для устройств  
D-Link серии NetDefend (DFL-210/260/800/860/1600/2500)**

**Руководство по установке  
Руководство по использованию**

Версия 1.9.8.927

## Содержание

Описание источника: роутеры D-Link серии NetDefend.....	3
История версий.....	5
Системные требования.....	8
Поддерживаемые устройства.....	9
Описание принципов работы.....	10
Установка.....	12
Ручная установка базы данных.....	16
Лицензирование.....	22
Настройка устройства.....	24
Первоначальная настройка.....	27
Установка и настройка web-интерфейса.....	31
Заключительные положения.....	40

## Описание источника: роутеры D-Link серии NetDefend

По мере того, как бизнес-процессы становятся все более зависимыми от сетевой инфраструктуры, капиталовложения, сделанные в решения по безопасности становятся все более



значимыми. D-Link представляет межсетевые экраны серии NetDefend нового поколения, являющиеся комплексным решением по обеспечению безопасности сетей предприятий. Серия NetDefend учитывает растущие требования, предъявляемые к сетевой безопасности, защите от атак хакеров, вирусным угрозам и повышению конфиденциальности информации. Каждый межсетевой экран этой серии обеспечивает высокий процент возврата инвестиций, благодаря поддержке широкого набора функций, гибкой настройке и высокому уровню защиты сети.

Устройства серии NetDefend представляют собой законченное решение в области безопасности, включающее встроенную поддержку межсетевого экрана, балансировки нагрузки, функций отказоустойчивости, механизма Zone-Defense, фильтрации содержимого, аутентификации пользователей, блокировки «мгновенных» сообщений и приложений P2P, защиты от атак «отказ в обслуживании» DoS и виртуальных локальных сетей VPN. Эти устройства соответствуют требованиям предприятий к безопасности и удаленному доступу, обеспечивая высокопроизводительное решение по разумной цене. В межсетевых экранах гармонично объединены расширенные функции, предоставляющие администраторам сетей решение безопасности «все в одном» business-класса.

Для того чтобы минимизировать влияние аварийной ситуации на всю сеть, межсетевые экраны поддерживают специальную функцию – Zone-Defense, представляющую собой механизм, позволяющий им работать с коммутаторами локальных сетей D-Link и обеспечивающий активную сетевую безопасность. Функция Zone-Defense автоматически изолирует инфицированные компьютеры сети и предотвращает распространение ими вредоносного трафика.

Аппаратная спецификация межсетевых экранов NetDefend включает высокоскоростные процессоры, большие базы данных и вычислительные мощности,

позволяющие обрабатывать до миллиона параллельных сессий. Устройства поставляются с несколькими, настраиваемыми пользователями интерфейсами, включая порты Gigabit Ethernet, позволяя развертывать гибкие, масштабируемые и свободные от «узких» мест сети, объединяющие между собой различные рабочие группы и предприятия.

Все межсетевые экраны данной серии поддерживают удаленное управление через Web-интерфейс или выделенное VPN-соединение. Они включают набор функций для мониторинга и поддержания состояния и безопасности сети, в том числе отправку уведомлений по email, ведение журнала системных событий и предоставление статистики в режиме реального времени. Эти функции, наряду с возможностью обновления программного обеспечения, гарантируют, что межсетевой экран сможет предоставить максимальную производительность и безопасность для сети.

Дополнительную информацию вы можете найти на сайте производителя по адресу <http://www.dlink.ru/products/firewall.php>.

## История версий

### 1.9 - 2008/09/27

- Лицензирование версии 3
- Формирование информационного сообщения и типа версии при загрузке приложения/службы и отображение их в web-интерфейсе

[Web интерфейс]

- Исправление отображения в IE модуля настроек и авторизации
- Отображение типа версии (free или pro)
- Общие настройки, сохраняемые в БД
- Добавлено отображение только тех строк, переданный или полученный объем которых превышает установленное в настройках значение, а также средство информирования об этом и полного отображения
- Добавлено разбиение списка посещенных узлов/служб по страницам

### 1.8 - 2008/09/15

- Поддержка сохранения имени пользователя (экспериментально)

[Web интерфейс]

- Добавлены дневные и месячные лимиты для клиентов на принятый трафик
- Введена настройка `$_CFG['showall']`, при установке которой в true "галочка" показывать все в фильтре становится всегда выбранной и неактивной
- В пользователи введены наряду с клиентами - с возможностью установки лимитов и фильтрации
- Добавлена авторизация – на основе конфигурационного файла или базы данных. Если она включена, то неавторизованные пользователи могут смотреть только статистику своего IP адреса. Привилегии авторизации подразумевают просмотр полной статистики, установку лимитов для клиентов и пользователей и полный доступ

### 1.7 - 2008/09/09

- Мелкие доделки Web-интерфейса
- Исправление утилиты `mege`

- Обрато добавлен список интерфейсов WAN, при загрузке приложение использует оба списка
- Скорректирована обработка NAT ICMP

#### 1.6 - 2008/09/06

- Отдельные списки адресов и интерфейсов WAN заменены на список соответствия WAN адресов к интерфейсам
- Сохранение информации о порте назначения и внешнем интерфейсе
- Игнорирование пакетов, приходящих по NAT-правилам (в направлении LAN → WAN) с WAN-адресом в назначении

#### 1.5 - 2008/08/28

- Добавлена поддержка conn\_close\_natsat путем учета пакетов по action=close
- Изменен учет отброшенных пакетов - по action=drop
- Добавлено исключение на ошибку в логе ALG, где перед url не ставится пробел
- Скорректирована обработка DROP-пакетов
- Добавлено логгирование пакетов, вызвавших ошибки выполнения
- Добавлено логгирование пакетов, которые были отброшены из обработки FILTER

#### [Приложение]

- Переработан интерфейс
- Добавлена функция сохранения в файл
- По умолчанию приложение не обрабатывает данные, включается это "галочкой"
- Добавлена мультиязычность
- Добавлено отображение обработанных URL и пакетов (принятых и отправленных)
- Пакеты помещаются не в многостроковой редактор, а в список, с подсветкой по строкам, копирование из которого в буфер осуществляется двойным щелчком
- Добавлен вызов настроек

- Добавлен фильтр в списке SysLog, возможность отключать отображение обработанных пакетов

#### 1.4 - 2008/08/20

- Переименование в dfltc
- Добавлена поддержка разделения с какого роутера (адреса) пришли данные
- Добавлена настройка внешних IP адресов - они будут сохраняться как локальные
- Добавлена поддержка сохранения информации с пакетов, прошедших по drop
- Добавлен список интерфейсов, пакеты между которыми будут игнорироваться
- Изменен дизайн web-интерфейса
- Добавлен фильтр по устройству
- Добавлены настройки клиентов и устройств

#### 1.3 - 2008/08/11

- Логгирование syslog, если соответствующая папка создана
- В приложение добавлен парсинг файла

#### 1.2 - 2008/01/04

- В daemon\_dfl800 добавлена поддержка нескольких локальных интерфейсов

#### 1.1 - 2007/02/24

- Информация о пакетах заносится в буфер в памяти и по таймеру переносится в БД

#### 1.0 - 2007/01/17

- Первая версия. Попакетная запись в БД

## Системные требования

Для корректного функционирования программного комплекса DFL Traffic Counter вам необходимы следующие условия:

1. IBM PC-совместимый компьютер под управлением операционной системы Microsoft Windows 2000 Professional, 2000 Server, XP Professional или Server 2003 с достаточными для установки и настройки службы и системного DSN (административными) правами, а также конфигурацией, обеспечивающей достаточно требуемое быстродействие (рекомендуется процессор не менее 1 ГГц, оперативная память не менее 256 МБ, 10 МБ на жестком диске для установки).

**Важно!** Поскольку требования к оперативной памяти и процессору являются константными и могут возрасти лишь с увеличением количества обрабатываемых данных, то требования к дисковому пространству будут увеличиваться постоянно так как в БД будут сохраняться данные за все предыдущие периоды. Пожалуйста учтите это и обеспечьте достаточный объем дискового пространства.

2. База данных MySQL версии 4.1, 5.0 или выше, обеспечивающая совместимость с синтаксисом версии 4.1.
3. Средства выполнения PHP скриптов с поддержкой MySQL, например web-сервер Apache HTTP Server версии 1.3, 2.0 или 2.2, PHP версии 5.0 с соответствующими настройками.
4. Драйвер MyODBC версии 3.51 (включен в дистрибутив).

**Важно!** Драйвер MyODBC версии 5.0 не поддерживается!

## Поддерживаемые устройства

От версии к версии, зачастую, меняется специфика формирования логов устройства. Исходя из этого, данный раздел содержит список устройств и версий их программного обеспечения, которые были протестированы.

- DFL-210
  - 2.12.00
  - 2.20.02
- DFL-800
  - 2.12.00
  - 2.20.01
  - 2.20.02

Если DFL Traffic Counter правильно работает и с другими устройствами/ версиями ПО, свяжитесь с нами по адресу [info@raesoftware.ru](mailto:info@raesoftware.ru) и мы дополним список!

## Описание принципов работы

Основным принципом работы программного комплекса DFL Traffic Counter является обработка только тех записей, которые подаются на его принимающую часть (приложение или службу). Обработка полученных данных производится на основании настроек программы, которые позволяют «разделить» пакеты, несущие информацию об использованном или отброшенном трафике от, например, служебных или отображающих запрошенные URL.

Структура базы данных программы подразумевает разделение на 2 части – «буфер» текущего дня (filter), в котором данные хранятся на почасовой основе, и суммарные данные, которые средством просмотра статистики через web разделяются по дням (total). Перенос данных с их аккумуляцией (для уменьшения размера БД) выполняется специальной отдельной программой (merge) по расписанию. Рекомендуемое время – в момент перехода суток.

Привязка запрошенных пользователями IP адресов к DNS осуществляется путем анализа ALG записей устройства (это означает, что использование ALG обязательно для получения привязки к DNS). Запрошенные пользователями DNS собираются в отдельной таблице и впоследствии привязываются к IP адресам утилитой dns.

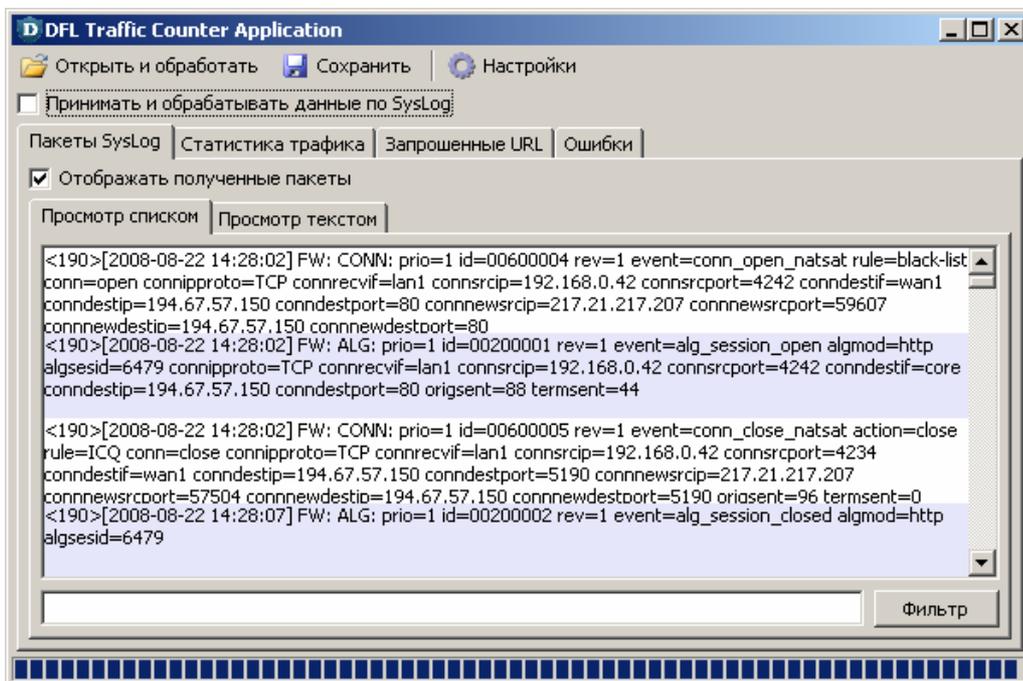
### Получение данных

Как отмечалось выше, данные получают специальным компонентом системы. Для удобства их выполнено даже 2 – приложение, обладающее графическим интерфейсом, предназначенное для отработки новых настроек, и служба, которая будет работать в режиме 24/7.

**Важно!** Возможна одновременная работа либо службы, либо приложения.

Оба компонента основываются на едином файле конфигурации, поэтому его изменение отразится и на приложении, и на службе (после их перезапуска).

Как отмечалось выше, приложение обладает графическим интерфейсом. Он позволяет вам фильтровать полученные записи при просмотре списком, просматривать текстом, приостанавливать обработку получаемых сообщений, обрабатывать сохраненные в файл сообщения SysLog.



Основным его назначением является проверка правильности конфигурации системы в моменты запуска и ввода новых функций.

### Периодические утилиты

Система подразумевает периодическое выполнение утилит merge (tcmrg.exe) и dns (tcdns.exe) – первую раз в сутки, вторую – раз в небольшое время, позволяющее успевать привязывать DNS и IP адреса.

Рекомендуется сделать это посредством планировщика Windows или другой аналогичной программы.

### Просмотр статистики

Просмотр собранных и обработанных данных выполняется путем отображения их через web-интерфейс.

**Важно!** Для web-интерфейса необходимы средства выполнения РНР с поддержкой MySQL.

В web-интерфейсе реализован просмотр как «буферной» (filter) части, так и суммарной (total) с поддержкой различной фильтрации. Также через него осуществляется привязка IP адресов устройств DFL и клиентов.

## Установка

**Важно!** Необходимо установить сервер базы данных MySQL и обеспечить его работу и доступность с компьютера, на котором будет выполняться программа DFL Traffic Counter.

Установка программы подразумевает создание и настройку базы данных, а также ODBC-источника, через который будет осуществляться доступ к базе данных, до начала использования программы. Вы можете выполнить установку полностью в автоматическом режиме или создать/обновить БД и источник ODBC вручную, что будет описано в следующем разделе.

В состав инсталлятора включен драйвер MyODBC, однако дистрибутив сервера MySQL из-за достаточно большого его объема и возможного присутствия во многих сетях, вам необходимо будет скачать самостоятельно с сайта производителя по ссылке <http://dev.mysql.com/downloads/mysql/4.1.html#windows32> (в случае использования версии 4.1) или <http://dev.mysql.com/downloads/mysql/5.0.html#windows32> (в случае использования версии 5.0).

**Важно!** Вы можете использовать и другие версии СУБД MySQL, однако они должны соответствовать поддержке версии 4.1 и иметь возможность подсоединения к ним драйвера MyODBC версии 3.51.

**Важно!** Драйвер MyODBC версии 5.0 не поддерживается!

### Установка сервера базы данных

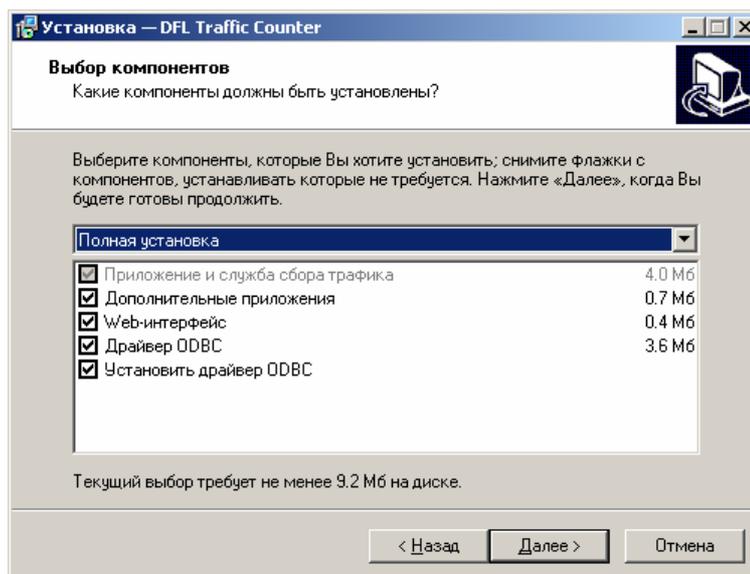
Если у вас нет установленной СУБД MySQL, скачанный инсталляционный пакет устанавливается практически автоматически – вам будет необходимо подтвердить папку установки на начальном этапе и выбрать диск для сохранения данных, а также указать административный пароль на завершающем – при конфигурировании.

### Установка пакета

Программа установки выполнена в виде традиционного инсталлятора Windows.



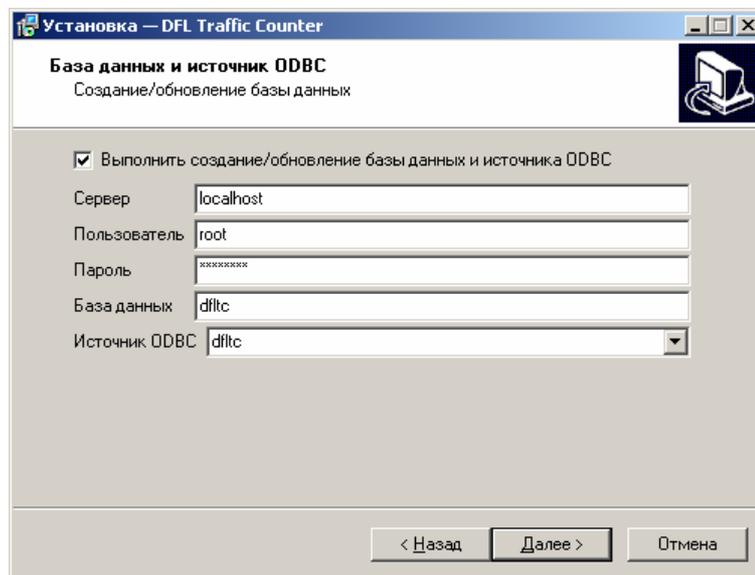
На начальном этапе вам необходимо будет выбрать устанавливаемые компоненты системы



Обязательный компонент **приложение и служба сбора трафика** является самым приложением, а также средством настройки. В состав **дополнительных приложений** входят такие утилиты, как получение MAC адреса устройств. **Web-интерфейс** скопирует, предложит установить отдельным инсталлятором и впоследствии настроить интерфейс для просмотра статистики, созданный на PHP. Также будет создан ярлык в меню Пуск, что позволит выполнить установку впоследствии. Если у вас еще не установлен драйвер MyODBC, то компонент **драйвер ODBC** скопирует его инсталлятор в подпапку ODBC папки установки программы, а задача **установить драйвер ODBC** – установит (или обновит) его.

При установке в первую очередь необходимо указать в какую папку установить программу и в какой группе разместить значки в меню Пуск.

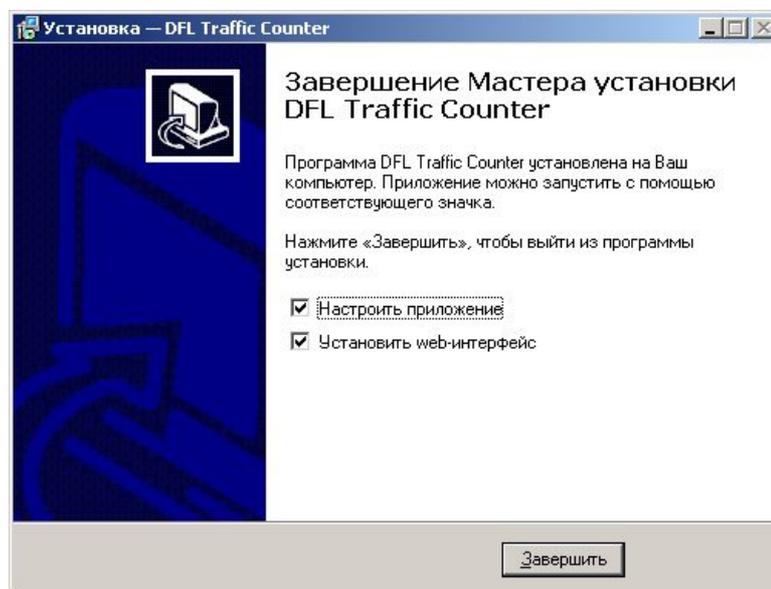
Завершающим, но очень важным шагом является инициализация/обновление базы данных. Введите параметры доступа к вашему серверу БД MySQL, название базы данных и имя источника ODBC (его можно выбрать из списка).



При каждом последующем обновлении вам необходимо будет вводить эти данные заново – это сделано для повышения безопасности.

Если вы не хотите выполнять автоматическую инициализацию/обновление БД, вам будет выдано соответствующее предупреждение. В этом случае, обратитесь к последующему разделу **«Ручная установка базы данных»**.

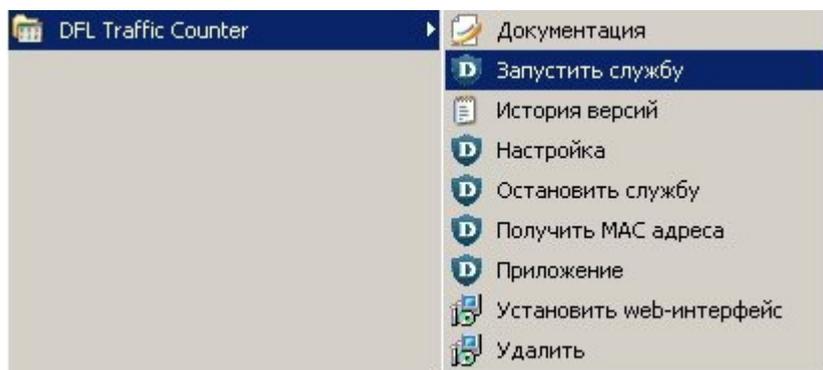
На последнем этапе программа установки предложит установить (распаковать и настроить) web-интерфейс (при условии его установки) и настроить приложение (второй из этих шагов будет описан в следующем разделе).



Вы можете выполнить любой из этих шагов или оставить их для последующего выполнения.

## Завершение установки

После этого, установку программы DFL Traffic Counter можно считать завершенной. В папку, указанную для установки, скопированы файлы и в меню Пуск созданы ярлыки



## Назначенные задания

В состав поставки программы входят 2 консольных приложения, которые служат для фоновой обработки данных из БД. Рекомендуется назначить их выполнение посредством инструмента «Назначенные задания»

- `tcdns.exe` – назначьте выполнение этой программы раз в 10-15 минут. Ее назначение – выбирать новые нераспознанные DNS-адреса из БД и делать привязку к IP адресам. Количество записей для единоразовой обработки задается в настройках.
- `tcmrg.exe` – программа для переноса первичной статистики (почасовой) в ежедневный архив. Назначьте ее выполнение сразу после окончания дня – она будет выбирать данные из ежедневных, удалять и помещать их в архив.

## Ручная установка базы данных

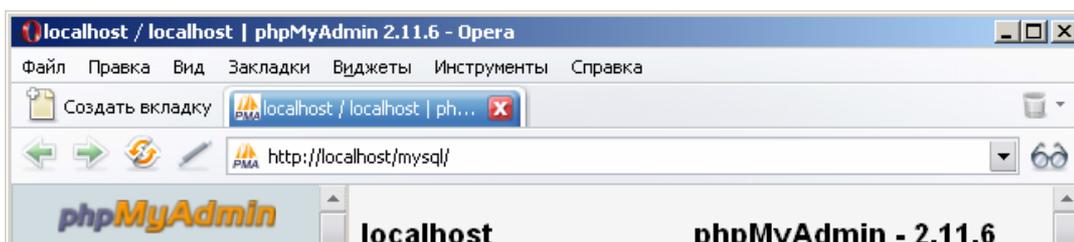
**Важно!** В ходе действий, описанных в этом разделе, вам могут понадобиться дополнительные средства администрирования MySQL, например MySQL Administrator (<http://dev.mysql.com/downloads/gui-tools/5.0.html>) или phpMyAdmin ([http://www.phpmyadmin.net/home\\_page/downloads.php](http://www.phpmyadmin.net/home_page/downloads.php)). Однако, это не означает обязательность этих продуктов. Вы можете использовать любые другие средства доступа к MySQL, обеспечивающие корректную работу.

### Создание базы данных

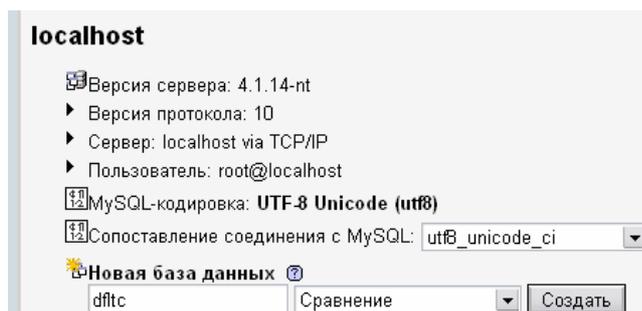
Подключитесь к серверу БД любым из удобных для вас средств – командной строкой, программами MySQL Administrator/Query Browser или phpMyAdmin. Дальнейшие действия будут приведены на примере обоих пакетов программ.

#### phpMyAdmin

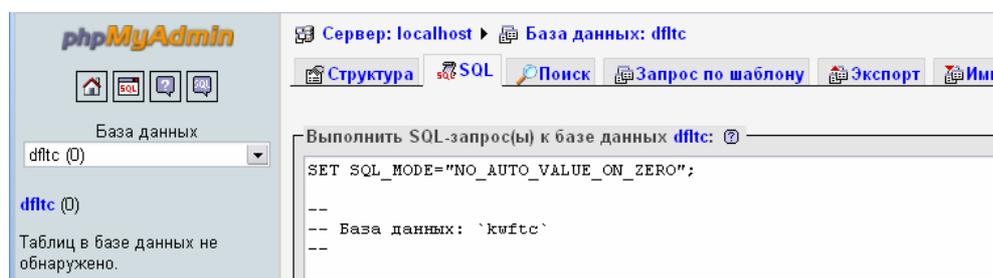
Для подключения к серверу БД в phpMyAdmin зайдите браузером на соответствующий адрес



Создайте пустую базу данных, например с именем `dfitc`.



Если администратор БД не перейдет в нее автоматически, выберите ее в списке слева, а потом выберите вкладку «SQL».



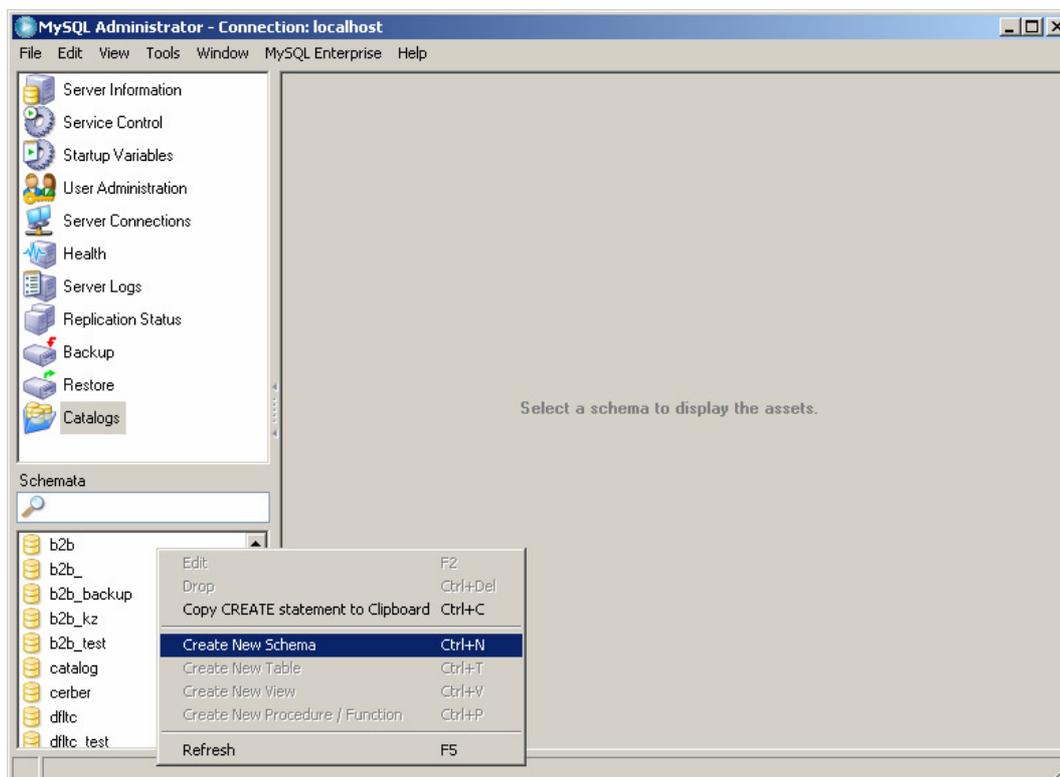
Вставьте в поле SQL-запроса код инициализации базы данных, находящийся в файле INITDB\base.sql и нажмите кнопку «ОК». Через несколько секунд, БД будет инициализирована.

## MySQL Administrator/Query Browser

Для подключения к серверу к серверу БД введите адрес, порт, логин и пароль для подключения к серверу.

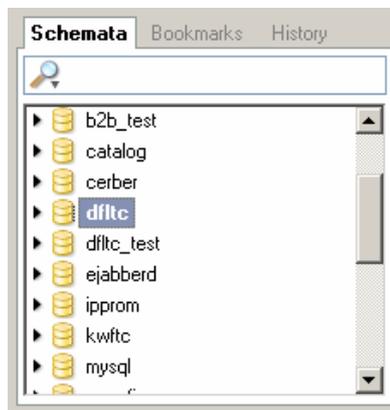


Создайте пустую базу данных (схему), например с именем dfltc.

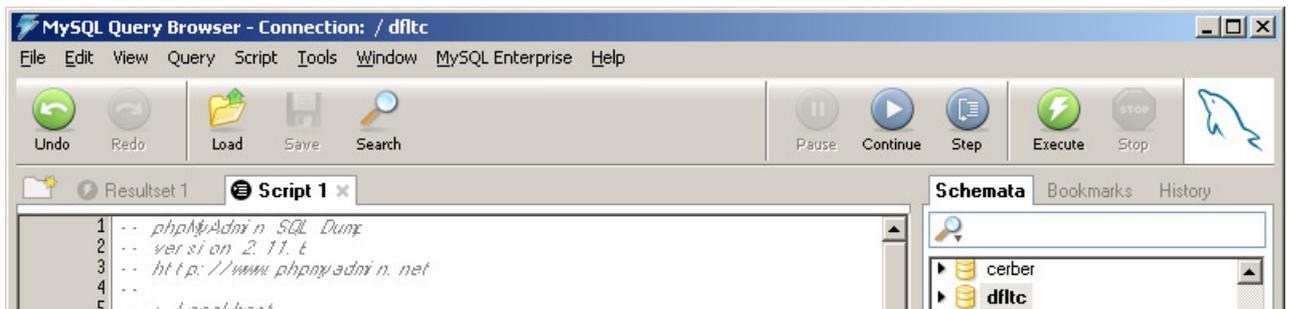


MySQL Administrator: SQL скрипт выполняется из программы MySQL Query Browser. Запустите его, выбрав пункт меню Tools-MySQL Query Browser.

Двойным щелчком выберите в списке справа созданную базу данных



Далее, откройте скрипт выбрав в меню File-Open Script.



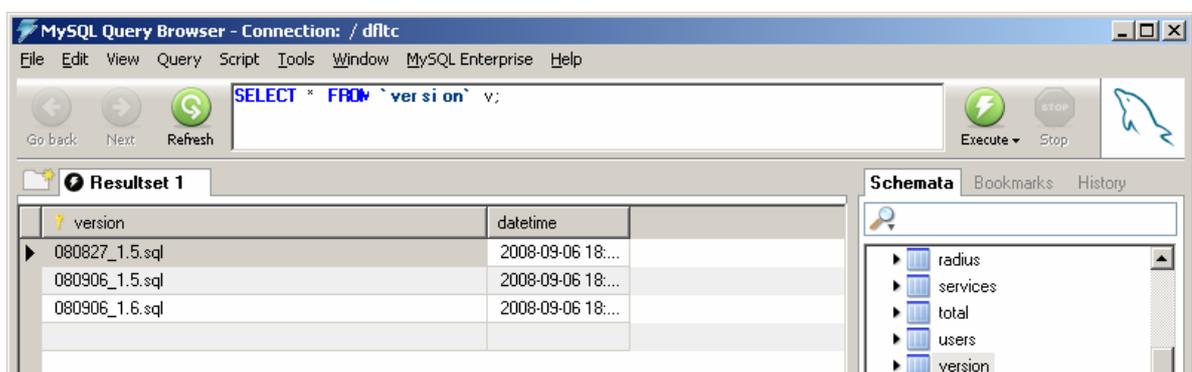
Для выполнения скрипта, нажмите кнопку Execute.

### Установка дополнений

Инициализационный скрипт базы данных содержит структуру БД версии 1.4. Для увеличения совместимости с другими версиями продуктов, все последующие изменения были выполнены в виде отдельных файлов.

В порядке следования имен (которые указывают на версии изменений), выполните остальные SQL-файлы (при условии наличия) из папки INITDB – они содержат обновления базы данных в зависимости от версий.

**Важно!** Для предотвращения повторного выполнения файлов при автоматическом обновлении БД, единожды выполненные файлы заносятся в таблицу version.



Если вы планируете впоследствии использовать автоматическое обновление структуры БД, добавляйте имена файлов установленных обновлений в эту таблицу. При использовании SQL это, например, можно сделать так:

```
INSERT IGNORE INTO version (version) VALUES ('имя файла.sql');
```

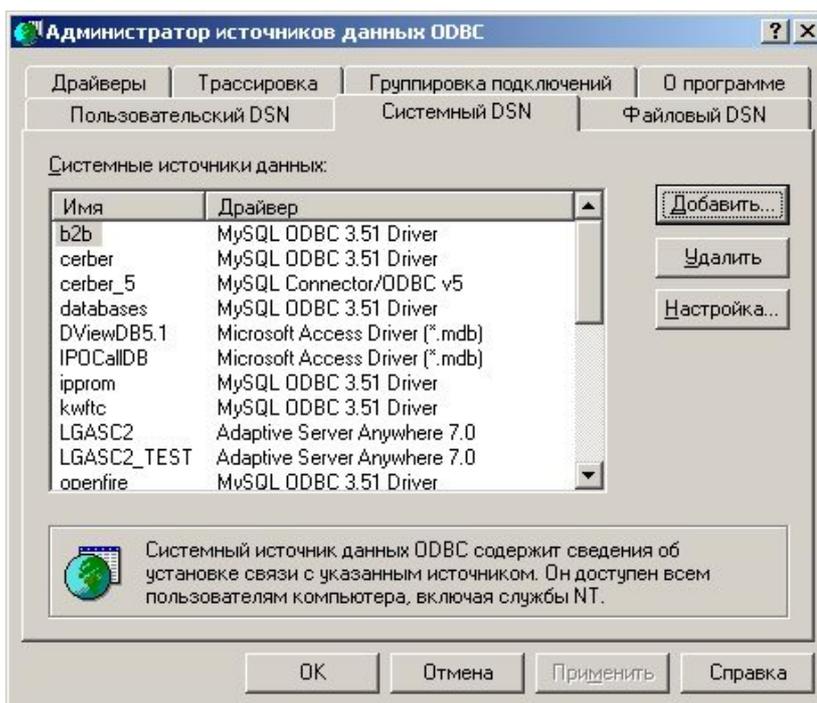
### Драйвер MyODBC

Драйвер MyODBC выполнен в виде Windows-инсталлятора mysql-connector-odbc-3.51.26-win32.msi и поставляется вместе с устанавливаемым приложением. Также всегда его можно скачать с сайта разработчика по адресу <http://dev.mysql.com/downloads/connector/odbc/3.51.html#windows>.

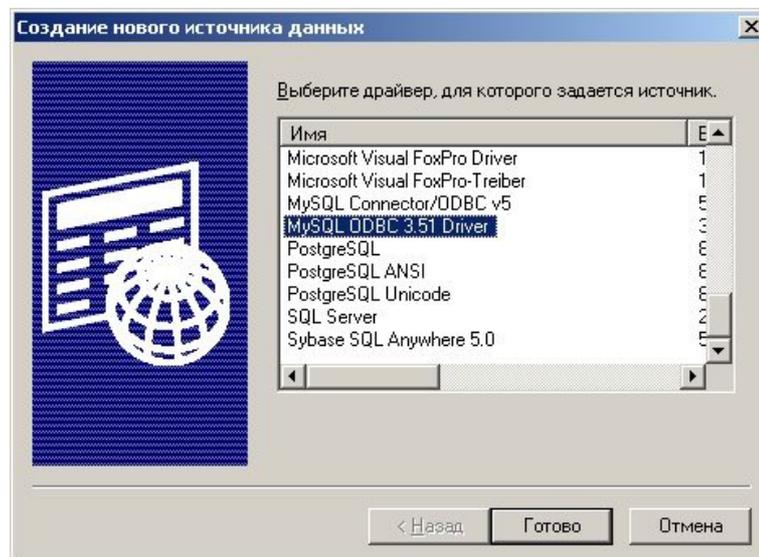
### Установка ODBC источника

После успешной установки драйвера необходимо создать ODBC-источник.

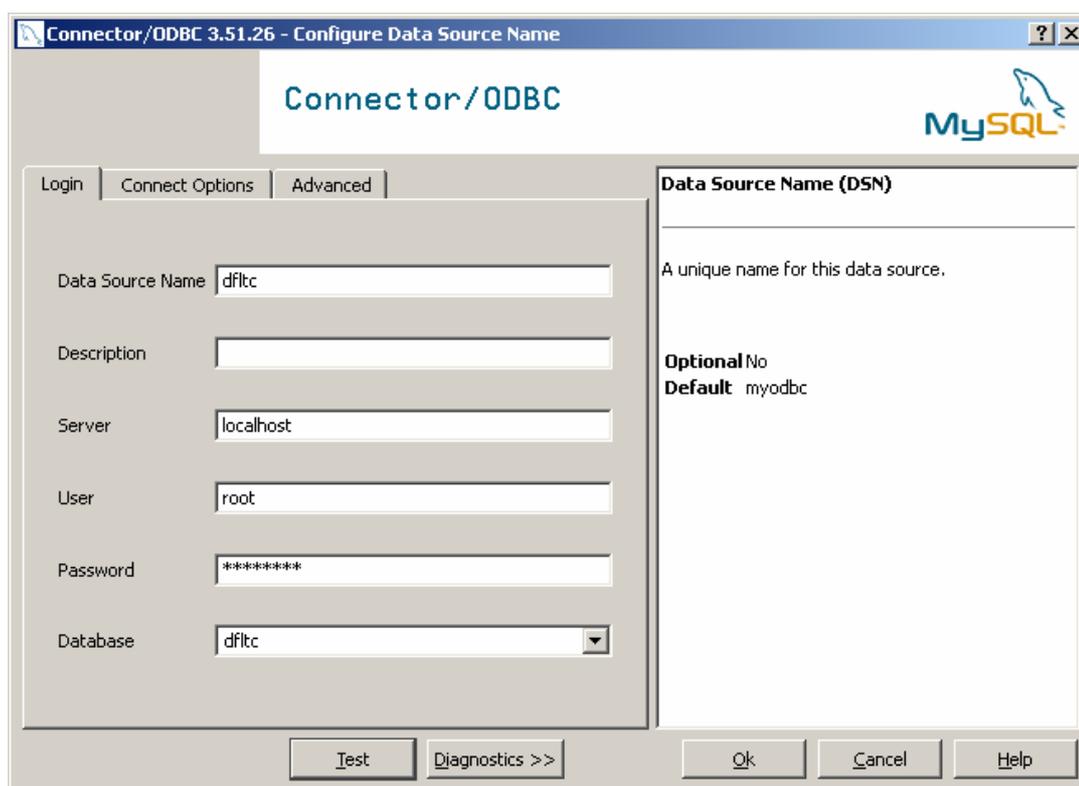
Запустите утилиту «Администратор источников данных ODBC», выбрав соответствующий пункт из меню Пуск → Настройки → Панель управления → Администрирование и выберите вкладку «Системный DSN».



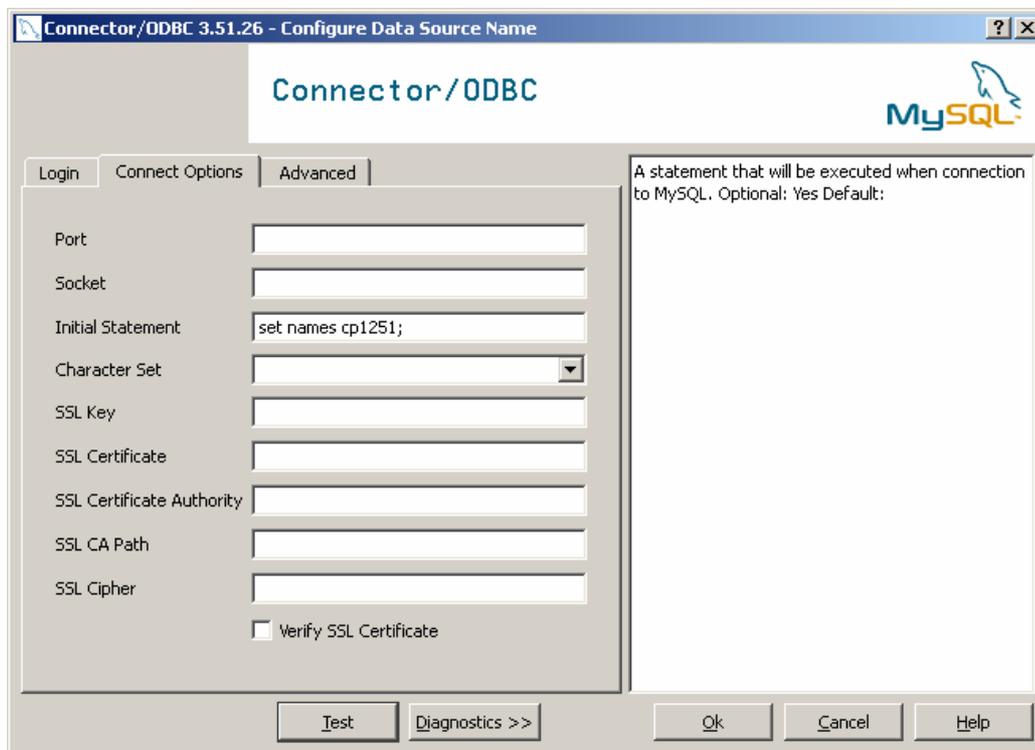
Нажмите кнопку «Добавить» и выберите в появившемся списке драйвер MySQL ODBC 3.51 Driver.



В появившемся окне введите название источника – «dfitc» и данные для доступа к БД – сервер, логин и пароль, а также выберите из списка БД ранее созданную для работы. Если вы хотите изменить название источника, не забудьте скорректировать соответствующие параметры при настройке программы.



Перейдите на вкладку Connect Options и укажите в поле Initial Statement выражение «set names cp1251;»



После указания всех параметров, нажмите кнопку «Test» – нижеследующее сообщение означает, что все прошло успешно.



Нажмите кнопку «OK» для сохранения источника.

## Лицензирование

Программный комплекс DFL Traffic Counter поставляется в двух вариантах:

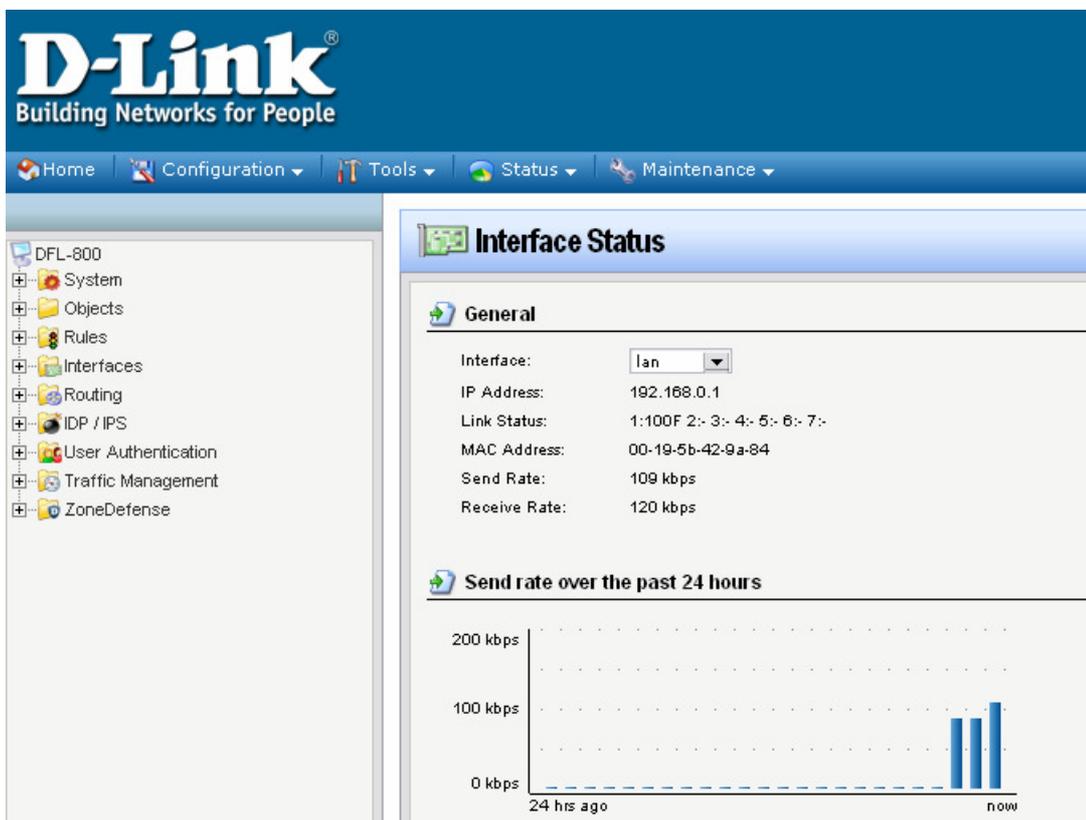
- FREE – бесплатно, имеет ограничения
  - Количество компьютеров для учета трафика ограничено 10
  - Количество устройств, с которых принимается информация, ограничено 1
- PRO – поставляется на платной основе, однако не содержит в себе вышеуказанных ограничений – учитывает информацию о трафике со всех компьютеров и неограниченного количества устройств.

Для перевода вашей версии FREE в PRO, свяжитесь с разработчиками по адресу [sales@raresoftware.ru](mailto:sales@raresoftware.ru), однако для регистрации вам необходимо будет получить список MAC адресов вашего устройства (устройств).

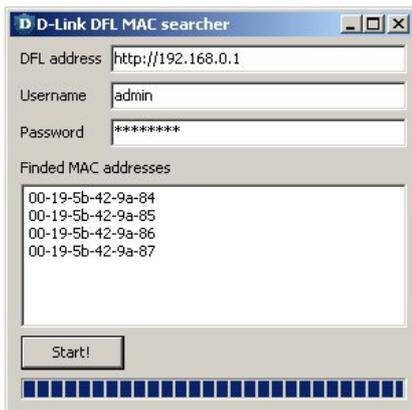
### Получение MAC адресов

Для того, чтобы вы могли зарегистрировать вашу версию программы и использовать все ее возможности, наряду с оплатой необходимы данные вашего роутера. Из можно получить двумя способами:

1) Подключившись по web-интерфейсу к роутеру, выбрав Status → Interfaces, и там перебирая, получить полный список MAC адресов



2) При помощи входящей в комплект программы DFL MAC searcher – запустите указанную программу из меню Пуск.



Введите данные для доступа и нажмите кнопку «Start» – через несколько секунд программа отобразит список MAC адресов вашего устройства.

**Важно!** В текущих версиях поддерживается только HTTP метод доступа (не HTTPS).

### Лицензионный файл

До загрузки лицензионного ключевого файла, ваша копия программы будет работать в ограниченном режиме.

После получения лицензионного файла, для загрузки его в программу, скопируйте его в подпапку LIC в папке установки программы и перезапустите службу/приложение.

После этого, зайдите в web интерфейс и проверьте, что логотип программы изменился



Статистика  
[Данные текущего дня](#)

Фильтр. Поля с незадаанными значениями

## Настройка устройства

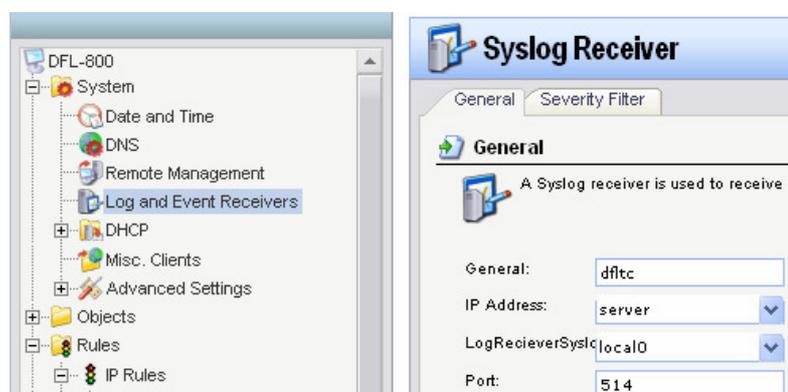
Кроме настройки программы по обработке поступающей информации, вам необходимо настроить логгирование.

### Настройка syslog

Во-первых, необходимо создать получателя для отправки сообщений. Зайдите в System-Log and Event Receivers и добавьте Add-Syslog Receiver.



Введите аналогичные приведенным ниже настройки для доступа к вашему серверу. Учтите, что по идеологии устройства, желательно вместо прямого указания IP адреса использовать запись из Address Book.



Перейдите на вкладку Severity Filter и добавьте Debug в список отправляемых сообщений.

### Логгирование правил

Программный комплекс DFL Traffic Counter будет получать лишь ту информацию, которая к нему будет отправляться. Поэтому для всех правил, трафик по которым необходимо учитывать, необходимо включить логгирование.

Перейдите в Rules-IP Rules и по очереди, выбирая соответственные правила, установите им настройки логгирования.

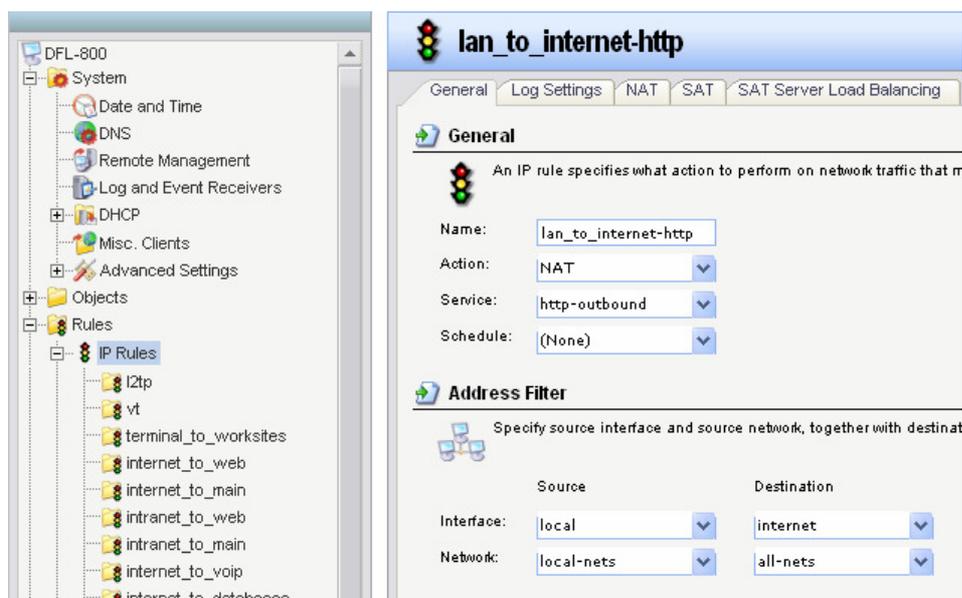


Учтите описанный выше нюанс логгирования SAT-правил – либо лог включается для Allow-правила, либо для SAT.

## Логгирование URL

Кроме учета трафика, в возможности программы входит обработка и последующее отображение запрошенных адресов. Для этого вам необходимо отдельное правило для службы HTTP со включенным ALG, которое должно быть «выше» пропускающего правила по умолчанию:

26	lan_to_internet-http	NAT	local	gMain	internet	all-nets	http-outbound
27	lan_to_internet-https	NAT	local	gMain	internet	all-nets	https
28	lan_to_internet	NAT	local	gMain	internet	all-nets	all_services



Важно учесть, что сервис http-outbound (на примере) использует ALG



The image shows a screenshot of the Mikrotik WinBox configuration interface. On the left is a tree view of the device configuration, with 'Services' selected under the 'Objects' category. The main panel displays the configuration for the 'http-outbound' service.

**General**

A TCP/UDP Service is a definition of an TCP or UDP protocol with specific parameters.

Name: http-outbound  
Type: TCP  
Source: 0-65535  
Destination: 80

Pass returned from ICMP error messages from destination  
 SYN flood protection (SYN Relay)

**Application Layer Gateway**

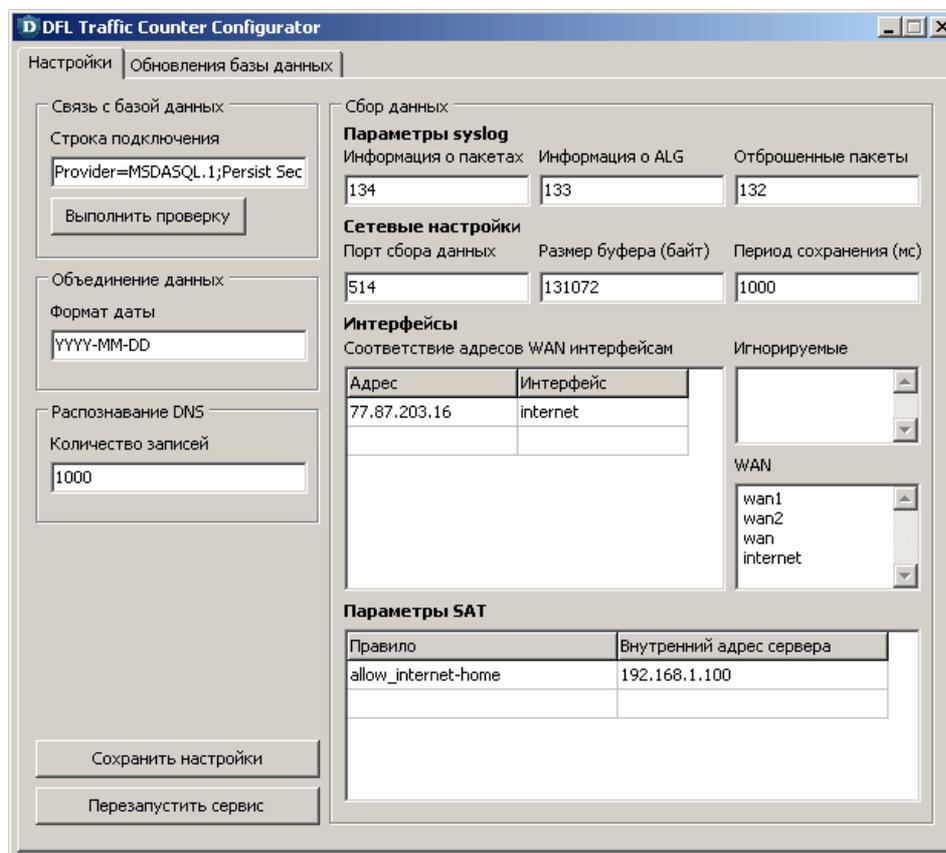
An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service

ALG: http-outbound  
Max Sessions: 1000

На этом настройка устройства завершена.

## Первоначальная настройка

Первоначальная (равно как и последующая) настройка программы выполняется специальным приложением, входящим в состав поставки или ручным редактированием файла config.ini.



Основными параметрами являются параметры сбора данных.

### Уровни сообщений

Одним из составляющих syslog-стандарта является указание, с каким уровнем идут сообщения. Исходя из этого, их можно разделять еще до детального анализа, что существенно ускоряет работу программы.

Ниже представлены начала трех основных обрабатываемых сообщений

- Закрытия соединения (условием отбора является наличие подстроки event=conn\_close)  
<134>[2008-08-11 08:49:47] FW: CONN: prio=1 id=00600002 rev=1 event=conn\_close action=close  
<134>[2008-08-26 19:32:23] FW: CONN: prio=1 id=00600005 rev=1 event=conn\_close\_natsat action=close
- Отброшенных пакетов (условием является event=ruleset\_drop\_packet)  
<132>[2008-08-11 07:49:21] FW: RULE: prio=3 id=06000051 rev=1 event=ruleset\_drop\_packet action=drop
- Адресов HTTP (условием отбора является event=request\_url)  
<133>[2008-08-11 16:42:40] FW: ALG: prio=2 id=00200125 rev=1 event=request\_url

Соответственно вашим пакетам, внесите цифровые (на примерах выделены цветом) значения уровней.

**Важно!** Если вы не знаете, с какими уровнями идут ваши сообщения, запустите приложение `dflltcarr.exe` – оно аналогично службе, но отображает лог на экран.

### **Сетевые настройки**

Немаловажными являются сетевые настройки. Стандартным портом для получения `syslog`-сообщений является 514, однако он может быть изменен при необходимости.

Размер буфера определяется в байтах и должен быть тем больше, чем активнее обмен пакетами.

Период сохранения указывается в миллисекундах и в секунды переводится делением на 1000 (т.е., 5000 это 5 секунд).

### **Интерфейсы и SAT**

На логику разбора пакетов очень сильно влияют параметры интерфейсов.

В списке **соответствия адресов WAN интерфейсам** внесите все внешние – на физических и логических WAN интерфейсах – IP адреса и соответствующие им интерфейсы. Такая привязка требуется из-за специфики обработки устройствами D-Link DFL HTTP-трафика – сначала получение со внешнего интерфейса устройством, а потом отдача в сеть от `core`. Сами списки WAN интерфейсов и их адресов необходимы для корректного определения направления трафика.

Если у вас есть **WAN интерфейсы**, которые не вошли в предыдущий список по причине отсутствия статического IP адреса, внесите их в соответствующий список.

Если на вашем устройстве настроен логгинг также некоторых дополнительных правил, не выпускающих пакеты в Интернет, то учитывать их не надо. Для этого служит список **игнорируемых интерфейсов** – если пакет содержит оба интерфейса из этого списка, он не будет обрабатываться. Не забудьте включить туда «`core`» – сам роутер.

**Параметры SAT** предназначены для преобразования правил для порт-маппинга (SAT) в IP адреса внутренних компьютеров при логгировании Allow-правил.

Как вы знаете, для разрешения SAT необходимы 2 правила – SAT, которое выполнит маппинг порта, и Allow, которое разрешит доступ к устройству. Соответственно, первое без второго не будет работать, а второе без первого – бесполезно.

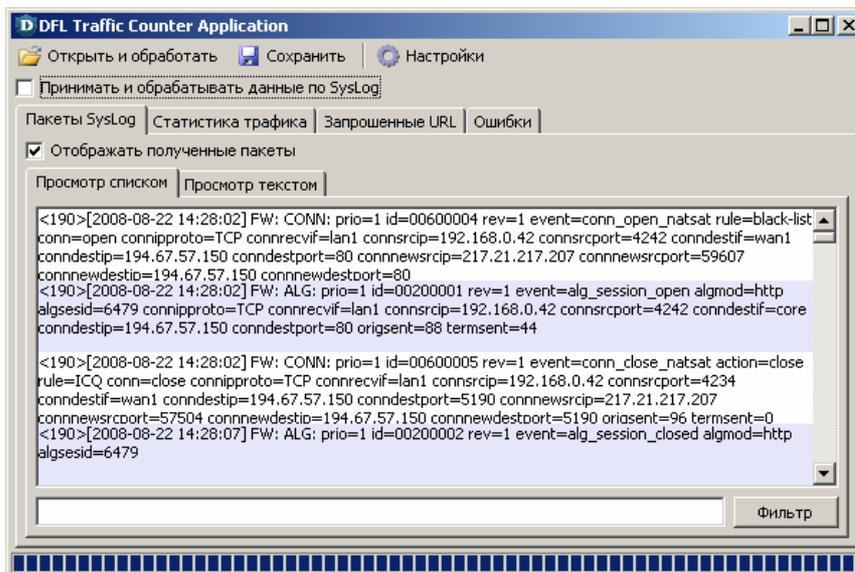
Существует 2 варианта логгирования SAT – по SAT-правилам и по Allow.

В первом случае, включите Log для всех правил SAT. Это позволит сразу получать корректные адреса внешнего источника и внутреннего назначения.

Для случая, когда это выполнить в силу различных причин невозможно, предусмотрена поддержка Allow правил. Неудобство их учета заключается в том, что в правиле фигурируют IP адреса внешнего клиента и WAN-порта устройства. Для этого в настройках программы предусмотрен раздел «Параметры SAT», в котором для каждого Allow-правила из цепочек SAT необходимо указать внутренний IP адрес используемого сервера, какой указан в соответствующих правилах SAT.

**Важно!** Включайте логгирование только либо SAT, либо Allow правил для одной цепочки правил порт-маппинга! Логгирование и тех и других может привести к неправильному отображению количества использованного трафика.

**Замечание.** Если у вас возникают трудности в момент настройки, то на этот период советуем вам использовать приложение вместо службы. Оно снабжено графическим интерфейсом с возможностью отображения, что позволит вам контролировать работу комплекса.



**Важно!** Не забудьте проверить подключение при помощи соответствующей кнопки, а также перезапустить службу после каждого изменения конфигурации!

Теперь, программа готова к работе!

## Установка и настройка web-интерфейса

**Важно!** Перед установкой web-интерфейса обеспечьте установку и функционирование средств выполнения PHP с поддержкой MySQL. Как это сделать на примере Apache HTTP Server, описано ниже.

### Готовые комплекты программ

Вместо ручной установки и настройки каждого компонента, вы можете воспользоваться инсталляторами требуемых продуктов и/или программами автоматической настройки.

К примеру, продукт проекта «Денвер» (<http://www.denwer.ru>) является уже настроенными требуемыми приложениями.

Также, вы можете скачать предустановленный комплект Apache+PHP с нашего сайта по адресу [http://www.raresoftware.ru/downloads/apache\\_php.zip](http://www.raresoftware.ru/downloads/apache_php.zip)

### Установка Apache HTTP Server

Для получения последней версии интересующей вас ветки продукта (1.3, 2.0 или 2.2) обратитесь к странице загрузки <http://httpd.apache.org/download.cgi>.

После скачивания инсталляционного пакета необходимой вам версии программы, запустите его. Процесс установки не потребует от вас сложных настроек – все будет выполнено автоматически и необходимо будет только подтвердить или указать отличную от стандартной папку для установки программы, а также указать параметры имени сервера и запуска.

### Установка и настройка PHP

Последнюю версию PHP можно скачать с официального сайта загрузки - <http://www.php.net/downloads.php>.

В отличие от Apache HTTP Server, PHP поставляется в виде архива и требует ручной установки.

Распакуйте скачанный вами архив в удобное вам место, например C:\PHP. В этой папке, переименуйте файл `php.ini-recommended` в `php.ini` и откройте для редактирования.

Найдите, раскомментируйте и укажите значение параметра `extension_dir` в соответствии с примером:

```
extension_dir = "c:/php/ext/"
```

Сохраните и закройте файл php.ini.

Откройте файл конфигурации Apache HTTP Server, выбрав пункт меню Пуск-Программы-Apache HTTP Server-Configure Apache Server-Edit the Apache httpd.conf Configuration File или открыв файл CONF\httpd.conf папки установки Apache HTTP Server.

Найдите блок <IfModule dir\_module> и установите его значение DirectoryIndex в соответствии с примером

```
DirectoryIndex index.php index.htm index.html
```

Перейдите в конец файла и добавьте строки

```
LoadModule php5_module "c:/php/php5apache.dll"
```

```
AddType application/x-httpd-php .php
```

```
PHPIniDir "C:/php/"
```

Имя загружаемой библиотеки php5apache.dll отличается в зависимости от версии Apache HTTP Server и может быть следующим:

- Для версии 1.3 – php5apache.dll
- Для версии 2.0 – php5apache2.dll
- Для версии 2.2 – php5apache2\_2.dll

Учтите это и необходимость изменять пути на соответствующие вашей конфигурации при настройке.

Сохраните файл httpd.conf и перезапустите службу Apache HTTP Server.

При необходимости (если будет не найдена) скопируйте библиотеку php5ts.dll из папки установки PHP в папку C:\WINDOWS\system32.

### **Включение поддержки MySQL**

**Важно!** Сервер MySQL должен быть установлен и функционировать.

Откройте файл php.ini в соответствующей папке.

Найдите строку extension=php\_mysql.dll и раскомментируйте (уберите символ «;» в начале строки) ее.

Сохраните файл php.ini и перезапустите службу Apache HTTP Server.

При необходимости (если будет не найдена) скопируйте библиотеку libmysql.dll из папки установки PHP в папку C:\WINDOWS\system32.

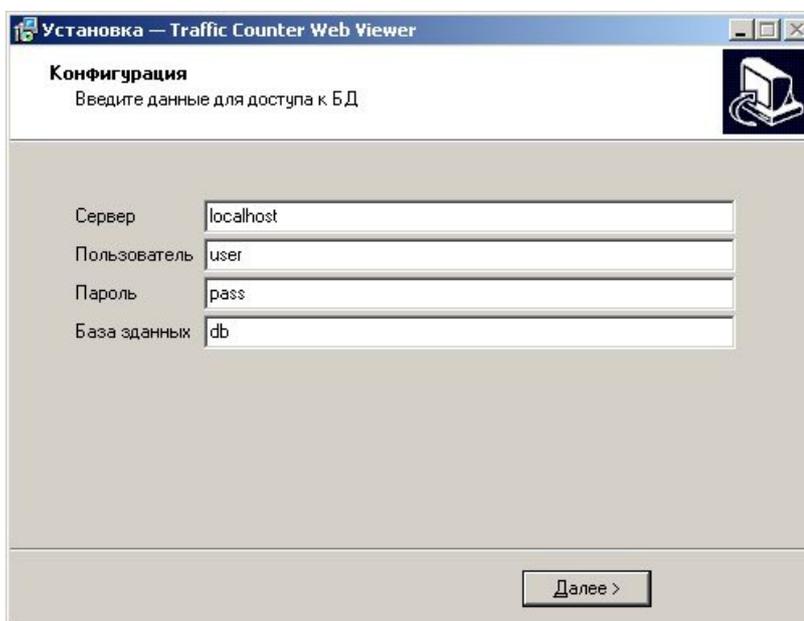
## Установка web-интерфейса

Web-интерфейс предлагается установить сразу после установки программы, однако при необходимости это можно выполнить позднее, выбрав соответствующий пункт в меню Пуск.

Установка web-интерфейса выполнена в виде аналогичного инсталлятора и потребует на начальном этапе только указания папки, куда следует копировать PHP скрипты.

**Важно!** Папка для установки web-интерфейса должна быть опубликованной вашим web-сервером. По умолчанию для Apache HTTP Server это C:\Program Files\Apache Software Foundation\Apache\htdocs.

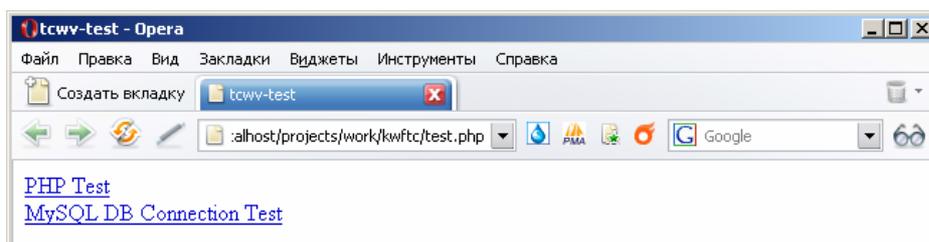
На завершающем этапе, при условии отсутствия в папке назначения файла конфигурации, вам будет предложено указать параметры доступа к БД.



После этого, файл конфигурации config.php будет создан и web-интерфейс готов к работе.

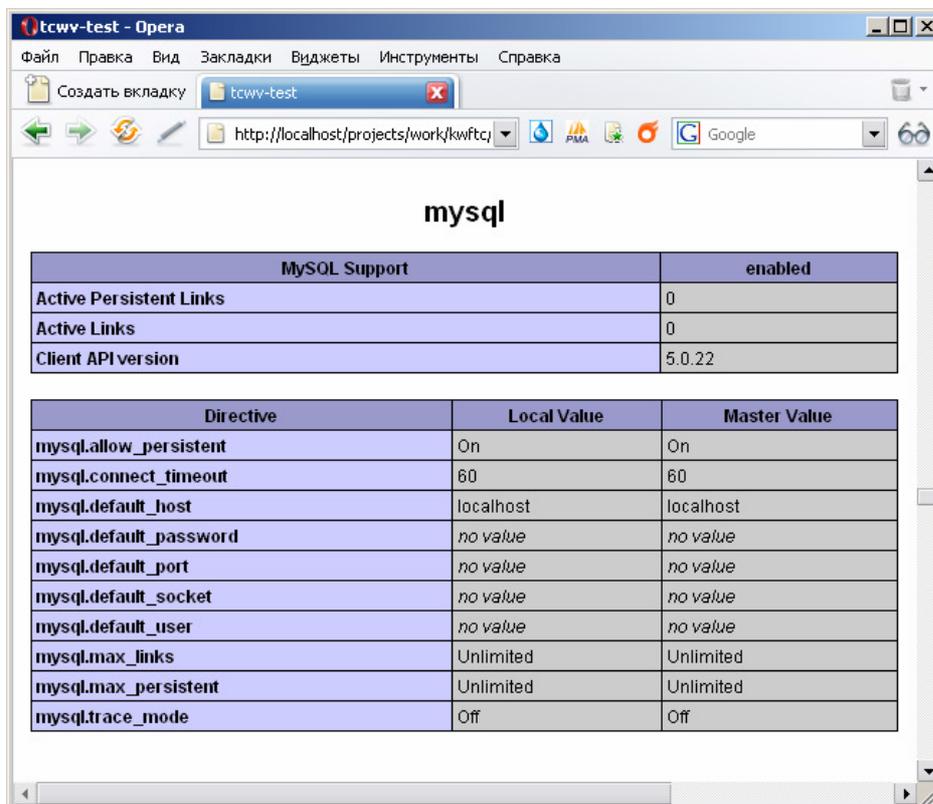
## Проверка работы web-интерфейса

Для проверки корректности установки web-интерфейса, вы можете открыть в браузере скрипт test.php



Этот скрипт содержит в себе 2 раздела – информацию о PHP и средство тестирования подключения.

В первом разделе в первую очередь можно проверить включено ли расширение mysql



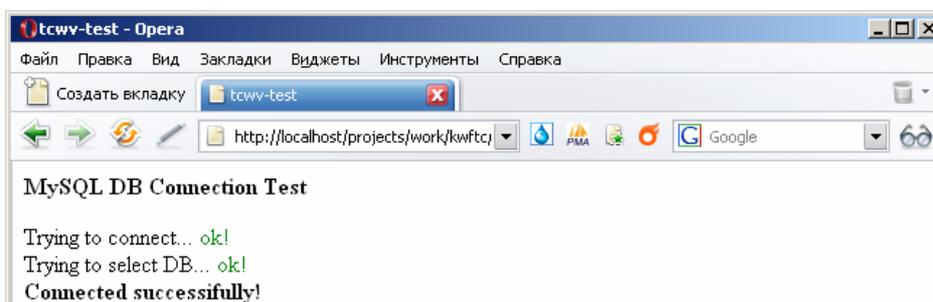
MySQL Support		enabled
Active Persistent Links	0	
Active Links	0	
Client API version	5.0.22	

Directive	Local Value	Master Value
mysql.allow_persistent	On	On
mysql.connect_timeout	60	60
mysql.default_host	localhost	localhost
mysql.default_password	no value	no value
mysql.default_port	no value	no value
mysql.default_socket	no value	no value
mysql.default_user	no value	no value
mysql.max_links	Unlimited	Unlimited
mysql.max_persistent	Unlimited	Unlimited
mysql.trace_mode	Off	Off

**Важно!** Если вы не находите раздела mysql, это означает, что оно не работает. Дальнейшую установку до решения проблемы продолжать нельзя!

Второй раздел содержит средство тестирования подключения к базе данных на основании конфигурационного файла.



```
MySQL DB Connection Test
Trying to connect... ok!
Trying to select DB... ok!
Connected successfully!
```

Если в ходе этого теста произойдут ошибки, они будут отображены с кратким описанием.

**Важно!** Скрипт тестирования конфигурации является источником информации о сервере. После удачного завершения тестирования, удалите его.

### Настройка клиентов и устройств

После установки и настройки web-интерфейса зайдите на него при помощи браузера.

The screenshot shows the 'D-Link DFL Traffic Counter' web interface. On the left, there is a navigation menu with 'Статистика' (Statistics) selected, containing links for 'Данные текущего дня' (Today's data), 'Вчера' (Yesterday), 'Этот месяц' (This month), and 'Суммарные данные' (Summary data). Below this is the 'Настройки' (Settings) section with links for 'Общие настройки' (General settings), 'Клиенты' (Clients), 'Пользователи' (Users), 'Устройства' (Devices), and 'Службы' (Services).

The main content area features a 'Фильтр' (Filter) section with dropdown menus for 'Компьютер' (Computer), 'Устройство' (Device), 'Интерфейс' (Interface), and 'Порт назначения' (Destination port), all set to '--- Выберите ---'. There are checkboxes for 'Показывать всех' (Show all) and 'Выделять превышения лимитов' (Highlight limit exceedances). A 'Показать' (Show) button is present. Below the filter is a table titled 'Статистика текущего дня' (Today's statistics).

Клиент (IP адрес)	Клиент (имя)	Принято ↑	Отправлено
192.168.0.101	fox-r50	203.23 Мбайт	7.09 Мбайт
192.168.1.100	home	1.26 Мбайт	624 Кбайт
Отброшенные пакеты		69 Кбайт	0 байт
Суммарно		204.56 Мбайт	7.70 Мбайт

Завершающим элементом его настройки является указание привязки имен компьютеров клиентов к их IP адресам и IP адресов ваших устройств DFL. Для этого зайдите в соответствующий раздел настроек, выделенный слева.

The first screenshot shows the 'Клиенты' (Clients) configuration page. It has a table with columns: 'IP адрес', 'Имя компьютера', 'Дневной лимит', 'Месячный лимит', and 'Добавить'. The table contains five entries with 'Удалить' (Delete) links.

IP адрес	Имя компьютера	Дневной лимит	Месячный лимит	Добавить
192.168.31.23	a23	11	0	Удалить
192.168.0.101	fox-r50	0	0	Удалить
192.168.1.100	home	0	0	Удалить
192.168.21.33	k33	100	0	Удалить
127.0.0.1	localhost	0	0	Удалить

The second screenshot shows the 'Пользователи' (Users) configuration page. It has a table with columns: 'Логин', 'Имя пользователя', 'Дневной лимит', 'Месячный лимит', and 'Добавить'. The table contains two entries with 'Удалить' (Delete) links.

Логин	Имя пользователя	Дневной лимит	Месячный лимит	Добавить
test	Test user	0	0	Удалить
uk33	user_k33	30	0	Удалить

Добавление осуществляется через функцию «Добавить».

IP адрес

Имя компьютера

Дневной лимит  в мегабайтах

Месячный лимит  в мегабайтах

Значения лимитов указываются в мегабайтах и предназначены для графического выделения превышения лимита в списках текущих и суммарных данных.

Управление устройствами аналогично при выборе раздела «Настройки устройств»

D-Link DFL Traffic Counter PRO

Статистика  
[Данные текущего дня](#)  
[Вчера](#)  
[Этот месяц](#)  
[Суммарные данные](#)

Настройки  
[Общие настройки](#)  
[Клиенты](#)  
[Пользователи](#)  
[Устройства](#)  
[Службы](#)

IP адрес	Имя компьютера	Добавить
192.168.0.1	local	<a href="#">Удалить</a>

Однако, кроме адреса и наименования, для устройств можно указать логин и пароль для доступа.

IP адрес	<input type="text" value="192.168.0.2"/>
Имя компьютера	<input type="text" value="dff-210"/>
Логин	<input type="text" value="dfftc"/>
Пароль	<input type="password" value="*****"/>
<input type="button" value="Изменить"/>	

Это необходимо для PRO-версий – лицензирование подразумевает доступ службы к устройству. Для FREE-версии настройка логина и пароля необязательна.

Дополнительно, начиная с версии 1.6, в составе базы данных поставляется небольшой набор соответствий портов и названий служб.

D-Link DFL Traffic Counter PRO

Статистика  
[Данные текущего дня](#)  
[Вчера](#)  
[Этот месяц](#)  
[Суммарные данные](#)

Настройки  
[Общие настройки](#)  
[Клиенты](#)  
[Пользователи](#)  
[Устройства](#)  
[Службы](#)

Порт	Наименование	Добавить
1494	citrix	<a href="#">Удалить</a>
2401	cvs	<a href="#">Удалить</a>
411	dc++	<a href="#">Удалить</a>
53	dns	<a href="#">Удалить</a>
79	finger	<a href="#">Удалить</a>
21	ftp	<a href="#">Удалить</a>
989	ftps	<a href="#">Удалить</a>
990	ftps	<a href="#">Удалить</a>
70	gopher	<a href="#">Удалить</a>
1720	h.323	<a href="#">Удалить</a>

При необходимости, добавьте необходимые вам службы.

Начиная с версии 1.9, web интерфейс имеет также настройки общего характера.

D-Link DFL Traffic Counter PRO

Статистика  
[Данные текущего дня](#)  
[Вчера](#)  
[Этот месяц](#)  
[Суммарные данные](#)

Настройки  
[Общие настройки](#)  
[Клиенты](#)  
[Пользователи](#)  
[Устройства](#)  
[Службы](#)

Автообновление страниц со статистикой (секунд)	<input type="text" value="60"/>
Список клиентов/пользователей	
Всегда отображать всех клиентов/пользователей	<input checked="" type="checkbox"/>
Минимальный объем трафика для отображения (байт)	<input type="text" value="100000"/>
Список посещенных узлов/служб	
Минимальный объем трафика для отображения (байт)	<input type="text" value="100000"/>
Количество записей для отображения на странице	<input type="text" value="100"/>
<input type="button" value="Сохранить"/>	

Параметр автообновления страниц указывает, через какое количество секунд будут автоматически обновляться страницы со статистикой. Если установить этот параметр равным нулю, автообновления не будет.

Далее, параметры поделены на две группы: настраивающие список клиентов/пользователей и посещенных узлов/служб.

Первая опция означает постоянное отображение всех клиентов/пользователей, всегда «включая» опцию «Показывать всех» фильтра.

**Фильтр.** Поля с незадаанными значениями или значениями «--- Выберите ---» не учитываются. Конечная дата указывается на 1 день больше.

Компьютер    Устройство    Интерфейс    Порт назначения     Показывать всех  
 --- Выберите --- Выберите --- Выберите --- Выберите     Выделять превышения лимитов  
 Показать

Опции минимального трафика для отображения задают, какой минимальный объем будет показан в списках клиентов/посещенных узлов. При заполнении этих параметров, в соответствующих разделах не будут отображаться (но в статистике будут также учитываться) строки, объем переданной или полученной информации которых меньше. Учитывайте, что число задается в байтах, т.е. 1 Кбайт = 1024 байт, 1 Мбайт = 1048576 байт.

При этом, в списке будет отмечено, что не отображены строки, не подходящие по условию и содержаться ссылка для отображения полного списка

Суммарно	204.56 Мбайт	7.70 Мбайт
----------	--------------	------------

В соответствии с настройками, не были отображены строки, объем переданной или полученной информации в которых не превышал 97 Кбайт  
[Показать все строки](#)

Параметр количества записей на страницу задает, сколько записей будет выводиться за раз при разбивке списка посещенных узлов/служб на страницы.

Статистика клиента **192.168.0.101**

Показать статистику по: [серверам](#), [службам](#)

Страница 1 [Следующая >>](#)

Сервер (IP адрес)	Сервер (имя)	Принято t	Отправлено
80.239.159.59		52.88 Мбайт	0.95 Мбайт
80.231.128.111		44.72 Мбайт	830 Кбайт
195.34.30.58		37.20 Мбайт	718 Кбайт
195.122.149.178		16.10 Мбайт	300 Кбайт
195.34.30.57		15.35 Мбайт	312 Кбайт
195.34.30.55		4.07 Мбайт	84 Кбайт
193.138.233.44		3.97 Мбайт	107 Кбайт
85.95.170.177		3.61 Мбайт	515 Кбайт
128.242.183.159		3.42 Мбайт	218 Кбайт
88.212.205.30		1.90 Мбайт	116 Кбайт
Суммарно (отображено)		183.25 Мбайт	4.08 Мбайт
Суммарно		203.23 Мбайт	7.09 Мбайт

Для отключения разбивки на страницы, задайте значение параметра равным нулю.

## Авторизация

Начиная с версии 1.8, web-интерфейс поддерживает 2 способа подключаемой авторизации:

1. На основе конфигурационного файла
2. На основе базы данных

**Важно!** Возможна работа лишь одного из методов авторизации!

Каждый метод авторизации поддерживает 4 уровня доступа:

- Статистика своего IP адреса (неавторизованные пользователи)
- Просмотр полной статистики (view)
- Установка лимитов для клиентов и пользователей (limit)
- Полный доступ (admin)

Оба метода доступа имеют предустановленных пользователей view, limit и admin с соответствующими правами и паролями, равными логинам.

**Авторизация на основе конфигурационного файла** включается переименованием файла `_auth_php.php` в `auth_php.php` (убрать подчеркивание в начале файла).

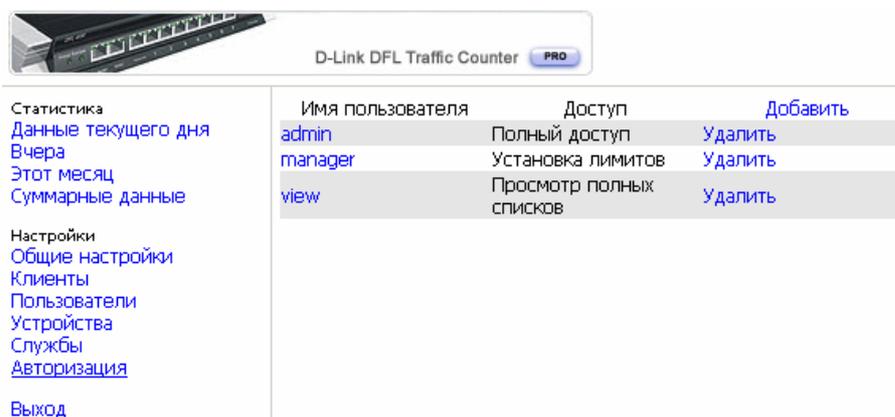
Доступ изменяется редактированием файла:

```
$USERS=array(  
    'admin'=>array(  
        'password'=>'admin',  
        'rights'=>$ADMIN,  
    ),  
    'manager'=>array(  
        'password'=>'manager',  
        'rights'=>$LIMIT,  
    ),  
    'view'=>array(  
        'password'=>'view',  
        'rights'=>$VIEW,  
    ),  
);
```

Пароль устанавливается в значении password для каждого пользователя, а уровень доступа – в значении rights и указывается одним из следующих – \$ADMIN, \$LIMIT, \$VIEW.

**Авторизация на основе базы данных** включается переименованием файла `_auth_mysql.php` в `auth_mysql.php` (убрать подчеркивание в начале файла).

После этого в списке настроек добавится пункт «Авторизация»



The screenshot shows the web interface of a D-Link DFL Traffic Counter. At the top, there is a header with the device name and a 'PRO' badge. Below the header, there is a navigation menu on the left with options like 'Статистика', 'Настройки', and 'Выход'. The main content area displays a table of users with columns for 'Имя пользователя', 'Доступ', and 'Добавить'. The table contains three entries: 'admin' with 'Полный доступ', 'manager' with 'Установка лимитов', and 'view' with 'Просмотр полных списков'. Each entry has a 'Удалить' link next to it.

Имя пользователя	Доступ	Добавить
admin	Полный доступ	Удалить
manager	Установка лимитов	Удалить
view	Просмотр полных списков	Удалить

Добавление и редактирование пользователей осуществляется через стандартный интерфейс и включает в себя имя пользователя, пароль и уровень доступа, соответствующий приведенным выше.

Имя пользователя	<input type="text" value="admin"/>
Пароль	<input type="password" value="*****"/>
Доступ	<input type="text" value="Полный доступ"/>
	<input type="button" value="Изменить"/>

## **Заключительные положения**

Если у вас возникли вопросы, предложения или замечания по использованию данной программы, свяжитесь с нами по адресу [info@raresoftware.ru](mailto:info@raresoftware.ru).

Последнюю информацию, а также модификации и коррекции программы можно найти на сайте <http://www.raresoftware.ru/>.

Названия компаний и программных продуктов, указанных в документе, являются зарегистрированными торговыми марками их владельцев.

© raresoftware.ru 2008