"СОФТ ПИ АЙ"

fSonar 1.5

Инструкция по настройке и эксплуатации

Версия документа: 1.0

Дата документа: апрель 2011 г.

Содержание

Назначение

Программа **fSonar** является NetFlow сенсором и предназначена для генерации потока данных в формате протокола NetFlow (версий 5 или 9) о сетевой активности на одном или группе сетевых интерфейсов компьютера, работающего под управлением операционной системы Windows (Microsoft). Поток этих данных направляется на компьютер, с установленным на нем NetFlow коллектором (любого производителя) для дальнейшего анализа сетевой активности с помощью соответствующей программы.

Протокол NetFlow является разработкой компании Cisco Systems и широко используется в сетевых устройствах как этой компании, так и других производителей. Однако, не все сетевые устройства имеют функцию, обеспечивающую формирование данных этого протокола. Кроме этого, если, например, маршрутизатор и поддерживает NetFlow протокол, а коммутаторы ЛВС не поддерживают, то используя данные маршрутизатора, не возможно получить полное представление о сетевой активности внутри ЛВС. Эти и другие причины обуславливают необходимость устанавливать на компьютеры (серверы) NetFlow сенсоры.

Программа fSonar может использоваться, как в крупных сетях, для анализа входящего/исходящего сетевого трафика серверов и обычных компьютеров, так и домашними пользователями для анализа трафика своего компьютера. Анализ сетевого трафика на домашних компьютерах может быть полезен для выявления сетевой активности вредоносных программ (троянских программ, вирусов и других), выявления приложений генерирующих наибольший сетевой трафик, скрытой сетевой активности легитимных приложений и т.п..

fSonar отслеживает сетевой трафик IP протокола как версии 4 (IPv4), так и версии 6 (IPv6), что позволяет облегчить перевод сети компании на IPv6 или контролировать оба типа протоколов.

fSonar может формировать информацию о MAC адресах, что позволяет при анализе NetFlow протокола однозначно выявить сетевое устройство, генерирующее трафик, если в сети используется автоматическое назначения IP адресов.

На основании данных, полученных от программы fSonar, можно выявить информацию о:

- количестве трафика, проходящего через компьютер/интерфейс (в том числе и в режиме реального времени);

- загруженности устройства/интерфейса (в том числе и в режиме реального времени);
- направлении трафика (страна, город);
- приложениях, участвующих в обмене данных (в том числе и в режиме реального времени);
- протоколах, использующихся при передаче данных;
- активности того или иного IP адреса или группы адресов при взаимодействии с компьютером;
- а также ряд другой информации.

Описание программы

Программа fSonar работает в качестве службы операционной системы Windows. Она просматривает сетевой трафик, проходящий через заданные интерфейсы компьютера, формирует на его основе поток данных в формате NetFlow и передает этот поток на IP адрес заданного компьютера для сбора и анализа (рисунок 1). Сбор данных, отправляемых программой fSonar, выполняется программой NetFlow коллектор любого производителя. Анализ NetFlow данных также может выполняться различными программами, предназначенными для этой цели.

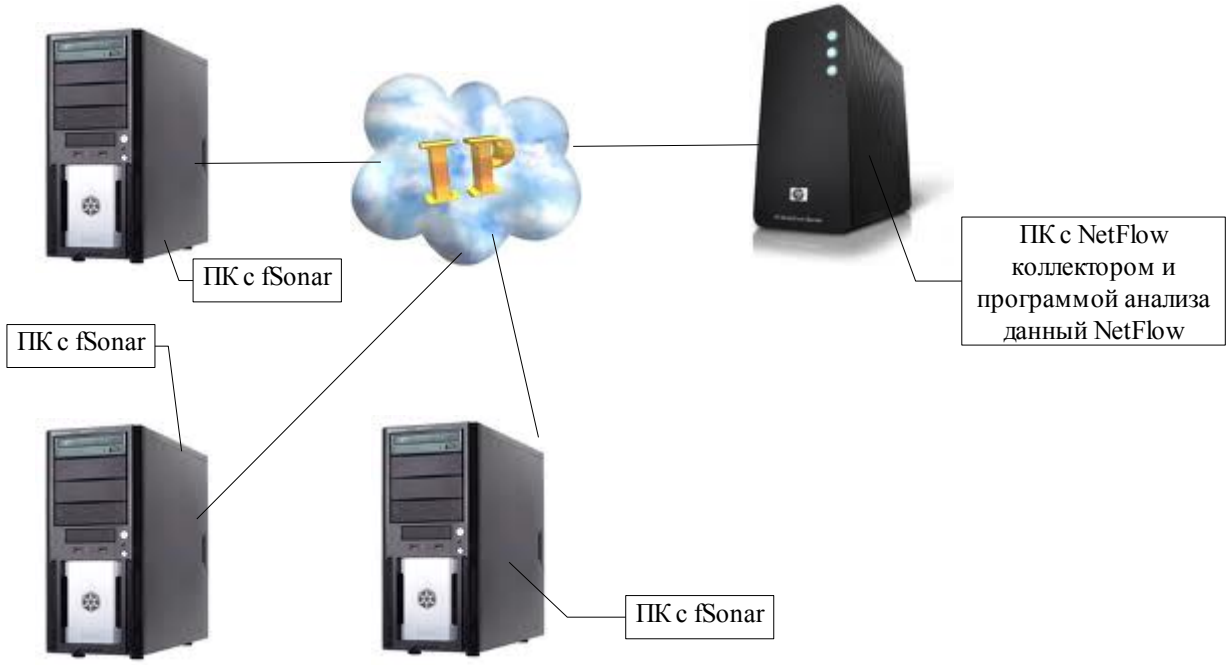

Рисунок 1

Программа fSonar, NetFlow коллектор и программа анализа сетевых потоков могут быть установлены как на одном компьютере, так и разнесены на различных компьютерах, объединенных IP сетью.

Пользователь fSonar может выбрать версию протокола NetFlow, которая будет использоваться для экспорта информации о сетевых потоках. Поддерживаются версии 5 и 9.

О том, что такое протокол NetFlow, какое различие между версия этого протокола можно найти много информации в интернет. Одним из таких документов является статья: "Что такое NetFlow" (http://softpi.com.ua/files/what_is_NetFlow.pdf).

При использовании в fSonar версии 5 NetFlow протокола формируются следующие параметры:

- IP адрес компьютера,
- наименования входящего и исходящего интерфейсов,
- IP адрес источника информации,
- IP адрес приемника информации,
- дата, время сессии,
- объем принятых/переданных данных,
- порты источника и приемника данных,
- тип протокола,
- тип сервиса,
- IP адрес следующего маршрутизатора (hop).

При использовании программы fSonar с протоколом NetFlow версии 5 в качестве программы, которая должна осуществлять сбор, обработку сетевого трафика, выполнять заданную реакцию на сетевые события, рекомендуем использовать систему Flansys (SoftPI). Описание, документация и триал-версия программы Flansys доступны на сайте: http://www.softpi.com.ua

Для протокола NetFlow версии 9, пользователь может выбирать перечень необходимых полей, которые будут экспортироваться. Не все поля протокола NetFlow версии 9 применимы для компьютеров, работающих под операционной системой Windows. Не поддерживается также режим выборки пакетов.

Основные преимущества, которые может получить пользователь при использовании в fSonar версии 9 протокола NetFlow:
- получение информации о сетевых потоках как с IPv4, так и с IPv6;
- получение информации об MAC адресах сетевых устройств.

fSonar может работать как в сети IPv4, так и в IPv6, то есть можно задавать IP адрес программы коллектора NetFlow потока как для IP сети версии 4, так и для версии 6.

Аппаратные и программные требования

Для работы программы fSonar компьютер должен обладать следующими техническими параметрами:
- Процессор не ниже Pentium III 1 Ггц (x86 или x64);
- ОЗУ не менее 256 Мбайт;
- Наличие хотя бы одного сетевого адаптера.

Компьютер должен соответствовать следующим требованиям к программному обеспечению:
- операционная система Windows 2000/XP/2003/Vista/7 (x86 или x64 редакции);
- наличие .NET Framework 3.5 (дистрибутивный пакет Microsoft .NET Framework 3.5 (x86) можно загрузить по следующей ссылке: . http://www.microsoft.com/downloads/ru-ru/details.aspx?FamilyID=333325fd-ae52-4e35-b531-508d977d32a6. Если компьютер при инсталляции fSonar имеет выход в интернет, то загрузка и инсталляция указанного пакета выполниться автоматически).

Инсталляция программы

Перед инсталляцией убедитесь, что на компьютере установлены среда .NET Framework 3.5. Если эта среда отсутствует и компьютер на момент инсталляции не имеет выхода в интернет, то необходимо загрузить .NET Framework 3.5 по ссылке, указанной в предыдущем разделе и установите на компьютере. Если на момент инсталляции компьютер имеет выход в интернет, то эта среда будет загружена и установлена автоматически.

Для инсталляции программы fSonar запустите на выполнение файл sonarsetup.exe. Последнюю версию инсталляционного файла можно скачать с сайта компании "Софт Пи Ай": http://softpi.com.ua

После запуска инсталляционного файла появится окно, показанное на рисунке 2.

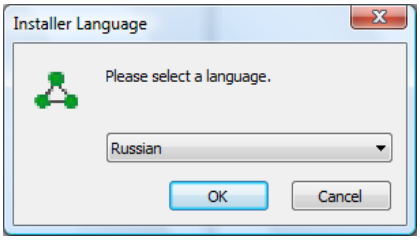

Рисунок 2

Имеется возможность выбора одного из 2-х языков (английский или русский), которых будет использоваться в мастере инсталляции и программе настройки параметров fSonar. Выберите требуемый язык и щелкните по кнопке "ОК". Появится окно, показанное на рисунке 3.

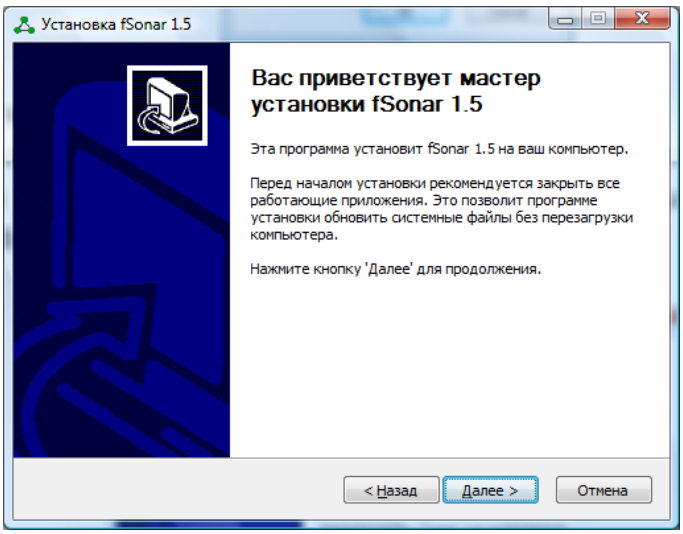

Рисунок 3

Щелкните по кнопке "Далее", в результате появится окно, показанное на рисунке 4. В этом окне необходимо выбрать папку, в которую будет проинсталлирована программа. По умолчанию предлагается папка: ….:\Program Files\SoftPI\fSonar\. Пользователь при желании может сменить эту папку на любую другую. Далее следует щелкнуть по кнопке "Далее", что приведет к появлению окна (рисунок 5), позволяющего определить наименование программы в меню кнопки "Пуск". По умолчанию предлагается название fSonar.

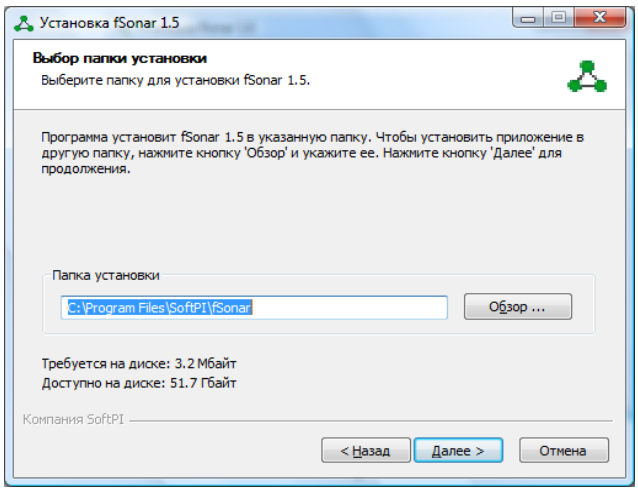

Рисунок 4

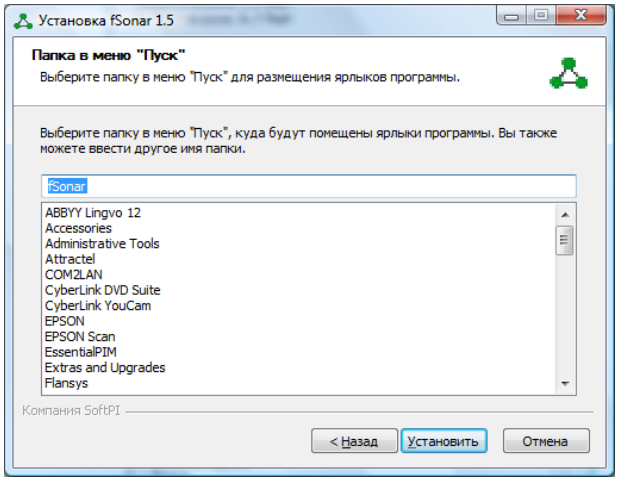

Рисунок 5

Далее щелкните по кнопке "Установить" в результате чего будет произведена установка программы fSonar.

Регистрация fSonar

Если планируется постоянное использование программы fSonar (не для ознакомительных целей), надо приобрести лицензию на нее и провести регистрацию программы.

Для регистрации программы выберите в меню Windows: "Пуск" → "Все программы" → "fSonar" → "Настройка сенсора NetFlow". В результате загрузки программы появится окно, показанное на рисунке 6.

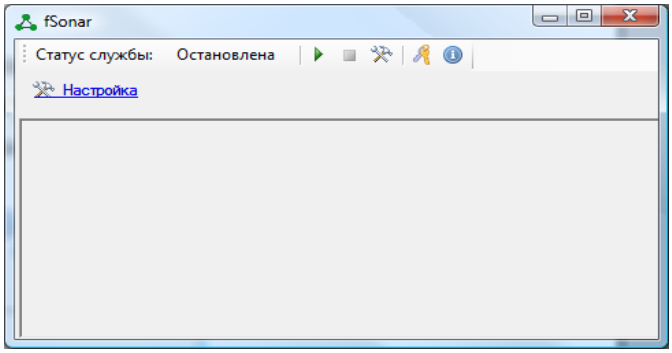

Рисунок 6

Щелкните по кнопке  , в результате чего появится окно, показанное на рисунке 7.

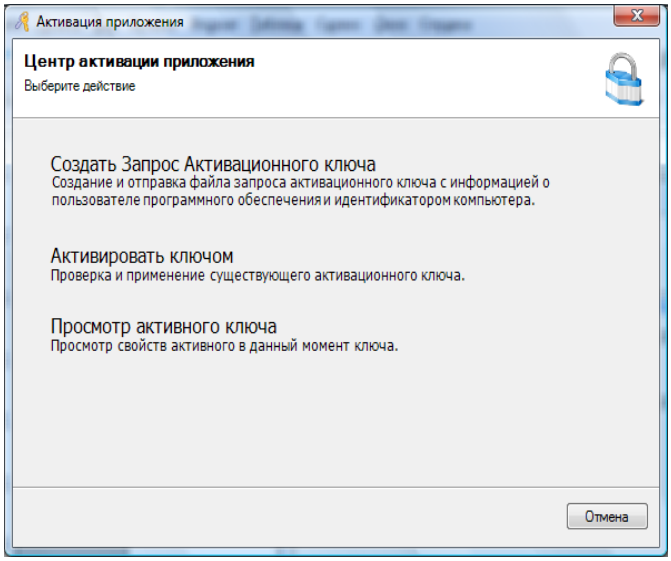

Рисунок 7

В этом окне щелкните по надписи "Создать Запрос Активационного ключа", окно "Активация приложения" примет вид, показанный на рисунке 8.

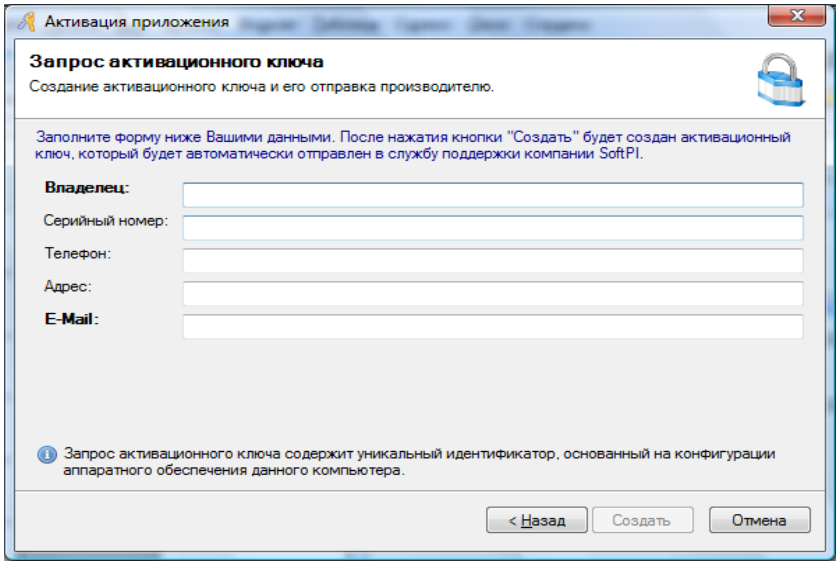

Рисунок 8

В позициях этого окна введите требуемую информацию.

Внимание. *Проверьте правильность введенных данных, особенно таких параметров, как: Владелец, Серийный номер и E-Mail. Неправильно введенные значение 1-х двух параметров не позволят идентифицировать владельца и, соответственно, создать регистрационный ключ. Неправильно введенный адрес электронной почты не позволит Вам получить активационный ключ.*

Щелкните по кнопке "Создать". Регистрационная информация будет автоматически переслана собственнику программы, если компьютер в этот момент имеет подключение к интернет. В противном случае появится окно, показанное на рисунке 9, где предлагается отправить регистрационную информацию через электронную почту вручную на указанный электронный адрес (support@softpi.com.ua).

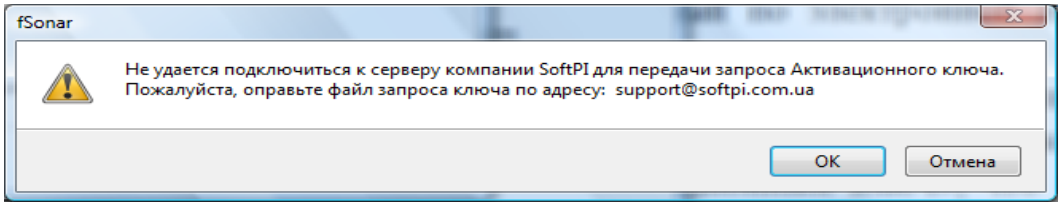

Рисунок 9

Щелкните по кнопке "ОК", что приведет к появлению стандартного Windows окна "Сохранить как", обеспечивающего выбор требуемой папки для сохранения файла register.rk.

Выберите требуемую папку и щелкните по кнопке "Сохранить".

После сохранения файла отправьте его в службу технической поддержки компании SoftPI по адресу: support@softpi.com.ua

На основании высланной регистрационной информации будет

сформирован активационный ключ, который по электронной почте будет направлен вам.

После получения файла – активационного ключа следует вновь щелкнуть по кнопке , в результате чего появится окно, показанное на рисунке 7. Далее щелкните по надписи "Активировать ключом", что приведет к появлению окна, показанного на рисунке 10.

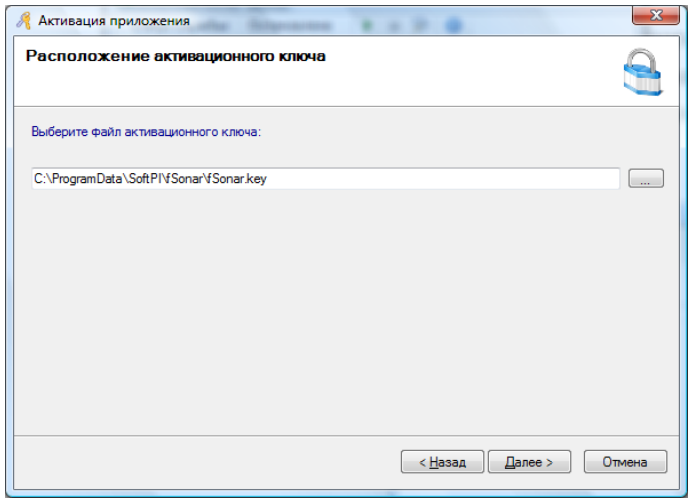

Рисунок 10

С помощью кнопки "…" этого окна выберите папку, в которой находится файл активационного ключа и щелкните по кнопке "Далее". Появится окно, в котором будут отражены параметры активационного ключа. Далее щелкните по кнопке "Готово".

На этом регистрация программы считается законченной.

Если пользователь пожелает просмотреть параметры активационного ключа, то в окне, показанном на рисунке 7, необходимо выбрать пункт "Просмотр активного ключа".

Настройка, запуск, остановка службы

Для настройки программы fSonar запустите ее, выбрав в меню Windows "Пуск" → "Все программы" → "fSonar" → "Настройка сенсора NetFlow". В результате загрузки программы "Конфигурация" появится окно, показанное на рисунке 6.

Окно содержит панель инструментов, где в позиции "Статус службы" отображается текущее состояние службы fSonar (на рисунке 6 служба остановлена) и иконки, значение которых приведено в таблице 1.

Таблица 1

Иконка	Название	Назначение
	Старт	Запуск службы fSonar
	Стоп	Останов службы fSonar
	Настройка	Настройка параметров службы
	Активация	Создание регистрационной информации, применение активационного ключа, просмотр параметров действующего активационного ключа
	О программе	Отображается окно с информацией о версии программы

При первоначальном запуске программы следует установить параметры службы fSonar, для чего следует щелкнуть по иконке "Настройка" или по ссылке "Настройка". В результате этого появится окно, подобное тому, которое показано на рисунке 11.

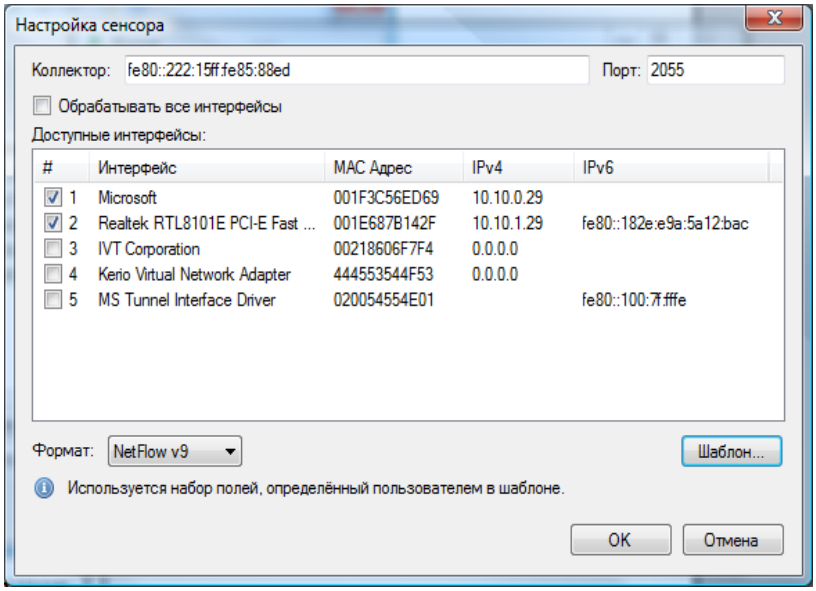

Рисунок 11

В позиции "Коллектор" следует ввести IP адрес компьютера в формате IPv4 или IPv6, где установлен коллектор, собирающий NetFlow или IPFIX потоки, а в позиции "Порт" — IP порт по которому будет приниматься эти потоки. Этот порт должен соответствовать номеру порта, который задан в NetFlow коллекторе.

В таблице "Доступные интерфейсы" отображается список доступных на компьютере сетевых интерфейсов. В соответствующих столбцах отображаются:

- наименование интерфейса;
- MAC адрес интерфейса;
- адрес IPv4;
- адрес IPv6.

Пользователь может задать конкретные интерфейсы, установив флаг в позиции "#". При необходимости выбора всех сетевых интерфейсов можно либо установить флаг напротив каждого из интерфейсов, либо установить флаг в позиции "Обрабатывать все интерфейсы".

Пользователь может может ограничить перечень обрабатываемых программой сетевых пакетов путем задания фильтра для конкретного интерфейса. Для этого следует дважды щелкнуть на строке таблицы, содержащей нужный интерфейс. После этого отобразится окно, аналогичное приведенному на рисунке 12.

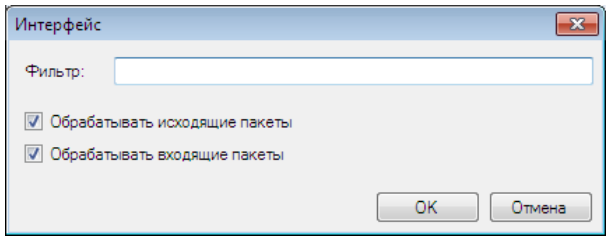

Рисунок 12

В этом окне можно задать, будут ли обрабатываться только входящие пакеты, только исходящие пакеты, и установить фильтр по конкретным параметрам. Фильтр определяет, какие пакеты будут обрабатываться для этого интерфейса. Синтаксис фильтра аналогичен синтаксису, используемому в программах tcpdump, Wireshark, и т.п. Описание синтаксиса можно загрузить, например по адресу: http://www.tcpdump.org/tcpdump_man.html .

Некоторые примеры фильтров приведены в Приложении 1. Если пользователю не нужны данные о всей информации, проходящей через

конкретный интерфейс, рекомендуем с помощью фильтра задать выбор только требуемой информации. Это позволит снизить нагрузку на процессор и интерфейс, через который будет пересылаться поток данных, в случае если коллектор информации расположен на другом компьютере сети.

Из списка "Формат" (рисунок 11) выберите протокол, который будет использоваться для экспорта информации. Для выбора доступны протоколы:
- NetFlow v5,
- NetFlow v9.

Для того, чтобы определить какой из протоколов вам более всего подходить следует проанализировать перечень полей, которые поддерживает каждый из протоколов. При этом следует учитывать, что не все поля, указанные для версии 9 NetFlow протокола поддерживаются (они отображаются в программе серым цветом).

Для протоколов NetFlow v9 можно настроить шаблон - набор полей которые будут экспортироваться. Протокол NetFlow v5 имеет фиксированный набор полей, все из которых передаются. Для выбора требуемых полей протоколов NetFlow v9 необходимо выбрать этот протокол в списке "Формат" и щелкнуть по кнопке "Шаблон...", что приведет к появлению окна, показанного на рисунке 13.

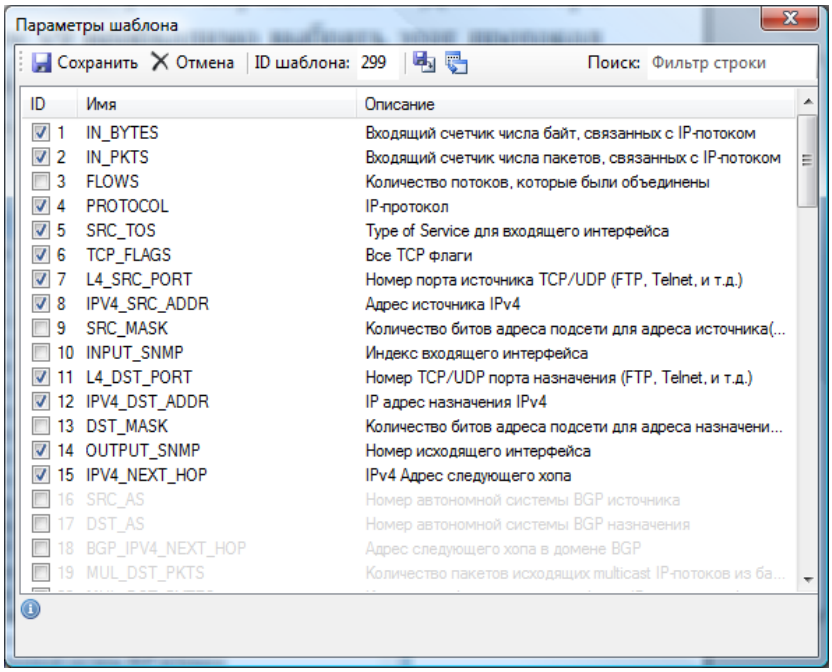

Рисунок 13

В окне "Параметры шаблона" можно выбрать те поля, которые должны присутствовать в экспортируемом потоке. Для ускорения поиска необходимого поля можно использовать поле "Поиск". При вводе символов в

этом поле будут отфильтровываться записи, которые содержат данный набор символов. По окончании выбора необходимых полей щелкните по кнопке "Сохранить", что обеспечит дальнейшее использование именно выбранных полей.

Пользователь может сохранить параметры шаблона во внешний файл для их дальнейшего использования на этом компьютере либо для применения на других компьютерах, например, при настройке специфического набора полей, который необходимо задать на N числе компьютеров. Для этого следует щелкнуть по кнопке "Экспорт параметров" и в появившемся окне "Сохранить как" выбрать необходимую папку и задать имя файла.

Для задания перечня полей из сохраненного файла следует щелкнуть по кнопке "Загрузить параметры", в результате чего откроется стандартное окно "Открыть", где необходимо выбрать требуемый файл.

На этом настройка параметров fSonar закончена.

Для запуска службы fSonar щелкните по иконке "Старт".

Для остановки службы fSonar щелкните по иконке "Стоп".

Управление службой fSonar возможно также через апплет "Службы" операционной системы Windows, где она имеет название "fSonar sensor".

В позиции "Журнал" отображается журнал работы службы fSonar. Отображаются дата и время запуска/останова службы fSonar, перечень интерфейсов, по которым формируется NetFlow поток, а также ошибки, которые могут возникнуть в процессе эксплуатации.

Журнал событий службы fSonar также доступен через "Консоль управления" Windows → "Просмотр событий" → "Журналы приложений и служб" → nfSonar. Через эту Консоль можно сохранить журнал во внешний файл, очистить, осуществить поиск интересующего события.

Контактная информация

По всем вопросам, связанным с поддержкой, сопровождением программы fSonar, обращайтесь:

Телефон: +38 (057)-393-06-11
Электронная почта: support@softpi.com.ua
Сайт: http://softpi.com.ua/
Почтовый адрес: 61115, г. Харьков, ул. Соколова, 3, офис 5.

Приложение 1. Синтаксис фильтра

Синтаксис фильтра аналогичен синтаксису tcpdump, Wireshark, и т.п. Описание синтаксиса можно загрузить по адресу: http://www.tcpdump.org/tcpdump_man.html .

Некоторые примеры фильтров:

Захват трафика только с или на IP адрес 172.18.5.4:

host 172.18.5.4

Захват трафика с или на диапазон адресов:

net 192.168.0.0/24

или

net 192.168.0.0 mask 255.255.255.0

Захват трафика с диапазона адресов:

src net 192.168.0.0/24

или

src net 192.168.0.0 mask 255.255.255.0

Захват трафика на диапазон адресов:

dst net 192.168.0.0/24

или

dst net 192.168.0.0 mask 255.255.255.0

Захват только трафика по протоколу DNS (порт 53):

port 53

Захват не-HTTP и не-SMTP трафика:

host www.example.com and not (port 80 or port 25)

или

host www.example.com and not port 80 and not port 25

Захват всего трафика, кроме ARP и DNS:

port not 53 and not arp

Захват трафика из диапазона портов:

(tcp[2:2] > 1500 and tcp[2:2] < 1550) or (tcp[4:2] > 1500 and tcp[4:2] < 1550)

или

tcp portrange 1501-1549