Руководство администратора

(настройка управления антивирусом DrWeb).

TraffPro (Traffic & Protection).

Цель разработки:

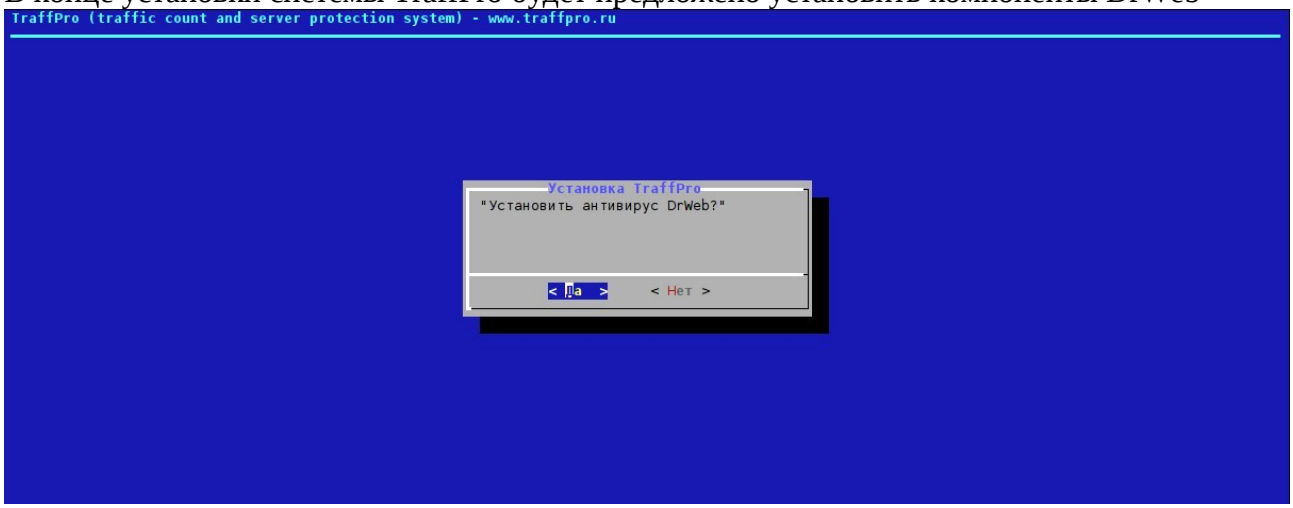
Плагины позволяют на вашем «Корпоративным шлюзе интернет TraffPro»:
Осуществлять конфигурацию модулей DrWeb в удобном WEB интерфейсе.
Осуществлять контроль и проверку на вирусы проходящего www трафика.
Осуществлять проверку каталогов сервера по расписанию.

(В последующих версиях будет введён функционал проверки спама и контроля на вирусы почтовым сервером)

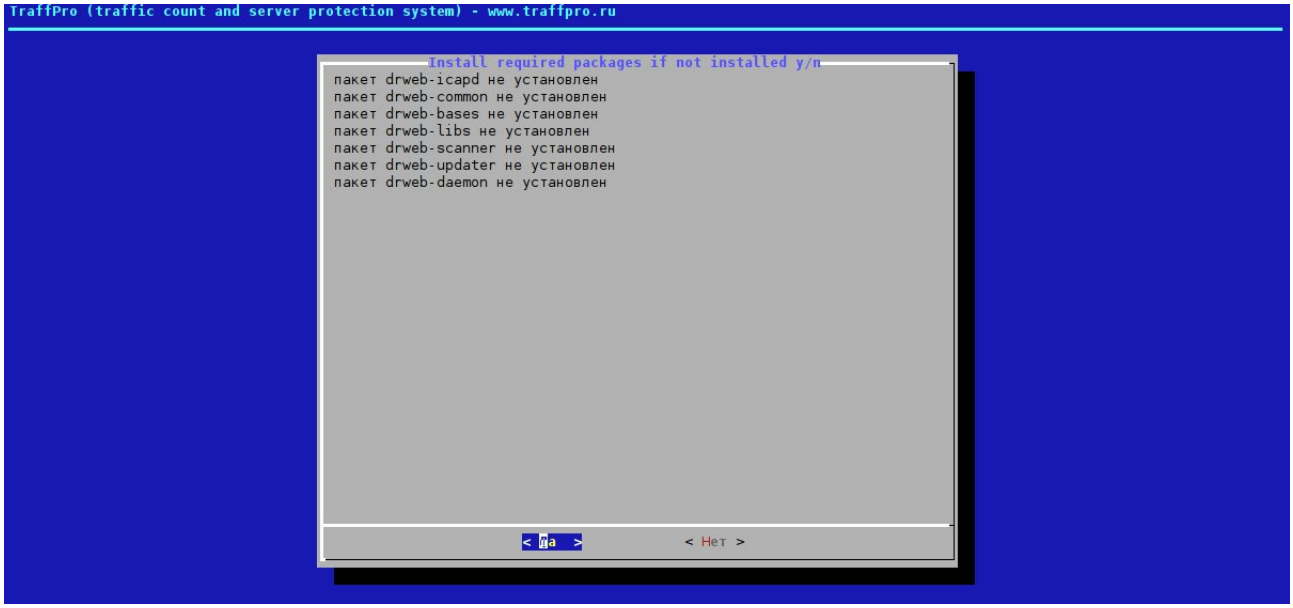
Оглавление:

Установка

В конце установки системы TraffPro будет предложено установить компоненты DrWeb



После подтверждения будет выведен список пакетов которые требуется установить:



так же установку можно осуществить и вручную, для этого требуется подключить репозитории DrWeb:

Для Fedora,RH,CentOs и совместимые:

Создать файл drweb.repo в каталоге /etc/yum.repos.d с содержимым:

Для 64х битных систем:

[drweb]
 name=DrWeb - stable

baseurl=http://officeshield.drweb.com/drweb/el5/stable/x86_64/
gpgcheck=0
enabled=1
gpgkey=http://officeshield.drweb.com/drweb/drweb.key
Для 32х битных систем:
[drweb]
name=DrWeb - stable
baseurl=http://officeshield.drweb.com/drweb/el5/stable/i386/
gpgcheck=0
enabled=1
gpgkey=http://officeshield.drweb.com/drweb/drweb.key

Для Ubuntu,Debian и совместимых:
В файл /etc/apt/sources.list добавить строку:
Ubuntu:
deb http://officeshield.drweb.com/drweb/ubuntu stable non-free
Debian:
deb http://officeshield.drweb.com/drweb/debian stable non-free

Выполнить команду apt-get update для обновления списка репозитория и доступных пакетов.

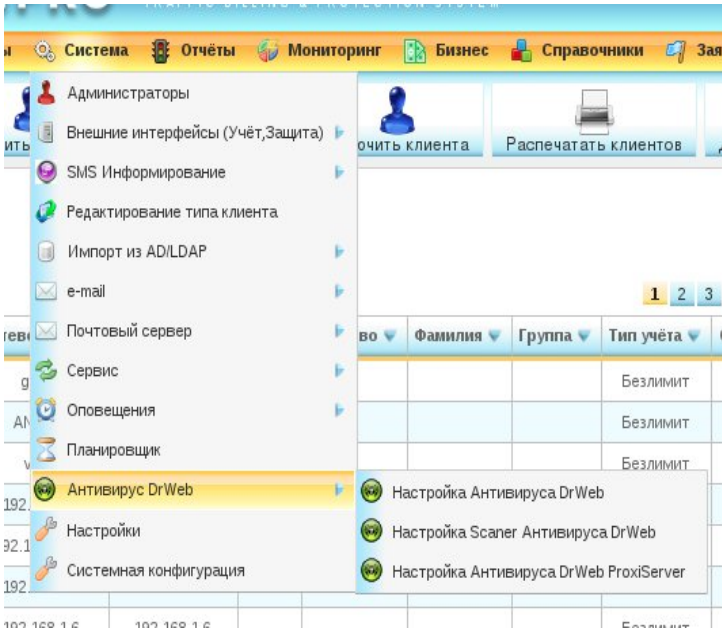
После этого выполнить команду для установки требуемых пакетов:
Для Fedora,RH,CentOs и совместимые:
yum install drweb-icapd drweb-common drweb-bases drweb-libs drweb-scanner drweb-updater drweb-daemon
Для Ubuntu,Debian и совместимых:
aptitude install -y drweb-icapd drweb-common drweb-bases drweb-libs drweb-scanner drweb-updater drweb-daemon

Установка защитного ключа антивируса drweb.

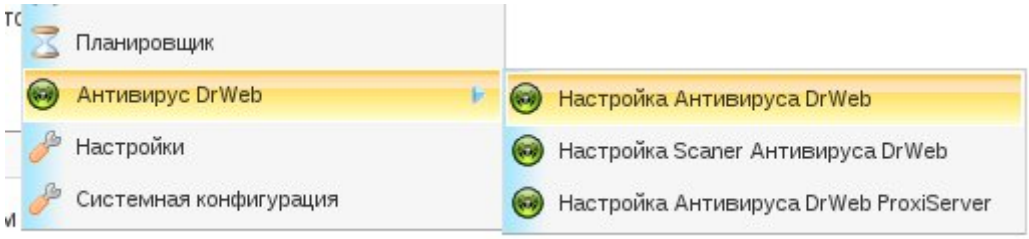
Для корректной работы антивируса DrWeb требуется ключ, без которого DrWeb не запустит модули и не начнёт проверку вашей системы. Для этого, полученный вайл ключа (обычно это drweb32.key) скопируйте в каталог /etc/traffpro/.

Web консоль управления

В административной консоли TraffPro присутствуют пункты меню для управления DrWeb позволяющие произвести настройку и подключить необходимые модули для проверки файловой системы и проходящего www трафика.



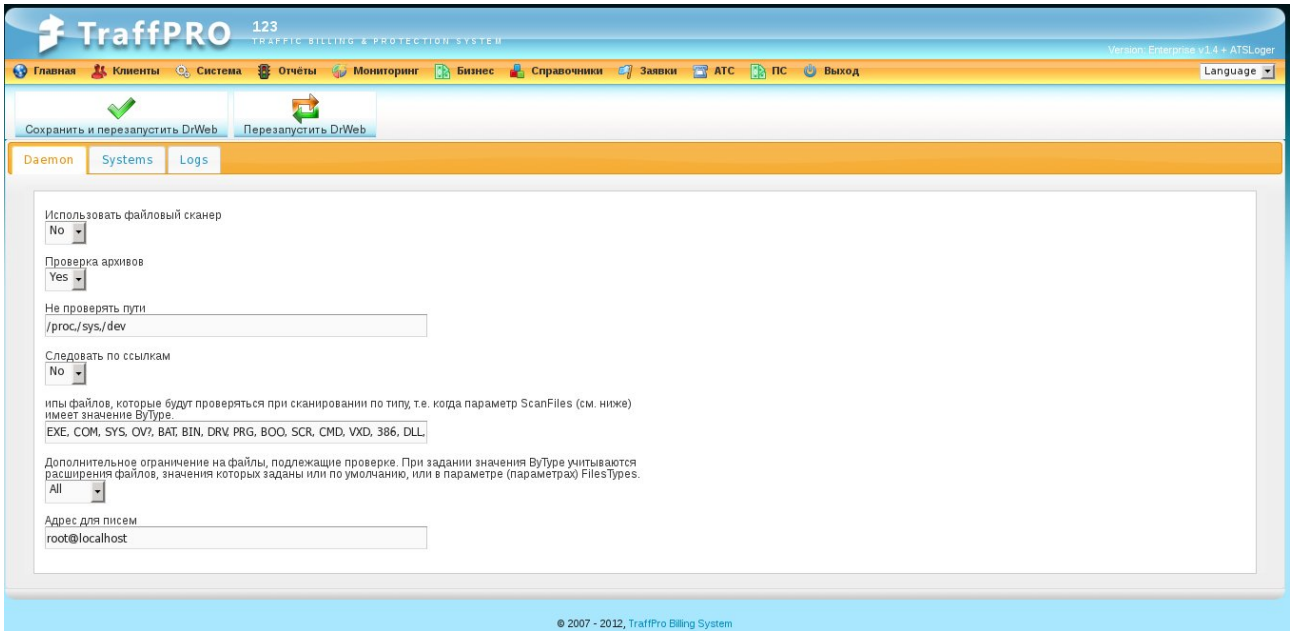
Пункт меню «Настройка антивируса DrWeb»:



Позволяет настроить основной модуль Daemon, который требуется для корректной работы модулей Drweb (таких как drweb-icap и прочих).

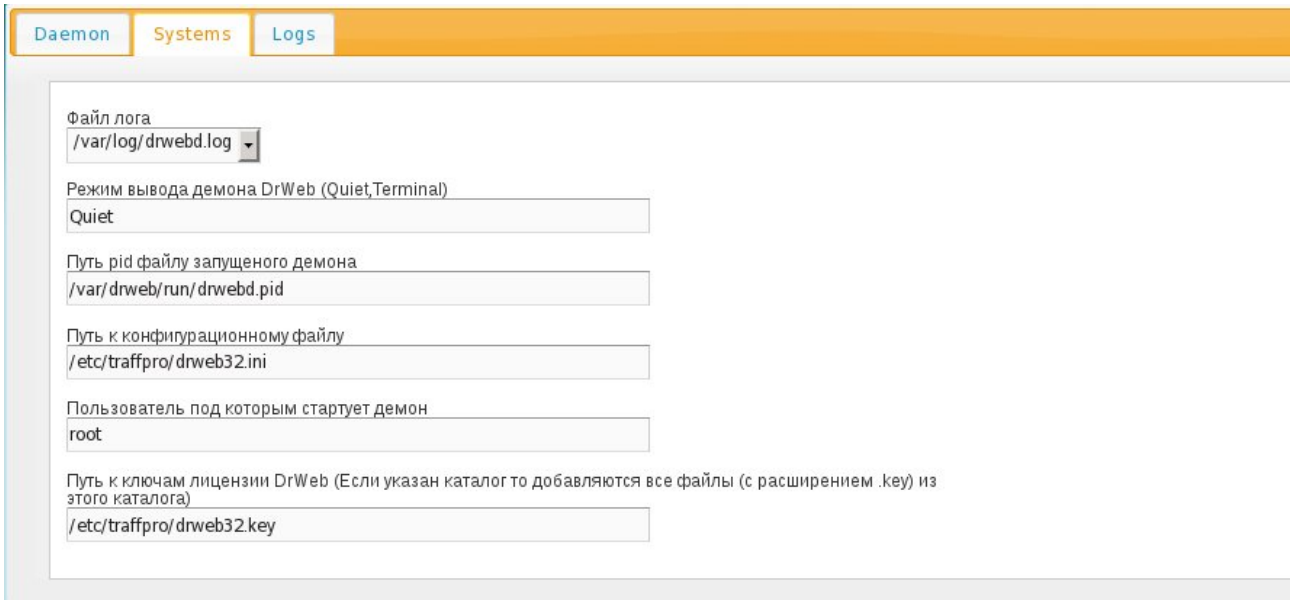
Страница с настройками имеет несколько закладок и органы управления для сохранения и перезапуска демона DrWeb.

Закладка Daemon:



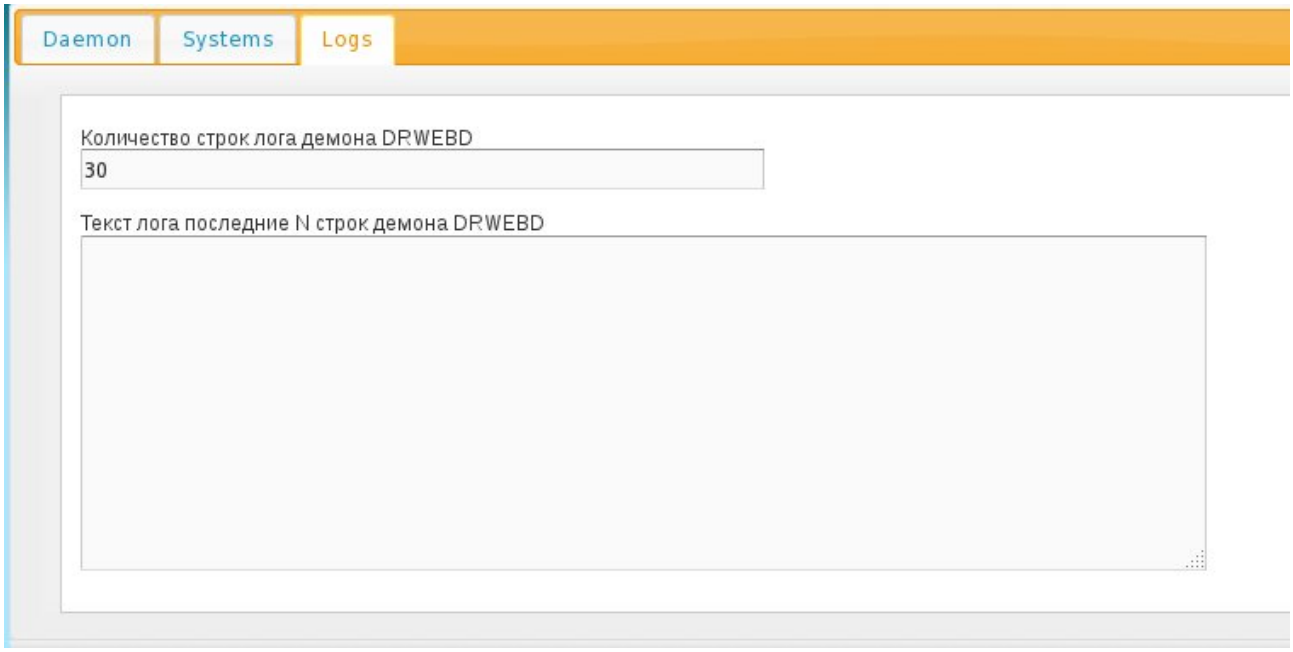
Содержит основные настройки антивирусного модуля, такие как Включение модуля в работу, пути исключённые из проверки, типы файлов для проверки и прочие настройки с которыми вы можете ознакомится в документации к антивирусу Drweb.

Закладка Systems:



Представляет основную информацию, такую как: Режим логирования, пути к файлам конфигурации и ключам.

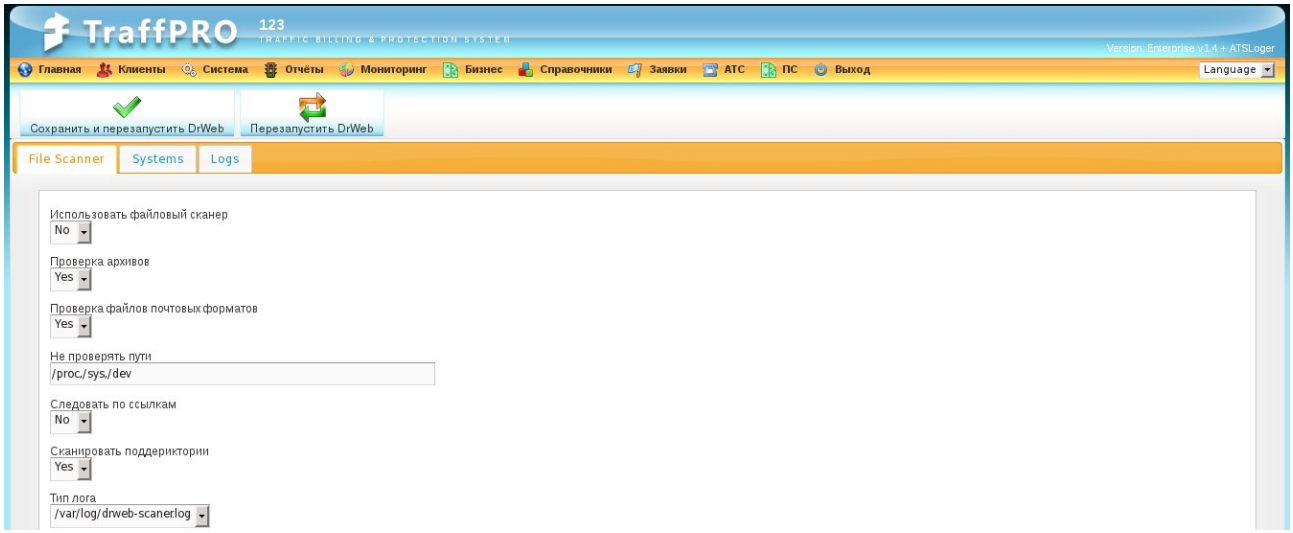
Закладка Logs:



Предоставляет просмотр выводимого лога DrWeb, что позволяет просмотреть как результаты работы программы так и устранить ошибки если они возникают во время работы.

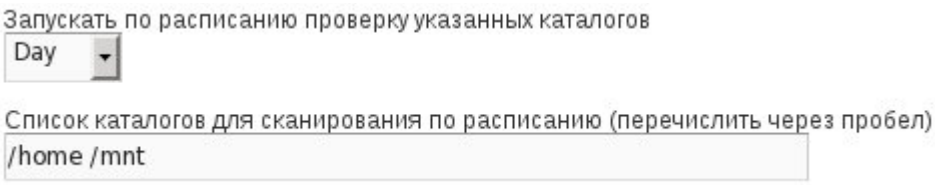
Пункт меню «Настройка Scaner антивируса DrWeb»:

Позволяет настроить сканирование директорий вашего сервера (например общих ресурсов и т.п.), произвести сканирование немедленно или по расписанию (например раз в сутки, или один раз в неделю), указать каталоги для сканирования и произвести настройку реакции на найденные заражённые файлы.



Так же имеются несколько закладок для общих настроек (включение модуля, условия проверки, реакция на найденные заражённые файлы и прочие), системных настроек (расположение ключа, тип логирования и т.д.), просмотр лога работы программы и результатов проверки.

Особое внимание следует уделить пунктам управления проверкой по расписанию:



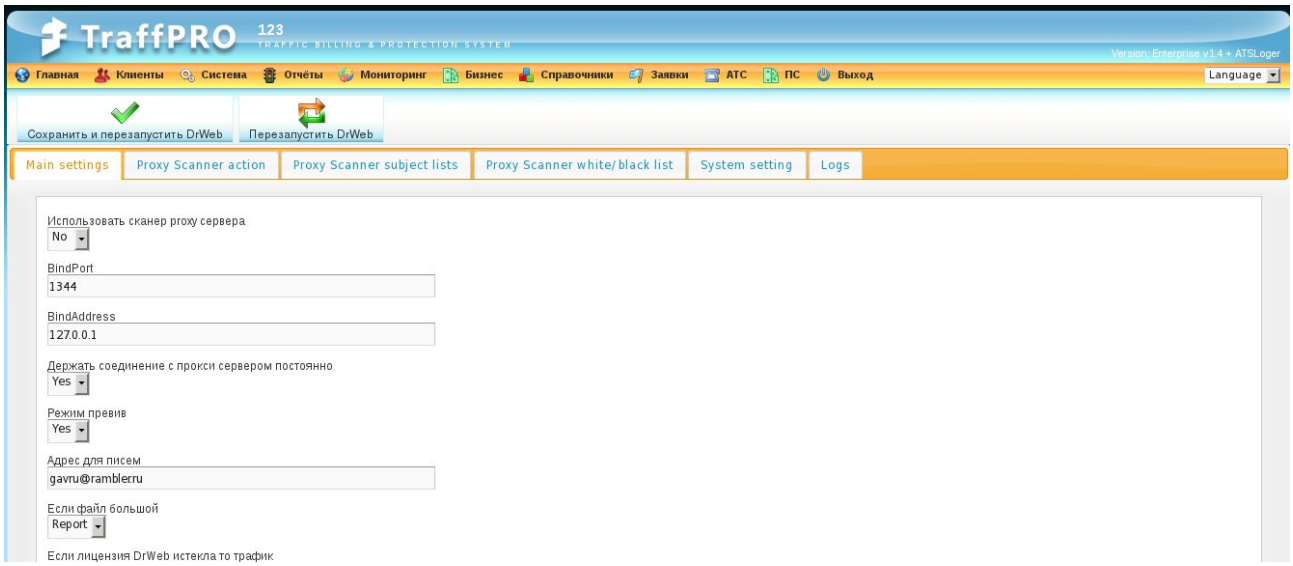
Здесь вы можете указать когда производить запуск сканирования.

Параметр «Запускать по расписанию проверку указанных каталогов»:
No — не производить сканирование.
Now — сейчас (произвести сканирование сразу после нажатия на кнопку сохранения параметров), после запуска проверки параметр меняет значение «Now» на значение «No».
Day — производить проверку раз в сутки, запуск проверки осуществляется в 00:00 часов следующего дня (если проверка ранее не осуществлялась проверка начнётся немедленно).
Week — производить проверку раз в неделю, проверка производится в 00:00 часов первого дня следующей недели(если проверка ранее не осуществлялась проверка начнётся немедленно).
Month — производить проверку раз в месяц,проверка производится 1го дня месяца в 00:00 часов (если проверка ранее не осуществлялась проверка начнётся немедленно).

Параметр «Список каталогов для сканирования по расписанию»:
Строка содержащая список каталогов для проверки, пути должны быть разделены пробелами, например:
/home/ivanov /home/petrov/download /mnt/data/share

Пункт меню «Настройка аентивируса DrWeb ProxyServer»:

Данный раздел отвечает за совместную работу DrWeb и ProxyServer, что позволяет осуществлять проверку на вирусы и контроль доступа к ресурсам, транзитного www трафика для пользователей сети интернет.

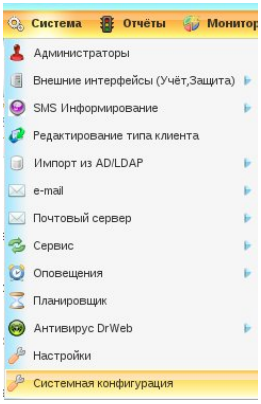


Страница имеет закладки с необходимыми настройками, такими как:
Основные настройки.
Настройки реакции на события.
Списки контроля доступа к ресурсам.
Дополнительные белые и чёрные списки контроля доступа.
Системные настройки.
Лог работы программы.

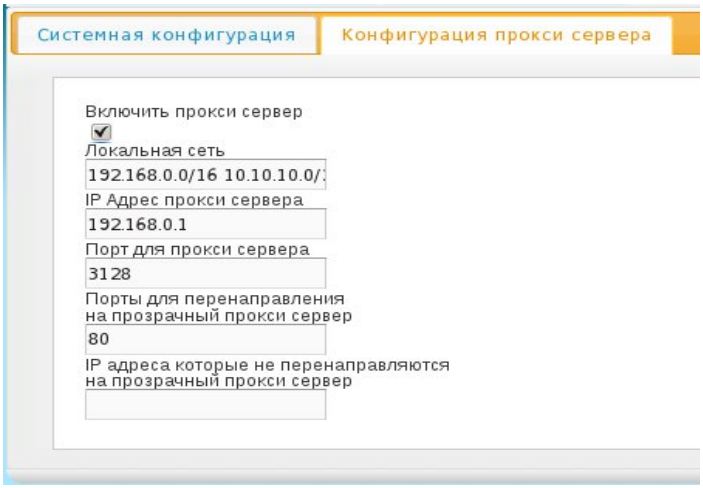
Настройка модуля

Для корректной работы модуля требуется произвести дополнительные настройки системы TraffPro для использования прозрачного ProxyServer. Для Этого необходимо в административной консоли системы TraffPro перейти в пункт меню «система->системная

конфигурация»:



На второй закладке «Конфигурация прокси сервера» страницы:



Требуется включить в работу прокси сервер и установить требуемые параметры (более подробно смотрите документацию по настройке прокси сервера), особое внимание обратите на то, что при редактировании системных параметров traffpro, в случае если доступ к базе данных mysqk осуществляется с паролем, ввод пароля к базе данных (на первой закладке «Системная конфигурация») обязателен!!!

Обновление DrWeb

Обновление вирусных баз и исполняемых модулей осуществляется в автоматическом режиме после установки и запуска единоразово после ввода в работу любого из модулей DrWeb, последующие обновления осуществляются один раз в неделю если хотя бы один из модулей DrWeb задействован.

Дополнительная информация

Большинство названий в параметрах модулей DrWeb сохранено и имеет значение из первоисточника: Справка по антивирусной программе DrWeb

Программа DrWeb не поставляется совместно с Корпоративным шлюзом интернет TraffPro, и приобретается у производителя, на данный момент требуется наличие ключа для модулей Daemon,Scaner,Icap для шлюзов Unix. Наличие в ключие нужного функционала можно уточнить по параметрам:
FileServer=Yes
InetGateway=Yes