Microolap EtherSensor

Руководство администратора

2018

Содержание

1. Microolap EtherSensor

Microolap EtherSensor, версия 5.1.0.13519
Руководство администратора.

В документе описано назначение и применение Microolap EtherSensor, сформулированы его общие характеристики как объекта администрирования, определены основные технические операции и мероприятия по подготовке объектов администрирования ко вводу в действие, определен порядок обновления ПО, определен регламент работы объекта администрирования в аварийных ситуациях.

1.1. Краткое описание возможностей

Microolap EtherSensor - высокопроизводительная платформа извлечения событий и сообщений из сетевого трафика в реальном времени со следующими свойствами:

- Значительное количество (несколько тысяч) известных **Microolap EtherSensor** Интернет-сервисов;
- Высокая производительность: работа с потоками на канале 20GBps и выше;
- Доставка событий, сообщений и метаданных в любые подсистемы SOC (DLP, SIEM, eDiscovery и т.п.);
- Высокие показатели непрерывной работы без обслуживания;
- Работа на серийном оборудовании с низким потреблением ресурсов.

Microolap EtherSensor состоит из нескольких служб ОС Windows, в совокупности решающих задачу перехвата и анализа сообщений уровня приложения и их метаданных (как правило, это - сообщения пользователей сети). Затем сообщения, их метаданные или извлеченные из сообщений данные доставляются системам-потребителям.

Отличительной особенностью и главным принципом работы **Microolap EtherSensor** является его неучастие в процессе передачи трафика контролируемой сети и, как следствие этого - независимость надежности сети от его работы. При этом **Microolap EtherSensor** гарантированно обеспечивает полный контроль трафика в сетях с нагрузкой 20GBps и выше, детектируя сообщения нескольких тысяч Интернет-сервисов.

Методы фильтрации трафика на всех уровнях, - как на уровне IP пакетов, так и на уровне уже реконструированных объектов уровня приложения, - позволяют добиться минимального расхода ресурсов для желаемого уровня контроля сетевых коммуникаций.

Расширяемость **Microolap EtherSensor** позволяет как принимать данные от внешних источников (SPAN/TAP трафик, ICAP-клиенты, лог транзакций Lotus Notes, PCAP-файлы), так и поставлять реконструированные сообщения внешним системам-потребителям.

Независимость сервисов **Microolap EtherSensor** от работы службы журналирования (служба **EtherSensor Watcher** позволяет настраивать сложные комбинации типа "уровень журналирования/направление журналирования" для сообщений каждого типа данных, что не будет влиять на производительность.

Ниже приведено описание функций **Microolap EtherSensor**, сгруппированных по функциональным модулям.

Веб-почта (WM)

Извлечение из трафика исходящих сообщений сервисов веб почты: Mail.RU, Yandex.RU, Pochta.RU, GMail и т.п. (более 40 доменов), а также все сервисы на базе ядра "SquirrelMail". Для получения сообщений, отправляемых по зашифрованному каналу (протоколу HTTPS), следует дополнительно использовать ICAP-сервер либо **SSLSplitter**.

Социальные сети (SN)

Извлечение из трафика разных типов данных (аутентификационные данные, текстовые сообщения, комментарии и т.п.) при использовании:

- социальных сетей, таких как: Vk.com, Facebook, LinkedIn, Mamba.ru;
- форумов, функционирующих на базе ядра phpbb, ipb, vbulletin, mybb;
- сервисов отправки сообщений SMS/MMS (более 500 доменов).

Для получения сообщений, отправляемых по зашифрованному каналу (протоколу HTTPS), следует дополнительно использовать ICAP-сервер либо **SSLSplitter**.

Email (EM)

Извлечение из трафика сообщений электронной почты, передаваемых по протоколам SMTP и POP3.

ICAP-сервер (IS)

Позволяет использовать в качестве источника трафика для выделения сообщений HTTP- и FTP-трафик, поставляемый по протоколу ICAP внешними системами, такими как: SQUID, Blue Coat Proxy SG, Cisco WSA, Webwasher, Websense, McAfee Web Gateway, FortiGate, Entensys UserGate и т.п.

Мгновенные сообщения (IM)

Извлечение из трафика сообщений, отправляемых и получаемых через сервисы мгновенных сообщений, работающие по протоколам Skype, XMPP/Jabber, IRC, MSN, YAHOO и OSCAR.

Lotus Notes (LN)

Извлечение из трафика событий системы **Lotus Notes**, таких как сообщения, события календаря и другие. В случае шифрования трафика сообщения извлекаются из **Lotus Notes Transaction Log**. Данные методы не оказывают влияния на работу **Lotus Notes**.

Передача файлов (FT)

Извлечение из трафика файлов, передаваемых по протоколам SMB, HTTP, FTP и WebDAV. Для получения сообщений, отправляемых по зашифрованному каналу, следует дополнительно использовать **SSLSplitter** либо ICAP-сервер.

Поиск работы (CV)

Извлечение из трафика событий (регистрация, аутентификация, отклик на вакансии, актуализация резюме), размещаемых на сервисах вакансий и поиска работы, таких как HH.ru, SuperJob.ru, Job.ru и т.п. (более 150 доменов). Для получения сообщений, отправляемых по зашифрованному каналу (протоколу HTTPS), следует дополнительно использовать **SSLSplitter** либо ICAP-сервер.

ПО "EtherSensor Agent" (AG)

ПО "EtherSensor Agent" устанавливается на рабочих станциях в случае, если установка полноценного end-point DLP-решения по каким-то причинам невозможна.

Служит для привязки TCP-соединений, создаваемых локальными процессами на рабочих станциях, к именам пользователей и именам рабочих станций при использовании в сети организации NAT, терминальных серверов и т.п.

Кроме того, **ПО "EtherSensor Agent"** решает задачу отслеживания изменений (оборудование, процессы и т.п.) на рабочей станции и передачи данных о таких событиях на серверы **Microolap EtherSensor** и **EtherStat**.

1.2. Область применения EtherSensor

Microolap EtherSensor используется для анализа трафика с уровня L2 по уровень L7 модели OSI и извлечения контента и метаданных сообщений и соответствующих им событий.

При разработке **Microolap EtherSensor** были поставлены требования:

Адаптивность к системе-потребителю:
Microolap EtherSensor должен уметь передавать любой системе-потребителю как данные, так и метаданные обнаруженного объекта в любой требуемой форме и тем транспортом, который она понимает. Тип и назначение потребителя могут быть любыми: SIEM, DLP, eDiscovery, UEBA, Enterprise Search, файловая система, пользовательские системы и т.п.

Одновременная работа с многими источниками и потребителями:
Количество систем-потребителей, с которыми одновременно работает **Microolap**

EtherSensor, не должно быть ограничено.
Количество источников данных, с которыми одновременно работает **Microolap EtherSensor**, также не должно быть ограничено.

Полнота контроля:
Microolap EtherSensor должен обнаруживать любой объект уровня приложения, переданный по сети вне зависимости от его типа. Специализированная система-потребитель должна получить результат обработки такого объекта.

Реальное время:
Microolap EtherSensor должен работать в реальном времени на самых скоростных каналах передачи данных, доступных корпорациям. В текущей версии **Microolap EtherSensor** на серийном оборудовании уверенно обрабатывает потоки данных на сети 20GBps и выше.

Отчуждаемость:
Microolap EtherSensor должен разворачиваться "из коробки" и не должен требовать постоянного внимания ни разработчика, ни Заказчика. В идеале - полностью необслуживаемый элемент информационной инфраструктуры.

Наиболее часто **Microolap EtherSensor** находит применение при решении следующих групп задач:

Системы архивирования сообщений (Compliance Archiving):
Извлечение из трафика документов и других объектов электронной почты, мессенджеров, социальных сетей, блогов, форумов и других средств коммуникации.

Примеры потребителей:

- Bloomberg Vault;
- Global Relay;
- Google Vault (help);
- IBM Content Collector;
- Mailarchiva;
- Smarsh;
- Somansa Mail-i;
- Veritas eDiscovery Platform (ранее Clearwell);
- Veritas Enterprise Vault.

SIEM-системы, UEBA, анализаторы логов:
Извлечение из трафика метаданных перехваченных объектов уровня приложения и связанных с ними событий (в том числе и в реальном времени из контента объекта) для регистрации в SIEM-системах.

Примеры потребителей:

- AlienVault;
- ArcSight Enterprise Security Manager (ESM) (ранее HP ArcSight);
- Elastic Stack (ранее ELK Stack: Elasticsearch, Logstash, Kibana);

- EventTracker;
- FortiSIEM (ранее AccelOps);
- Graylog;
- IBM QRadar;
- LogRhythm;
- ManageEngine EventLog Analyzer;
- McAfee Enterprise Security Manager (ESM);
- Micro Focus Sentinel (ранее NetIQ);
- RuSIEM;
- SolarWinds Log & Event Management (LEM);
- Splunk;
- SQLstream;
- Trustwave SIEM;
- Любое ПО, принимающее данные по SYSLOG, NETFLOW или другому TCP/UDP-протоколу.

Предотвращение утечек конфиденциальных данных (DLP-системы)
Извлечение из трафика контента сообщений уровня приложения (7 уровень OSI) внешних и внутренних коммуникационных сервисов с последующей отправкой системе-потребителю: DLP-системе, системе архивирования почтовых сообщений, системе документооборота, локальной поисковой системе и любой другой системе, имеющей функцию архивирования документов.

Примеры потребителей:

- DeviceLock DLP;
- Forcepoint DLP;
- Proofpoint Email DLP;
- Symantec DLP;
- Trustwave DLP;
- Falcongaze SecureTower;
- InfoWatch Traffic Monitor.

1.3. Условия функционирования

Минимальные системные требования физического сервера для функционирования **Microolap EtherSensor**:

Канал	50 Mbps	150 Mbps	250 Mbps	500 Mbps	750 Mbps	1.5 Gbps	2.5 Gbps	5 Gbps	10 Gbps	15 Gbps	20 Gbps

Пользователей	100	300	500	1000	1500	3000	5000	10000	20000	30000	40000
CPU	1CPU*2 Cores	1CPU*4 Cores	1CPU*4 Cores	1CPU*4 Cores	1CPU*4 Cores	1CPU*6 Cores	1CPU*8 Cores	2CPU*6 Cores	2CPU*10 Cores	4CPU*10 Cores	4CPU*12 Cores
RAM	1 GB	4 GB	4 GB	8 GB	8 GB	32 GB	64 GB	128 GB			
HDD	75 GB SATA	2x75 GB SATA RAID1	2x75 GB SATA RAID1	2x150 GB SATA RAID1	2x150 GB SATA RAID1	2x146 GB SAS RAID1	4x300 GB SSD RAID10	4x500 GB SSD RAID10	6x500 GB SSD RAID10	8x500 GB SSD RAID10	8x900 GB SSD RAID10
NIC	1 x 1Gbps	1 x 1Gbps	2 x 1Gbps	4 x 1Gbps	4 x 1Gpbs	1 x 10Gbps	2 x 10Gbps	4 x 10Gbps	4 x 10Gbps	6 x 10Gbps	6 x 10Gbps

Дисковая подсистема используется только в частных случаях для кэширования сетевых объектов, а также для хранения результатов анализа в случае ***временной*** недоступности системы-потребителя. Ввиду этого объем дисковой подсистемы рассчитывается самостоятельно исходя из предполагаемого времени простоя системы-потребителя.

В качестве операционной системы используется ОС Windows Server 2008, Windows Server 2012 или Windows Server 2016 x64, файловая система - только NTFS. Для достижения максимального быстродействия рекомендуется использовать ОС Windows Server 2012 или Windows Server 2016 на платформе x64.

Для корректной работы **Microolap EtherSensor** требуется наличие последних обновлений ОС Windows. При отключенной службе обновления полноценная работа **Microolap EtherSensor** не гарантируется.

1.4. Описание функционирования

Microolap EtherSensor состоит из набора служб, работающих на отдельном аппаратном или виртуальном сервере ("сенсоре").

Сенсор подключен к Ethernet порту активного сетевого устройства, на котором настроено дублирование сетевого трафика (mirroring, rx и tx пакеты) с заданных портов, либо к сетевому ответвителю (network tap). Для захвата трафика используется разработанная в ООО "Микроолап Текнолоджис" технология захвата трафика Packet Sniffer SDK с нулевыми потерями пакетов при нагрузке в 20GBps и выше.

Сенсор - сервер с несколькими сетевыми интерфейсами, один из которых является административным, а другие используются для приема ответвленного сетевого трафика. Сетевой стек ОС на сенсоре сконфигурирован только на административном сетевом интерфейсе, который служит также для передачи перехваченных сообщений внешним потребителям по назначенным в транспортных профилях протоколам.

Политика сенсора хранится в его конфигурационных файлах и является набором правил, определяющих захват IP пакетов, анализ контента перехваченных сообщений уровня приложения, и, в зависимости от результата, формат, способ отправки и направление транспортировки результата перехвата.

На сенсоре функционируют следующие службы:

Службы, работающие с источниками данных.

Служба извлечения сообщений уровня приложения из Ethernet-трафика (EtherSensor EtherCAP, ethersensor_ethercap.exe)

Предназначена для пассивного перехвата трафика на одном или нескольких Ethernet-адаптерах, а также для обработки трафика из PCAP-файлов. Служба **EtherSensor EtherCAP** извлекает из обрабатываемого трафика сообщения уровня приложений в модели OSI и передаёт эти сообщения для дальнейшей обработки в службу анализа сообщений **EtherSensor Analyser**.

Служба извлечения сообщений уровня приложения из данных, предоставляемых ICAP клиентами (EtherSensor ICAP, ethersensor_icap.exe)

Отвечает за получение трафика по протоколу ICAP в режиме REQMOD+RESPMOD от любых ICAP-клиентов (Squid, Blue Coat Proxy SG, Cisco WSA и т.п.). Полученные от ICAP-клиентов объекты передаёт службе **EtherSensor Analyser** для дальнейшего анализа.

Служба извлечения сообщений из Lotus Notes Transaction Log (EtherSensor LotusTXN, ethersensor_lotustxn.exe)

Служба **EtherSensor LotusTXN** позволяет вести мониторинг и реконструкцию сообщений системы **Lotus Notes** методом извлечения их из **Lotus Notes Transaction Log** (журнала транзакций Lotus Notes). Служба извлекает сообщения из файлов Lotus Notes Transaction Log, и затем передаёт эти сообщения для дальнейшей обработки в службу **EtherSensor Analyser.**

Служба анализа сообщений, извлеченных из Ethernet-трафика (EtherSensor Analyser, ethersensor_analyser.exe)

Служба **EtherSensor Analyser** отвечает за детектирование, анализ и фильтрацию перехваченных сообщений и сетевых событий. Служба анализирует объекты протоколов уровня приложений в модели OSI, полученные от служб **EtherSensor EtherCAP**, **EtherSensor ICAP** и **EtherSensor LotusTXN** с целью детектирования сообщений и сетевых событий, передаваемых по сети.

Затем на основе настраиваемых пользователем правил фильтрующий механизм службы принимает решение:

1. о прекращении обработки сообщения;

2. о транспортировке сообщения системе-потребителю (DLP, UEBA, архив, eDiscovery-система, Enterprise Search и т.п.);

3. о формировании произвольной строки на основе данных, извлечённых из сообщения (как правило, syslog-строка для SIEM-системы).

Также служба EtherSensor Analyser отвечает за взаимодействие с экземплярами EtherSensor Agent, помечающими сессии для привязки к рабочейстанции в случае использования NAT, терминальных сервисов и т.п.

Служба доставки результатов анализа трафика (EtherSensor Transfer, ethersensor_transfer.exe)

EtherSensor Transfer является подсистемой **Microolap EtherSensor**, предназначенной для транспортировки результатов перехвата (само сообщение, либо заранее сконфигурированная syslog-строка) различным потребителям по различным протоколам в соответствии с заранее определенными профилями.

Служба журналирования EtherSensor (EtherSensor Watcher, ethersensor_watcher.exe)

EtherSensor Watcher является подсистемой **Microolap EtherSensor**, предназначенной для работы с журналами, отслеживания текущего состояния **Microolap EtherSensor**.

Служба обновления Microolap EtherSensor (EtherSensor Updater, ethersensor_updater.exe)

Предназначена для загрузки и установки файлов обновлений и лицензий **Microolap EtherSensor** при выходе новых версий и/или исправлений.

Для просмотра статистики работы сенсора используйте **ПО "Конфигуратор EtherSensor" (ethersensor_console.exe)** из директории установки **Microolap EtherSensor**.

Для управления политикой сенсора также используйте **ПО "Конфигуратор EtherSensor"**, либо редактируйте конфигурационные файлы служб сенсора в директории **[INSTALLDIR]\config**.

1.5. Уровень подготовки администратора

Системный администратор **Microolap EtherSensor** должен:

- Иметь базовые знания о стеке протоколов TCP/IP, в частности по прикладным протоколам SMTP, HTTP;
- Иметь базовые знания по администрированию сетевых интерфейсов и системных служб ОС семейства Windows Server;
- Обладать знаниями и навыками по администрированию служб **Microolap EtherSensor** и уметь с их помощью реализовывать корпоративную политику безопасности в части, относящейся к использованию внешних коммуникационных сервисов.

1.6. Перечень эксплуатационных документов

Для эксплуатации и администрирования **Microolap EtherSensor**, а также для понимания основных операций по вводу служб **Microolap EtherSensor** в эксплуатацию, администратору необходимо ознакомиться со следующими документами:

- Настоящее Руководство;
- Документация на внешние системы-потребители сообщений и/или связанных с сообщениями событий (в зависимости от целей использования **Microolap EtherSensor**).

2. Установка Microolap EtherSensor

Для установки **Microolap EtherSensor** необходимо запустить инсталлятор, входящий в комплект поставки. В процессе работы инсталлятора будет установлено ПО, необходимое для его корректной работы, а именно:

- Microsoft .Net Framework 4.0;
- Microsoft Visual C++ 2015 redistributable runtime;

> **Внимание!**
> Для корректной установки **Microolap EtherSensor** требуются права администратора в том виде, в каком они устанавливаются по умолчанию при установке ОС Windows. Введение искусственных ограничений прав администратора может привести к некорректной работе.

В процессе установки **Microolap EtherSensor** устанавливаются следующие службы:

EtherSensor EtherCAP (процесс **ethersensor_ethercap.exe**):

Служба пассивного перехвата трафика на сетевых адаптерах, обработки трафика из PCAP-файлов и извлечения сообщений;

EtherSensor ICAP (процесс **ethersensor_icap.exe**):

Служба получения и обработки сетевого трафика по протоколу ICAP от ICAP-клиентов и извлечения сообщений;

EtherSensor LotusTXN (процесс **ethersensor_lotustxn.exe**):

Служба получения сообщений **Lotus Notes** из журнала транзакций (*Lotus Notes Transaction Log*);

EtherSensor Analyser (процесс **ethersensor_analyser.exe**):

Служба детектирования, анализа и фильтрации перехваченных сообщений;

EtherSensor Transfer (процесс **ethersensor_transfer.exe**):

Служба доставки результатов анализа извлечённых из трафика объектов системам-потребителям;

EtherSensor Watcher (процесс **ethersensor_watcher.exe**):

Служба журналирования **Microolap EtherSensor**. Запускается первой и от нее зависят остальные службы **Microolap EtherSensor**.

Служба обновления EtherSensor (процесс **ethersensor_updater.exe**):

Служба автоматического обновления **Microolap EtherSensor**.

Помимо служб устанавливаются приложения:

ПО "Конфигуратор EtherSensor" (процесс **ethersensor_console.exe**):

Утилита конфигурирования **Microolap EtherSensor**, наблюдения за производительностью, а также сбора информации о работе **Microolap EtherSensor** для создания диагностических отчётов.

После завершения настройки сенсора следует провести настройку установленных служб.

2.1. Состав и содержание дистрибутива ПО

Для подготовки **Microolap EtherSensor** к работе предварительно необходимо иметь следующие дистрибутивы:

- ОС Windows Server 2008, Windows Server 2012, Windows Server 2012 x64 или Windows Server 2016. Рекомендуемая операционная система - Windows Server 2016.
  Возможна установка **Microolap EtherSensor** и на пользовательские x64 версии Windows, но следует учитывать возможное снижение производительности, обусловленное ограничениями архитектуры таких ОС;
- Дистрибутив **Microolap EtherSensor**.

В состав дистрибутива **Microolap EtherSensor** входят:

- Инсталляторы **Microolap EtherSensor** для платформ Windows x86 и x64;
- Инсталляторы **ПО "Служба обновления EtherSensor"** (**EtherSensor Updater**) для платформ Windows x86 и x64;
- Настоящее руководство.

Инсталлятор **Microolap EtherSensor** содержит в себе все зависимости и инсталляторы необходимых для его работы платформ. Его следует использовать для первоначальной установки продукта на новый сервер: это гарантирует отсутствие любых проблем, связанных с зависимостями от другого ПО или пререквизитов.

Служба обновления не выполняет обновление до актуальной версии, если не установлена базовая версия. В любом случае требуется установка базовой версии, и только затем Службой обновления будет произведено обновление до актуальной версии.

2.2. Подключение Microolap EtherSensor к Ethernet

Для подключения сенсора к сети организации необходимо выполнить следующие действия:

1. Подключить сетевой интерфейс управления;
2. Подключить сетевые интерфейсы прослушивания трафика;
3. Настроить коммутаторы;
4. Обеспечить совместимость со сторонними средствами защиты информации.

2.2.1. Интерфейс управления

Для работы **Microolap EtherSensor** требуется подключение к сети сетевых интерфейсов управления и прослушивания.

Интерфейс управления представляет собой стандартный сетевой интерфейс, с установленным адресом TCP/IP, маской подсети и, при необходимости, адресом маршрутизатора по умолчанию.

Для работы **Microolap EtherSensor** желательно, чтобы при его настройке были указаны серверы DNS, на которых работает обратное распознавание адресов (от IP к hostname) хостов локальной сети: это позволит определять имена хостов, которые участвовали в соединении, особенно в случае применения для настройки адресов TCP/IP на хостах локальной сети протокола DHCP.

Данные, получаемые от DNS-сервера, кэшируются, что позволяет сократить дополнительную нагрузку на DNS-серверы. Параметры кэширования настраиваются утилитой **Конфигуратор EtherSensor** (ethersensor_console.exe).

Скорость подключения интерфейса управления должна быть достаточной, чтобы пропускать через себя весь объем перехваченных сообщений, не приводя к их накоплению на сенсоре. Допускается использование сетевых интерфейсов 100/1000/10000 Mbit/s.

При конфигурации сетевого интерфейса управления необходимо учесть особые настройки **Microolap EtherSensor**, при которых будет производиться фильтрация распознанных данных, отправляемых через сетевой интерфейс управления. Подробно про данные настройки указано в разделе Служба EtherSensor EtherCAP.

2.2.2. Интерфейс прослушивания

Для прослушиваемого сетевого интерфейса не требуется настройка стека протоколов TCP/IP, а также других протоколов. С данного сетевого интерфейса происходит захват пакетов для анализа содержимого. Трафик на этот интерфейс может подаваться с Mirror-порта коммутатора, с концентратора (hub), либо с ответвителя (network tap).

Для нормальной работы требуется, чтобы трафик на интерфейсе прослушивания содержал все сетевые пакеты: как от сервера (RX), так и от клиента (TX).

Помните:
Наличие или отсутствие тегов VLAN в трафике для работы **Microolap EtherSensor** значения не имеет, так как они удаляются драйвером сетевого адаптера.

Пропускная способность интерфейса прослушивания должна быть на 20% больше поступающего потока. Только в этом случае можно иметь уверенность, что пакеты не будут теряться при захвате на сетевом оборудовании и качество перехвата будет высоким.

Сенсор может на одном сервере обрабатывать более одного интерфейса прослушивания. Максимальное их количество в среде выполнения **Microolap EtherSensor** никак не ограничено, но зависит от производительности сетевых интерфейсов, а также от производительности среды выполнения **Microolap EtherSensor** в целом (количества оперативной памяти, характеристик процессоров).

2.2.3. Настройка коммутаторов

Ниже приведен пример настроек Mirror-порта (SPAN) для коммутаторов Cisco Catalyst (такие коммутаторы позволяют настроить 2 активные SPAN-сессии):

```
monitor session 1 source interface gigabitEthernet 1/0/24 both
monitor session 1 destination interface gigabitEthernet 1/0/23
```

Здесь "1/0/24" - порт коммутатора, копию трафика с которого необходимо направлять на анализ в **Microolap EtherSensor**, а "1/0/23" - порт коммутатора, к которому подключен сенсор.

Ниже приведена типовая схема включения сенсора в локальной сети:

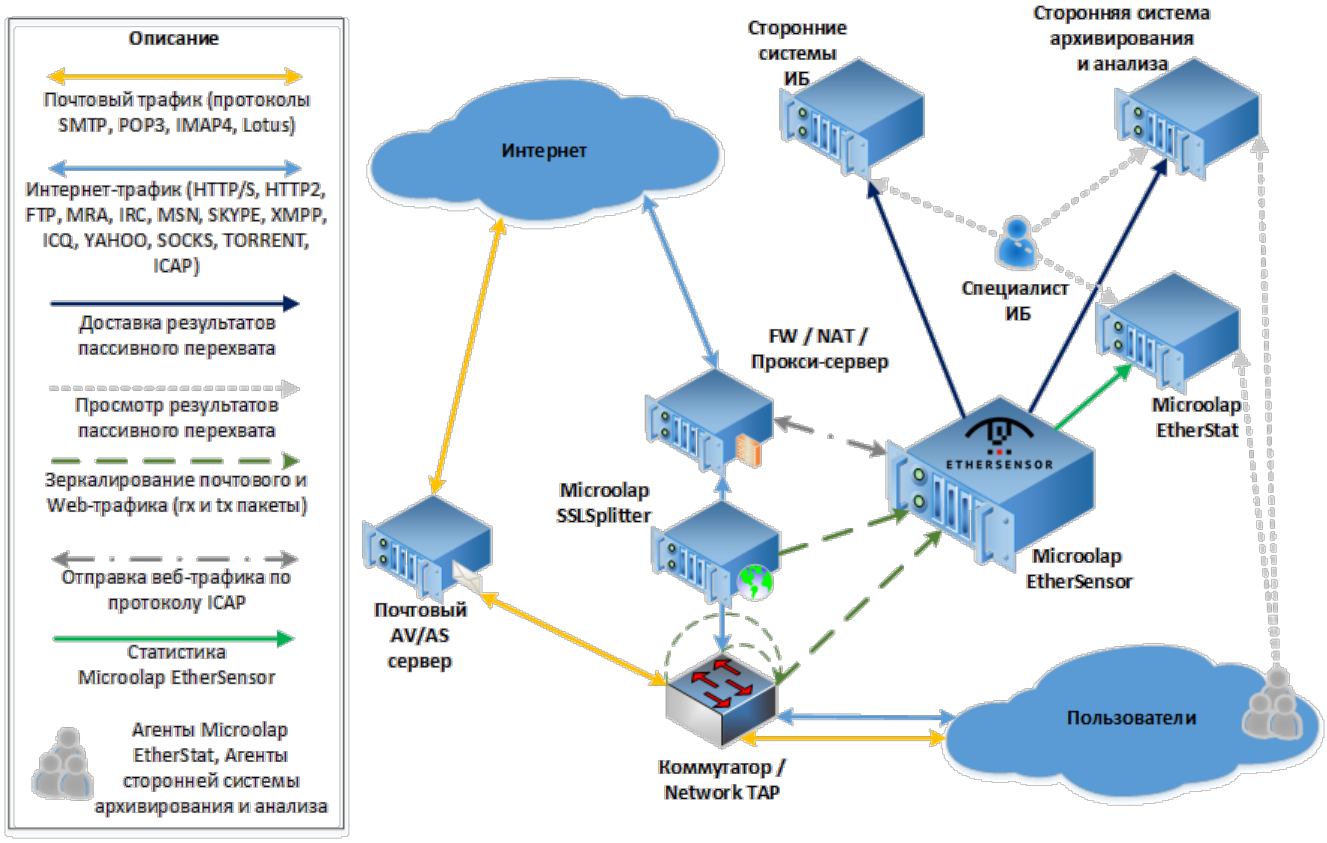

Рис.1. Типовая схема включения Microolap EtherSensor в локальной сети.

2.2.4. Работа со сторонними СЗИ

Для обеспечения стабильной работы **Microolap EtherSensor** следует учитывать совместимость со сторонними средствами защиты информации (СЗИ) и другими компонентами инфраструктуры:

- **Microolap EtherSensor** по умолчанию устанавливается в директорию **C:\Program Files\Microolap EtherSensor.** Возможна также установка и в другие директории, по выбору администратора. В директории, где установлено **Microolap EtherSensor**, расположены рабочие директории. Следует исключать данный путь и все его поддиректории из контроля средств, аналогичных антивирусам, поисковым индексаторам, а также средствам контроля целостности. Никакое ПО не должно блокировать файлы в данных директориях от создания, удаления, перемещения и изменения.
- **Microolap EtherSensor** представляет собой следующие службы Windows: **EtherSensor EtherCAP**, **EtherSensor ICAP**, **EtherSensor LotusTXN**, **EtherSensor Analyser**, **EtherSensor Transfer**, **EtherSensor Watcher**, а также службу обновления **EtherSensor Updater**. Эти службы должны запускаться с правами локальной системы, так как им требуется доступ к функциям ядра.

- **Microolap EtherSensor** требует для нормальной работы отправку сообщений по протоколу SMTP, FTP, SMB, SYSLOG или IMAP на удаленный сервер. СЗИ не должны проверять, модифицировать, или ограничивать соединения на сервер, куда **Microolap EtherSensor** отправляет данные. Аналогично, СЗИ не должны препятствовать службе **EtherSensor Transfer** открывать соединения на порты, используемые для отправки сообщений.
- **Microolap EtherSensor** требует для своей работы подключения к системному модулю NDIS. Сторонние СЗИ не должны препятствовать службе **EtherSensor EtherCAP** использовать функции доступа к этому модулю.
- При установке и функционировании процессы **Microolap EtherSensor** используют вызовы, требующие высоких привилегий. Политика безопасности ОС должна позволять операции над драйверами, управление процессами и доступ к сетевым интерфейсам для **Microolap EtherSensor**.
- В процессе перехвата **Microolap EtherSensor** способно оперировать большими объемами файлов в рабочих директориях. Файловая система среды выполнения **Microolap EtherSensor** должна располагать достаточным свободным объемом для записи и хранения данных.
- При работе с большими сетевыми потоками рекомендуется монтировать директорию **[INSTALLDIR]\data** как отдельную партицию на рейд-контроллере с оптимизацией по скорости доступа и записи *(raid10)*.

3. Настройки сенсора

Перед началом эксплуатации сенсора следует произвести следующие настройки:

1. Обеспечить наличие файла лицензии в директории установки **Microolap EtherSensor**;

2. Настроить источники данных;

3. Настроить доставку результатов перехвата;

4. Настроить службу журналирования;

5. Настроить службу анализа сообщений;

6. Настроить фильтр HTTP-объектов;

7. Настроить службу обновления.

3.1. Источники сообщений

В текущей версии **Microolap EtherSensor** (5.1.0.13519) на сенсоре функционируют следующие службы, предназначенные для работы с источниками данных: **EtherSensor EtherCAP**, **EtherSensor ICAP** и **EtherSensor LotusTXN.**

Общая схема работы служб выглядит следующим образом:

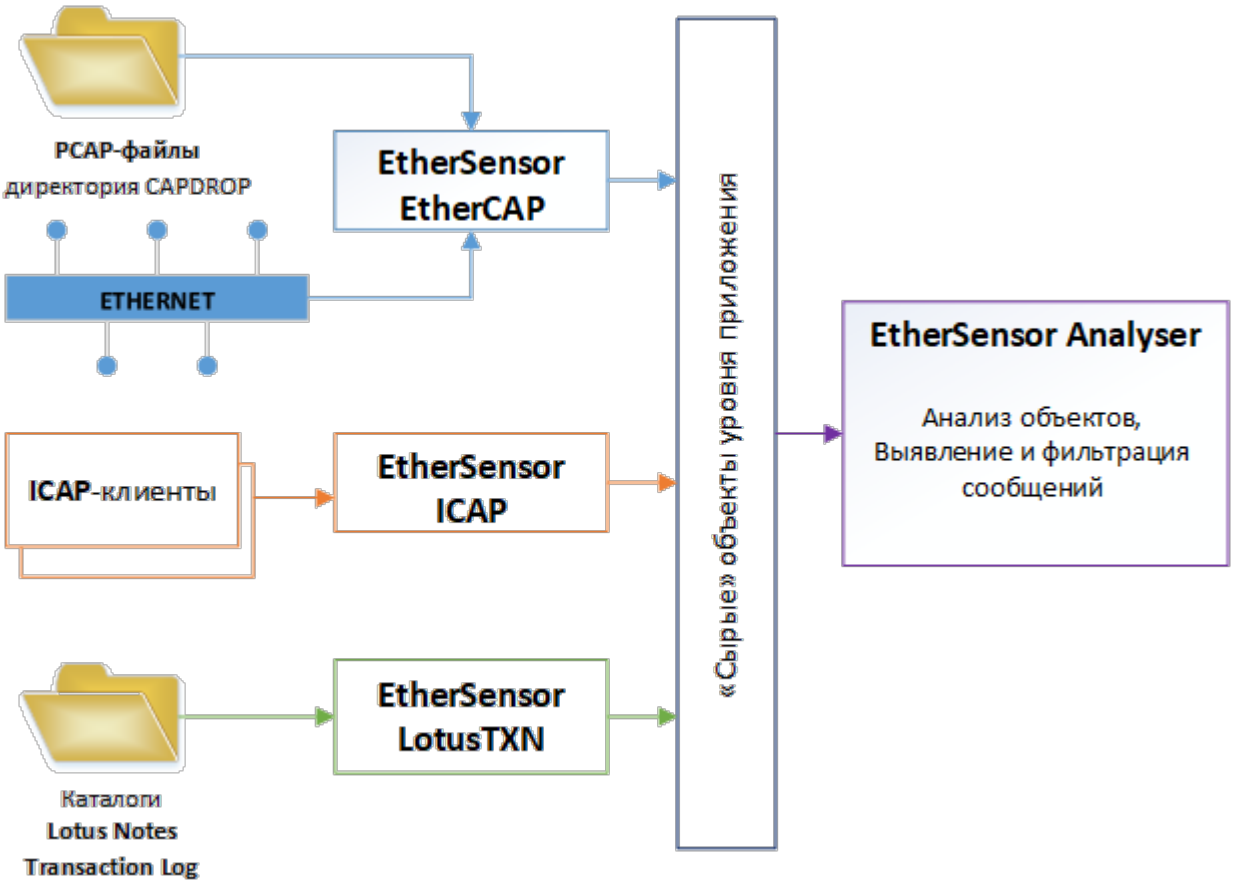

Рис.2. Схема работы служб EtherSensor EtherCAP, EtherSensor ICAP, EtherSensor LotusTXN.

Служба **EtherSensor EtherCAP** отвечает за пассивный захват трафика на сетевых адаптерах, обработку трафика из PCAP-файлов и реконструкцию сессий протоколов уровня приложения:

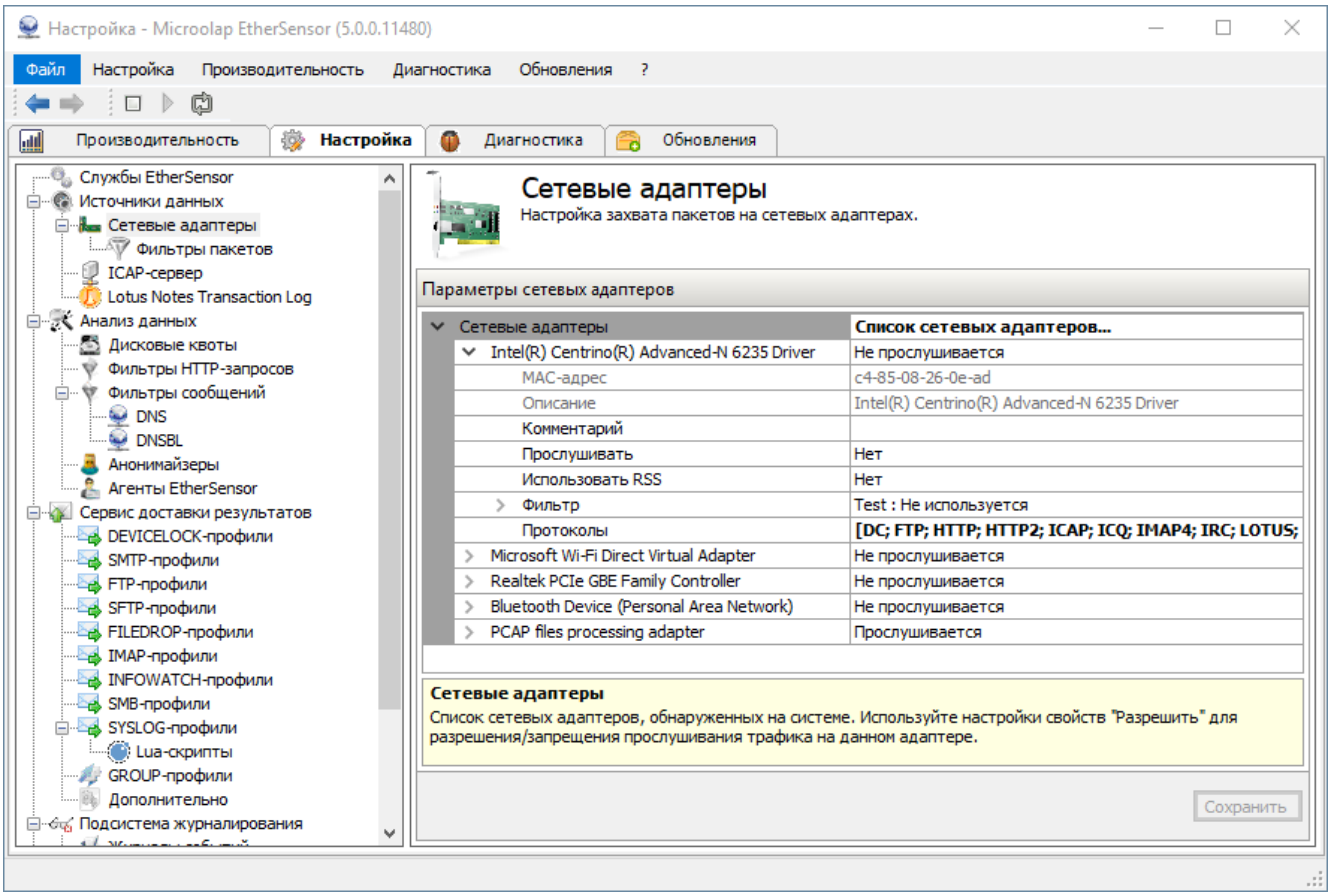

Рис.3. Окно настройки службы EtherSensor EtherCAP.

Служба **EtherSensor ICAP** отвечает за получение трафика по протоколу ICAP от любых ICAP-клиентов и дальнейшую передачу полученных объектов в службу **EtherSensor Analyser**:

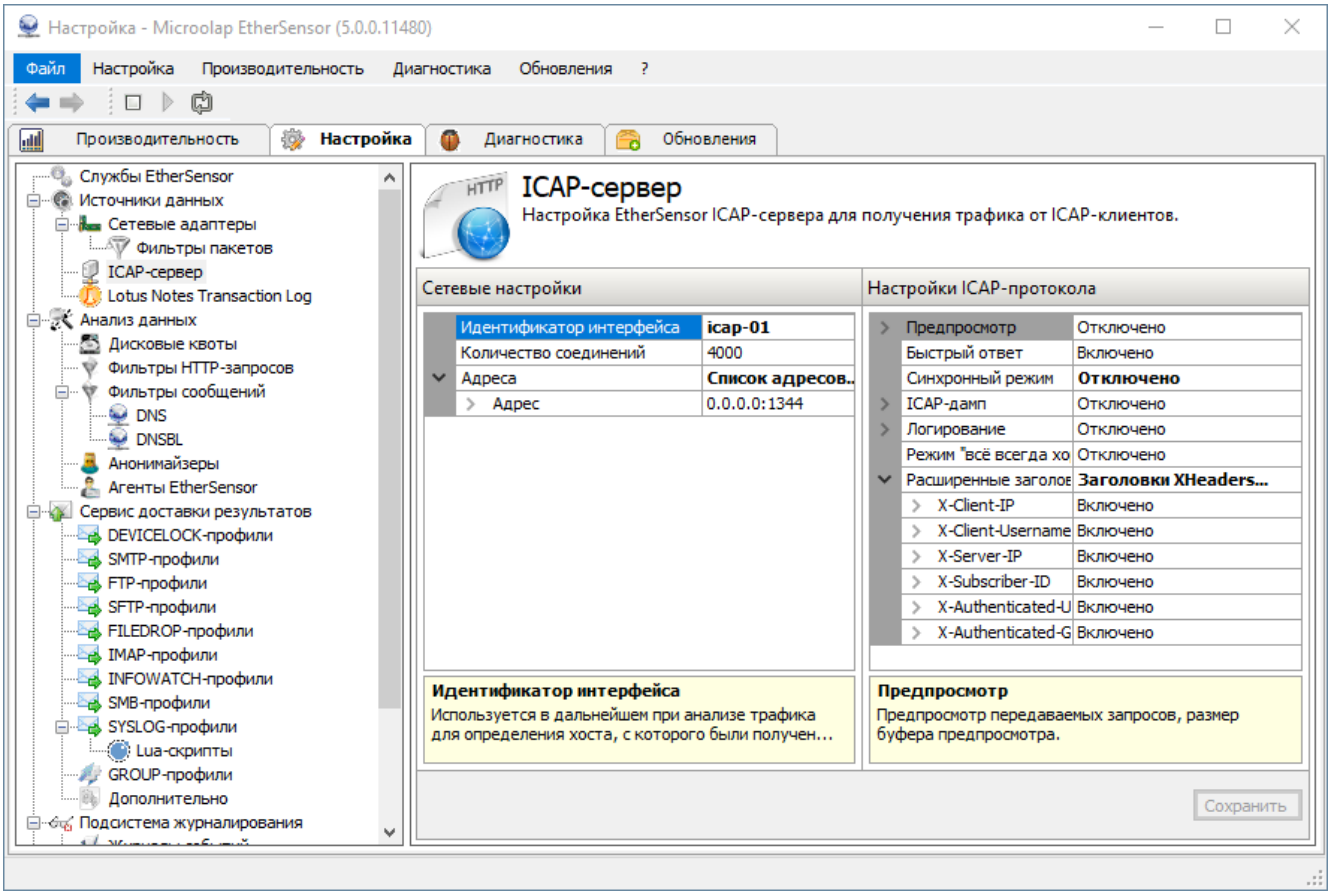

Рис.4. Окно настройки службы EtherSensor ICAP.

Служба **EtherSensor LotusTXN** отвечает за извлечение сообщений из файлов **Lotus Notes Transaction Log**:

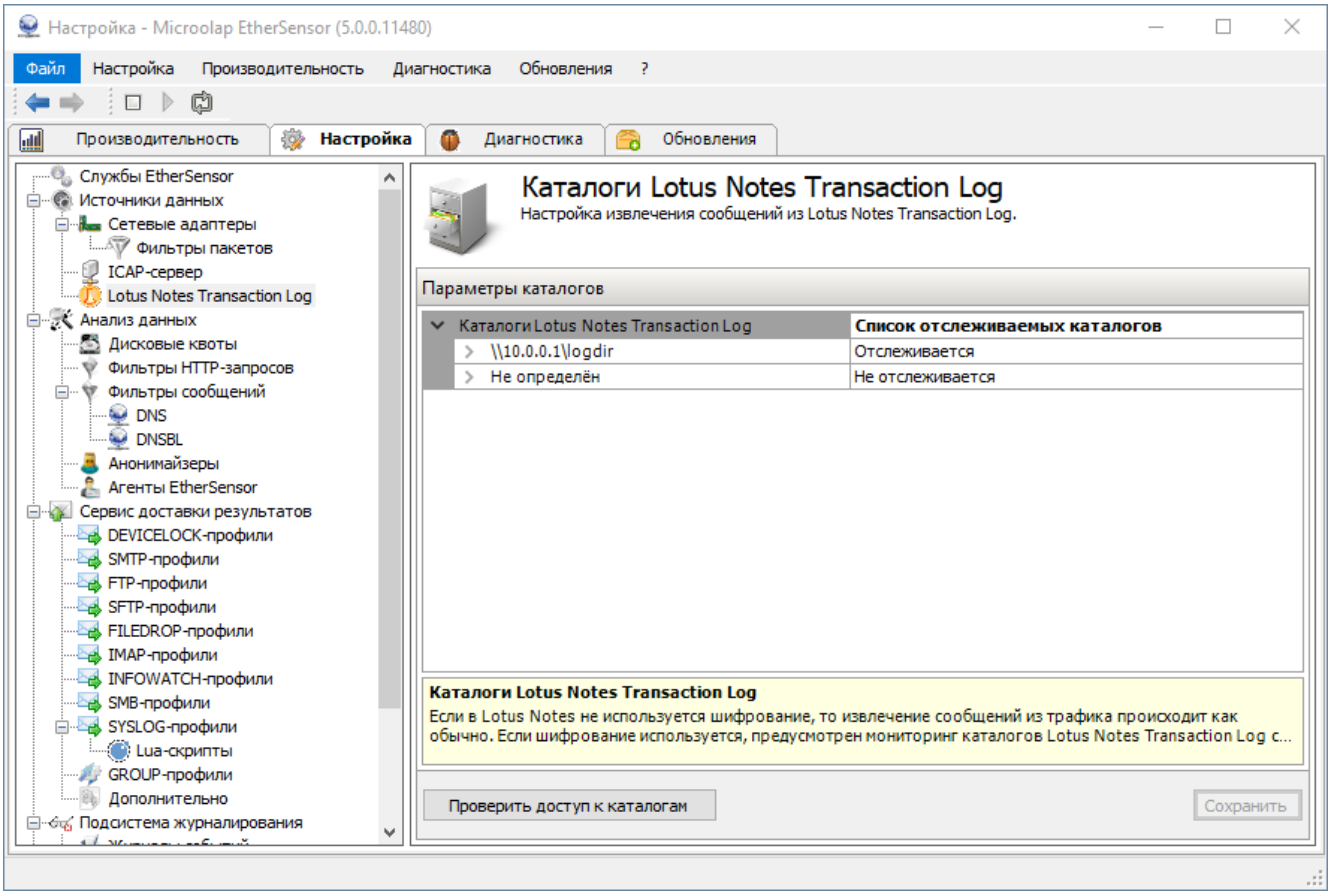

Рис.5. Окно настройки службы EtherSensor LotusTXN.

Результатом работы этих служб являются реконструированные объекты, переданные в службу анализа результатов **EtherSensor Analyser.**

Для запуска и остановки служб **EtherSensor EtherCAP, EtherSensor ICAP** и **EtherSensor LotusTXN** можно использовать как штатную оснастку **Службы** ОС Windows, так и **Конфигуратор EtherSensor** (утилита **ethersensor_console.exe**) из директории установки **Microolap EtherSensor**:

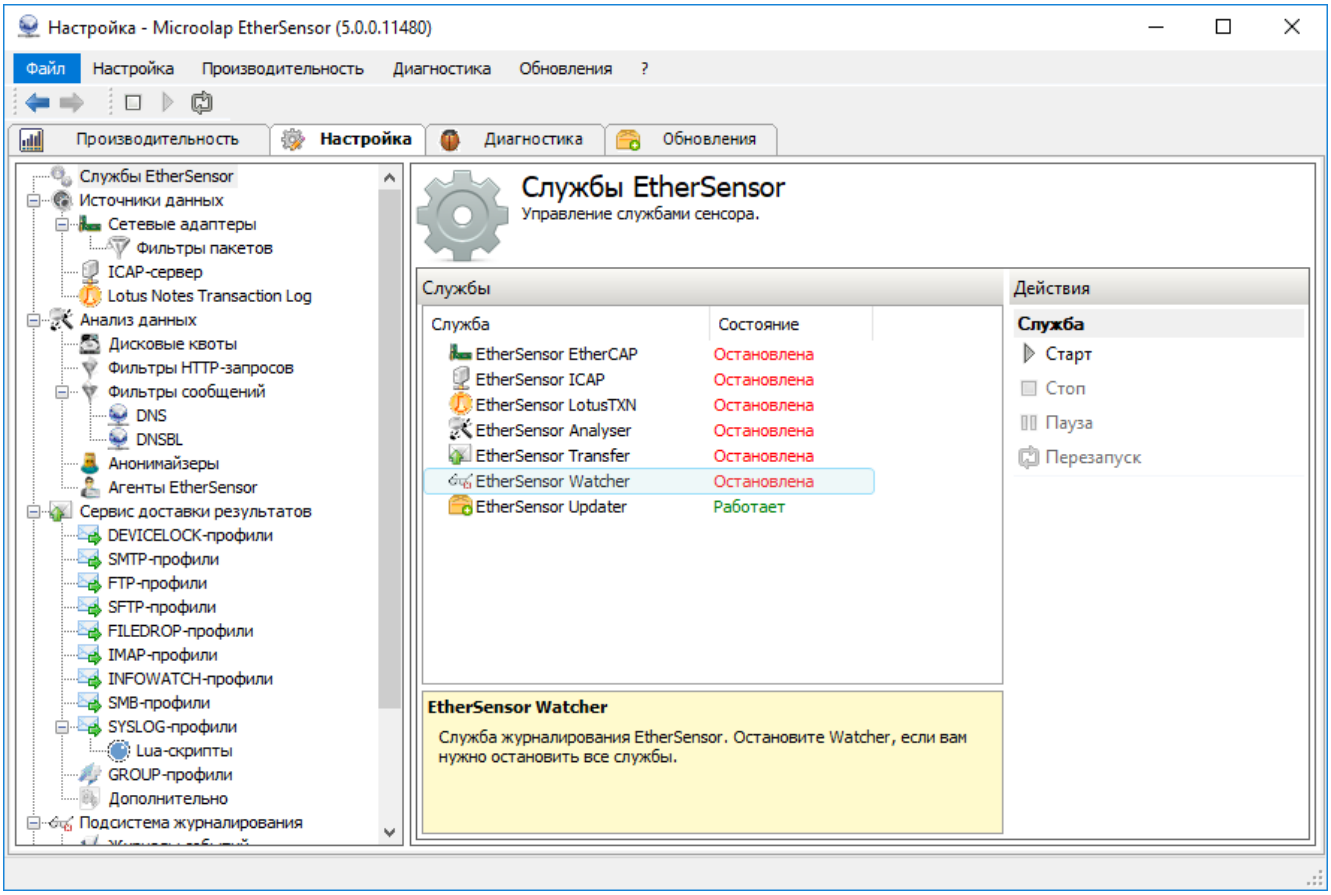

Рис.6. Запуск и остановка служб-источников данных.

3.1.1. Служба EtherSensor EtherCAP

Служба **EtherSensor EtherCAP** отвечает за пассивный захват трафика на сетевых адаптерах, а также за обработку трафика из PCAP-файлов в форматах **tcpdump/libpcap/pcapng**.

Служба извлекает из обрабатываемого трафика объекты уровня приложения (L7) модели OSI, и передаёт эти объекты для дальнейшей обработки в службу **EtherSensor Analyser**.

EtherSensor EtherCAP умеет обрабатывать следующие протоколы третьего уровня модели OSI:

IP:

Обычный трафик;

GRE:

Туннелированный трафик, например соединения не шифрованного протокола Ethernet over GRE или IP-over-IP;

IPv6-over-IPv4:

Инкапсулированный протокол IPv6 (как правило, встречается в крупных сетях и на магистральных каналах).

Во всех случаях **Microolap EtherSensor** обрабатывает в основном TCP- и UDP-потоки.

В текущей версии **Microolap EtherSensor** (5.1.0.13519) служба **EtherSensor EtherCAP** умеет распознавать и обрабатывать следующие наиболее часто используемые интернет-протоколы передачи данных уровня приложений:

HTTPv1/HTTPv2:

Все виды запросов, передача сообщений, передача файлов;

SMTP:

Передача исходящих почтовых сообщений;

POP3:

Передача входящих почтовых сообщений;

IMAP4:

Передача входящих и исходящих почтовых сообщений;

ICQ:

Передача входящих и исходящих мгновенных сообщений, списков контактов, файлов;

DC:

Передача мгновенных сообщений по протоколам NMDC и ADC (DC++);

LOTUS:

Передача почтовых сообщений, календарей, задач системы **Lotus Notes**;

MRA:

Передача мгновенных сообщений, списков контактов и файлов при помощи утилиты Mail.Ru Агент;

MSN:

Передача мгновенных сообщений, списков контактов и файлов при помощи утилиты MSN;

XMPP:

Передача мгновенных сообщений,списков контактов и файлов при помощи XMPP-клиентов (Google Talk и др.);

IRC:

Передача мгновенных сообщений и файлов;

SKYPE:

Детектирование факта использования клиентов skype, извлечение сообщений;

SSL:

Детектирование факта использования протокола SSL;

TORRENT:

Детектирование факта использования Torrent-клиентов;

FTP:

Передача файлов;

YAHOO:

Передача мгновенных сообщений, файлов;

ICAP:

Перехват данных, передаваемых по протоколу ICAP;

SOCKS:

Перехват данных, передаваемых по протоколу SOCKS.

WEBSOCKET:

Перехват данных, передаваемых по протоколу WEBSOCKET.

Общая схема работы службы **EtherSensor EtherCAP:**

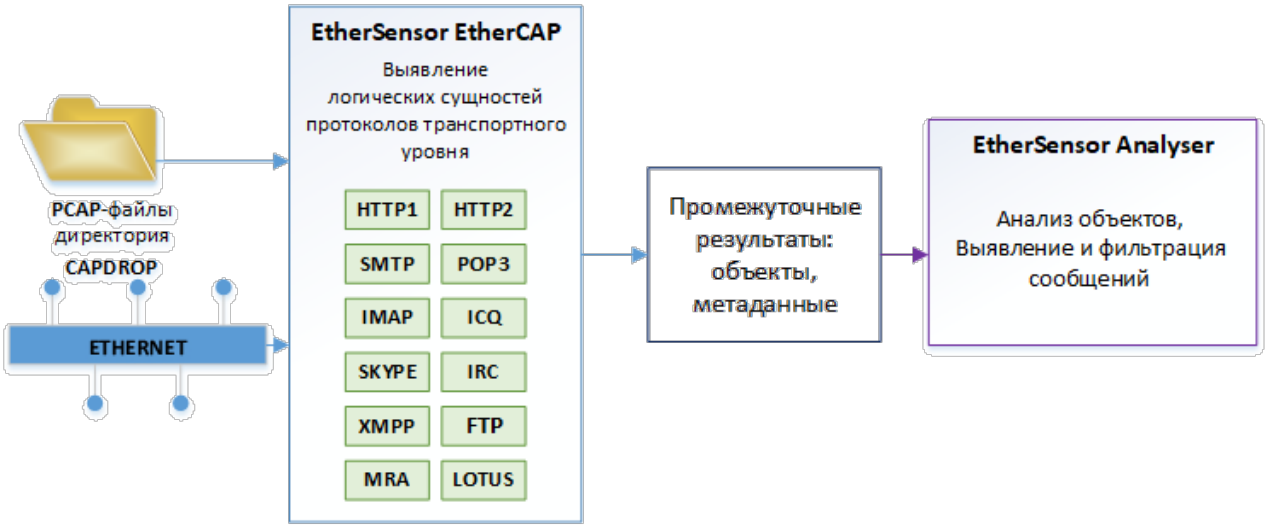

Рис.7. Схема работы службы EtherSensor EtherCAP

Служба **EtherSensor EtherCAP** позволяет вести одновременный перехват трафика со всех доступных Ethernet интерфейсов, а также отслеживать локальную директорию для обработки помещённых в неё PCAP-файлов.

Размер необходимых аппаратных ресурсов на каждый прослушиваемый сетевой интерфейс можно рассчитать исходя из того, что среднее количество памяти, необходимое для обработки одного TCP соединения составляет приблизительно 40 Кбайт:

Пропускная способность сетевого интерфейса	Расход оперативной памяти на кэш обрабатываемых пакетов
10000 Mbit	2000 МБайт
5000 Mbit	1000 МБайт
1000 Mbit	200 МБайт
100 Mbit	50 Мбайт
10 Mbit	10 Мбайт

Таким образом, для одновременного отслеживания 10000 TCP сессий через сетевой интерфейс с пропускной способностью 1 Gbps **Microolap EtherSensor** необходимо иметь следующее количество доступной физической памяти:

200 МБайт + 10000 * 40 Кбайт - около 600 МБайт

Служба **EtherSensor EtherCAP** позволяет для оптимизации обработки трафика назначать для каждого прослушиваемого сетевого интерфейса пакетный фильтр, а также необходимые для отслеживания сетевые протоколы.

Варианты организации работы службы:

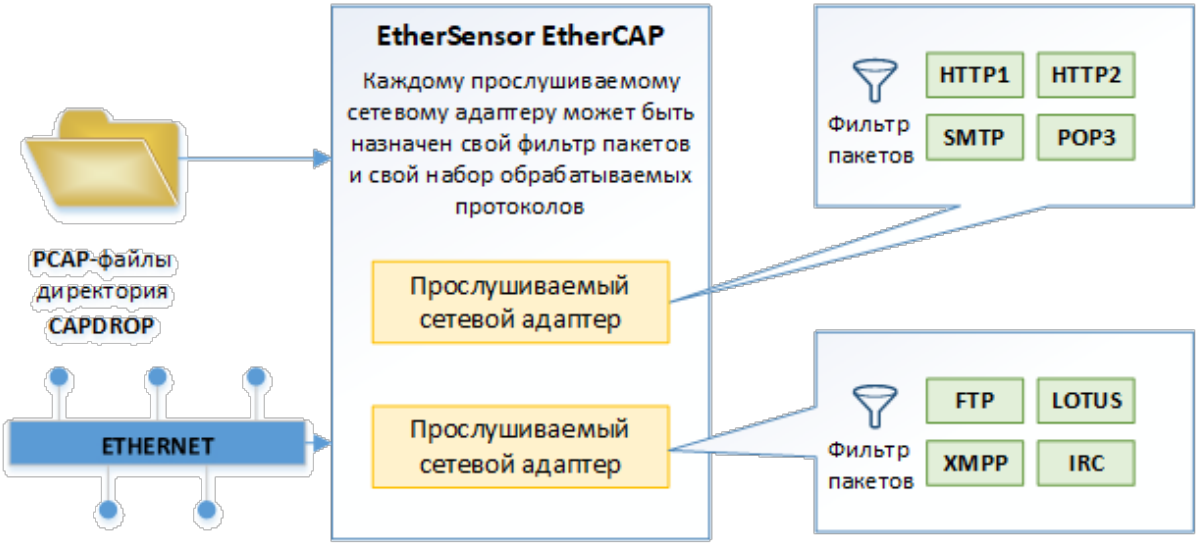

Рис.8. Варианты организации работы службы EtherSensor EtherCAP.

Для обработки PCAP-файлов служба эмулирует работу с сетевым интерфейсом, настройку которого можно произвести, используя конфигурационный файл службы. Этому сетевому интерфейсу в конфигурационном файле назначено уникальное имя **capdrop**. В текущей версии **Microolap EtherSensor** (5.1.0.13519) службой **EtherSensor EtherCAP** поддерживается только два самых распространенных формата PCAP-файлов - **tcpdump/libpcap** и **pcapng**.

Параметры командной строки

Служба Windows **EtherSensor EtherCAP** в ходе инсталляции **Microolap EtherSensor** устанавливается с автоматическим запуском. Однако, при необходимости процесс **ethersensor_ethercap.exe** можно запустить как приложение Windows со следующими параметрами командной строки:

/process

Запускает процесс **ethersensor_ethercap.exe** как обычный Windows Win32-процесс (возможно использование для отладки).

/service

Запускает как службу Windows.

/config

Сохраняет конфигурацию службы по умолчанию.

3.1.1.1. Настройка в конфигураторе

Служба **EtherSensor EtherCAP** позволяет прослушивать как аппаратные сетевые интерфейсы, установленные в среде выполнения **Microolap EtherSensor**, так и специальное виртуальное устройство **PCAP files processing adapter**, предназначенное для обработки трафика, предварительно накопленного в файлах формата **tcpdump/libpcap/pcapng**.

Настройки аппаратных сетевых интерфейсов

Информация о настройках сетевых интерфейсов и пакетных фильтрах содержится в файле **ethcap.xml**, находящемся в директории **[INSTALLDIR]\config**, который может быть отредактирован как в конфигураторе, так и любым текстовым редактором.

В утилите конфигуратора (файл **ethersensor_console.exe**) настройка службы **EtherSensor EtherCAP** происходит следующим образом:

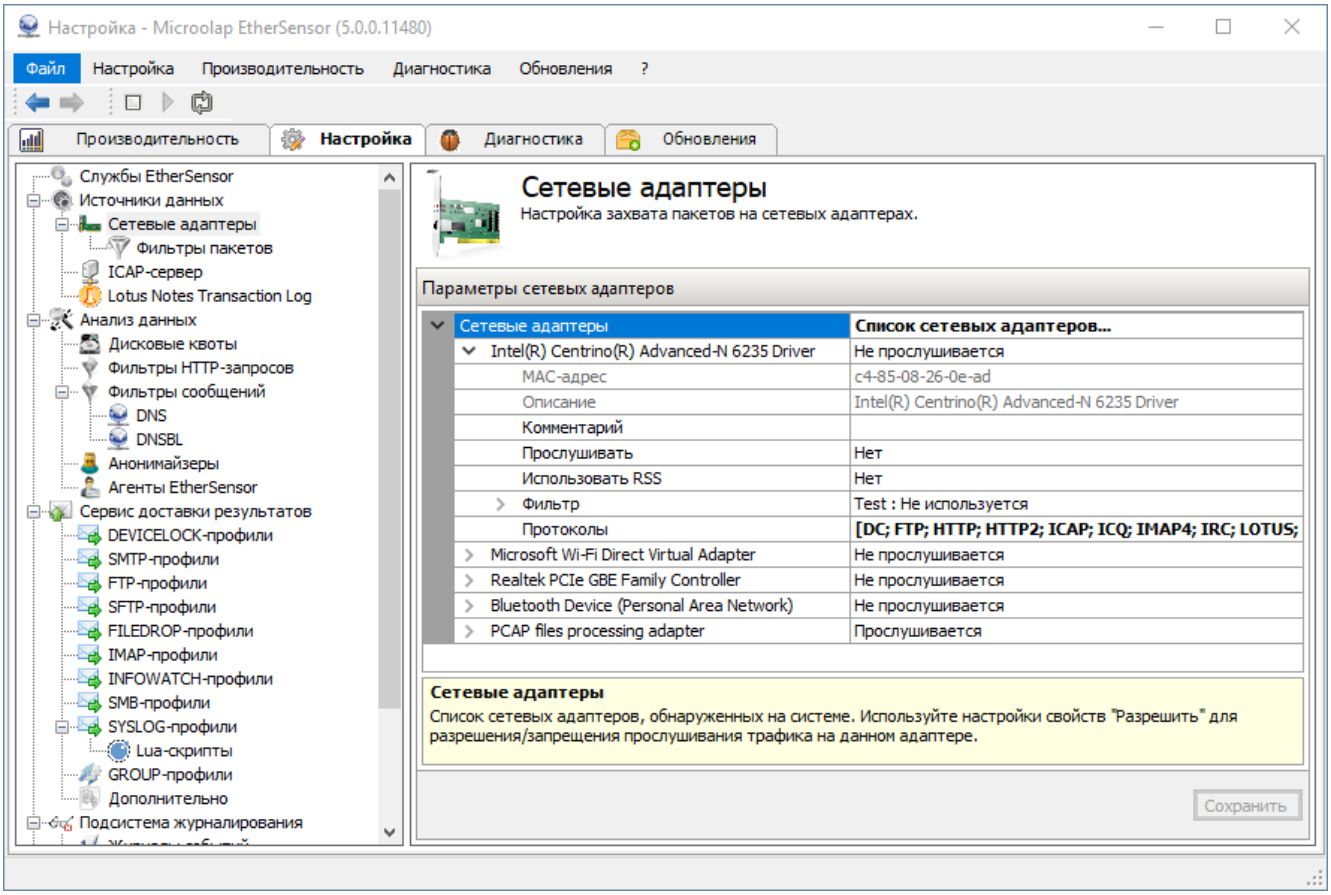

Рис.9. Настройка службы EtherSensor EtherCAP

MAC-адрес:

MAC-адрес настраиваемого сетевого интерфейса. Значение MAC-адреса попадает в сообщения, отправляемые **Microolap EtherSensor** системе-потребителю.

Прослушивать:

Включение/выключение прослушивания данного адаптера службой **EtherSensor EtherCAP**. Возможно одновременное прослушивание нескольких адаптеров. Служба **EtherSensor EtherCAP** будет прослушивать все несконфигурированные интерфейсы.

Чтобы прослушивать интерфейс, который сконфигурирован для ОС, необходимо установить для него флаг **Прослушивать** в **Да.** Чтобы не прослушивать те интерфейсы, на которых не установлен стек ОС, необходимо их флаги **Прослушивать** установить в **Нет.**

Использовать RSS:

Включение/выключение использования технологии RSS . Receive Side Scaling (RSS) - технология, которая равномерно распределяет нагрузку по обработке сетевых пакетов между ядрами процессора, позволяя оптимизировать производительность.

Фильтр:

Отображается название фильтра, ассоциированного с данным адаптером и статус его использования (**Используется/Не используется**). Заготовленных заранее фильтров может быть сколь угодно много, но применяться одновременно на одном и том же сетевом адаптере может только один.

Имя фильтра:

Поле выбора пакетного фильтра из числа уже имеющихся. Фильтры хранятся в файле **[INSTALLDIR]\config\ethcap.xml.**

Применить:

Включение/выключение использования указанного фильтра на данном сетевом интерфейсе.

Протоколы:

Позволяет в целях экономии ресурсов отключить неиспользуемые фильтры протоколов. Например, если нет необходимости в работе с мгновенными сообщениями, следует отключить фильтры для протоколов **DC, ICQ, IRC, MRA, MSN, SKYPE** и **YAHOO**.

PCAP files processing adapter

PCAP files processing adapter является специальным виртуальным устройством, предназначенным для обработки трафика, предварительно сохраненного в PCAP-файлах (например, полученных в другом сегменте сети). Настройки **PCAP files processing adapter** не отличаются от настроек аппаратных адаптеров:

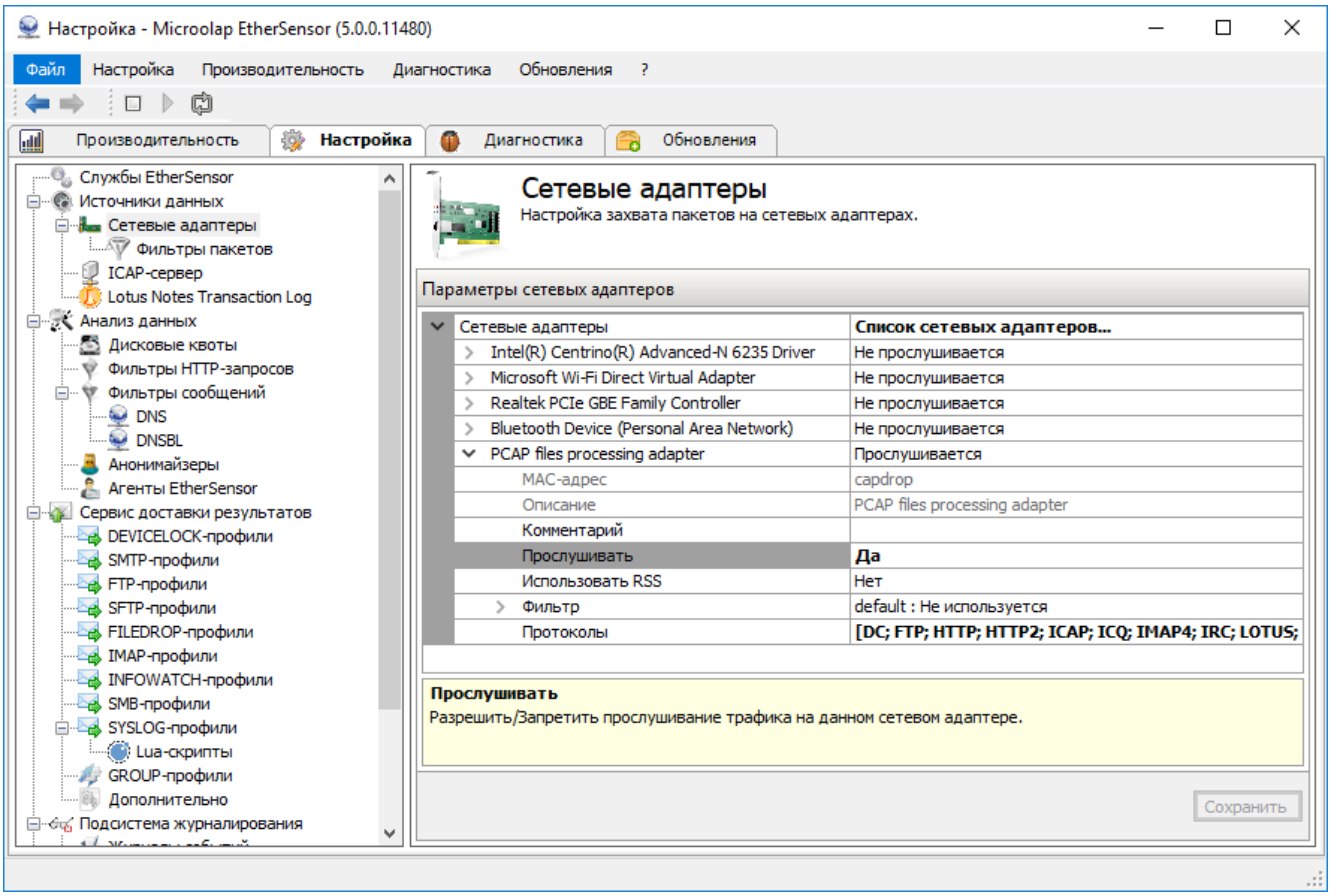

Рис.10. Настройки PCAP files processing adapter.

Для обработки PCAP-файлов необходимо скопировать их в директорию **[INSTALLDIR]\data\capdrop**, и затем разрешить прослушивание **PCAP files processing adapter** из конфигуратора. PCAP-файлы "прослушиваются" в порядке FIFO: файл, помещенный в директорию **[INSTALLDIR]\data\capdrop** первым (т.е., имеющий более раннюю дату модификации с точки зрения файловой системы), будет "прослушан" первым, помещенный туда вторым будет "прослушан" вторым и т.д.

Если **PCAP files processing adapter** находится в состоянии **Прослушивается**, директория **[INSTALLDIR]\data\capdrop** была пуста, и в неё был помещен PCAP-файл, то этот файл немедленно начнет "прослушиваться".

Если **PCAP files processing adapter** находится в состоянии **Не прослушивается**, в директории **[INSTALLDIR]\data\capdrop** имелись PCAP-файлы, то "прослушивание" файлов начнется немедленно после перевода адаптера в состояние **Прослушивается**.

> Обработанные таким образом PCAP-файлы помещаются в директорию **[INSTALLDIR]\data\capdrop\processed** без каких-либо изменений, что позволяет повторять процесс обработки сколько угодно раз (например, для отладки фильтров).

Сообщения, полученные службой **EtherSensor EtherCAP** из PCAP-файлов, далее обрабатываются обычным образом.

Создание и настройка фильтров пакетов

Для создания и редактирования пакетных фильтров используйте форму конфигуратора в секции **Фильтры пакетов**:

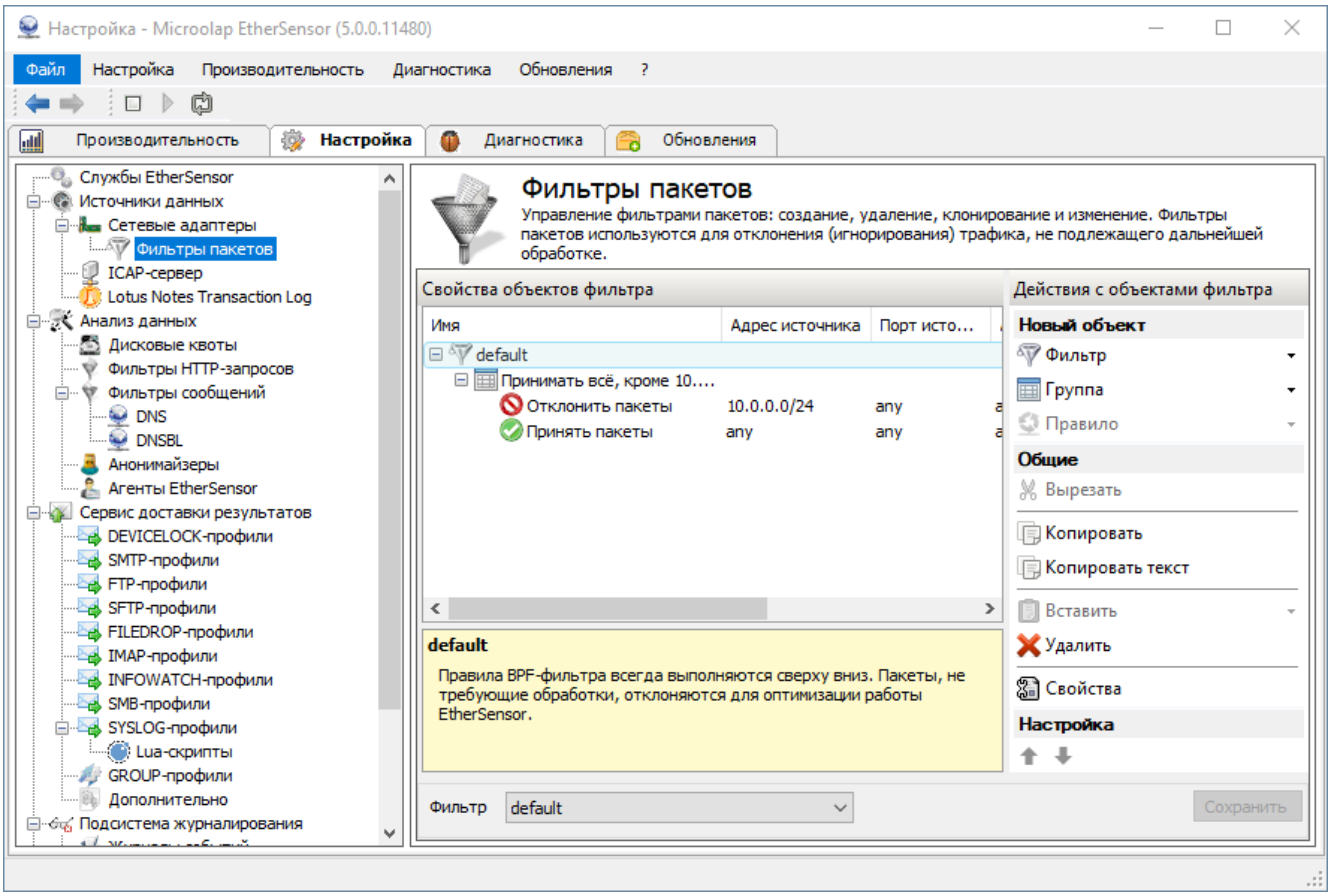

Рис.11. Настройки пакетных фильтров.

Панель **Действия с объектами фильтра:**
Создание, клонирование и удаление фильтров и их объектов: групп и правил.

Панель **Свойства объектов фильтра**
Редактирование свойств самого фильтра, групп и правил.

Панель редактирования свойств объекта вызывается двойным щелчком мыши по соответствующему объекту: фильтру, группе правил или правилу:

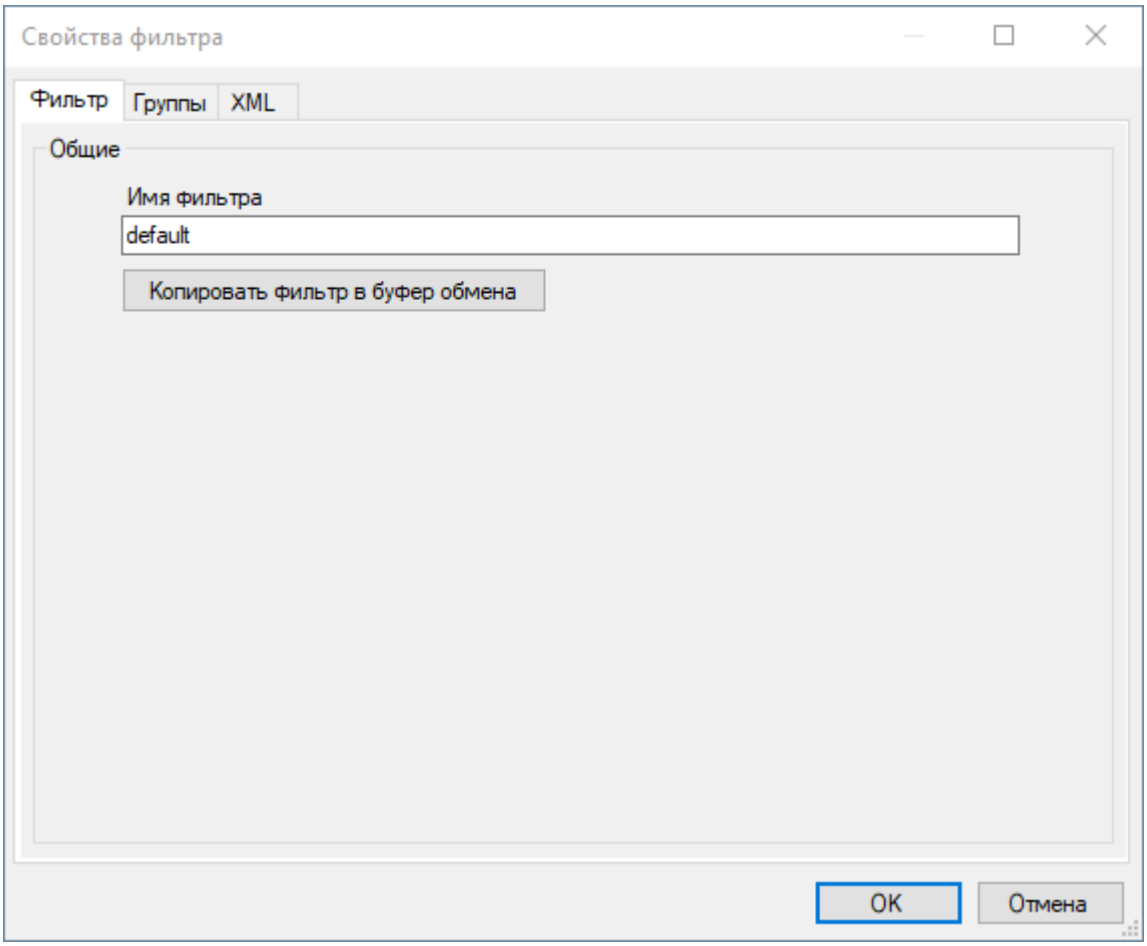

Рис.12. Панель редактирования свойств фильтра.

Имя фильтра:
Название фильтра (на усмотрение администратора).

Вкладка групп правил фильтрации:
BPF-программа не ограничивается по длине и количество правил в фильтре может быть весьма велико. Для удобства работы с правилами используйте возможность объединения их в группы с информативными названиями.

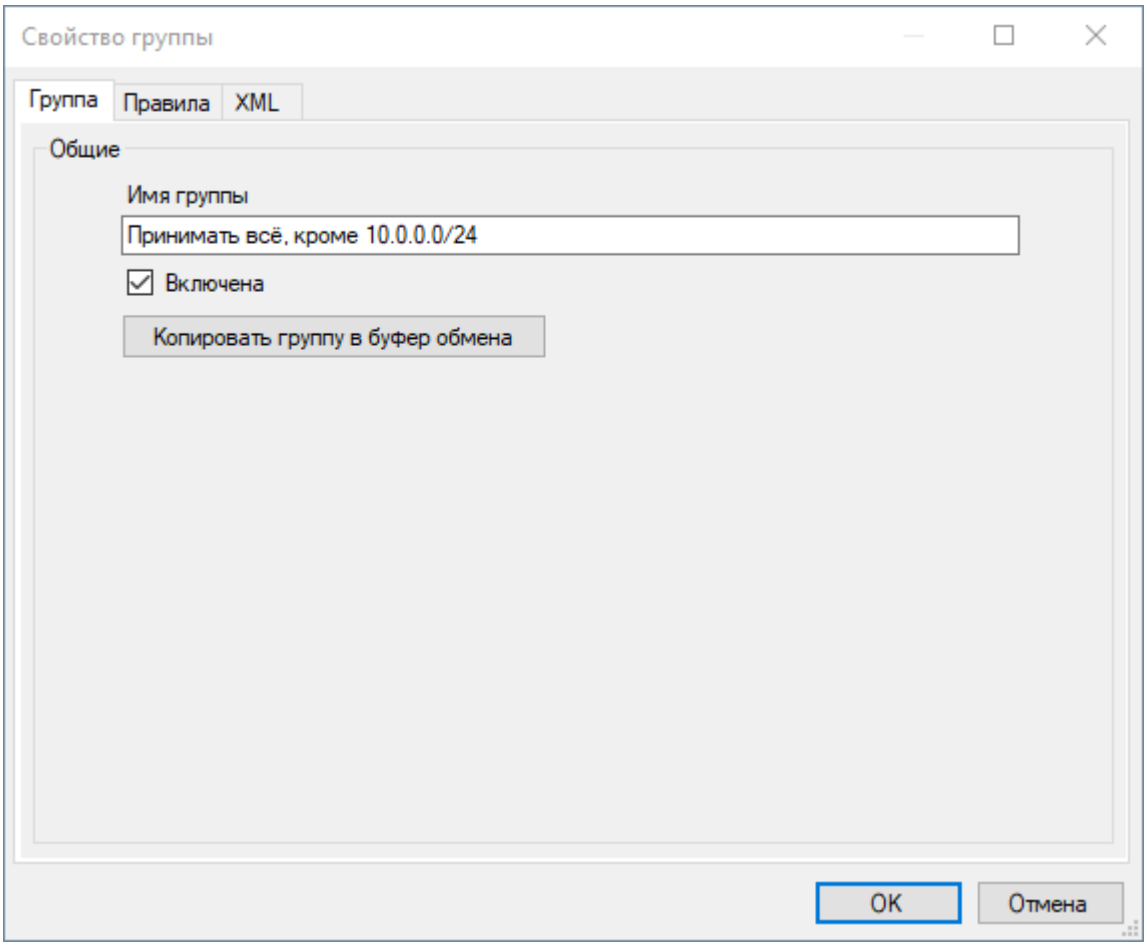

Рис.13. Панель редактирования свойств группы правил.

Имя группы:

Имя группы правил (на усмотрение администратора).

Чекбокс **Включена:**
Позволяет отключать/подключать группу правил.

Вкладка **Правила:**
К редактированию правил можно получить доступ как с уровня фильтра, так и из вкладки **Правила** свойств группы правил.

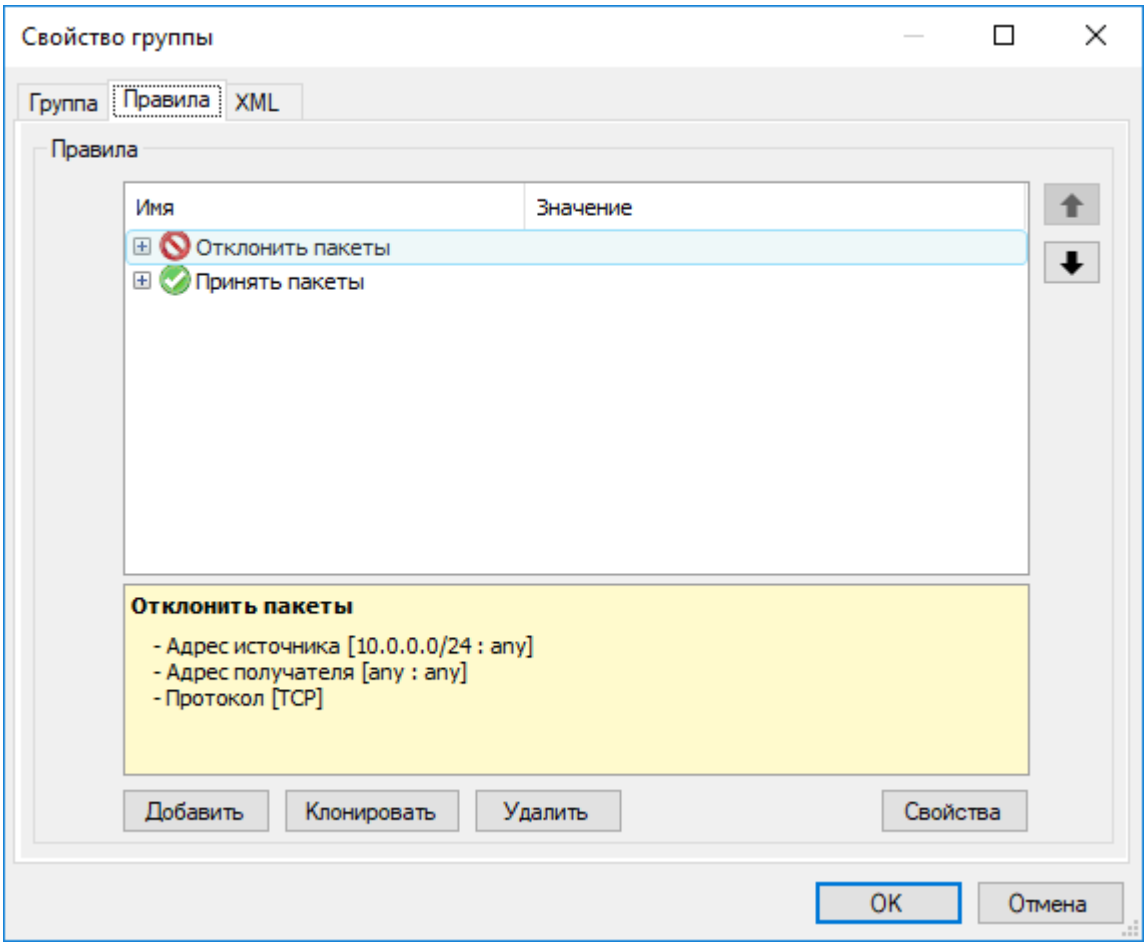

Рис.14. Панель редактирования правила.

Панель редактирования действия и условий правила вызывается двойным щелчком мыши по названию правила.

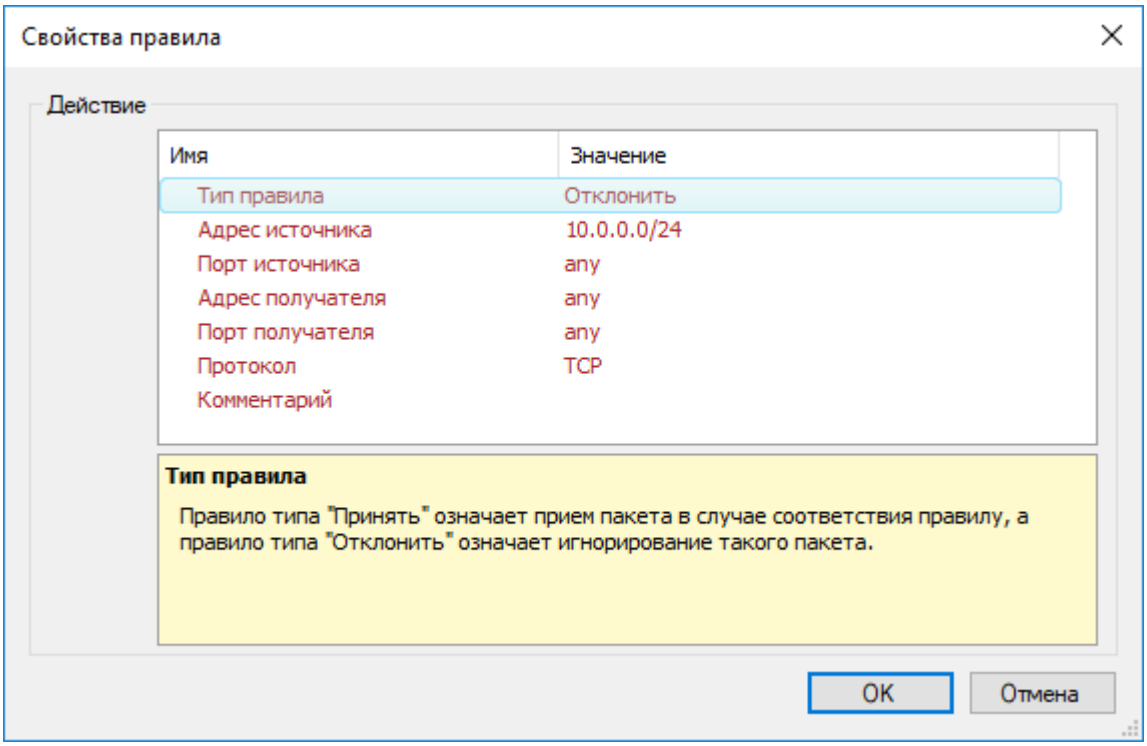

Рис.15. Панель редактирования правила.

Тип правила:

Определено два типа правил: **Принять** и **Отклонить**. Правило типа **Принять** означает прием пакета в случае соответствия условиям правила, а правило типа **Отклонить** означает игнорирование такого пакета.

Внимание!
Правила фильтра применяются всегда последовательно, перестановка правил в фильтре может в корне изменить результат его работы.

Адрес источника:

Адрес источника. Например: **any** или **10.0.0.0/24** или **10.0.0.0-10.0.0.255** или список через запятую вида **100.100.100.1-100.100.100.255, 192.168.0.0/8.**

Порт источника:

Порт источника, например: **any** или **80** или **80-8080** (с 80 по 8080), или **80-8000, 9000-10000** (с 80 по 8000 и с 9000 по 10000).

Адрес получателя:

Адрес получателя. Например: **any** или **10.0.0.0/24** или **10.0.0.0-10.0.0.255** или список через запятую вида **100.100.100.1-100.100.100.255, 192.168.0.0/8.**

Порт получателя:

Порт получателя, например: **any** или **80** или **80-8080** (с 80 по 8080), или список через запятую **80-8000, 9000-10000** (с 80 по 8000 и с 9000 по 10000).

Протокол:

Один из **TCP, UDP, GRE, IP6,** либо **any**.

Комментарий

Ваш комментарий к данному правилу фильтрации.

Подробнее с настройками службы **EtherSensor EtherCAP** можно ознакомиться в разделе "Ручная настройка (файл конфигурации)".

3.1.1.2. Ручная настройка (файл конфигурации)

Конфигурация службы **EtherSensor EtherCAP** содержится в XML-файле **ethcap.xml,** расположенном в общей директории конфигураций **Microolap EtherSensor [INSTALLDIR] \config**

```
<?xml version="1.0" encoding="utf-8"?>
<EtherCapConfig version="4.2"
 flow_count="16"
 flow_buff_count="512"
 flow_buff_size="524288">
  <NetworkAdapters>
   <NetworkAdapter enabled="true" rss="true" mac="00-1F-C6-2D-EA-40"
    description="Marvell Yukon 88E8056 PCI-E Gigabit Ethernet Controller">
     <Filter enabled="true" name="internet" />
     <Protocol enabled="true" name="dc" />
     <Protocol enabled="true" name="ftp" />
     <Protocol enabled="true" name="http" />
     <Protocol enabled="true" name="icq" />
     <Protocol enabled="true" name="imap4" />
     <Protocol enabled="true" name="irc" />
     <Protocol enabled="true" name="lotus" />
     <Protocol enabled="true" name="mra" />
     <Protocol enabled="true" name="msn" />
     <Protocol enabled="true" name="pop3" />
     <Protocol enabled="true" name="skype" />
     <Protocol enabled="true" name="smtp" />
     <Protocol enabled="true" name="ssl" />
     <Protocol enabled="true" name="xmpp" />
     <Protocol enabled="true" name="yahoo" />
   </NetworkAdapter>
   <NetworkAdapter enabled="true" mac="capdrop"
    description="PCAP files processing adapter">
    <Filter enabled="true" name="default" />
    <Protocol enabled="true" name="dc" />
    <Protocol enabled="true" name="ftp" />
    <Protocol enabled="true" name="http" />
    <Protocol enabled="true" name="icq" />
    <Protocol enabled="true" name="imap4" />
    <Protocol enabled="true" name="irc" />
    <Protocol enabled="true" name="lotus" />
    <Protocol enabled="true" name="mra" />
    <Protocol enabled="true" name="msn" />
    <Protocol enabled="true" name="pop3" />
    <Protocol enabled="true" name="skype" />
    <Protocol enabled="true" name="smtp" />
    <Protocol enabled="true" name="ssl" />
    <Protocol enabled="true" name="xmpp" />
    <Protocol enabled="true" name="yahoo" />
   </NetworkAdapter>
  </NetworkAdapters>

 <Filters>

  <Filter name="default">
   <RuleGroup enabled="true" name="">
    <Rule
     type="accept"
     src="any"
     srcport="any"
     dst="any"
     dstport="any"
     proto="tcp"
     comment="Comment to the rule" />
   </RuleGroup>
  </Filter>

  <Filter name="internet">
   <RuleGroup enabled="true" name="">
    <Rule
```

```
     type="reject"
     src="192.168.0.1"
     srcport="any"
     dst="any"
     dstport="any"
     proto="tcp"
     comment="Comment to the rule" />
    <Rule
     type="reject"
     src="*"
     srcport="any"
     dst="192.168.0.1"
     dstport="any"
     proto="tcp" />
    <Rule
     type="accept"
     src="any"
     srcport="any"
     dst="any"
     dstport="any"
     proto="tcp" />
   </RuleGroup>
  </Filter>

 </Filters>
</EtherCapConfig>
```

Тег EtherCapConfig

Является корневым тегом конфигурации службы. В его атрибуте **version** указывается версия файлов конфигурации.

Атрибут **flow_count** используется для указания количества одновременно обрабатываемых потоков. Весь перехватываемый трафик равномерно распределяется между потоками обработки. Распределение трафика происходит на уровне ядра операционной системы, тем самым обеспечивается параллелизм обработки данных.

Атрибут **flow_buff_count** используется для указания количества буферов данных в потоке обработки трафика. Данная характеристика совместно с атрибутом **flow_buff_size** задаёт статический объём памяти, используемой для одного потока обработки.

Атрибут **flow_buff_size** используется для указания размера буфера данных в потоке обработки трафика. Величина указывается в байтах. Данная характеристика совместно с атрибутом **flow_buff_count** задаёт статический объём памяти, используемой для одного потока обработки. Объём памяти для одного потока будет составлять (**flow_buff_count** * **flow_buff_size**) = (512 * 524288 = 256 Мб)

Внимание!
Указанные выше атрибуты используются для тонкой инженерной настройки **Microolap EtherSensor** и требуют глубокого понимания функционирования продукта: не экспериментируйте с ними на рабочей системе.

Тег NetworkAdapters

Определяет настройки прослушиваемых сетевых интерфейсов.

Тег NetworkAdapter

Тег **NetworkAdapter** является вложенным в тег **NetworkAdapters** и указывает на описание настроек конкретного сетевого интерфейса. В атрибуте **enabled** указывается статус активности сетевого интерфейса, и если данный атрибут выставлен в значение **false**, то сетевой интерфейс не будет использоваться в обработке данных (трафик, поступающий с этого интерфейса, будет игнорироваться).

Атрибут **rss** используется для использования технологии Receive Side Scaling (RSS). Это технология, которая равномерно распределяет нагрузку по обработке сетевых пакетов между ядрами процессора, позволяя оптимизировать производительность.

Атрибут **mac** используется для указания имени сетевого интерфейса. Данный атрибут не должен изменяться, и предназначен только для чтения. Атрибут **description** используется для указания описания сетевого интерфейса и заполняется на усмотрение администратора.

Тег Filter

Тег **Filter** является вложенным в тег **NetworkAdapter** и указывает на описание используемого IP-фильтра для данного сетевого интерфейса. В атрибуте **enabled** указывается статус использования IP-фильтра, и если данный атрибут выставлен в значение **false**, то для данного сетевого интерфейса не будет использоваться IP-фильтр в обработке данных. В атрибуте **name** указывается имя профиля IP-фильтра. Профили IP-фильтров указываются в теге **Filters**.

Тег Protocol

Тег **Protocol** является вложенным в тег **NetworkAdapter** и указывает на описание используемого интернет-протокола для обработки данных. В атрибуте **enabled** указывается статус использования интернет-протокола, и если данный атрибут выставлен в значение **false**, то для данного сетевого интерфейса данный интернет-протокол будет игнорироваться. В атрибуте **name** указывается имя интернет-протокола. Данный атрибут используется только для чтения и не подлежит изменению.

Пример 1:

Настройки сетевого интерфейса для перехвата сообщений клиентов DC, ICQ, IRC, MRA, MSN, XMPP/Jabber, YAHOO:

```
<NetworkAdapter
 enabled="true"
 mac="capdrop"
 description="PCAP files processing adapter">
  <Filter enabled="true" name="default" />
   <Protocol enabled="true"  name="dc" />
   <Protocol enabled="false" name="ftp" />
   <Protocol enabled="false" name="http" />
   <Protocol enabled="true"  name="icq" />
   <Protocol enabled="false" name="imap4" />
   <Protocol enabled="true"  name="irc" />
   <Protocol enabled="false" name="lotus" />
   <Protocol enabled="true"  name="mra" />
   <Protocol enabled="true"  name="msn" />
   <Protocol enabled="false" name="pop3" />
   <Protocol enabled="false" name="skype" />
   <Protocol enabled="false" name="smtp" />
   <Protocol enabled="false" name="ssl" />
   <Protocol enabled="true"  name="xmpp" />
   <Protocol enabled="true"  name="yahoo" />
</NetworkAdapter>
```

Тег Filters

Определяет настройки профилей IP-фильтров.

Тег Filter

Тег **Filter** является вложенным в тег **Filters** и указывает на описание настроек IP-фильтра. Атрибут **name** используется для указания имени профиля IP-фильтра. Значение данного атрибута может быть использовано в качестве значения атрибута **NetworkAdapter/Filter/name** для указания IP-фильтра сетевому интерфейсу.

Тег RuleGroup

Тег **RuleGroup** является вложенным в тег **Filter** и служит для группировки правил фильтрации, относящихся к конкретной решаемой задаче фильтрации трафика. Атрибут **name** используется для указания имени (описания) группы правил фильтрации. Значение данного атрибута может оставаться пустым.

Тег Rule

Тег **Rule** является вложенным в тег **RuleGroup** и указывает на описание правила фильтрации сетевого трафика. В атрибуте **type** указывается тип правила, и если данный атрибут выставлен в значение **accept**, то сетевые пакеты, подходящие под данное правило, будут пропущены для дальнейшей обработки, иначе, если атрибут выставлен в значение **reject**, сетевые пакеты, подходящие под данное правило будут отклонены. В атрибутах **src, dst** указывается IP-адрес(а), диапазон IP-адресов или параметры сети для фильтрации необходимых IP-адресов, подходящих под указанное значение. В атрибуте **comment** можно указать комментарий к правилу фильтрации пакетов.

Пример 2:

Отклонить пакеты, проходящие между компьютерами 10.1.5.10, 10.1.5.15-10.1.5.59 и сетью 10.1.6.0/255.255.255.0:

```
<Rule
 type="reject"
 src="10.1.5.10, 10.1.5.15-10.1.5.59"
 dst="10.1.6.0/255.255.255.0"
 proto="tcp"
 comment="" />

<Rule type="reject"
 src="10.1.6.0/255.255.255.0"
 dst="10.1.5.10, 10.1.5.15-10.1.5.59"
 proto="tcp" />
```

В атрибутах **srcport, dstport** указываются необходимые для фильтрации TCP порты или диапазоны TCP портов.

Пример 3:

Отклонить пакеты, проходящие между компьютерами 10.1.5.10, 10.1.5.15-10.1.5.59 и сетью 10.1.6.0/255.255.255.0 на портах 80, 443-1024:

```
<Rule
 type="reject"
 src="10.1.5.10, 10.1.5.15-10.1.5.59"
 srcport="80, 443-1024"
 dst="10.1.6.0/255.255.255.0"
 proto="tcp" />

<Rule
 type="reject"
 src="10.1.6.0/255.255.255.0"
 dst="10.1.5.10, 10.1.5.15-10.1.5.59"
 dstport="80, 443-1024"
 proto="tcp" />
```

Правила применяются линейно, т.е. сверху вниз. Верхняя строчка - это первая инструкция фильтра, соответственно нижняя - последняя. Каждая строчка отсекает или пропускает только тот тип пакетов, который она описывает. Таким образом, для того, чтобы отсечь соединение между двумя хостами или группой хостов, необходимо отсекать трафик в обе стороны соединения.

Например:

```
<Rule
 type="reject"
 src="10.31.5.212"
 dst="10.31.5.57"
 dstport="1025"
 proto="tcp" />

<Rule
 type="reject"
 src="10.31.5.57"
 srcport="1025"
 dst="10.31.5.212"
 proto="tcp" />
```

Также необходимо помнить, что если не определено ни одно правило фильтрации, то мы получаем весь трафик. И наоборот, если есть правила фильтрации, то обрабатывается только трафик, описанный этими правилами.

Например:

1. Получить все соединения только с хостом 10.31.5.57

```
<Rule
 type="accept"
 src="10.31.5.57"
 srcport="*"
 dst="*"
 dstport="*"
 proto="tcp" />

<Rule
 type="accept"
 src="*"
 srcport="*"
 dst="10.31.5.57"
 dstport="*"
 proto="tcp" />
```

2. Для того, чтобы отсечь группу хостов, необходимо сначала отклонить пакеты этой группы, затем обязательно пропустить все остальные пакеты, иначе весь трафик будет пропускаться без анализа:

```
<Rule
 type="reject"
 src="10.31.5.212"
 dst="10.31.5.57"
 dstport="1025"
 proto="tcp" />

<Rule
 type="reject"
 src="10.31.5.57"
 srcport="1025"
 dst="10.31.5.212"
 proto="tcp" />

<Rule
 type="accept"
 src="*"
 srcport="*"
 dst="*"
 dstport="*"
 proto="tcp" />
```

Таким образом можно отсекать трафик с нужной стороны прокси-сервера.

3. Если описать правила, пропускающие трафик только для определённых хостов, и запретить остальной трафик, будет обрабатываться трафик только этих хостов:

```
<Rule
 type="accept"
 src="10.31.5.212"
 dst="10.31.5.57"
 dstport="1025"
 proto="tcp" />

<Rule type="accept"
 src="10.31.5.57"
 srcport="1025"
 dst="10.31.5.212"
 proto="tcp" />
```

3.1.2. Служба EtherSensor ICAP

Служба **EtherSensor ICAP** является ICAP-сервером, предназначенным для получения сетевого трафика по протоколу ICAP от любых ICAP-клиентов в режиме REQMOD.

Протокол ICAP (Internet Content Adaptation Protocol) предназначен для работы только с протоколом HTTP и используется для контентной фильтрации и определения вредоносного содержимого (вирусы, spyware/malware).

В качестве клиента ICAP выступает система, через которую передается HTTP-трафик. Такой системой могут выступать различные HTTP-прокси, поддерживающие ICAP (например, SQUID, Blue Coat Proxy SG, Cisco IronPort S, Webwasher). После получения данных от клиента некоторые ICAP-серверы выполняют их обработку и, если это необходимо, то и модификацию данных.

Затем данные возвращаются клиенту ICAP, и он их передает дальше серверу или клиенту в зависимости от того, в каком направлении они передавались.

Поскольку ICAP-сервер **Microolap EtherSensor** использует трафик, получаемый от ICAP-клиентов, только для анализа, трафик всегда возвращается ICAP-клиенту без изменений. Архитектура системы при использовании протокола ICAP:

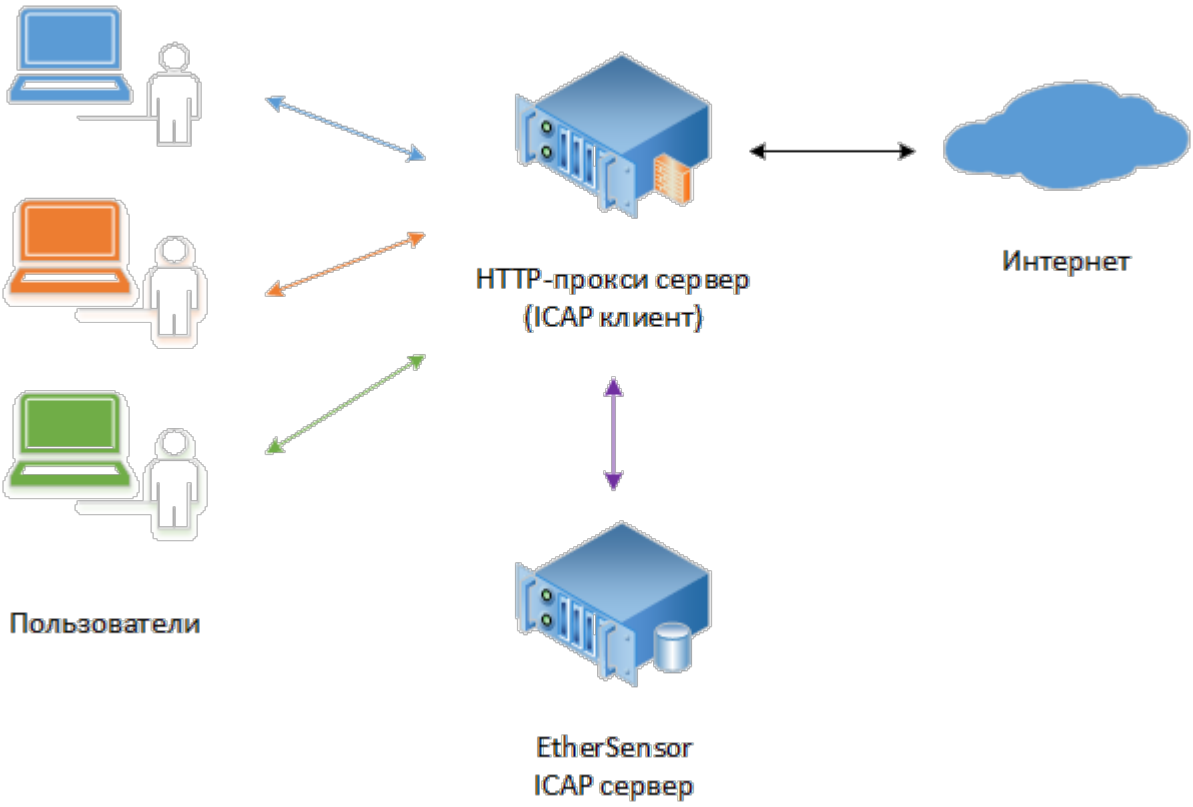

Рис.16. Схема взаимодействия службы EtherSensor ICAP и ICAP-клиента.

Некоторые клиенты ICAP используют расширения заголовков, что позволяет им передавать на ICAP-сервер информацию о пользователе, который авторизовался на прокси-сервере. Данная информация учитывается при дальнейшей обработке сообщений в **Microolap EtherSensor**.

Параметры командной строки

Служба Windows **EtherSensor ICAP** в ходе инсталляции **Microolap EtherSensor** устанавливается с автоматическим запуском. Однако, при необходимости процесс **ethersensor_icap.exe** можно запустить как приложение Windows со следующими параметрами командной строки:

/process

Запускает процесс **ethersensor_icap.exe** как обычный Windows Win32-процесс (возможно использование для отладки).

/service

Запускает как службу Windows.

/config

Сохраняет конфигурацию службы по умолчанию.

3.1.2.1. Настройка в конфигураторе

Служба **EtherSensor ICAP** является ICAP-сервером, предназначенным для работы с ICAP-клиентами, и имеющим свойственные этому типу серверов настройки:

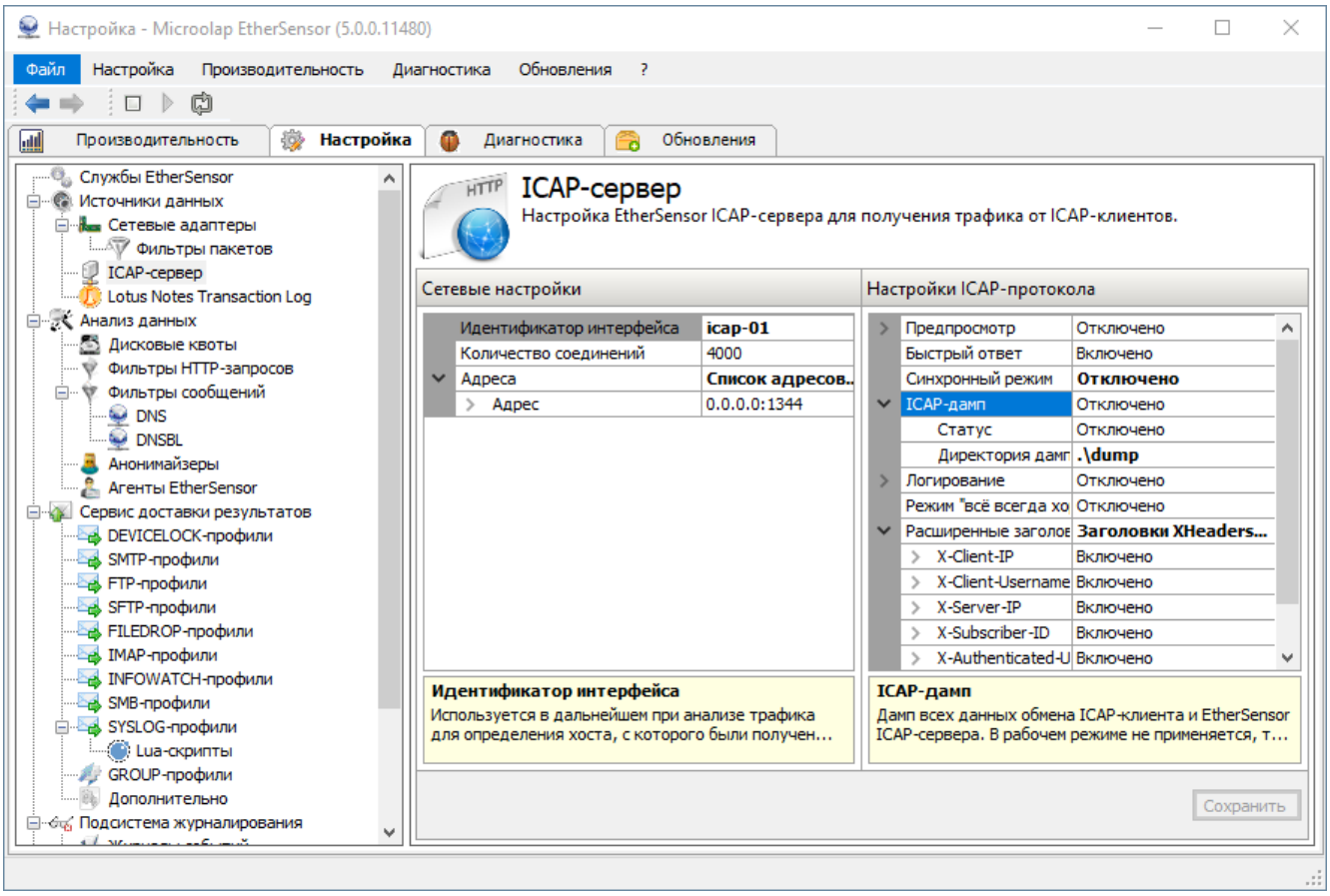

Рис.17. Настройки службы EtherSensor ICAP.

Количество соединений:

Максимальное количество соединений ICAP-сервера с клиентами. Примерное количество потребляемой на одно соединение оперативной памяти составляет около 8КБ.

Адреса:

IP-адреса/порты, прослушиваемые ICAP-сервером.

Предпросмотр:

Разрешение/запрещение предпросмотра, размер буфера.

Быстрый ответ:

Разрешение/запрещение быстрого короткого ответа **Allow 204** (**No modifications**).

Синхронный режим:

Разрешение/запрещение использования синхронного режима работы ICAP-сервера. В синхронном режиме ICAP-сервер сначала получает весь запрос целиком, и только потом

его отправляет обратно ICAP-клиенту, даже если такой запрос представляет собой значительный объем данных, например, ISO-образ диска и т.п. Необходимость синхронного режима может вытекать из настроек ICAP-клиента (например, Blue Coat, IronPort и т.п.).

ICAP-дамп:

Дамп всех данных обмена ICAP-клиента и сервера. Применяется только для отладки взаимодействия со сторонним ПО.

Логирование:

Журналирование ICAP-сервером HTTP-запросов для службы **EtherSensor Watcher**.

Режим "всё всегда хорошо":

В этом режиме ICAP-сервер при обнаружении ошибок в ICAP-протоколе со стороны клиента отвечает ему не соответствующим кодом ошибки, а кодом **Allow 204** (**No modifications**).

Расширенные заголовки ICAP-протокола:

Позволяет уведомлять ICAP-клиентов о том, что сервер поддерживает указанные заголовки.

Поддерживаемые имена расширенных ICAP заголовков:

X-Client-IP;

X-Server-IP;

X-Client-Username;

X-Subscriber-ID;

X-Authenticated-User;

X-Authenticated-Groups.

Данные заголовки в процессе обработки ICAP-трафика в случае обнаружения сигнатуры сообщения преобразуются в заголовки при отправке почтового сообщения с распознанными данными:

X-Sensor-Icap-Client-Username

X-Sensor-Icap-Subscriber-ID

X-Sensor-Icap-Authenticated-User

X-Sensor-Icap-Authenticated-Groups

Значения заголовков **X-Client-IP** и **X-Server-IP** сохраняются в заголовках **X-Sensor-Src-Address**, **X-Sensor-Dst-Address**.

Подробнее с настройками службы **EtherSensor ICAP** можно ознакомиться в разделе "Ручная настройка ICAP (файл конфигурации)".

3.1.2.2. Ручная настройка (файл конфигурации)

Конфигурация службы **EtherSensor ICAP** содержится в XML-файле **icap.xml,** расположенном в общей директории конфигураций **Microolap EtherSensor [INSTALLDIR]\config**.

Пример файла конфигурации **icap.xml**:

```
<?xml version="1.0" encoding="utf-8"?>
<IcapConfig version="3.0">
 <SensorId>icap-01</SensorId>
 <Network max_connections="4000">
  <ListenAddress
   address="0.0.0.0:1344"
   ssl="false" />
  <ListenAddress
   address="0.0.0.0:1345"
   ssl="true" />
 </Network>
 <Icap>
  <XHeader
   enabled="true"
   name="X-Client-IP" />
  <XHeader
   enabled="true"
   name="X-Server-IP" />
  <XHeader
   enabled="true"
   name="X-Client-Username" />
  <XHeader
   enabled="true"
   name="X-Subscriber-ID" />
  <XHeader
   enabled="true"
   name="X-Authenticated-User" />
  <XHeader
   enabled="true"
   name="X-Authenticated-Groups" />
  <AlwaysOk
   enabled="true" />
  <Preview
   enabled="false"
   size="4096" />
  <Allow204
   enabled="true" />
  <SyncMode
   enabled="false" />
  <RawLog
   enabled="false"
   path=".\raw-log" />
  <RequestLog
   enabled="false"
   http_enabled="true"
   channel="ICAP-REQUEST" />
 </Icap>
</IcapConfig>
```

Тег IcapConfig

Является корневым тегом конфигурации службы. В его атрибуте **version** указывается версия конфигурации.

Тег SensorId

Задаёт идентификатор интерфейса. Используется в дальнейшем при анализе трафика для определения хоста, с которого были получены сообщения. Хотя ICAP-сервер **Microolap EtherSensor** обладает высокой производительностью, если соединений очень много, имеет смысл распределить их обработку на несколько серверов **Microolap EtherSensor**.

Тег Network

Определяет сетевые настройки TCP/IP-сервера службы. Атрибут **max_connections** указывает максимальное количество одновременных соединений от ICAP-клиента, которое будет способен обрабатывать сервер. Значение атрибута **max_connections** по умолчанию установлено в 4000. На оборудовании класса 2xDualCore Intel Xeon 2,3GHz 8GB RAM сервер ICAP способен обрабатывать до 10000 одновременных соединений.

Увеличение производительности возможно за счет расширения количества процессорных ядер, производительности дисковой подсистемы и количества оперативной памяти.

Тег ListenAddress

Тег **ListenAddress** является вложенным в тег **Network** и указывает сетевой адрес (IP-адрес и порт), на котором происходит приём новых соединений от ICAP-клиентов. Возможно указать от 1 до 60 тегов **ListenAddress** с различными сетевыми адресами, на которых должен быть запущен сервер. Если сервер должен быть запущен на всех настроенных на машине адресах, то необходимо указать один единственный тег с общим IP-адресом 0.0.0.0. Атрибут **ssl** определяет будет ли использован протокол SSL для защиты информации в данном соединении.

Например, конфигурация

```
<Network max_connections="4000">
 <ListenAddress
    address="0.0.0.0:1344"
    ssl="false" />
</Network>
```

указывает запустить службу на всех настроенных на сенсоре IP-адресах на порту 1344.

```
<Network max_connections="4000">
 <ListenAddress
    address="1.2.3.4:1344"
    ssl="false" />
 <ListenAddress
    address="1.2.3.5:1345"
    ssl="true" />
 </Network>
```

указывает запустить службу на сетевом интерфейсе с IP-адресом "1.2.3.4:1344" и сетевом интерфейсе с IP-адресом "1.2.3.5:1345".

Тег Icap

Объединяет настройки, относящиеся к ICAP-протоколу и его обработке.

Тег Preview

Тег **Preview** является вложенным в тег **Icap** и указывает параметры использования режима **preview** в ICAP-протоколе. Режим **preview** - это режим предпросмотра в протоколе ICAP, позволяющий сначала отправлять только часть данных, и только после их анализа либо передавать оставшуюся часть данных на обработку, либо завершать обработку.

Использование в **Microolap EtherSensor** режима предпросмотра значения не имеет, так как служба всегда получает весь трафик для анализа. Данный режим поддерживается в связи с тем, что этого требуют некоторые ICAP-клиенты, а так же для полноты поддержки спецификации протокола ICAP согласно **RFC 3507**.

Атрибут **enabled** тега **Preview** указывает активность режима предпросмотра:

enabled="true" - режим предпросмотра включен

enabled="false" - режим предпросмотра отключен

Атрибут **size** тега **Preview** задаёт размер данных, отправляемых для предпросмотра в байтах. Рекомендованный размер составляет 4096 (4 килобайта). Размер 0 означает, что для предпросмотра будут посылаться только заголовки запроса или ответа HTTP.

Всегда рекомендуется отключать данный режим (**enabled="false"**) и включать только в том случае, если ICAP-клиент не может без этого работать - так можно значительно сэкономить на трафике между ICAP-клиентом и сервером.

Тег Allow204

Тег **Allow204** является вложенным в тег **Icap** и определяет можно ли ICAP-серверу подсистемы использовать короткий ответ с кодом **204**. Короткий ответ означает, что ICAP-сервер службы, получив данные от ICAP-клиента, не отправляет их обратно, а отправляет только ответ с кодом **204**. Это позволяет экономить на отправке трафика в обратную сторону от ICAP-сервера к ICAP-клиенту и, снизив таким образом нагрузку, ускорить работу службы в целом.

Атрибут **enabled** тега **Allow204** указывает, разрешено ли серверу использовать короткий ответ:

enabled="true" - разрешено использовать код 204;

enabled="false" - запрещено использовать код 204.

Всегда рекомендуется включать данный режим (**enabled="true"**), и отключать, только если ICAP-клиент не поддерживает обработку ответа с кодом 204.

Тег RawLog

Тег **RawLog** является вложенным в тег **Icap** и определяет параметры использования **RawLog** ICAP-запросов/ответов сервера. **RawLog** - это режим журналирования "сырых" данных обмена между ICAP-клиентом и ICAP-сервером. Этот режим стоит использовать только в экстренных случаях, когда не удаётся другими способами установить причины неработоспособности взаимодействия ICAP-клиента с ICAP-сервером.

Атрибут **enabled** тега **RawLog** указывает активность режима **RawLog**:

enabled="true" - режим журналирования сырых данных включен

enabled="false" - режим журналирования сырых данных отключен

Атрибут **path** тега **RawLog** указывает путь к директории, в которую будут складываться сырые данные TCP-сессий взаимодействия ICAP-клиента и ICAP-сервера.

Всегда рекомендуется отключать данный режим (**enabled="false"**), т.к. его включение при большой нагрузке очень существенно снижает скорость работы службы в целом и интенсивно нагружает дисковую подсистему среды выполнения **Microolap EtherSensor**.

В случае если не удалось выяснить причины, по которым ICAP-клиент не может взаимодействовать с ICAP-сервером, следует отправить разработчику **Microolap EtherSensor** файлы данных **RawLog** с подробным описанием поведения ICAP-клиента и ICAP-сервера, а также указание сообщений, которые ICAP-клиент сохранял в свои штатные журналы.

Тег RequestLog

Тег **RequestLog** является вложенным в тег **Icap** и определяет параметры режима журналирования ошибок протоколов ICAP и HTTP, а также HTTP-запросов, обрабатываемых ICAP-сервером. В этот журнал сохраняются ошибки, которые могут возникать при взаимодействии ICAP-клиента и сервера, относящиеся к неправильным форматам данных, отправляемых ICAP-клиентом, некорректному использованию протокола ICAP и т.п.

Атрибут **enabled** тега **RequestLog** указывает активность режима журналирования ошибок протоколов ICAP и HTTP:

enabled="true" - режим журналирования включен

enabled="false" - режим журналирования отключен

Атрибут **http_enabled** тега **RequestLog** указывает активность режима журналирования HTTP-запросов:

http_enabled="true" - режим журналирования HTTP-запросов включен

http_enabled="false" - режим журналирования HTTP-запросов отключен

По умолчанию (если атрибут отсутствует), подразумевается что данный режим включен.

Атрибут **channel** тега **RequestLog** указывает внутреннее системное имя для канала журналирования HTTP-запросов. Значение данного параметра всегда должно быть **channel="ICAP-REQUEST"** и должно меняться только при прямом указании разработчика **Microolap EtherSensor**.

Тег AlwaysOk

Тег **AlwaysOk** является вложенным в тег **Icap** и включает режим "всё всегда хорошо". В этом режиме сервер ICAP при обнаружении ошибок в ICAP-протоколе со стороны клиента отвечает ему не соответствующим кодом ошибки, а кодом **204 (No modifications)**.

Атрибут **enabled** тега **AlwaysOk** указывает активность режим "всё всегда хорошо":

enabled="true" - режим включен;

enabled="false" - режим отключен.

Если тег отсутствует, то по умолчанию принимается, что данный режим **отключен**.

Если режим включен, то код ответа **204** отправляется на ошибки, даже если тег **Allow204** это запрещает.

Включать режим стоит только в крайних случаях, так как в некоторых случаях это может приводить к непредсказуемым сбоям в работе ICAP-клиента, поставляющего трафик.

Тег SyncMode

Тег **SyncMode** является вложенным в тег **Icap** и включает режим "синхронной работы ICAP-протокола". В этом режиме сервер ICAP-сервер сначала получает от ICAP-клиента запрос целиком, и только потом отправляет ответ, даже в случае передачи больших запросов (скачивание/передача ISO образов, или других больших фалов). Когда синхронный режим выключен, ICAP-сервер работает в потоковом режиме. Это означает, что сервер не ждёт, пока клиент передаст ему весь запрос, а сразу же, как только может, начинает передавать ему ответ. Таким образом получается, что с точки зрения пользователя не происходит задержки в передаче файла. Это особенно актуально, когда через ICAP проходит мультимедийный трафик (например, потоковое видео). Пользователь не ждёт сначала полной загрузки видео потока на ICAP-прокси, потом на ICAP-сервер, затем получения его от ICAP-сервера обратно и только потом его отправки с ICAP-прокси пользователю.

Необходимость включения синхронного режима связана с особенностью работы некоторых ICAP-клиентов, ориентированных в основном на работу по протоколу ICAP с антивирусами. Антивирусам, как правило, необходимо сначала полное получение объекта (какого бы размера он ни был), и лишь потом они могут принять решение, какой именно ответ отдавать ICAP-клиенту.

Атрибут **enabled** тега **SyncMode** указывает активность режима "синхронной работы ICAP-протокола":

enabled="true" - режим включен

enabled="false" - режим отключен

Если тег отсутствует, то по умолчанию принимается, что данный режим **включен**.

Тег XHeader

Тег **XHeader** управляет расширенными заголовками ICAP-протокола. Тег позволяет уведомлять ICAP-клиента о том, поддерживает ли сервер указанный заголовок. Тем самым разрешается или запрещается отправка со стороны ICAP-клиента соответствующего заголовка на ICAP-сервер.

Атрибут **enabled** тега **XHeader** указывает активность поддержки указанного заголовка:

enabled="true" - поддержка заголовка включена;

enabled="false" - поддержка заголовка отключен.

Если тег отсутствует, то по умолчанию подразумевается, что данный заголовок **поддерживается**.

Атрибут **name** тега **XHeader** указывает имя расширенного заголовка.

Поддерживаемые имена расширенных ICAP-заголовков:

X-Client-IP

X-Server-IP

X-Client-Username

X-Subscriber-ID

X-Authenticated-User

X-Authenticated-Groups

Данные заголовки в процессе обработки ICAP-трафика, в случае обнаружения отправляемого сообщения преобразуются в заголовки:

X-Sensor-Icap-Client-Username

X-Sensor-Icap-Subscriber-ID

X-Sensor-Icap-Authenticated-User

X-Sensor-Icap-Authenticated-Groups

Значения заголовков **X-Client-IP**, **X-Server-IP** сохраняются в заголовках **X-Sensor-Src-Address**, **X-Sensor-Dst-Address**.

По умолчанию (если теги **XHeader** не указаны в файле конфигурации) подразумевается, что все заголовки поддерживаются.

3.1.3. Служба EtherSensor LotusTXN

Служба **EtherSensor LotusTXN** предназначена для извлечения сообщений **Lotus Notes** из журнала транзакций (*Lotus Notes Transaction Log*).

Служба извлекает сообщения из файлов **Lotus Notes Transaction Log**, и затем передаёт эти сообщения для дальнейшей обработки в службу **EtherSensor Analyser**.

В текущей версии **Microolap EtherSensor** (5.1.0.13519) служба может отслеживать одновременно сразу несколько директорий **Lotus Notes Transaction Log**. Это даёт возможность администратору с помощью одной инсталляции **Microolap EtherSensor** отслеживать одновременно несколько систем **Lotus Notes**, при этом директории **Lotus Notes Transaction Log** могут быть как локальными, так и удалёнными.

Рис.18. Схема работы службы EtherSensor LotusTXN.

Параметры командной строки

Служба Windows **EtherSensor LotusTXN** в ходе инсталляции **Microolap EtherSensor** устанавливается с автоматическим запуском. Однако, при необходимости процесс **ethersensor_lotustxn.exe** можно запустить как приложение Windows со следующими параметрами командной строки:

/process

Запускает процесс **ethersensor_lotustxn.exe** как обычный Windows Win32-процесс (возможно использовать для отладки).

/service

Запускает как службу Windows.

/config

Сохраняет конфигурацию службы по умолчанию.

3.1.3.1. Настройка в конфигураторе

Служба **EtherSensor LotusTXN** позволяет вести мониторинг и реконструкцию сообщений системы **Lotus Notes** методом извлечения их из **Lotus Notes Transaction Log** (журнала транзакций **Lotus Notes**).

> **Внимание:**
> В случае, если в системе **Lotus Notes** не применяется шифрование, за извлечение сообщений **Lotus Notes** из трафика наравне с SMTP/POP3/IMAP4 отвечает служба **EtherSensor EtherCAP**.

Для того, чтобы настроить службу **EtherSensor LotusTXN** для отслеживания сообщений, ей необходимо указать отслеживаемые директории журнала транзакций **Lotus Notes**.

Информация о настройках директорий **Lotus Notes Transaction Log** содержится в файле **lotustxn.xml**, находящемся в директории **[INSTALLDIR]\config**, и она может быть отредактирована непосредственно в файле конфигурации любым текстовым редактором.

В утилите конфигуратора (файл **ethersensor_console.exe**) настройка службы **EtherSensor LotusTXN** происходит следующим образом:

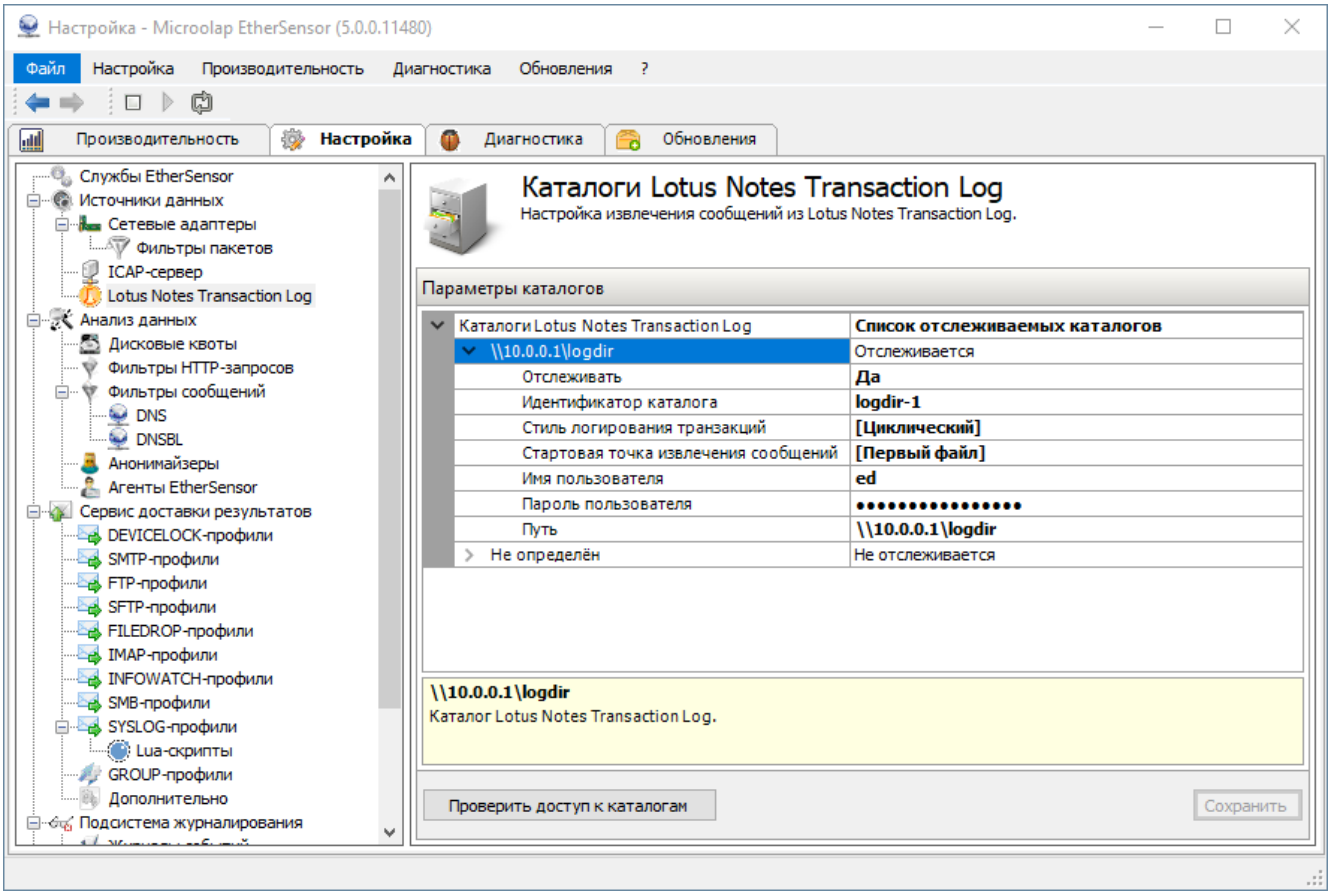

Рис.19. Настройки службы EtherSensor LotusTXN.

Идентификатор каталога:

Идентификатор директории **Lotus Notes Transaction Log** используется для идентификации источника данных в **Microolap EtherSensor**.

Стиль логирования транзакций:

Служит для указания стиля журналирования транзакций, который использует система **Lotus Notes** для данной директории.

Стартовая точка извлечения сообщений:

Стартовая точка извлечения сообщений служит для того, чтобы указать **Microolap EtherSensor** с какого файла в директории **Lotus Notes Transaction Log** начинать процесс извлечения.

Имя пользователя:

Определяет имя пользователя Windows для доступа к директории транзакций. Значение данного параметра должно быть указано в UPN (user principal name) формате. Пример: **administrator@example.com**, где **administrator** - имя пользователя, **example.com** - домен пользователя. Если данный параметр не указан, то для доступа к файлам журнала транзакций используются права учётной записи, под которой запущена служба **EtherSensor LotusTXN**. Следует отметить, что при установке **Microolap EtherSensor** по умолчанию все службы запускаются с правами пользователя SYSTEM.

Пароль пользователя:

Определяет пароль пользователя для доступа к директории транзакций **Lotus Notes**.

Путь:

Полный путь к директории с журналами транзакций **Lotus Notes**.

3.1.3.2. Ручная настройка (файл конфигурации)

Конфигурация службы **EtherSensor LotusTXN** указывается в XML-файле **lotustxn.xml,** расположенном в общей директории конфигураций **[INSTALLDIR]\config**.

Пример файла конфигурации **lotustxn.xml**:

```
<?xml version="1.0" encoding="utf-8"?>
<LotusTXNConfig version="1.0">
 <Capture>

  <Directory
   enabled="true"
   logstyle="linear"
   start="currentfile"
   id="logdir-1"
   path="\\10.31.5.16\logdir">
   <UserName>XFw5OUpKPj4=</UserName>
   <UserPassword>OTkLCzg4DAw=</UserPassword>
  </Directory>

  <Directory
   enabled="true"
   logstyle="circular"
   start="firstfile"
   id="logdir-2"
   path="D:\lotus\data\logdir">
   <UserName>Cg46PgIGPjoHAzs/fno4PHx4SEwOCjQwcHQ=</UserName>
   <UserPassword>V1cxMVZWMzNGRiAg</UserPassword>
  </Directory>

 </Capture>
</LotusTXNConfig>
```

Тег LotusTXNConfig

Является корневым тегом конфигурации службы. В его атрибуте **version** указывается версия конфигурации.

Тег Capture

Задаёт блок, описывающий отслеживаемые директории.

Тег Directory

Является вложенным в тег **Capture,** указывает описание настроек отслеживаемой директории. В атрибуте **enabled** указывается статус активности директории, и если данный атрибут выставлен в значение **false**, то директория не будет использоваться в обработке данных.

Атрибут **logstyle** используется для указания, в каком стиле система **Lotus Notes** ведёт журналирования транзакций. Данный атрибут может принимать значения:

- **linear** - линейный стиль журналирования;
- **circular** - циклический стиль журналирования.

Для более подробного описания следует ознакомиться с документацией системы **Lotus Notes**.

Атрибут **start** используется для указания стартовой точки перехвата сообщений, и если данный атрибут выставлен в значение **firstfile**, то извлечение сообщений будет выполняться с первого файла **Lotus Notes Transaction Log**. Если значение атрибута выставлено в **currentfile**, то извлечение сообщений будет выполняться, начиная с текущего файла **Lotus Notes Transaction Log**.

Атрибут id задаёт идентификатор отслеживаемой директории. Используется в дальнейшем при анализе сообщений для определения директории, из которой были получены сообщения.

Атрибут path задаёт полный путь к директории с файлами **Lotus Notes Transaction Log**.

Тег UserName

Является вложенным в тег **Directory,** определяет имя пользователя Windows для доступа к директории транзакций. Значение данного параметра должно быть указано в UPN (user principal name) формате. Пример: **administrator@example.com**, где **administrator** - имя пользователя, **example.com** - домен пользователя. Если данный параметр не указан, то для доступа к файлам журнала транзакций используются права учётной записи, под которой запущена служба **EtherSensor LotusTXN**. Следует отметить, что при установке **Microolap EtherSensor** по умолчанию все службы запускаются с правами пользователя SYSTEM.

Тег UserPassword

Является вложенным в тег **Directory,** определяет пароль пользователя для доступа к директории транзакций.

3.2. Доставка результатов перехвата

Служба **EtherSensor Transfer** отвечает за транспортировку результатов работы **EtherSensor Analyser** внешним системам-потребителям.

Доставка результатов анализа извлечённых из трафика объектов выполняется согласно транспортных профилей следующих типов:

Универсальные
Служат для транспортировки контента сообщений уровня приложения внешним системам-потребителям: DLP-системам, eDiscovery, Enterprise Archiving, Enterprise Search и т.п. Включают в себя SMTP/SMTPS, FTP/FTPS, SFTP, IMAP, FILEDROP (локальная файловая система), SMB/CIFS (сетевой каталог).

Проприетарные
Служат для транспортировки контента сообщений уровня приложения внешним системам-потребителям. В текущей версии *5.1.0.13519* поддерживаются транспортные профили, обеспечивающие работу по проприетарным протоколам, например, DeviceLock Enterprise Server и InfoWatch Traffic Monitor.

Групповые
Включают в себя обычные транспортные профили с заранее установленными весами, служат для балансировки нагрузки между системами-потребителями.

SYSLOG-профили
Используются для транспортировки результатов системам-потребителям, принимающим данные о событиях через SYSLOG-сервер (как правило, это SIEM-системы). SYSLOG-строка может быть сформирована как в результате работы фильтра, так и посредством обработки извлечённого из трафика объекта заранее подготовленным Lua-скриптом. Это позволяет в реальном времени подготовить данные в произвольном специфическом для данной системы-потребителя формате без так называемых "коннекторов".

Назначение транспортного профиля сообщению происходит с помощью фильтра сообщений во время анализа данных сообщения. Если в процессе анализа сообщения выяснилось, что ему не был назначен ни один транспортный профиль, то оно доставляется профилем по умолчанию. После успешной доставки сообщение удаляется из кэша сообщений, вся имеющаяся информация о сообщении уничтожается.

Один и тот же объект или же результаты его обработки *многими способами* могут быть доставлены *многим потребителям* с использованием *многих транспортных профилей*.

Например:
Контент email-сообщения доставляется одновременно в корпоративную DLP-систему и в eDiscovery-систему, а метаданные - в формате CEF - в SIEM-систему, работающую в составе внешнего SOC на стороне MSSP.

Основной формат, в котором **Microolap EtherSensor** поставляет контент реконструированных объектов системам-потребителям - EML-конверт. Также служба **EtherSensor Transfer** способна передавать данные в собственном внутреннем XML и/или JSON форматах в тех случаях, когда EML-конверт не является обязательной составляющей протокола доставки (копирование данных в директории или использование FTP-протокола).

Архитектура системы при использовании незащищённых протоколов передачи данных:

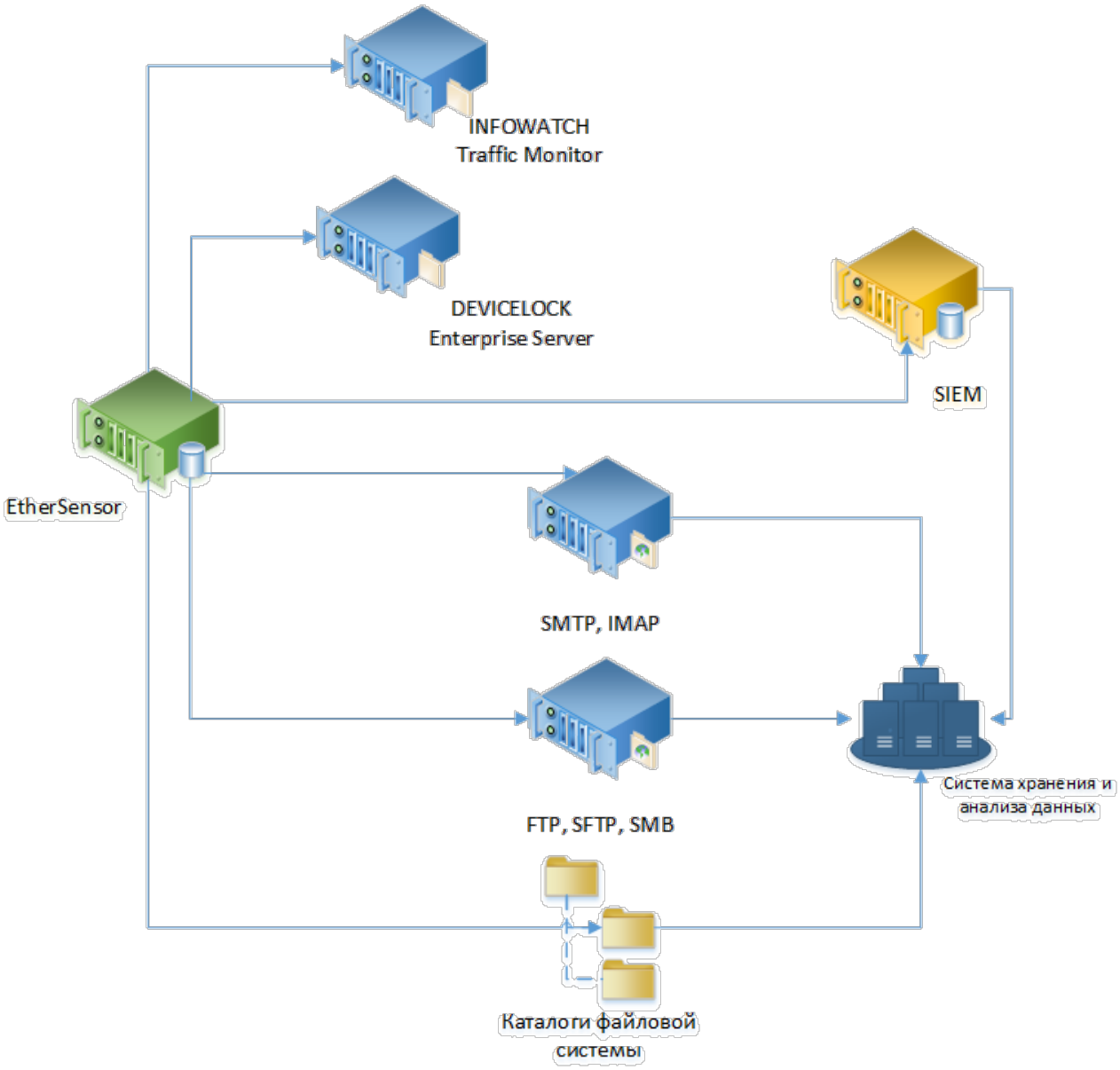

Рис.20. Схема работы службы EtherSensor Transfer.

Архитектура системы при использовании защищённых протоколов передачи данных:

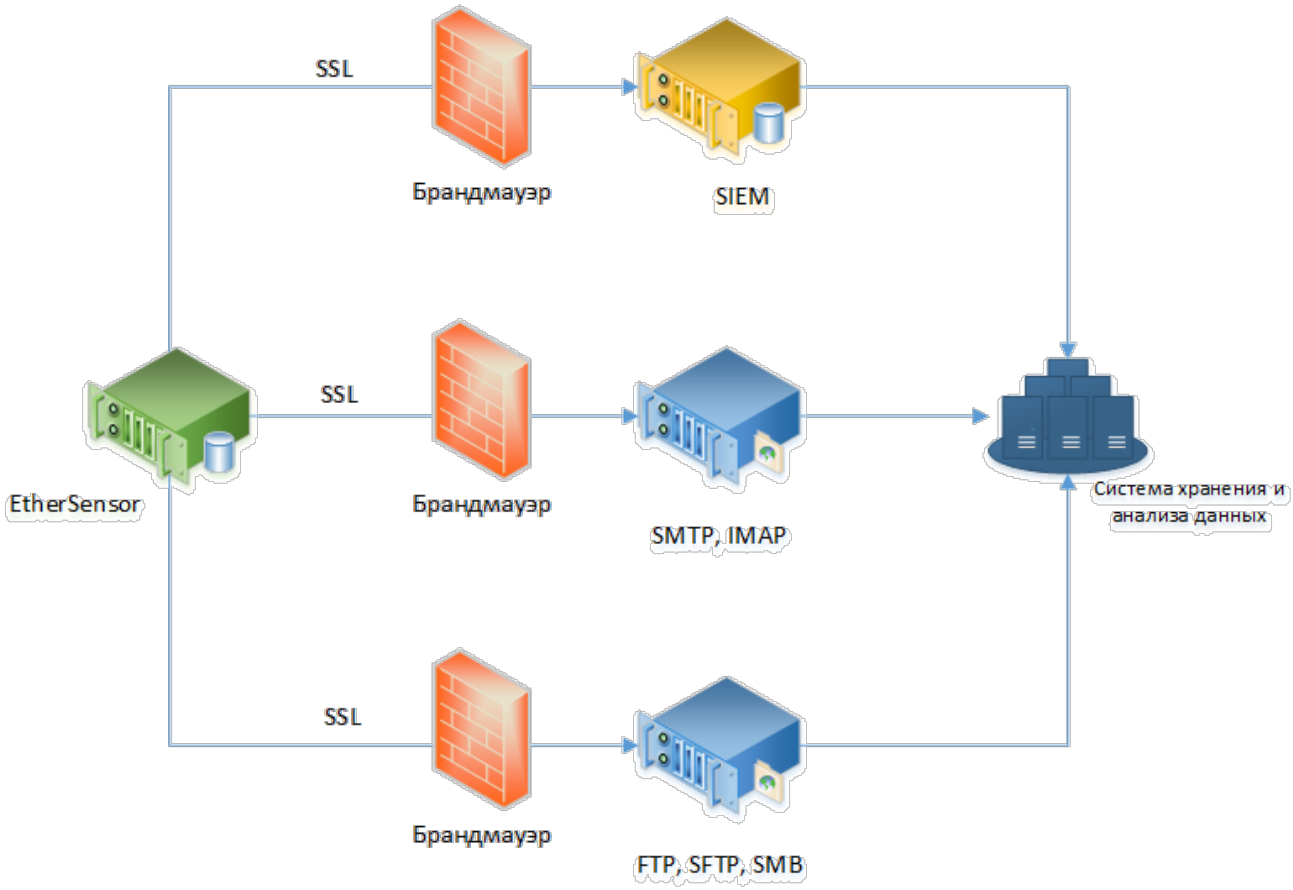

Рис.21. Работа службы EtherSensor Transfer с защищенными протоколами

Для транспортировки данных перехвата служба **EtherSensor Transfer** отслеживает локальные спулы директорий. При появлении данных в спулах служба производит их отправку. Для отправки служба **EtherSensor Transfer** использует транспортные профили, в которых указаны действия, которые необходимо выполнить с отправляемыми данными. Транспортный профиль может быть назначен службой **EtherSensor Analyser** в процессе анализа данных, тогда информация о транспортном профиле указывается в метаданных результата перехвата. Если же профиль в результате перехвата не указан, тогда используется профиль по умолчанию:

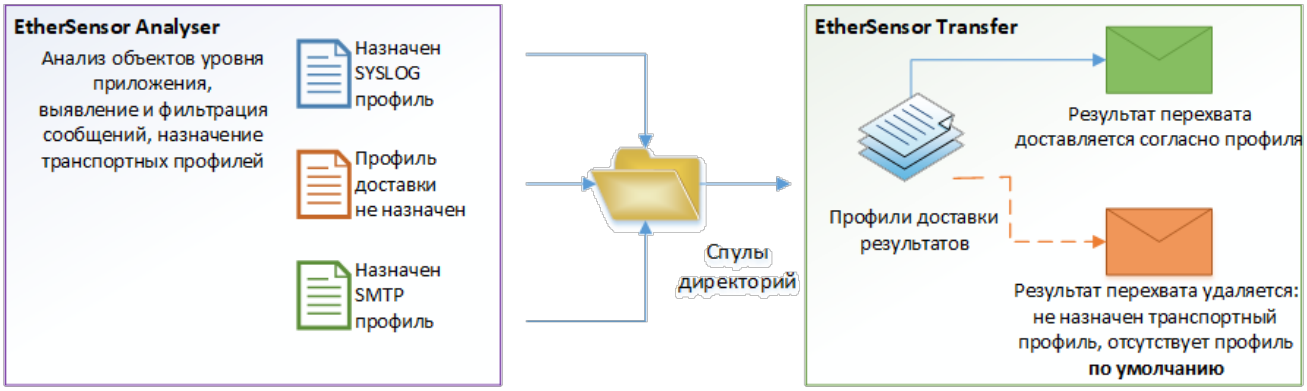

Рис.22. Процесс назначения профиля доставки результата.

Параметры командной строки

Служба **EtherSensor Transfer** в ходе процедуры установки **Microolap EtherSensor** устанавливается как служба Windows, настроенная на автоматический запуск. Однако, она также может быть запущена как приложение Windows **ethersensor_transfer.exe** и имеет следующие параметры командной строки:

/process

Запускает процесс **ethersensor_transfer.exe** как обычный Windows Win32-процесс (возможно использовать для отладки).

/service

Запускает как службу Windows.

/config

Сохраняет конфигурацию службы по умолчанию.

3.2.1. Настройка в конфигураторе

Основной идеей службы **EtherSensor Transfer** является понятие заранее определенного транспортного профиля.

Профиль содержит данные о сервере и аутентификации на нем, если потребитель перехваченных сообщений является сервером или путь к локальной директории, а также требования к сохраняемым объектам, если речь идет о профилях типа FILEDROP, SMB, FTP или SFTP.

В правилах фильтрации сообщений службы **EtherSensor Analyser** один профиль в случае необходимости может быть мгновенно заменен другим, а так как профили созданы администратором заранее и тщательно проверены, вероятность ошибок в этой части настроек службы минимальна.

3.2.1.1. DEVICELOCK-профили

Настройка DEVICELOCK-профилей

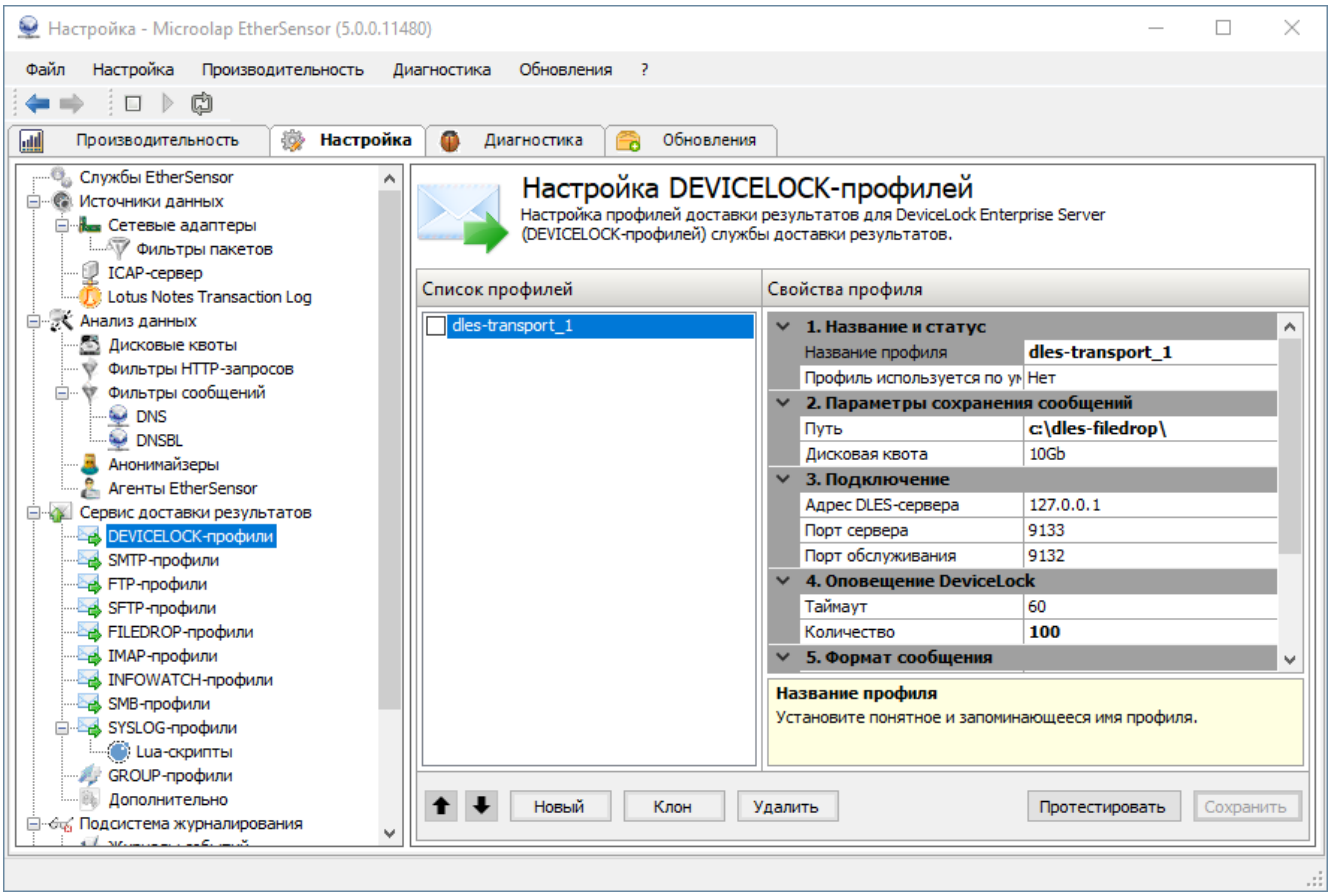

Рис.23. Настройки DEVICELOCK-профилей.

1. Название и статус

Название профиля:

Удобное, запоминающееся и информативное название профиля, на усмотрение администратора.

Профиль используется по умолчанию:

Да означает, что данный профиль используется по умолчанию.

2. Параметры сохранения сообщений

Путь:

Путь к локальной директории, в которую будут сохраняться перехваченные сообщения. Используется для промежуточного хранения результатов, отправляемых в DEVICELOCK Enterprise Server.

Дисковая квота:

Размер квоты дискового пространства для хранения сообщений. Пример: **10GB**, **500MB**, **100KB** или **10000**. При исчерпании квоты сохранение файлов приостанавливается до тех пор, когда квота вновь позволит это делать. Чтобы возобновить сохранение файлов, следует либо освободить место, либо увеличить квоту.

3. Подключение

Адрес DLES-сервера:

IP-адрес или доменное имя DEVICELOCK Enterprise Server.

Порт сервера:

Порт, через который происходит оповещение DEVICELOCK Enterprise Server о наличии сообщений (событий).

Порт обслуживания:

Порт, через который DEVICELOCK Enterprise Server "забирает" результаты (сообщения/события).

4. Оповещение DeviceLock

Таймаут:

Устанавливает таймаут оповещения DEVICELOCK Enterprise сервера в секундах. По истечении таймаута, при наличии неотправленных сообщений будет выполнено оповещение DLES-сервера о наличии результатов.

Количество:

Устанавливает количество накапливаемых сообщений, по достижении которого будет выполнено оповещение DEVICELOCK Enterprise сервера.

5. Формат сообщения

Дублировать заголовки:

Разрешить/запретить сохранение стандартных заголовков сообщения, а также заголовков **X-Sensor** дополнительно, в отдельном вложении сообщения - **microolap_msis_headers.txt**.

Возможные варианты:

Все

Сохранять все заголовки сообщения;

X-Sensor

Сохранять заголовки с префиксом **X-Sensor;**

Другие

Сохранять стандартные заголовки **From, To, Cc, Bcc** и другие, не попадающие под действие флагов **xsensor;**

Нет

Запрещает сохранение заголовков сообщения в отдельном вложении.

6. Обработка ошибок

Таймаут после отказа:

Время ожидания для транспортировки сообщений в случае отказа приёмника. Значение параметра задаётся в секундах.

7. Для GROUP-профилей

Вес:

Задаёт пропорцию распределения сообщений между приёмниками. Параметр может принимать значения от **1** до **10**, и действителен только в составе группового профиля.

Резервный профиль:

Включает или выключает использование резервного профиля Если этот флаг включён, то доставка сообщений с использованием данного профиля будет задействована в случае отказа основных (не резервных) транспортных профилей. Параметр действителен только в составе группового профиля.

3.2.1.2. FALCONGAZE-профили

Настройка FALCONGAZE-профилей

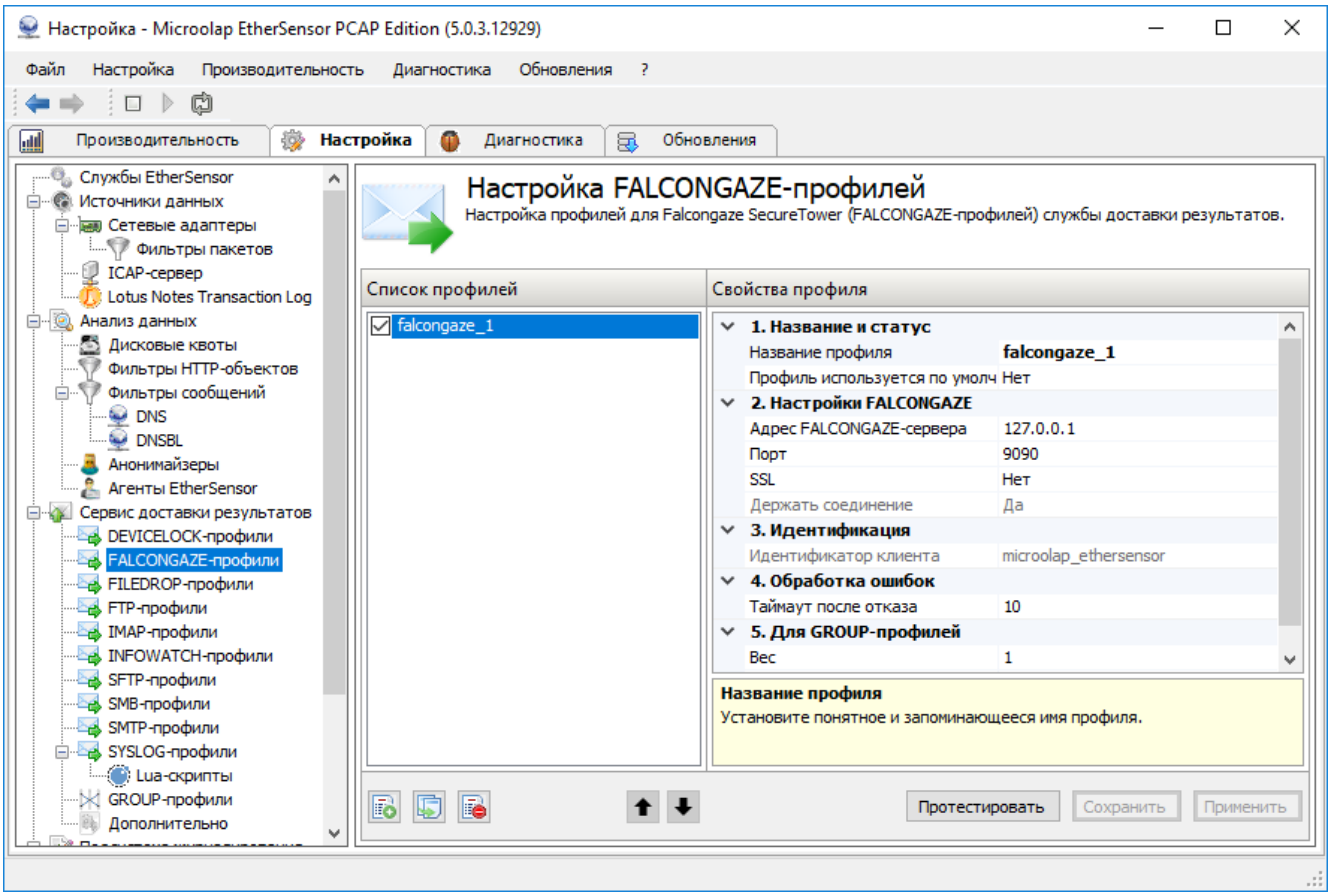

Рис.24. Настройки FALCONGAZE-профилей.

1. Название и статус

Название профиля:

Удобное, запоминающееся и информативное название профиля, на усмотрение администратора.

Профиль используется по умолчанию:

Да означает, что данный профиль используется по умолчанию.

2. Настройки FALCONGAZE

Адрес FALCONGAZE-сервера:

IP-адрес или имя сервера Falcongaze SecureTower для доставки результатов.

Порт:

Порт сервера Falcongaze SecureTower для отправки сообщений..

SSL:

Разрешить/запретить использовать SSL-шифрование при передаче перехваченных сообщений на сервер.

Держать соединение:

Отправлять сообщения в одном и том же соединении с сервером, принимающим сообщения. Если этот флаг выключен, то каждое отправляемое сообщение будет отправлено в отдельном TCP соединении.

3. Идентификация

Идентификатор клиента

Уникальный идентификатор клиента. Служит для регистрации клиента в Falcongaze SecureTower для отправки сообщений.

4. Обработка ошибок

Таймаут после отказа:

Время ожидания для транспортировки сообщений в случае отказа приёмника. Значение параметра задаётся в секундах.

5. Для GROUP-профилей

Вес:

Задаёт пропорцию распределения сообщений между приёмниками. Параметр может принимать значения от **1** до **10**, и действителен только в составе группового профиля.

Резервный профиль:

Включает или выключает использование резервного профиля Если этот флаг включён, то доставка сообщений с использованием данного профиля будет задействована в случае отказа основных (не резервных) транспортных профилей. Параметр действителен только в составе группового профиля.

3.2.1.3. SMTP-профили

Настройка SMTP-профилей

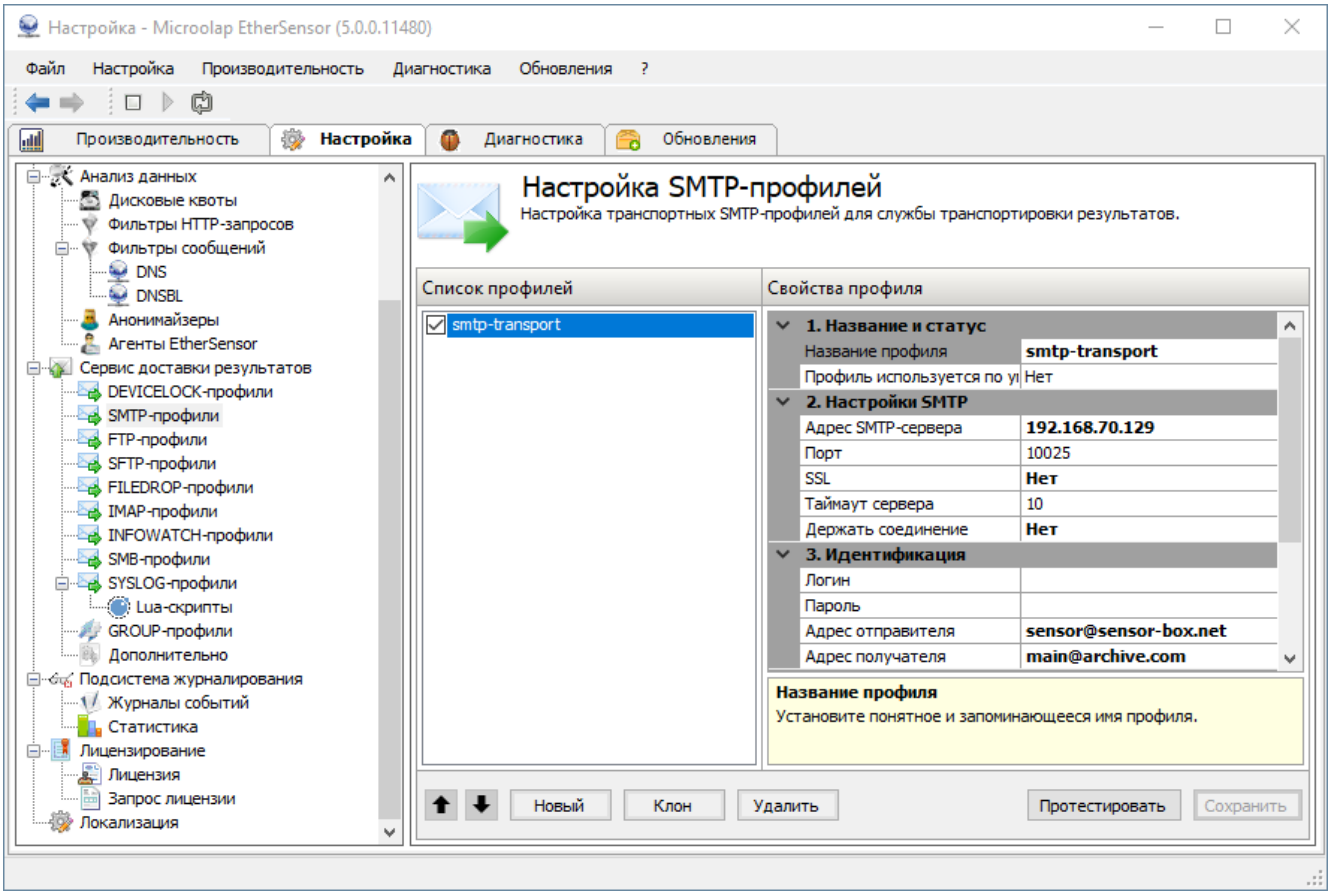

Рис.25. Настройки SMTP-профилей.

1. Название и статус

Название профиля:

Удобное, запоминающееся и информативное название профиля, на усмотрение администратора.

Профиль используется по умолчанию:

Да означает, что данный профиль используется по умолчанию.

2. Настройки SMTP

Адрес SMTP-сервера:

IP-адрес или доменное имя SMTP-сервера.

Порт:

Порт сервера.

SSL:

Разрешить/запретить использовать SSL-шифрование при передаче перехваченных сообщений на сервер.

Таймаут сервера:

Допустимое время ожидания ответа сервера.

Держать соединение:

Отправлять сообщения в одном и том же соединении с сервером, принимающим сообщения. Если этот флаг выключен, то каждое отправляемое сообщение будет отправлено в отдельном TCP соединении.

3. Идентификация

Логин:

Логин на доступ к SMTP-серверу.

Пароль:

Пароль на доступ к SMTP-серверу.

Адрес отправителя:

Полностью на усмотрение администратора, но стоит учитывать возможные проверки адреса почтовой системой.

Адрес получателя:

Работающий Email-адрес потребителя перехваченных сообщений.

4. Формат сообщения

Дублировать заголовки:

Разрешить/запретить сохранение стандартных заголовков сообщения, а также заголовков **X-Sensor** дополнительно, в отдельном вложении сообщения - **microolap_msis_headers.txt**.

Возможные варианты:

Все

Сохранять все заголовки сообщения;

X-Sensor

Сохранять заголовки с префиксом **X-Sensor;**

Другие

Сохранять стандартные заголовки **From, To, Cc, Bcc** и другие, не попадающие под действие флагов **xsensor;**

Нет

Запрещает сохранение заголовков сообщения в отдельном вложении.

5. Обработка ошибок

Таймаут после отказа:

Время ожидания для транспортировки сообщений в случае отказа приёмника. Значение параметра задаётся в секундах.

6. Для GROUP-профилей

Вес:

Задаёт пропорцию распределения сообщений между приёмниками. Параметр может принимать значения от **1** до **10**, и действителен только в составе группового профиля.

Резервный профиль:

Включает или выключает использование резервного профиля Если этот флаг включён, то доставка сообщений с использованием данного профиля будет задействована в случае отказа основных (не резервных) транспортных профилей. Параметр действителен только в составе группового профиля.

3.2.1.4. FTP-профили

Настройка FTP-профилей

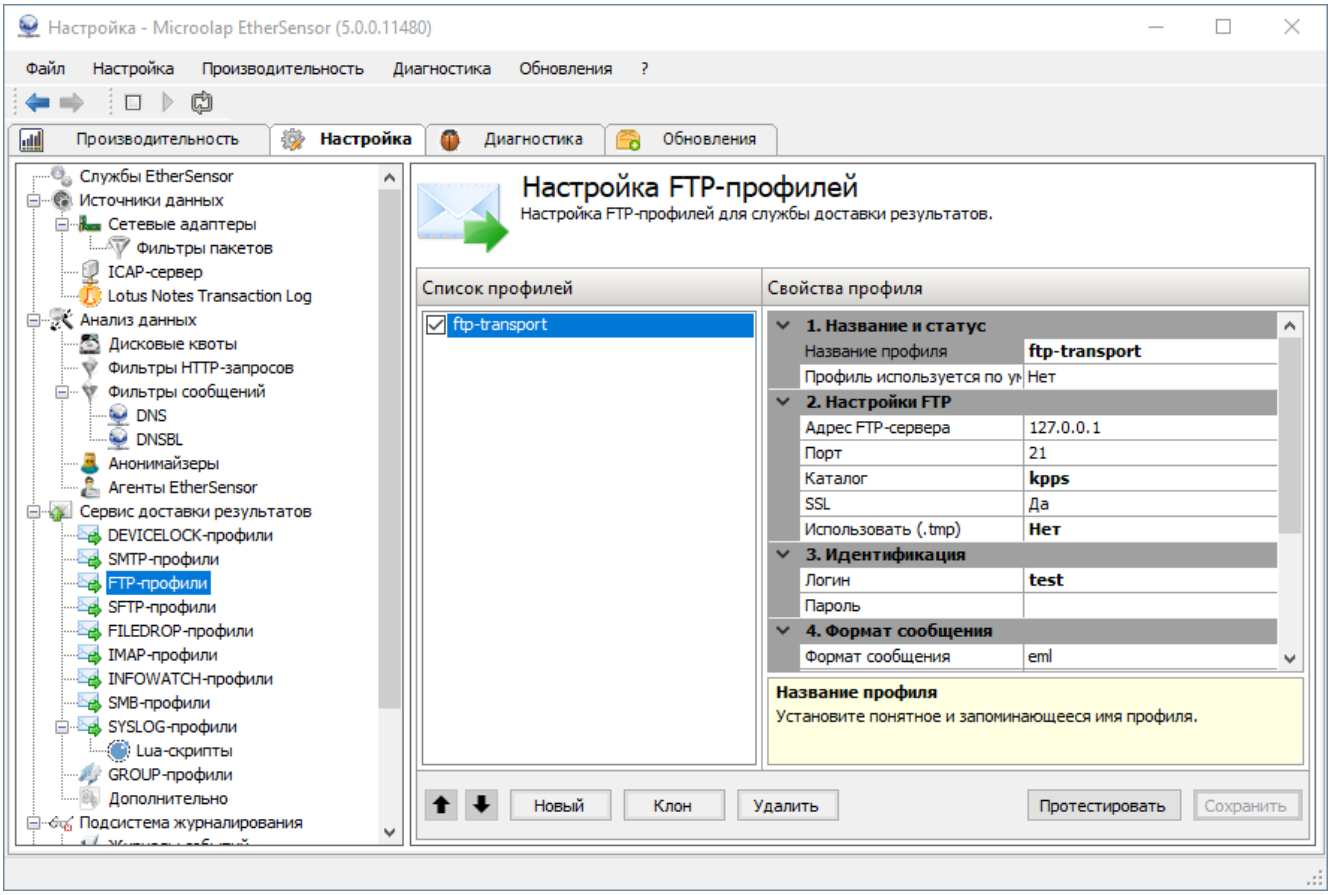

Рис.26. Настройки FTP-профилей.

1. Название и статус

Название профиля:

Удобное, запоминающееся и информативное название профиля, на усмотрение администратора.

Профиль используется по умолчанию:

Да означает, что данный профиль используется по умолчанию.

2. Настройки FTP

Адрес FTP-сервера:

IP-адрес или доменное имя FTP-сервера с указанием директории, в которую будут сохраняться перехваченные сообщения.

Порт:

Порт FTP-сервера для отправки сообщений.

Каталог:

Каталог на FTP-сервере для сохранения сообщений.

SSL:

Разрешить/запретить использовать SSL-шифрование при передаче перехваченных сообщений на сервер.

Использовать (.tmp):

Разрешить/запретить использовать двухэтапное перемещение файлов:

Да: файл перемещается с временным расширением (например, 2012-01-08-15-29-48-586.7.M.zip.tmp), после завершения перемещения файл переименовывается (удаляется временное расширение);

Нет: файл перемещается сразу с указанным расширением (например, 2012-01-08-15-29-48-586.7.M.zip).

3. Идентификация

Логин:

Логин на FTP-сервере.

Пароль:

Пароль на FTP-сервере.

4. Формат сообщения

Формат сообщения:

Формат сохраняемого сообщения (EML, XML, JSON....).

Сохранять как ZIP:

Заворачивать ли сохраняемые сообщения в ZIP-архив. Если этот флаг включен совместно с флагом "**Сохранять как EML**", то EML-конверты сообщений будут упаковываться в ZIP-архив. Если этот флаг включен и при этом флаг "**Сохранять как EML**" отключена, то в ZIP-архив будут упаковываться сообщения во внутреннем формате **Microolap EtherSensor**.

Степень сжатия ZIP-архива:

Возможные значения данного параметра находятся в диапазоне от **0** до **9**, где **0** - без сжатия, **1** - минимальное сжатие, но высокая скорость, **9** - максимальное сжатие.

Дублировать заголовки:

Разрешить/запретить сохранение стандартных заголовков сообщения, а также заголовков **X-Sensor** дополнительно, в отдельном вложении сообщения - **microolap_msis_headers.txt**.

Возможные варианты:

Все

Сохранять все заголовки сообщения;

X-Sensor

Сохранять заголовки с префиксом **X-Sensor;**

Другие

Сохранять стандартные заголовки **From, To, Cc, Bcc** и другие, не попадающие под действие флагов **xsensor;**

Нет

Запрещает сохранение заголовков сообщения в отдельном вложении.

5. Обработка ошибок

Таймаут после отказа:

Время ожидания для транспортировки сообщений в случае отказа приёмника. Значение параметра задаётся в секундах.

6. Для GROUP-профилей

Вес:

Задаёт пропорцию распределения сообщений между приёмниками. Параметр может принимать значения от **1** до **10**, и действителен только в составе группового профиля.

Резервный профиль:

Включает или выключает использование резервного профиля Если этот флаг включён, то доставка сообщений с использованием данного профиля будет задействована в случае отказа основных (не резервных) транспортных профилей. Параметр действителен только в составе группового профиля.

3.2.1.5. SFTP-профили

Настройка SFTP-профилей

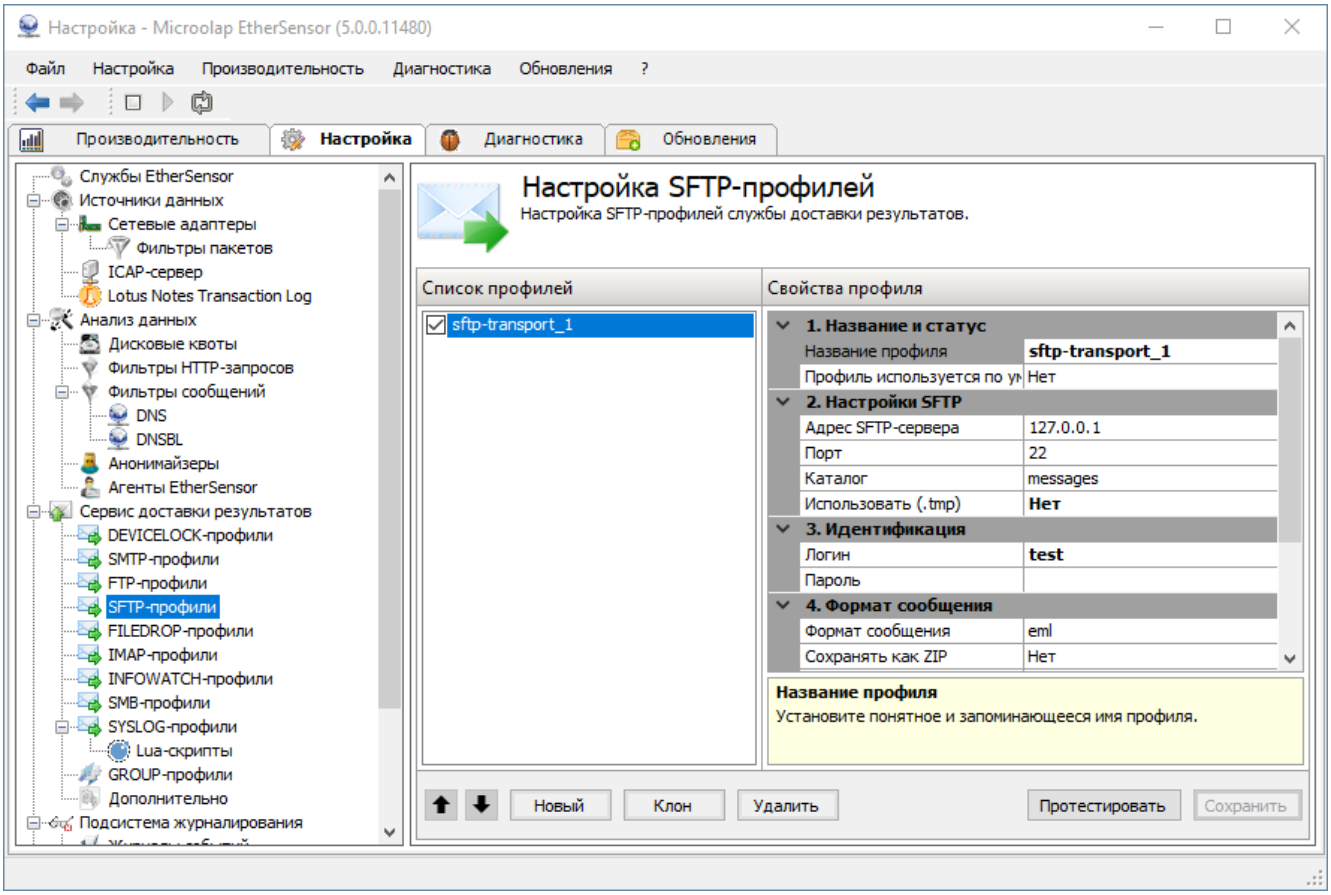

Рис.27. Настройки SFTP-профилей.

1. Название и статус

Название профиля:

Удобное, запоминающееся и информативное название профиля, на усмотрение администратора.

Профиль используется по умолчанию:

Да означает, что данный профиль используется по умолчанию.

2. Настройки SFTP

Адрес SFTP-сервера:

IP-адрес или доменное имя SFTP-сервера с указанием директории, в которую будут сохраняться перехваченные сообщения.

Порт:

Порт SFTP-сервера.

Каталог:

Имя каталога для сохранения сообщений.

Использовать (.tmp):

Разрешить/запретить использовать двухэтапное перемещение файлов:

Да: файл перемещается с временным расширением (например, 2012-01-08-15-29-48-586.7.M.zip.tmp), после завершения перемещения файл переименовывается (удаляется временное расширение);

Нет: файл перемещается сразу с указанным расширением (например, 2012-01-08-15-29-48-586.7.M.zip).

3. Идентификация

Логин:

Логин на SFTP-сервере.

Пароль:

Пароль на SFTP-сервере.

4. Формат сообщения

Формат сообщения:

Формат сохраняемого сообщения (EML, XML, JSON....).

Сохранять как ZIP:

Заворачивать ли сохраняемые сообщения в ZIP-архив. Если этот флаг включен совместно с флагом "**Сохранять как EML**", то EML-конверты сообщений будут упаковываться в ZIP-архив. Если этот флаг включен и при этом флаг "**Сохранять как EML**" отключена, то в ZIP-архив будут упаковываться сообщения во внутреннем формате **Microolap EtherSensor**.

Степень сжатия ZIP-архива:

Возможные значения данного параметра находятся в диапазоне от **0** до **9**, где **0** - без сжатия, **1** - минимальное сжатие, но высокая скорость, **9** - максимальное сжатие.

Дублировать заголовки:

Разрешить/запретить сохранение стандартных заголовков сообщения, а также заголовков **X-Sensor** дополнительно, в отдельном вложении сообщения - **microolap_msis_headers.txt**.

Возможные варианты:

Все

Сохранять все заголовки сообщения;

X-Sensor

Сохранять заголовки с префиксом **X-Sensor;**

Другие

Сохранять стандартные заголовки **From, To, Cc, Bcc** и другие, не попадающие под действие флагов **xsensor;**

Нет

Запрещает сохранение заголовков сообщения в отдельном вложении.

5. Обработка ошибок

Таймаут после отказа:

Время ожидания для транспортировки сообщений в случае отказа приёмника. Значение параметра задаётся в секундах.

6. Для GROUP-профилей

Вес:

Задаёт пропорцию распределения сообщений между приёмниками. Параметр может принимать значения от **1** до **10**, и действителен только в составе группового профиля.

Резервный профиль:

Включает или выключает использование резервного профиля Если этот флаг включён, то доставка сообщений с использованием данного профиля будет задействована в случае отказа основных (не резервных) транспортных профилей. Параметр действителен только в составе группового профиля.

3.2.1.6. FILEDROP-профили

Настройка FILEDROP-профилей

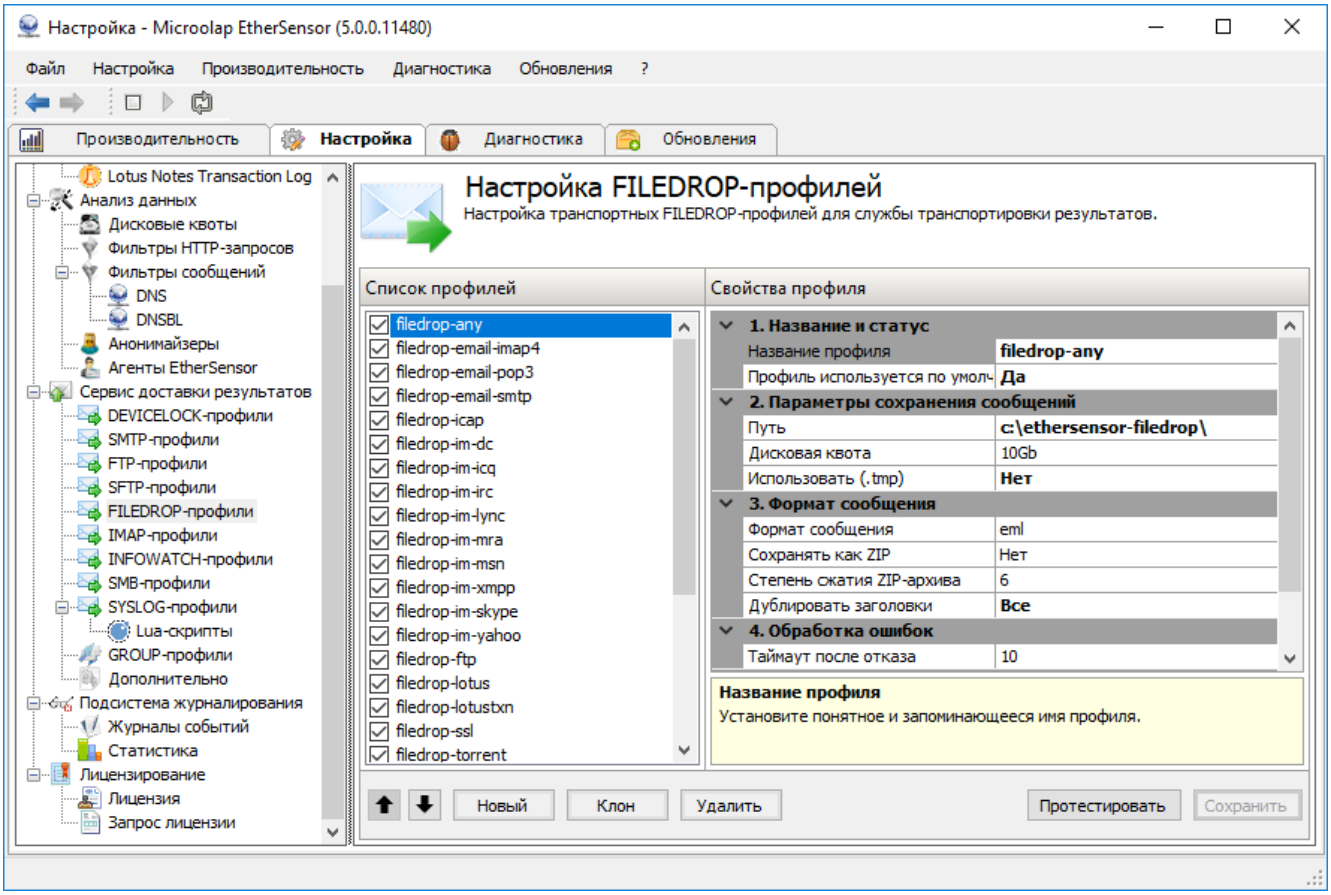

Рис.28. Настройки FILEDROP-профилей.

1. Название и статус

Название профиля:

Удобное, запоминающееся и информативное название профиля, на усмотрение администратора.

Профиль используется по умолчанию:

Да означает, что данный профиль используется по умолчанию.

2. Параметры сохранения сообщений

Путь:

Путь к локальной директории, в которой будут сохраняться сообщения.

Дисковая квота:

Размер квоты дискового пространства для хранения сообщений. Пример: **10GB**, **500MB**, **100KB** или **10000**. При исчерпании квоты сохранение файлов приостанавливается до тех пор, когда квота вновь позволит это делать. Чтобы возобновить сохранение файлов, следует либо освободить место, либо увеличить квоту.

Использовать (.tmp):

Разрешить/запретить использовать двухэтапное перемещение файлов:

Да: файл перемещается с временным расширением (например, 2012-01-08-15-29-48-586.7.M.zip.tmp), после завершения перемещения файл переименовывается (удаляется временное расширение);

Нет: файл перемещается сразу с указанным расширением (например, 2012-01-08-15-29-48-586.7.M.zip).

3. Формат сообщения

Формат сообщения:

Формат сохраняемого сообщения (EML, XML, JSON....).

Сохранять как ZIP:

Заворачивать ли сохраняемые сообщения в ZIP-архив. Если этот флаг включен совместно с флагом "**Сохранять как EML**", то EML-конверты сообщений будут упаковываться в ZIP-архив. Если этот флаг включен и при этом флаг "**Сохранять как EML**" отключена, то в ZIP-архив будут упаковываться сообщения во внутреннем формате **Microolap EtherSensor**.

Степень сжатия ZIP-архива:

Возможные значения данного параметра находятся в диапазоне от **0** до **9**, где **0** - без сжатия, **1** - минимальное сжатие, но высокая скорость, **9** - максимальное сжатие.

Дублировать заголовки:

Разрешить/запретить сохранение стандартных заголовков сообщения, а также заголовков **X-Sensor** дополнительно, в отдельном вложении сообщения - **microolap_msis_headers.txt**.

Возможные варианты:

Все

Сохранять все заголовки сообщения;

X-Sensor

Сохранять заголовки с префиксом **X-Sensor;**

Другие

Сохранять стандартные заголовки **From, To, Cc, Bcc** и другие, не попадающие под действие флагов **xsensor;**

Нет

Запрещает сохранение заголовков сообщения в отдельном вложении.

4. Обработка ошибок

Таймаут после отказа:

Время ожидания для транспортировки сообщений в случае отказа приёмника. Значение параметра задаётся в секундах.

5. Для GROUP-профилей

Вес:

Задаёт пропорцию распределения сообщений между приёмниками. Параметр может принимать значения от **1** до **10**, и действителен только в составе группового профиля.

Резервный профиль:

Включает или выключает использование резервного профиля Если этот флаг включён, то доставка сообщений с использованием данного профиля будет задействована в случае отказа основных (не резервных) транспортных профилей. Параметр действителен только в составе группового профиля.

3.2.1.7. IMAP-профили

Настройка IMAP-профилей

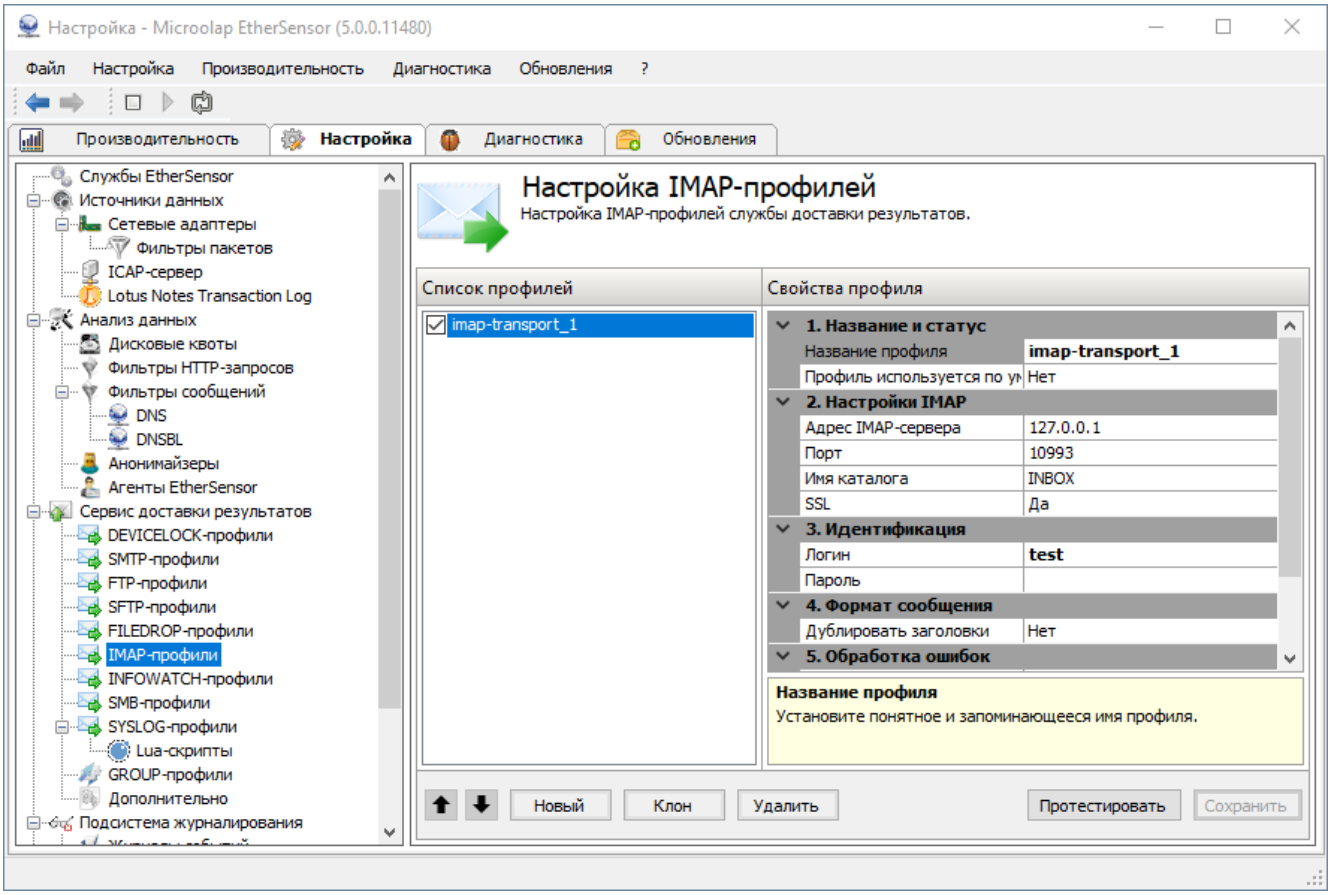

Рис.29. Настройки IMAP-профилей.

1. Название и статус

Название профиля:

Удобное, запоминающееся и информативное название профиля, на усмотрение администратора.

Профиль используется по умолчанию:

Да означает, что данный профиль используется по умолчанию.

2. Настройки IMAP

Адрес IMAP-сервера:

IP-адрес или доменное имя IMAP-сервера.

Порт:

Порт IMAP-сервера.

Имя каталога:

Имя каталога почтового ящика, в который будет отправлено сообщение.

SSL:

Разрешить/запретить использовать SSL-шифрование при передаче перехваченных сообщений на сервер.

3. Идентификация

Логин:

Логин на IMAP-сервере.

Пароль:

Пароль на IMAP-сервере.

4. Формат сообщения

Дублировать заголовки:

Разрешить/запретить сохранение стандартных заголовков сообщения, а также заголовков **X-Sensor** дополнительно, в отдельном вложении сообщения - **microolap_msis_headers.txt**.

Возможные варианты:

Все

Сохранять все заголовки сообщения;

X-Sensor

Сохранять заголовки с префиксом **X-Sensor;**

Другие

Сохранять стандартные заголовки **From, To, Cc, Bcc** и другие, не попадающие под действие флагов **xsensor;**

Нет

Запрещает сохранение заголовков сообщения в отдельном вложении.

5. Обработка ошибок

Таймаут после отказа:

Время ожидания для транспортировки сообщений в случае отказа приёмника. Значение параметра задаётся в секундах.

6. Для GROUP-профилей

Вес:

Задаёт пропорцию распределения сообщений между приёмниками. Параметр может принимать значения от **1** до **10**, и действителен только в составе группового профиля.

Резервный профиль:

Включает или выключает использование резервного профиля Если этот флаг включён, то доставка сообщений с использованием данного профиля будет задействована в случае отказа основных (не резервных) транспортных профилей. Параметр действителен только в составе группового профиля.

3.2.1.8. INFOWATCH-профили

Настройка INFOWATCH-профилей

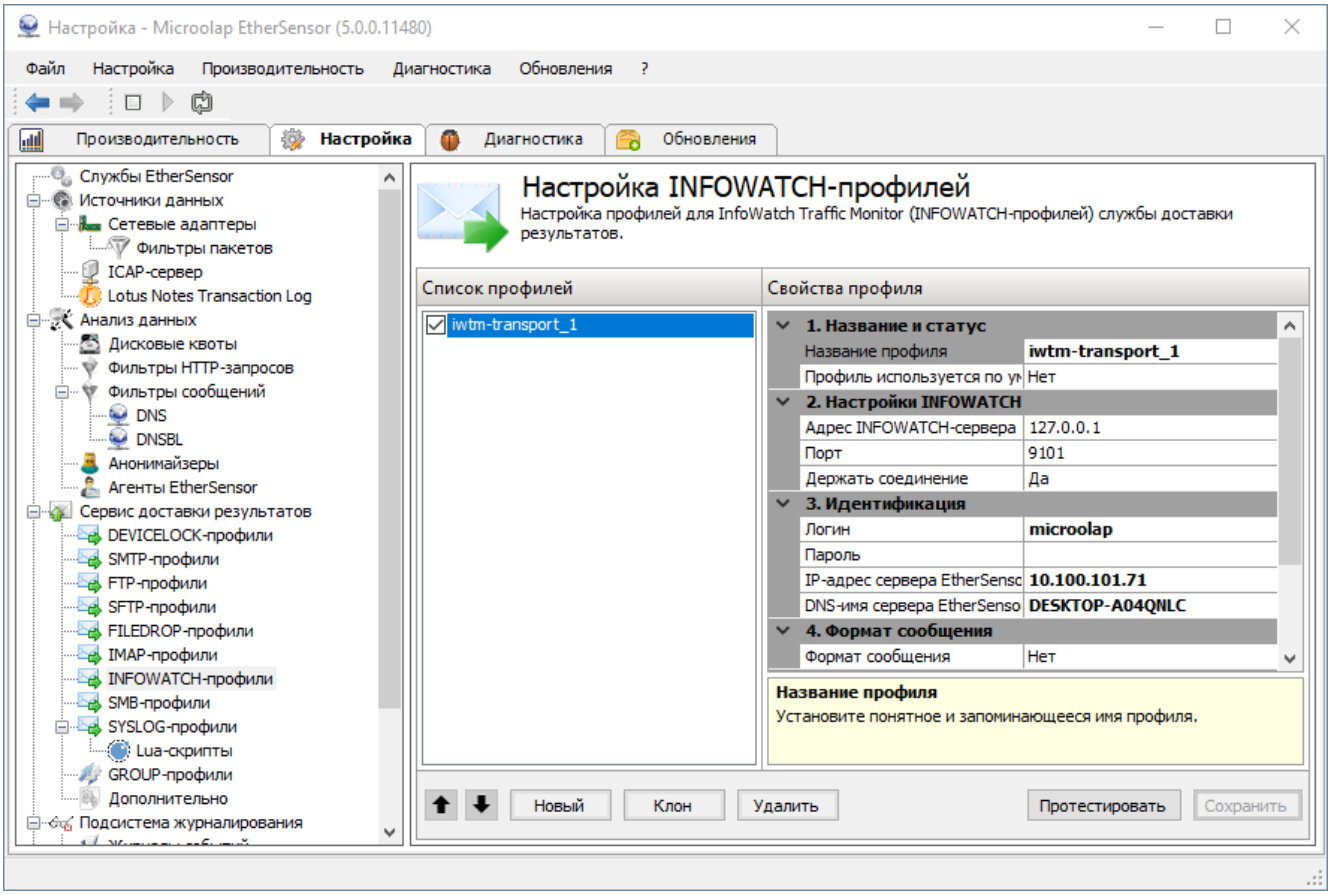

Рис.30. Настройки INFOWATCH-профилей.

1. Название и статус

Название профиля:

Удобное, запоминающееся и информативное название профиля, на усмотрение администратора.

Профиль используется по умолчанию:

Да означает, что данный профиль используется по умолчанию.

2. Настройки INFOWATCH

Адрес INFOWATCH-сервера:

IP-адрес или доменное имя сервера InfoWatch Traffic Monitor.

Порт:

Порт сервера InfoWatch Traffic Monitor (порт по умолчанию 9101).

Держать соединение:

Отправлять сообщения в одном и том же соединении с сервером, принимающим сообщения. Если этот флаг выключен, то каждое отправляемое сообщение будет отправлено в отдельном TCP соединении.

3. Идентификация

Имя токена:

Имя токена, указанное в настройках InfoWatch Traffic Monitor (по умолчанию microolap).

Содержание токена:

Содержание токена, указанное в настройках InfoWatch Traffic Monitor.

IP-адрес сервера EtherSensor:

IP-адрес сервера EtherSensor, позволяет InfoWatch Traffic Monitor различать различные экземпляры одного источника данных.

DNS-имя сервера EtherSensor:

DNS-имя сервера EtherSensor, позволяет серверу InfoWatch Traffic Monitor различать различные источники данных.

4. Формат сообщения

Формат сообщения:

Формат сохраняемого сообщения (EML, XML, JSON....).

5. Обработка ошибок

Таймаут после отказа:

Время ожидания для транспортировки сообщений в случае отказа приёмника. Значение параметра задаётся в секундах.

6. Для GROUP-профилей

Вес:

Задаёт пропорцию распределения сообщений между приёмниками. Параметр может принимать значения от **1** до **10**, и действителен только в составе группового профиля.

Резервный профиль:

Включает или выключает использование резервного профиля Если этот флаг включён, то доставка сообщений с использованием данного профиля будет задействована в случае отказа основных (не резервных) транспортных профилей. Параметр действителен только в составе группового профиля.

3.2.1.9. SMB-профили

Настройка SMB-профилей

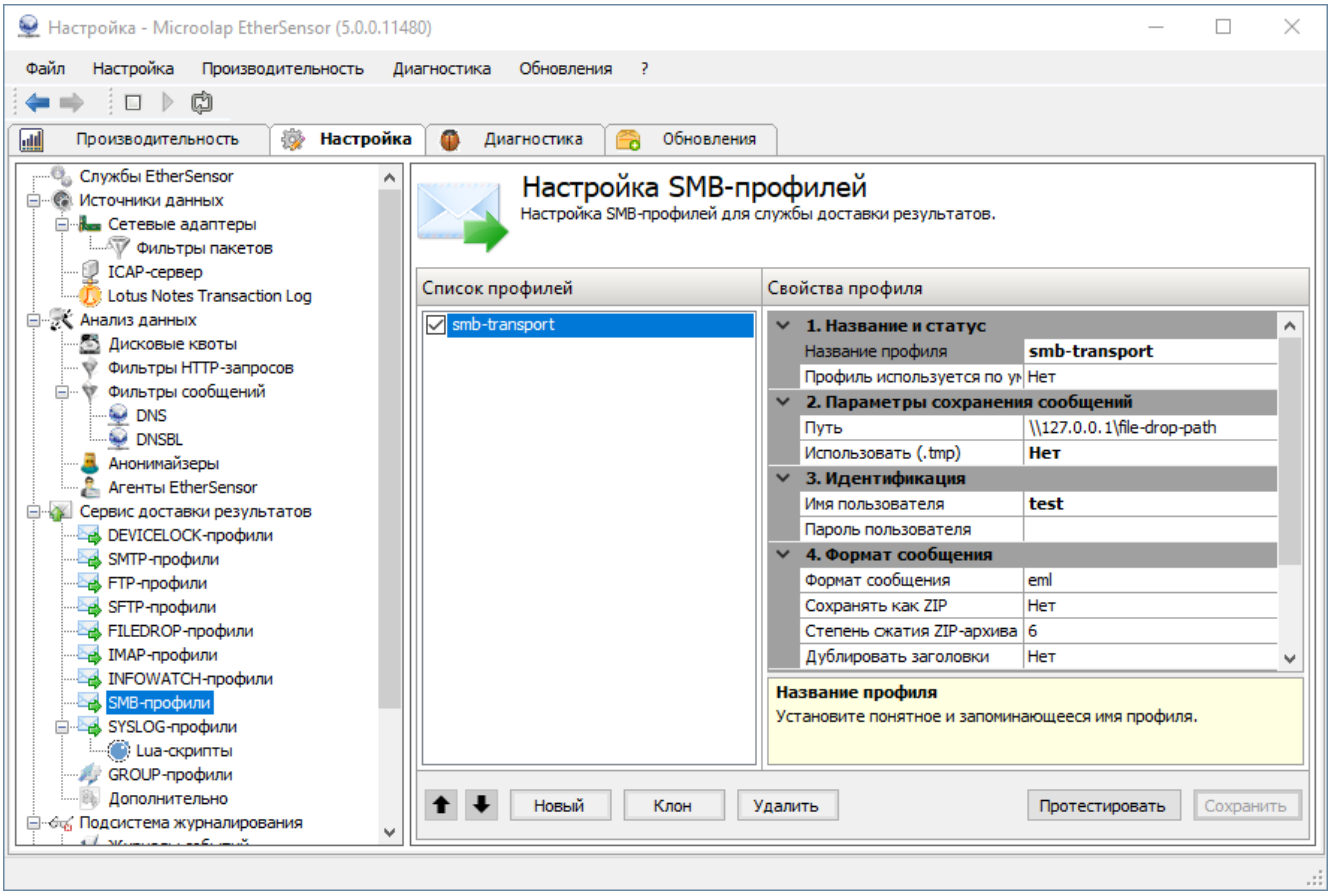

Рис.31. Настройки SMB-профилей.

1. Название и статус

Название профиля:

Удобное, запоминающееся и информативное название профиля, на усмотрение администратора.

Профиль используется по умолчанию:

Да означает, что данный профиль используется по умолчанию.

2. Параметры сохранения сообщений

Путь:

Путь к SMB/CIFS каталогу для записи сообщений.

Использовать (.tmp):

Разрешить/запретить использовать двухэтапное перемещение файлов:

Да: файл перемещается с временным расширением (например, 2012-01-08-15-29-48-586.7.M.zip.tmp), после завершения перемещения файл переименовывается (удаляется временное расширение);

Нет: файл перемещается сразу с указанным расширением (например, 2012-01-08-15-29-48-586.7.M.zip).

3. Идентификация

Имя пользователя:

Имя пользователя для доступа к SMB/CIFS каталогу для записи сообщения.

Пароль пользователя:

Пароль пользователя для доступа к SMB/CIFS каталогу для записи сообщения.

4. Формат сообщения

Формат сообщения:

Формат сохраняемого сообщения (EML, XML, JSON....).

Сохранять как ZIP:

Заворачивать ли сохраняемые сообщения в ZIP-архив. Если этот флаг включен совместно с флагом "**Сохранять как EML**", то EML-конверты сообщений будут упаковываться в ZIP-архив. Если этот флаг включен и при этом флаг "**Сохранять как EML**" отключена, то в ZIP-архив будут упаковываться сообщения во внутреннем формате **Microolap EtherSensor**.

Степень сжатия ZIP-архива:

Возможные значения данного параметра находятся в диапазоне от **0** до **9**, где **0** - без сжатия, **1** - минимальное сжатие, но высокая скорость, **9** - максимальное сжатие.

Дублировать заголовки:

Разрешить/запретить сохранение стандартных заголовков сообщения, а также заголовков **X-Sensor** дополнительно, в отдельном вложении сообщения - **microolap_msis_headers.txt**.

Возможные варианты:

Все

Сохранять все заголовки сообщения;

X-Sensor

Сохранять заголовки с префиксом **X-Sensor;**

Другие

Сохранять стандартные заголовки **From, To, Cc, Bcc** и другие, не попадающие под действие флагов **xsensor;**

Нет

Запрещает сохранение заголовков сообщения в отдельном вложении.

5. Обработка ошибок

Таймаут после отказа:

Время ожидания для транспортировки сообщений в случае отказа приёмника. Значение параметра задаётся в секундах.

6. Для GROUP-профилей

Вес:

Задаёт пропорцию распределения сообщений между приёмниками. Параметр может принимать значения от **1** до **10**, и действителен только в составе группового профиля.

Резервный профиль:

Включает или выключает использование резервного профиля Если этот флаг включён, то доставка сообщений с использованием данного профиля будет задействована в случае отказа основных (не резервных) транспортных профилей. Параметр действителен только в составе группового профиля.

3.2.1.10. SYSLOG-профили

Настройка SYSLOG-профилей

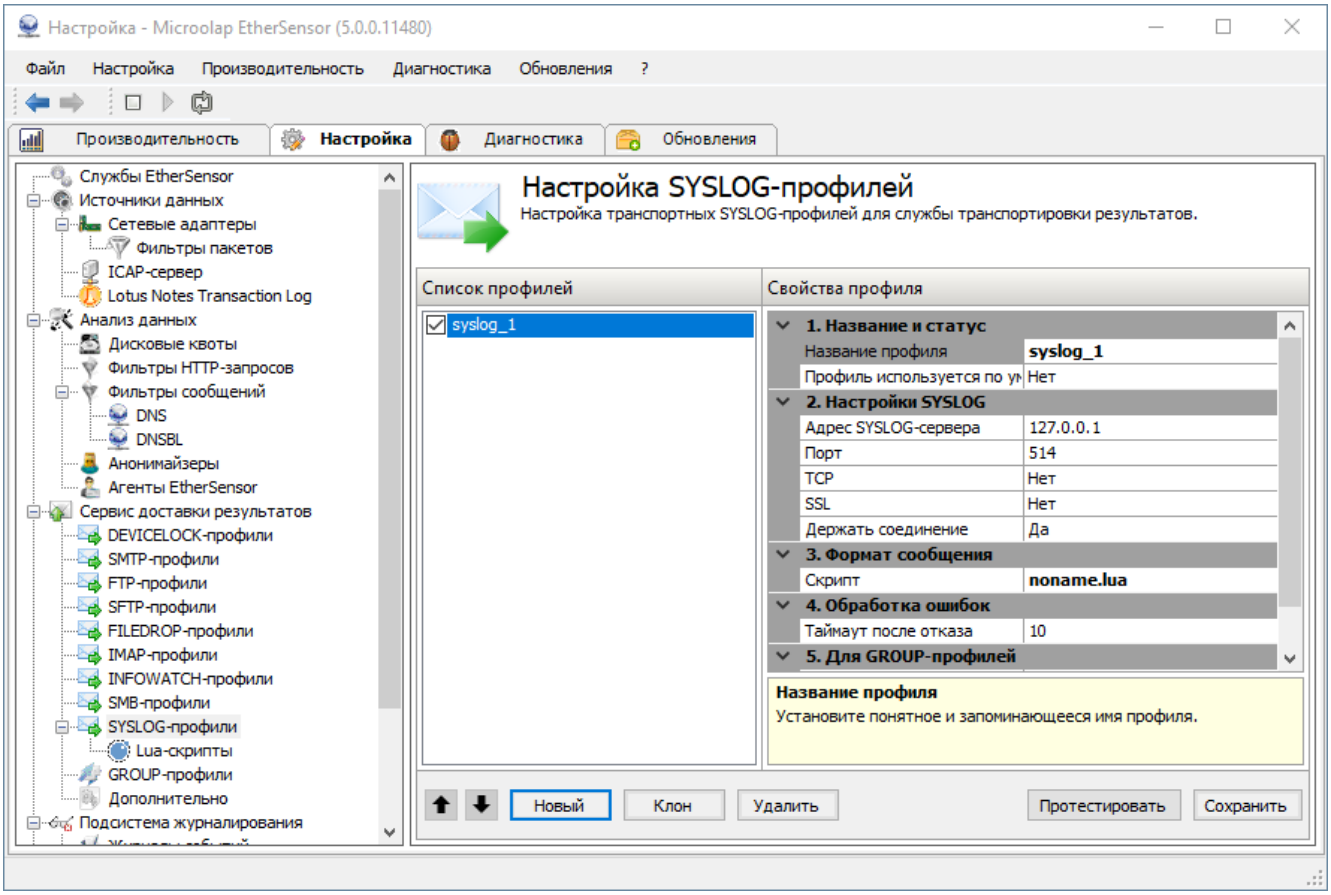

Рис.32. Настройки SYSLOG-профилей.

1. Название и статус

Название профиля:

Удобное, запоминающееся и информативное название профиля, на усмотрение администратора.

Профиль используется по умолчанию:

Да означает, что данный профиль используется по умолчанию.

2. Настройки SYSLOG

Адрес SYSLOG-сервера:

IP-адрес или имя SYSLOG-сервера для доставки результатов.

Порт:

Порт SYSLOG сервера.

TCP:

Позволяет использовать TCP протокол для отправки сообщений на SYSLOG-сервер.

Внимание!
Отправка на SYSLOG-сервер через SSL работает только при включенном TCP.

SSL:

Разрешить/запретить использовать SSL-шифрование при передаче перехваченных сообщений на сервер.

Держать соединение:

Отправлять сообщения в одном и том же соединении с сервером, принимающим сообщения. Если этот флаг выключен, то каждое отправляемое сообщение будет отправлено в отдельном TCP соединении.

3. Формат сообщения

Скрипт:

Имя файла *Lua-скрипта*, который будет использоваться для формирования сообщения. Файл скрипта должен находится в папке **[INSTALLDIR]\scripts**.

4. Обработка ошибок

Таймаут после отказа:

Время ожидания для транспортировки сообщений в случае отказа приёмника. Значение параметра задаётся в секундах.

5. Для GROUP-профилей

Вес:

Задаёт пропорцию распределения сообщений между приёмниками. Параметр может принимать значения от **1** до **10**, и действителен только в составе группового профиля.

Резервный профиль:

Включает или выключает использование резервного профиля Если этот флаг включён, то доставка сообщений с использованием данного профиля будет задействована в случае отказа основных (не резервных) транспортных профилей. Параметр действителен только в составе группового профиля.

3.2.1.10.1. Lua-скрипты

TBD

3.2.1.11. GROUP-профили

Настройка GROUP-профилей

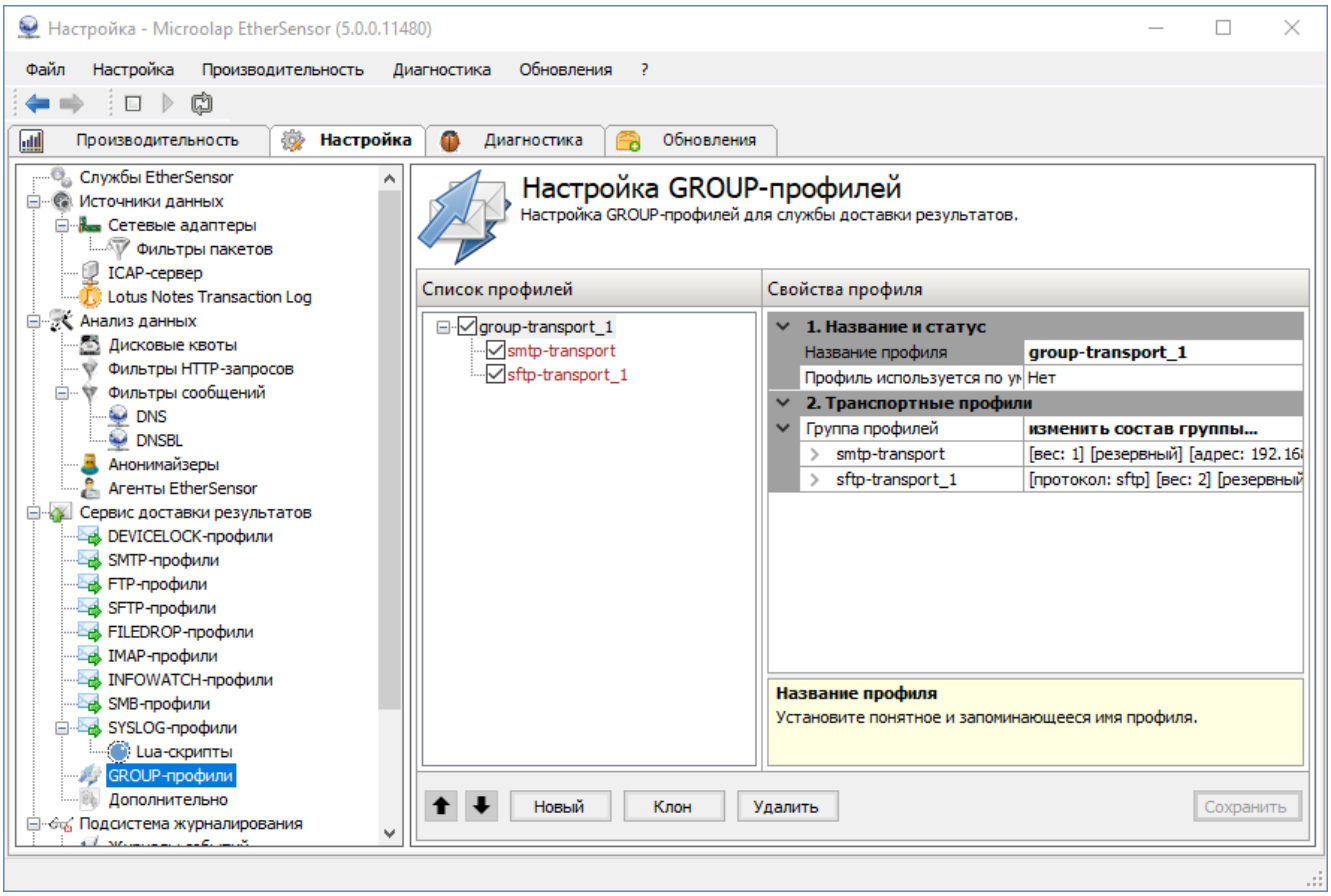

Рис.33. Настройки GROUP-профилей.

1. Название и статус

Название профиля:

Удобное, запоминающееся и информативное название профиля, на усмотрение администратора.

Профиль используется по умолчанию:

Да означает, что данный профиль используется по умолчанию.

2. Транспортные профили

Группа профилей:

Список уже существующих профилей доставки, используемых в составе группового профиля.

Работа группового транспортного профиля

Общие понятия

Групповой транспортный профиль, наравне с обычным транспортным профилем, может быть назначен как профиль по умолчанию, а также может быть назначен для использования с помощью правил фильтрации сообщений.

В отличие от стандартного транспортного профиля, где содержатся тонкие настройки доставки сообщений согласно используемому способу передачи сообщений, групповой профиль содержит только имена заранее созданных стандартных транспортных профилей.

В групповом профиле стандартные профили могут быть поделены на основные и резервные. Основные используются для доставки сообщений в нормальном режиме работы. Резервные профили используются для доставки сообщений, когда ни один из основных профилей доставить сообщение не может.

Также в групповом профиле стандартным профилям могут быть назначены веса для доставки сообщений к потребителям в необходимой пропорции. Веса могут назначаться как основным, так и резервным профилям.

Транспортировка сообщений с использованием группового профиля

Рассмотрим пример транспортировки сообщений с использованием группового профиля, в котором 3 стандартных транспортных профиля назначены как основные (SMTP 1, SMTP 2, SMTP 3) с равными весами, и один стандартный транспортный профиль (FILEDROP 1) назначен как резервный.

В данном примере в нормальном режиме работы сообщения в равной пропорции доставляются к приёмникам сообщений.

Если один из приёмников сообщений, описанный стандартным транспортным профилем, не может принять сообщения, то нагрузка по приёму сообщений ложится на остальные основные транспортные профили.

Если все основные транспортные профили (SMTP 1, SMTP 2, SMTP 3) не могут принять сообщения, то для доставки сообщений будет использоваться резервный транспортный профиль (FILEDROP 1) до тех пор, пока хотя бы один основной транспортный профиль не будет способен отправлять сообщения.

3.2.2. Ручная настройка (файл конфигурации)

Конфигурация службы **EtherSensor Transfer** содержится в XML-файле **transfer.xml,** расположенном в общей директории конфигураций **Microolap EtherSensor [INSTALLDIR] \config**.

Пример файла конфигурации **transfer.xml**:

```
<?xml version="1.0" encoding="utf-8"?>
<TransferConfig version="4.1">
 <SensorID>0AFE95E7-DC45-4993-B9FC-5E002D9B1BCA</SensorID>
 <TransportThreads>4</TransportThreads>

 <Profile name="smtp-main" enabled="true" default="false">
    <Option name="protocol" value="smtp" />
    <Option name="smtp-server" value="smtp.domain.com" />
    <Option name="smtp-port" value="465" />
    <Option name="enable-ssl" value="true" />
    <Option name="mail-from" value="sensor@internal.net" />
    <Option name="mail-to" value="archive@internal.net" />
    <Option name="tcp-timeout" value="10" />
    <Option name="save-headers" value="all" />
    <Option name="keep-connection" value="true" />
    <Option name="profile-fail-timeout" value="10" />
    <Option name="go-profile-weight" value="1" />
    <Option name="go-profile-reserve" value="false" />
 </Profile>

 <Profile name="imap-transport" enabled="true" default="false">
    <Option name="protocol" value="imap" />
    <Option name="imap-server" value="imap.domain.com" />
    <Option name="imap-port" value="10993" />
    <Option name="file-drop-path" value="INBOX" />
    <Option name="enable-ssl" value="true" />
    <Option name="username" value="administrator@domain.com" />
    <Option name="password" value="test123" />
    <Option name="tcp-timeout" value="10" />
    <Option name="save-headers" value="none" />
 </Profile>

 <Profile name="local-dir" enabled="true" default="true">
    <Option name="protocol" value="filedrop" />
    <Option name="file-drop-path" value="C:\FileDropPath\" />
    <Option name="enable-tmp" value="false" />
    <Option name="save-passport" value="false" />
    <Option name="save-eml" value="true" />
    <Option name="save-zip" value="false" />
    <Option name="zip-level" value="0" />
    <Option name="quota" value="10Gb" />
    <Option name="save-headers" value="xsensor, xkpps" />
    <Option name="profile-fail-timeout" value="10" />
    <Option name="go-profile-weight" value="1" />
    <Option name="go-profile-reserve" value="false" />
 </Profile>

 <Profile name="largefile-ftp" enabled="true" default="false">
    <Option name="protocol" value="ftp" />
    <Option name="file-drop-path" value="ftp://127.0.0.1/" />
    <Option name="enable-ssl" value="true" />
    <Option name="user-name" value="test" />
    <Option name="password" value="" />
    <Option name="enable-tmp" value="false" />
    <Option name="save-passport" value="true" />
    <Option name="save-eml" value="true" />
    <Option name="save-zip" value="false" />
    <Option name="zip-level" value="6" />
    <Option name="save-headers" value="none" />
    <Option name="profile-fail-timeout" value="10" />
    <Option name="go-profile-weight" value="1" />
    <Option name="go-profile-reserve" value="false" />
 </Profile>
```

```
<Profile name="net_share_1" enabled="true" default="false">
   <Option name="protocol" value="smb" />
   <Option name="file-drop-path" value="\\ARCHSERVER1\Messages" />
   <Option name="user-name" value="test" />
   <Option name="password" value="" />
   <Option name="enable-tmp" value="false" />
   <Option name="save-passport" value="false" />
   <Option name="save-eml" value="true" />
   <Option name="save-zip" value="false" />
   <Option name="zip-level" value="6" />
   <Option name="save-headers" value="none" />
   <Option name="profile-fail-timeout" value="10" />
   <Option name="go-profile-weight" value="1" />
   <Option name="go-profile-reserve" value="true" />
</Profile>

<Profile name="sftp-transport_1" enabled="true" default="false">
   <Option name="protocol" value="sftp" />
   <Option name="sftp-server" value="10.101.100.125" />
   <Option name="sftp-port" value="22" />
   <Option name="file-drop-path" value="messages" />
   <Option name="user-name" value="test" />
   <Option name="password" value="" />
   <Option name="enable-tmp" value="false" />
   <Option name="save-format" value="eml" />
   <Option name="save-zip" value="false" />
   <Option name="zip-level" value="6" />
   <Option name="save-headers" value="none" />
   <Option name="profile-fail-timeout" value="10" />
   <Option name="go-profile-weight" value="1" />
   <Option name="go-profile-reserve" value="true" />
</Profile>

<Profile name="iwtm-transport_1" enabled="true" default="false">
   <Option name="protocol" value="iwthrift" />
   <Option name="iwthrift-server" value="10.101.100.196" />
   <Option name="iwthrift-port" value="9101" />
   <Option name="iwthrift-company" value="microolap" />
   <Option name="iwthrift-token" value="" />
   <Option name="capture-server-ip" value="10.100.101.68" />
   <Option name="capture-server-host" value="sensor.chg" />
   <Option name="keep-connection" value="true" />
   <Option name="save-headers" value="none" />
   <Option name="profile-fail-timeout" value="10" />
   <Option name="go-profile-weight" value="1" />
   <Option name="go-profile-reserve" value="true" />
</Profile>

<Profile name="group-transport" enabled="true" default="false">
   <Option name="protocol" value="gprofile" />
   <Option name="profilename" value="smtp-main" />
   <Option name="profilename" value="net_share_1" />
</Profile>
</TransferConfig>
```

Тег TransferConfig

Является корневым тегом конфигурации службы. В его атрибуте **version** указывается версия конфигурации.

Тег SensorID

Задаёт идентификатор сенсора. Используется в дальнейшем при анализе трафика для определения физического источника, из которого были получены данные.

Тег TransportThreads

Определяет количество потоков, одновременно отправляющих сообщения. Максимальное количество отправляющих потоков не может быть больше чем текущее количество логических ядер **CPU*2** и не может быть меньше **1**.

Тег Profile

Тег **Profile** указывает описание профиля передачи данных. В атрибуте **name** указывается имя профиля. Атрибут **enabled** указывает статус активности профиля, и если данный атрибут выставлен в значение **false**, то профиль не будет использоваться в передаче данных. Атрибут **default** используется для указания статуса профиля по умолчанию. Данный атрибут может быть выставлен в значение **true** только для одного профиля из всего набора профилей.

Тег Option

Тег **Option** является вложенным в тег **Profile** и указывает на описание конкретного свойства профиля передачи данных. В атрибуте **name** указывается имя свойства. Атрибут **value** определяет значение свойства.

3.2.2.1. DEVICELOCK-профили

TBD

3.2.2.2. FALCONGAZE-профили

Enter topic text here.

3.2.2.3. SMTP-профили

Ниже показан пример настройки транспортного профиля, работающего по протоколу SMTP:

```
<Profile name="smtp-main" enabled="true" default="false">
    <Option name="protocol" value="smtp" />
    <Option name="smtp-server" value="smtp.domain.com" />
    <Option name="smtp-port" value="465" />
    <Option name="enable-ssl" value="true" />
    <Option name="mail-from" value="sensor@internal.net" />
    <Option name="mail-to" value="archive@internal.net" />
    <Option name="tcp-timeout" value="10" />
    <Option name="save-headers" value="all" />
    <Option name="keep-connection" value="false" />
    <Option name="profile-fail-timeout" value="10" />
    <Option name="go-profile-weight" value="1" />
    <Option name="go-profile-reserve" value="false" />
</Profile>
```

Описание свойств профиля SMTP:

protocol

Определяет протокол передачи данных;

smtp-server

Определяет сетевой адрес SMTP-сервера. Может быть указан в виде IP-адреса или в виде DNS-имени. Например: **smtp.domain.com** или **192.168.0.11;**

smtp-port

Определяет номер порта SMTP-сервера, например: **465**;

enable-ssl

Определяет статус использования SSL-туннеля. Пример: **true** или **false;**

mail-from

Определяет адрес отправителя сообщения. Пример: **sensor@internal.net**;

mail-to

Определяет адрес получателя сообщения. Пример: **sensor@internal.net**;

tcp-timeout

Определяет время на попытку соединения с SMTP-сервером в миллисекундах, например **10**;

keep-connection

Разрешает/запрещает отправку сообщений в одном и том же соединении с SMTP-сервером. Если данный параметр выключен, то каждое отправляемое сообщение будет отправлено в отдельном TCP-соединении;

save-headers

Разрешить/запретить сохранение стандартных заголовков сообщения, а также заголовков **X-Sensor** дополнительно, в отдельном вложении сообщения - **microolap_msis_headers.txt**.

Возможные варианты:

all

Сохраняются все заголовки сообщения;

xsensor

Сохраняются заголовки с префиксом **X-Sensor;**

other

Сохраняются стандартные заголовки **From, To, Cc, Bcc** и другие, не попадающие под действие флагов **xsensor;**

none

Запрещает сохранение заголовков сообщения в отдельном вложении.

profile-fail-timeout

Определяет время ожидания сервера для транспортировки сообщений в случае отказа приёмника. Значение параметра задаётся в секундах;

go-profile-weight

Задаёт пропорцию распределения сообщений между приёмниками. Параметр может принимать значения от **1** до **10**, и действителен только в составе группового профиля;

go-profile-reserve

Включает/выключает использование резервного профиля. Если данный флаг включён, то доставка сообщений с использованием данного профиля будет задействована в случае отказа основных (не резервных) транспортных профилей. Параметр действителен только в составе группового профиля.

3.2.2.4. FTP-профили

Ниже показан пример настройки транспортного профиля, работающего по протоколу FTP:

```
<Profile name="largefile-ftp" enabled="true" default="false">
    <Option name="protocol" value="ftp" />
    <Option name="file-drop-path" value="ftp://127.0.0.1/test" />
    <Option name="enable-ssl" value="true" />
    <Option name="user-name" value="test" />
    <Option name="password" value="" />
    <Option name="enable-tmp" value="false" />
    <Option name="save-passport" value="true" />
    <Option name="save-eml" value="true" />
    <Option name="save-zip" value="false" />
    <Option name="zip-level" value="0" />
    <Option name="save-headers" value="xsensor, xkpps" />
    <Option name="profile-fail-timeout" value="10" />
    <Option name="go-profile-weight" value="1" />
    <Option name="go-profile-reserve" value="false" />
</Profile>
```

Описание свойств профиля FTP:

protocol

Определяет протокол передачи данных, здесь - **ftp;**

file-drop-path

Определяет путь сохранения результата на FTP-сервере с точностью до директории. Пример: **ftp://127.0.0.1/test;**

enable-ssl

Определяет статус использования SSL-туннеля. Значения: **true** или **false;**

user-name

Определяет имя пользователя, который имеет необходимый доступ к ресурсу FTP-сервера, например, **test**;

password

Определяет пароль пользователя, который имеет необходимый доступ к ресурсу FTP-сервера, например, "**123456secret**"

enable-tmp

Разрешает/запрещает использование двухэтапного перемещения файлов. Значения: **true** или **false;**

save-passport

Определяет сохранение данных на FTP-сервере во внутреннем формате **Microolap EtherSensor**. Значения: **true** или **false;**

save-eml

Определяет сохранение данных на FTP-сервере в формате EML-конверта. Значения: **true** или **false.**

Внимание!
1. Свойство **save-eml** подавляет свойство **save-passport**: если и **save-eml** и **save-passport** выставлены в **true**, данные будут сохранены только в формате **EML**.
2. Если и **save-eml** и **save-passport** выставлены в **false**, транспортный профиль отработает, но данные сохранены не будут.

save-zip

Определяет сохранение данных на FTP-сервере в формате ZIP-архива. Пример: **true** или **false;**

zip-level

Определяет степень сжатия ZIP-архива. Возможные значения данного параметра находятся в диапазоне от **0** до **9**, где **0** - без сжатия, **1** - минимальное сжатие, но высокая скорость, **9** - максимальное сжатие**;**

save-headers

Разрешить/запретить сохранение стандартных заголовков сообщения, а также заголовков **X-Sensor** дополнительно, в отдельном вложении сообщения - **microolap_msis_headers.txt**.

Возможные варианты:

all

Сохраняются все заголовки сообщения;

xsensor

Сохраняются заголовки с префиксом **X-Sensor;**

other

Сохраняются стандартные заголовки **From, To, Cc, Bcc** и другие, не попадающие под действие флагов **xsensor;**

none

Запрещает сохранение заголовков сообщения в отдельном вложении.

profile-fail-timeout

Определяет время ожидания сервера для транспортировки сообщений в случае отказа приёмника. Значение параметра задаётся в секундах;

go-profile-weight

Задаёт пропорцию распределения сообщений между приёмниками. Параметр может принимать значения от **1** до **10**, и действителен только в составе группового профиля;

go-profile-reserve

Включает/выключает использование резервного профиля. Если данный флаг включён, то доставка данных с использованием данного профиля будет задействована в случае отказа основных (не резервных) транспортных профилей. Параметр действителен только в составе группового профиля.

3.2.2.5. SFTP-профили

Ниже показан пример настройки транспортного профиля, работающего по протоколу SFTP:

```
<Profile name="sftp-transport_1" enabled="true" default="false">
    <Option name="protocol" value="sftp" />
    <Option name="sftp-server" value="10.101.100.125" />
    <Option name="sftp-port" value="22" />
    <Option name="file-drop-path" value="messages" />
    <Option name="user-name" value="test" />
    <Option name="password" value="" />
    <Option name="enable-tmp" value="false" />
    <Option name="save-format" value="eml" />
    <Option name="save-zip" value="false" />
    <Option name="zip-level" value="6" />
    <Option name="save-headers" value="none" />
    <Option name="profile-fail-timeout" value="10" />
    <Option name="go-profile-weight" value="1" />
    <Option name="go-profile-reserve" value="true" />
</Profile>
```

Описание свойств профиля SFTP:

protocol

Определяет протокол передачи данных, здесь - **sftp;**

sftp-server

IP-адрес или доменное имя SFTP-сервера с указанием директории, в которую будут сохраняться перехваченные сообщения**;**

sftp-port

Порт SFTP-сервера**;**

file-drop-path

Имя каталога для сохранения сообщений**;**

user-name

Определяет имя пользователя, который имеет необходимый доступ к ресурсу SFTP-сервера, например, **test**;

password

Определяет пароль пользователя, который имеет необходимый доступ к ресурсу SFTP-сервера, например, "**123456secret**"

enable-tmp

Разрешает/запрещает использование двухэтапного перемещения файлов. Значения: **true** или **false.** Бывает полезно в случае отслеживания каким-либо процессом появления в каталоге SFTP сервера новых файлов (переименование - атомарная операция).

save-format

Сохранять сообщение в формате (eml, xml, json...)**;**

save-zip

Определяет сохранение данных на SFTP-сервере в формате ZIP-архива. Пример: **true** или **false;**

zip-level

Определяет степень сжатия ZIP-архива. Возможные значения данного параметра находятся в диапазоне от **0** до **9**, где **0** - без сжатия, **1** - минимальное сжатие, но высокая скорость, **9** - максимальное сжатие**;**

save-headers

Разрешить/запретить сохранение стандартных заголовков сообщения, а также заголовков **X-Sensor** дополнительно, в отдельном вложении сообщения - **microolap_msis_headers.txt**.

Возможные варианты:

all

Сохраняются все заголовки сообщения;

xsensor

Сохраняются заголовки с префиксом **X-Sensor;**

other

Сохраняются стандартные заголовки **From, To, Cc, Bcc** и другие, не попадающие под действие флагов **xsensor;**

none

Запрещает сохранение заголовков сообщения в отдельном вложении.

profile-fail-timeout

Определяет время ожидания сервера для транспортировки сообщений в случае отказа приёмника. Значение параметра задаётся в секундах;

go-profile-weight

Задаёт пропорцию распределения сообщений между приёмниками. Параметр может принимать значения от **1** до **10**, и действителен только в составе группового профиля;

go-profile-reserve

Включает/выключает использование резервного профиля. Если данный флаг включён, то доставка данных с использованием данного профиля будет задействована в случае отказа основных (не резервных) транспортных профилей. Параметр действителен только в составе группового профиля.

3.2.2.6. FILEDROP-профили

Ниже показан пример настройки транспортного профиля типа FILEDROP:

```
<Profile name="local-dir" enabled="true" default="true">
    <Option name="protocol" value="filedrop" />
    <Option name="file-drop-path" value=" C:\FileDropPath\" />
    <Option name="enable-tmp" value="false" />
    <Option name="save-passport" value="false" />
    <Option name="save-eml" value="true" />
    <Option name="save-zip" value="false" />
    <Option name="zip-level" value="6" />
    <Option name="quota" value="10Gb" />
    <Option name="save-headers" value="none" />
    <Option name="profile-fail-timeout" value="10" />
    <Option name="go-profile-weight" value="1" />
    <Option name="go-profile-reserve" value="false" />
</Profile>
```

Описание свойств профиля FILEDROP:

protocol

Определяет протокол передачи данных, здесь - **filedrop**;

file-drop-path

Определяет путь сохранения результата в локальную директорию. Пример: **C:\FileDropPath**;

enable-tmp

Разрешает/запрещает использование двухэтапного перемещения файлов. Значения: **true** или **false**;

save-passport

Определяет сохранение данных во внутреннем формате **Microolap EtherSensor**. Значения: **true** или **false**;

save-eml

Определяет сохранение данных в формате EML-конверта. Значения: **true** или **false**;

Внимание!
1. Свойство **save-eml** подавляет свойство **save-passport**: если и **save-eml** и **save-passport** выставлены в **true**, данные будут сохранены только в формате **EML**.
2. Если и **save-eml** и **save-passport** выставлены в **false**, транспортный профиль отработает, но данные сохранены не будут.

save-zip

Определяет сохранение данных в формате ZIP-архива. Значение: **true** или **false**;

zip-level

Определяет степень сжатия ZIP-архива. Возможные значения данного параметра находятся в диапазоне от **0** до **9**, где **0** - без сжатия, **1** - минимальное сжатие, но высокая скорость, **9** - максимальное сжатие**;**

quota

Определяет ограничение общего размера сохраняемых данных в указанной директории. Пример: **10GB, 500MB**, **100KB** или **10000**;

save-headers

Разрешить/запретить сохранение стандартных заголовков сообщения, а также заголовков **X-Sensor** дополнительно, в отдельном вложении сообщения - **microolap_msis_headers.txt**.

Возможные варианты:

all

Сохраняются все заголовки сообщения;

xsensor

Сохраняются заголовки с префиксом **X-Sensor;**

other

Сохраняются стандартные заголовки **From, To, Cc, Bcc** и другие, не попадающие под действие флагов **xsensor;**

none

Запрещает сохранение заголовков сообщения в отдельном вложении.

profile-fail-timeout

Определяет тайм-аут для транспортировки сообщений в случае отказа приёмника. Значение параметра задаётся в секундах;

go-profile-weight

Задаёт пропорцию распределения сообщений между приёмниками. Параметр может принимать значения от **1** до **10**, и действителен только в составе группового профиля;

go-profile-reserve

Включает/выключает использование резервного профиля. Если данный флаг включён, то доставка данных с использованием данного профиля будет задействована в случае отказа основных (не резервных) транспортных профилей. Параметр действителен только в составе группового профиля.

3.2.2.7. IMAP-профили

Ниже показан пример настройки транспортного профиля, работающего по протоколу IMAP:

```
<Profile name="imap-transport" enabled="true" default="false">
    <Option name="protocol" value="imap" />
    <Option name="imap-server" value="imap.domain.com" />
    <Option name="imap-port" value="10993" />
    <Option name="file-drop-path" value="INBOX" />
    <Option name="enable-ssl" value="true" />
    <Option name="username" value="administrator@domain.com" />
    <Option name="password" value="test123" />
    <Option name="tcp-timeout" value="10" />
    <Option name="save-headers" value="none" />
</Profile>
```

Описание свойств профиля IMAP:

protocol

Определяет протокол передачи данных;

imap-server

Определяет сетевой адрес IMAP-сервера. Может быть указан в виде IP-адреса или в виде DNS имени. Например: **imap.domain.com** или **192.168.0.11;**

imap-port

Определяет номер порта imap-сервера, например: **10993**;

file-drop-path

Определяет директорию для сохранения сообщений, например: **INBOX**;

enable-ssl

Определяет статус использования SSL-туннеля. Пример: **true** или **false;**

username

Определяет имя пользователя для доступа к почтовому ящику. Пример: **administrator@domain.com**;

password

Определяет пароль для доступа к почтовому ящику. Пример: **test123**;

tcp-timeout

Определяет время на попытку соединения с IMAP-сервером в миллисекундах, например **10**;

save-headers

Разрешить/запретить сохранение стандартных заголовков сообщения, а также заголовков **X-Sensor** дополнительно, в отдельном вложении сообщения - **microolap_msis_headers.txt**.

Возможные варианты:

all

Сохраняются все заголовки сообщения;

xsensor

Сохраняются заголовки с префиксом **X-Sensor;**

other

Сохраняются стандартные заголовки **From, To, Cc, Bcc** и другие, не попадающие под действие флагов **xsensor;**

none

Запрещает сохранение заголовков сообщения в отдельном вложении.

3.2.2.8. INFOWATCH-профили

Ниже показан пример настройки транспортного профиля, работающего по протоколу INFOWATCH:

```
<Profile name="iwtm-transport_1" enabled="true" default="false">
    <Option name="protocol" value="iwthrift" />
    <Option name="iwthrift-server" value="10.101.100.196" />
    <Option name="iwthrift-port" value="9101" />
    <Option name="iwthrift-company" value="microolap" />
    <Option name="iwthrift-token" value="" />
    <Option name="capture-server-ip" value="10.100.101.68" />
    <Option name="capture-server-host" value="sensor.chg" />
    <Option name="keep-connection" value="true" />
    <Option name="save-headers" value="none" />
    <Option name="profile-fail-timeout" value="10" />
    <Option name="go-profile-weight" value="1" />
    <Option name="go-profile-reserve" value="true" />
</Profile>
```

Описание свойств профиля INFOWATCH Traffic Monitor:

protocol

Определяет протокол передачи данных, здесь - **iwthrift;**

iwthrift-server

IP-адрес или доменное имя INFOWATCH Traffic Monitor-сервера**;**

iwthrift-port

Порт INFOWATCH Traffic Monitor-сервера**;**

iwthrift-company

Логин для доступа к INFOWATCH Traffic Monitor-серверу**;**

iwthrift-token

Пароль для доступа INFOWATCH Traffic Monitor-серверу;

capture-server-ip

IP-адрес сервера Microolap EtherSensor (позволяет ПО INFOWATCH Traffic Monitor сервера различать различные экземпляры одного источника данных)**;**

capture-server-host

DNS-имя сервера Microolap EtherSensor (позволяет ПО INFOWATCH Traffic Monitor сервера различать различные экземпляры одного источника данных)**;**

keep-connection

Рекомендуется для повышения производительности в случае большого потока сообщений. Отправлять сообщения в одном и том же соединении с сервером, принимающем сообщения. Если данный параметр выключен, то каждое отправляемое сообщение будет отправлено в отдельном TCP соединении**;**

save-headers

Разрешить/запретить сохранение стандартных заголовков сообщения, а также заголовков **X-Sensor** дополнительно, в отдельном вложении сообщения - **microolap_msis_headers.txt**.

Возможные варианты:

all

Сохраняются все заголовки сообщения;

xsensor

Сохраняются заголовки с префиксом **X-Sensor;**

other

Сохраняются стандартные заголовки **From, To, Cc, Bcc** и другие, не попадающие под действие флагов **xsensor;**

none

Запрещает сохранение заголовков сообщения в отдельном вложении.

profile-fail-timeout

Определяет время ожидания сервера для транспортировки сообщений в случае отказа приёмника. Значение параметра задаётся в секундах;

go-profile-weight

Задаёт пропорцию распределения сообщений между приёмниками. Параметр может принимать значения от **1** до **10**, и действителен только в составе группового профиля;

go-profile-reserve

Включает/выключает использование резервного профиля. Если данный флаг включён, то доставка данных с использованием данного профиля будет задействована в случае отказа основных (не резервных) транспортных профилей. Параметр действителен только в составе группового профиля.

3.2.2.9. SMB-профили

Ниже показан пример настройки транспортного профиля, работающего по протоколу SMB/CIFS:

```
<Profile name="net_share_1" enabled="true" default="false">
    <Option name="protocol" value="smb" />
    <Option name="file-drop-path" value="\\ARCHSERVER1\Messages" />
    <Option name="user-name" value="test" />
    <Option name="password" value="" />
    <Option name="enable-tmp" value="false" />
    <Option name="save-passport" value="false" />
    <Option name="save-eml" value="true" />
    <Option name="save-zip" value="false" />
    <Option name="zip-level" value="6" />
    <Option name="save-headers" value="none" />
    <Option name="profile-fail-timeout" value="10" />
    <Option name="go-profile-weight" value="2" />
    <Option name="go-profile-reserve" value="true" />
</Profile>
```

Описание свойств профиля SMB/CIFS:

protocol

Определяет протокол передачи данных, здесь - **smb;**

file-drop-path

Определяет путь сохранения результата на SMB-сервере с точностью до каталога. Пример: **\\ARCHSERVER1\Messages;**

user-name

Определяет имя пользователя для доступа к сетевому каталогу. Пример: **test;**

password

Определяет пароль пользователя для доступа к сетевому каталогу. Пример: "**123456secret**";

enable-tmp

Разрешает/запрещает использование двухэтапного перемещения файлов. Значения: **true** или **false;**

save-passport

Определяет сохранение данных на файл-сервере во внутреннем формате **Microolap EtherSensor**. Значения: **true** или **false**;

save-eml

Определяет сохранение данных на файл-сервере в формате EML-конверта. Значения: **true** или **false**;

Внимание!
1. Свойство **save-eml** подавляет свойство **save-passport**: если и **save-eml** и **save-passport** выставлены в **true**, данные будут сохранены только в формате EML.
2. Если и **save-eml** и **save-passport** выставлены в **false**, транспортный профиль отработает, но данные сохранены не будут.

save-zip

Определяет сохранение данных на файл-сервере в формате ZIP-архива. Значения: **true** или **false**;

zip-level

Определяет степень сжатия ZIP-архива. Возможные значения данного параметра находятся в диапазоне от **0** до **9**, где **0** - без сжатия, **1** - минимальное сжатие, но высокая скорость, **9** - максимальное сжатие**;**

save-headers

Разрешить/запретить сохранение стандартных заголовков сообщения, а также заголовков **X-Sensor** дополнительно, в отдельном вложении сообщения - **microolap_msis_headers.txt**.

Возможные варианты:

all

Сохраняются все заголовки сообщения;

xsensor

Сохраняются заголовки с префиксом **X-Sensor;**

other

Сохраняются стандартные заголовки **From, To, Cc, Bcc** и другие, не попадающие под действие флагов **xsensor;**

none

Запрещает сохранение заголовков сообщения в отдельном вложении.

profile-fail-timeout

Определяет время ожидания сервера для транспортировки сообщений в случае отказа приёмника. Значение параметра задаётся в секундах;

go-profile-weight

Задаёт пропорцию распределения сообщений между приёмниками. Параметр может принимать значения от **1** до **10**, и действителен только в составе группового профиля;

go-profile-reserve

Включает/выключает использование резервного профиля. Если данный флаг включён, то доставка данных с использованием данного профиля будет задействована в случае отказа основных (не резервных) транспортных профилей. Параметр действителен только в составе группового профиля.

3.2.2.10. SYSLOG-профили

TBD

3.2.2.11. GROUP-профили

Ниже показан пример настройки транспортного профиля типа GROUP (групповой профиль):

```
<Profile name="group-transport" enabled="true" default="false">
    <Option name="protocol" value="gprofile" />
    <Option name="profilename" value="smtp-main" />
    <Option name="profilename" value="net_share_1" />
</Profile>
```

Описание свойств профиля GROUP:

protocol

Определяет протокол передачи данных, здесь: **gprofile**;

profilename

Определяет имя заранее определённого транспортного профиля, который входит в состав группы.

3.3. Журналирование

Служба **EtherSensor Watcher** отвечает за сбор системных сообщений от других служб **Microolap EtherSensor** и записи их в зависимости от канала сообщения, уровня журналирования или других критериев в назначенные администратором файлы или syslog-серверы.

Параметры командной строки

Служба **EtherSensor Watcher** в ходе процедуры установки **Microolap EtherSensor** устанавливается в качестве службы Windows, настроенной на автоматический запуск. Однако, при необходимости она может быть запущена как приложение Windows **ethersensor_watcher.exe** со следующими параметрами командной строки:

/process

Запускает процесс **ethersensor_watcher.exe** как обычный Windows Win32-процесс (возможно использовать для отладки).

/service

Запускает как службу Windows.

/config

Сохраняет конфигурацию службы по умолчанию.

3.3.1. Настройка в конфигураторе

Служба **EtherSensor Watcher** отвечает за сбор системных сообщений от других служб **Microolap EtherSensor** и записи их в зависимости от канала сообщения, уровня журналирования или других критериев в назначенные администратором файлы или syslog-серверы.

Журналы событий

В окне, показанном ниже, можно отредактировать существующие правила журналирования событий **Microolap EtherSensor**.

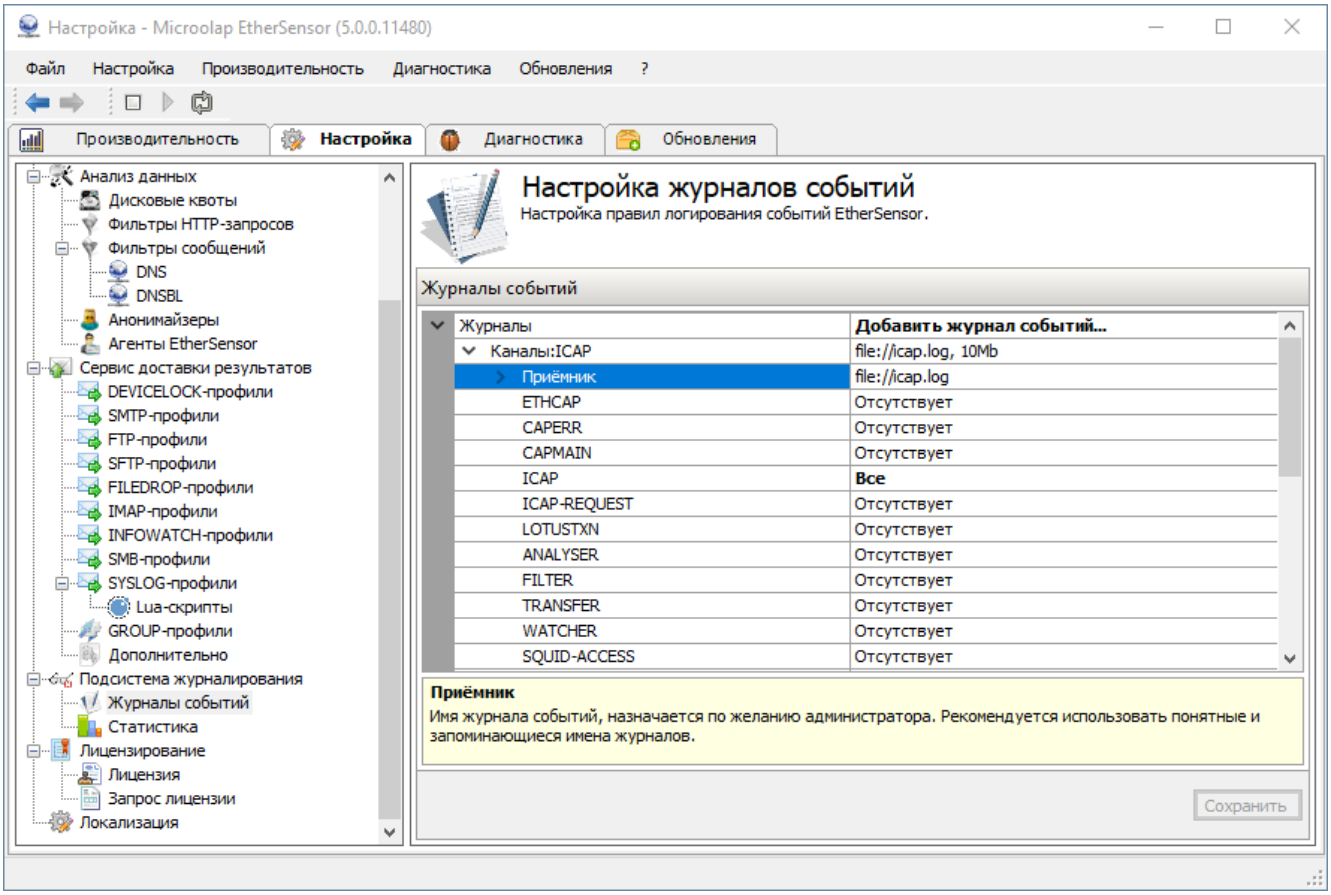

Рис.34. Настройки службы EtherSensor Watcher.

В случае необходимости определения дополнительных файлов журналов или изменения порядка записи сообщений в файлы, следует нажать кнопку справа от **"Добавить журнал событий..."**:

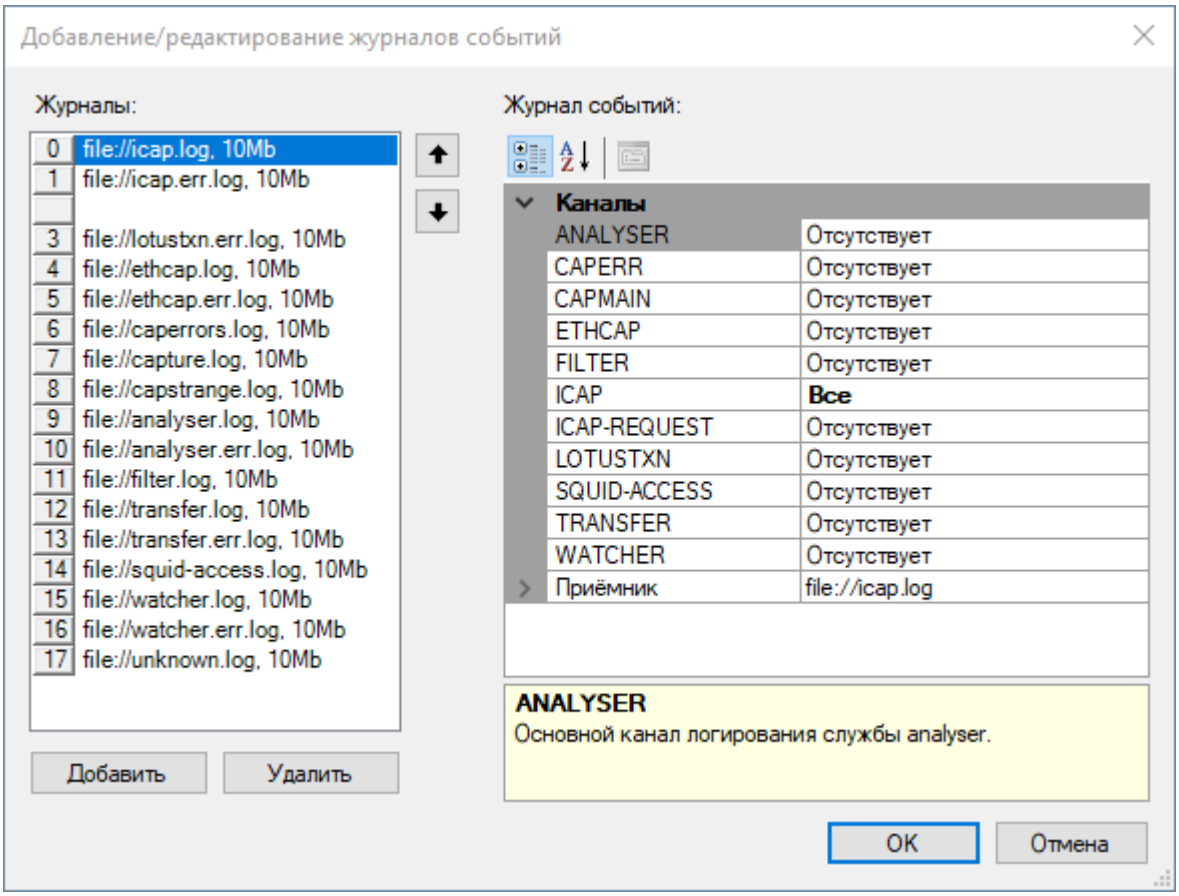

Рис.35. Детальная настройка правил журналирования.

Подробнее о каналах и уровнях журналирования смотрите в разделе "Ручная настройка службы EtherSensor Watcher (файл конфигурации)".

Статистика

В процессе детектирования сообщений **Microolap EtherSensor** позволяет накапливать различную статистику. Например: статистика TCP-соединений (MAC-адрес интерфейса, на котором было перехвачено соединение, время создания, время завершения соединения, IP-адреса и порты соединения, объём переданных данных от клиента к серверу и обратно, используемый протокол уровня приложений (HTTP, ICQ, SMTP, POP3...) и т.д.).

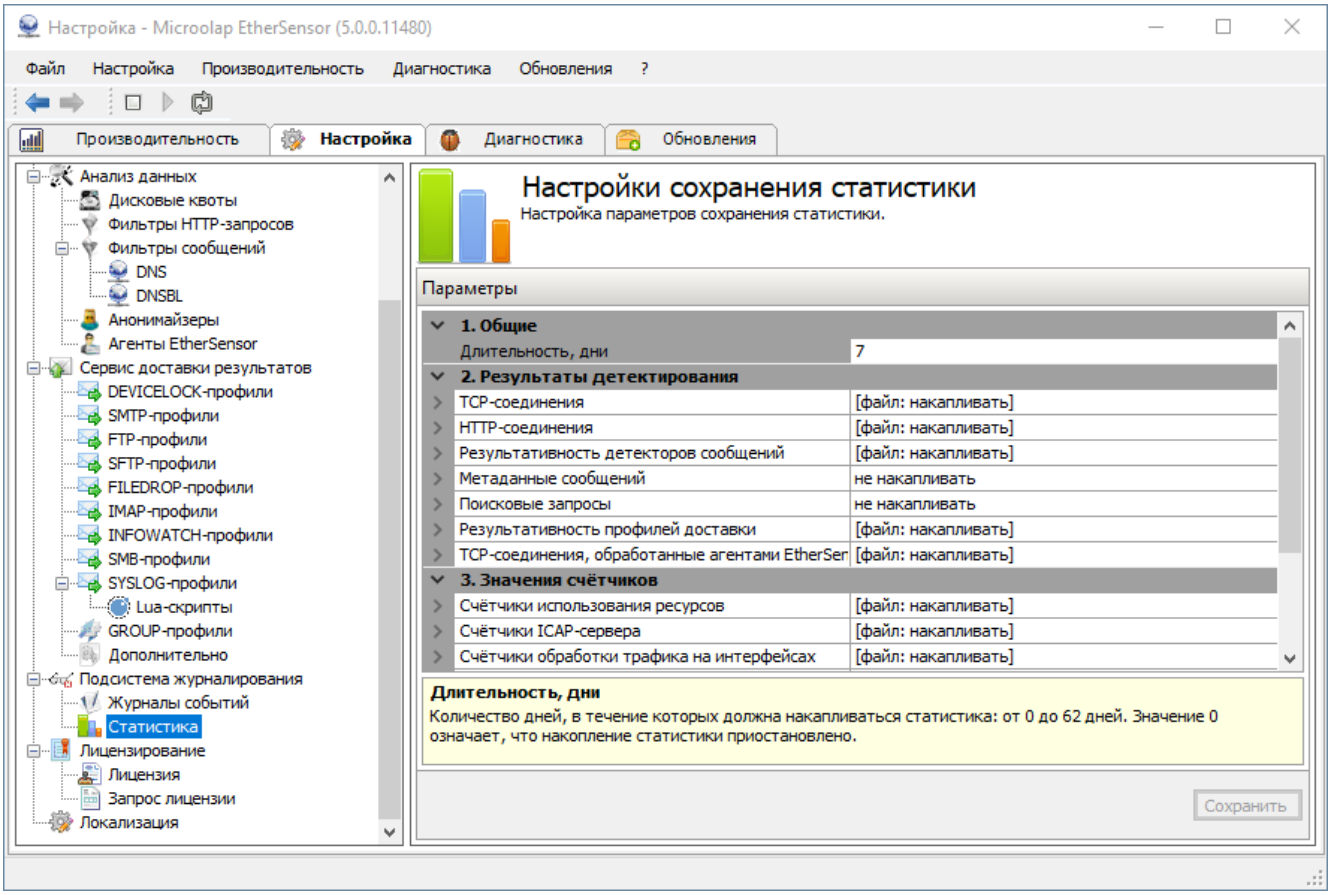

Рис.36. Настройка параметров сохранения статистики.

Полученная статистика накапливается либо в предназначенных для этого локальных директориях, либо может быть отправлена на syslog-сервер.

3.3.2. Ручная настройка (файл конфигурации)

Конфигурация службы **EtherSensor Watcher** содержится в XML-файле **watcher.xml,** расположенном в общей директории конфигураций Microolap EtherSensor **[INSTALLDIR]\config.**

Пример файла конфигурации **watcher.xml**:

```
<?xml version="1.0" encoding="utf-8"?>
<WatcherConfig version="4.1">
  <Syslog>
    <LogRule
      output="file://icap.log"
      maxsize="10Mb"
      encoding="utf-8"
      endline="CR,LF">
        <Channel
          name="ICAP"
          loglevels="all" />
    </LogRule>
    <LogRule
      output="file://icap.err.log"
      maxsize="10Mb"
      encoding="utf-8"
      endline="CR,LF">
        <Channel
          name="ICAP"
          loglevels="error, warning, criterr" />
    </LogRule>
    <LogRule output="file://ethcap.log"
             maxsize="10Mb"
             encoding="utf-8"
             endline="CR,LF">
      <Channel name="ETHCAP"
               loglevels="all" />
    </LogRule>
    <LogRule output="file://ethcap.err.log"
             maxsize="10Mb"
             encoding="utf-8"
             endline="CR,LF">
      <Channel name="ETHCAP"
               loglevels="error, warning, criterr" />
    </LogRule>
    <LogRule output="file://caperrors.log"
             maxsize="10Mb"
             encoding="utf-8"
             endline="CR,LF">
      <Channel name="CAPERR"
               loglevels="all" />
    </LogRule>
    <LogRule output="file://capture.log"
             maxsize="10Mb"
             encoding="utf-8"
             endline="CR,LF">
      <Channel name="CAPMAIN"
               loglevels="all" />
    </LogRule>
    <LogRule output="file://analyser.log"
             maxsize="10Mb"
             encoding="utf-8"
             endline="CR,LF">
      <Channel name="ANALYSER"
               loglevels="all" />
    </LogRule>
    <LogRule output="file://analyser.err.log"
             maxsize="10Mb"
             encoding="utf-8"
             endline="CR,LF">
      <Channel name="ANALYSER"
               loglevels="error, warning, criterr" />
    </LogRule>
    <LogRule output="file://filter.log"
```

```
            maxsize="10Mb"
            encoding="utf-8"
            endline="CR,LF">
      <Channel name="FILTER"
            loglevels="all" />
    </LogRule>
    <LogRule output="file://transfer.log"
            maxsize="10Mb"
            encoding="utf-8"
            endline="CR,LF">
      <Channel name="TRANSFER"
            loglevels="all" />
    </LogRule>
    <LogRule output="file://transfer.err.log"
            maxsize="10Mb"
            encoding="utf-8"
            endline="CR,LF">
      <Channel name="TRANSFER"
            loglevels="error, warning, criterr" />
    </LogRule>
    <LogRule output="file://watcher.log"
            maxsize="10Mb"
            encoding="utf-8" endline="CR,LF">
      <Channel name="WATCHER"
            loglevels="all" />
    </LogRule>
    <LogRule output="file://watcher.err.log"
            maxsize="10Mb"
            encoding="utf-8"
            endline="CR,LF">
      <Channel name="WATCHER"
            loglevels="error, warning, criterr" />
    </LogRule>
    <LogRule output="file://squid-access.log"
             maxsize="10Mb"
             encoding="us-ascii"
             endline="LF">
      <Channel name="SQUID-ACCESS"
             loglevels="all" />
    </LogRule>
  </Syslog>
  <Statistics daysnumber="7">
    <Detection>
      <Sessions>true</Sessions>
      <Hosts>true</Hosts>
      <Detectors>true</Detectors>
      <Messages>false</Messages>
      <Squeries>false</Squeries>
      <TransportProfiles>true</TransportProfiles>
    </Detection>
    <Counters>
      <Performance>true</Performance>
      <Icap>true</Icap>
      <Interfaces>true</Interfaces>
      <Parsers>true</Parsers>
      <Cache>true</Cache>
      <Analysers>true</Analysers>
      <Filters>true</Filters>
      <Quotas>true</Quotas>
      <Transports>true</Transports>
    </Counters>
  </Statistics>
</WatcherConfig>
```

Описание тегов файла конфигурации **watcher.xml**:

Тег WatcherConfig

Является корневым тегом конфигурации службы. В его атрибуте **version** указывается версия конфигурации.

Тег Syslog

Является корневым тегом для конфигурации доступа к syslog-серверам.

Тег LogRule

Определяет конфигурацию для файла журнала. В его атрибуте **output** указывается имя файла журнала, а в атрибуте **maxsize** максимальный размер файла. При достижении максимального размера файл журнала перемещается в поддиректорию **backup**, затем создается новый файл журнала с таким же именем и такими же параметрами. В атрибуте **encoding** указывается кодировка, в которой сохраняются сообщения, а в атрибуте **endline** указывается формат завершения строки сообщения.

Тег Channel

Тег **Channel** является вложенным в тег **LogRule** и содержит название канала сообщений служб, сообщения из которого будут сохранены в файле с именем **output**.

Канал является меткой принадлежности сообщения к службе, и в некоторых случаях детализирует функциональный модуль службы, во время исполнения которого возникло сообщение.

В атрибуте **name** тега **Channel** указывается имя канала. В текущей версии **Microolap EtherSensor** (5.1.0.13519) доступны следующие имена каналов:

Для службы EtherSensor EtherCAP:

ETHCAP
Основной канал сообщений службы;

CAPERR
Канал сообщений об ошибках анализа трафика;

CAPMAIN
Канал сообщений обрабатываемых соединений.

Для службы EtherSensor ICAP:

ICAP
Основной канал сообщений службы;

ICAP-REQUEST
Канал журналирования HTTP-запросов (ответов), принимаемых от ICAP-клиентов.

Для службы EtherSensor LotusTXN:

LOTUSTXN
Основной канал сообщений службы.

Для службы EtherSensor Analyser:

ANALYSER
Основной канал сообщений службы;

FILTER
Канал сообщений службы фильтрации данных службы **EtherSensor Analyser**.

Для службы EtherSensor Transfer:

TRANSFER
Основной канал сообщений службы.

Для службы EtherSensor Watcher:

WATCHER
Основной канал сообщений службы.

В случае, когда служба **EtherSensor Watcher** получила сообщение с именем канала, которого нет в конфигурации, оно будет сохранено в файле **unknown.log.**

Атрибут **loglevel** указывает уровни сообщений, которые могут быть записаны в данный файл журнала.

Возможные варианты:

all
Записываются все сообщения;

criterr
Критические ошибки;

error
Некритические ошибки/недоступность внешних ресурсов (файл, соединение);

warning
Предупреждения: неверные форматы данных, достижение квот и т.п.;

info
Обычные сообщения, сопровождающие нормальную работу;

debug
Отладочные сообщения;

detdebug
Детализированные отладочные сообщения.

Ter DbChangeInterval

Определяет временной интервал в минутах для ротации файлов базы данных счетчиков работы **Microolap EtherSensor**.

Ter Statistics

Является корневым тегом для конфигурации накопления статистики. В его атрибуте **daysnumber** указывается количество дней, в течение которых происходит накопление статистики. Данный параметр может принимать значения в диапазоне от 0 до 62 дней. 0 означает, что накопление статистики приостановлено.

Тег Detection

Тег **Detection** является вложенным в тег **Statistics** и содержит настройки накопления статистики по результатам детектирования сообщений.

Тег Sessions

Тег **Sessions** является вложенным в тег **Statistics** и содержит флаг накопления статистики TCP-соединений. Данная статистика накапливается в формате CSV в директорию **[INSTALLDIR]\data\statistics\YYYY-MM-DD\sessions** и включает в себя следующие параметры отслеживаемых соединений:

- MAC-адрес интерфейса, на котором было перехвачено соединение;
- время создания, время завершения соединения;
- IP-адреса и порты соединения;
- количество данных, переданных от клиента к серверу и обратно, используемый протокол поверх TCP/IP (HTTP, ICQ, SMTP, POP3).

Тег Hosts

Тег **Hosts** является вложенным в тег **Statistics** и содержит флаг накопления статистики HTTP-соединений. Данная статистика накапливается в формате CSV в директориях **[INSTALLDIR]\data\statistics\YYYY-MM-DD\hosts** и включает в себя следующие параметры отслеживаемых соединений:

- MAC-адрес интерфейса, на котором было перехвачено соединение;
- IP-адреса и порты соединения;
- DNS-имя сервера, к которому было выполнено соединение.

Тег Detectors

Тег **Detectors** является вложенным в тег **Statistics** и содержит флаг накопления статистики по результатам работы детекторов сообщений. Данная статистика накапливается в формате CSV в директориях **[INSTALLDIR]\data\statistics\YYYY-MM-DD\detectors** и включает в себя следующие параметры:

- Временная метка события;
- Имя детектора;
- Статус детектирования;
- Количество детектированных сообщений.

Тег Messages

Тег **Messages** является вложенным в тег **Statistics** и содержит флаг накопления метаданных сообщений. Данная статистика накапливается в формате XML в директориях **[INSTALLDIR]\data\statistics\YYYY-MM-DD\messages** и включает в себя метаданные перехваченных сообщений:

- Служебные заголовки сообщений, передаваемые согласно используемого протокола;
- Метаданные, сформированные **Microolap EtherSensor** при обработке сообщений (заголовки **X-Sensor-…**);
- Заголовки **From, To, Cc, Bcc, Subject**.

Тег Squeries

Тег **Squeries** является вложенным в тег **Statistics** и содержит флаг накопления поисковых запросов. Данная статистика накапливается в формате CSV в директориях **[INSTALLDIR]\data\statistics\YYYY-MM-DD\squeries** и включает в себя следующие параметры:

- Временная метка события;
- IP-адрес и порт отправителя поискового запроса;
- DNS-имя поискового сервиса;
- Фраза поискового запроса.

Тег TransportProfiles

Тег **TransportProfiles** является вложенным в тег **Statistics** и содержит флаг накопления статистики по результатам работы транспортных профилей. Данная статистика накапливается в формате CSV в директориях **[INSTALLDIR]\data\statistics\YYYY-MM-DD\transports** и включает в себя следующие параметры:

- Временная метка события;
- Имя транспортного профиля;
- Используемый протокол для отправки сообщения;
- Статус отправки сообщения.

Тег Counters

Тег **Counters** является вложенным в тег **Statistics** и содержит настройки накопления значений счётчиков производительности **Microolap EtherSensor**.

Тег Performance

Тег **Performance** является вложенным в тег **Counters** и содержит флаг накопления показаний счётчиков использования машинных ресурсов. Данная статистика накапливается в формате CSV в директориях **[INSTALLDIR]\data\statistics\YYYY-MM-DD\performance** и включает в себя следующие параметры:

- Временная метка события;
- Использование CPU (текущее, среднее, пиковое);

- Использование памяти (текущее, среднее, пиковое);
- Использование системных потоков;
- Использование дескрипторов системных объектов (файлы, события и т.д.);
- Общие показания загрузки ОС (CPU, память).

Тег Icap

Тег **Icap** является вложенным в тег **Counters** и содержит флаг накопления показаний счётчиков ICAP-сервера. Данная статистика накапливается в формате CSV в директориях **[INSTALLDIR]\data\statistics\YYYY-MM-DD\icap** и включает в себя показания счётчиков службы **EtherSensor ICAP**:

- Временная метка события;
- Количество соединений с ICAP-сервером;
- Количество обрабатываемых запросов (GET, POST, PUT).

Тег Interfaces

Тег **Interfaces** является вложенным в тег **Counters** и содержит флаг накопления показаний счётчиков обработки трафика на сетевых интерфейсах. Данная статистика накапливается в формате CSV в директориях **[INSTALLDIR]\data\statistics\YYYY-MM-DD\interfaces** и включает в себя следующие параметры:

- Временная метка события;
- Счётчики обработанных пакетов;
- Счётчики обрабатываемых TCP-соединений.

Тег Parsers

Тег **Parsers** является вложенным в тег **Counters** и содержит флаг накопления показаний счётчиков детектирования соединений по протоколам. Данная статистика накапливается в формате CSV в директориях **[INSTALLDIR]\data\statistics\YYYY-MM-DD\parsers** и включает в себя следующие параметры:

- Временная метка события;
- Счётчики обрабатываемых TCP-соединений по протоколам (SMTP, POP3, HTTP, FTP.).

Тег Cache

Тег **Cache** является вложенным в тег **Counters** и содержит флаг накопления показаний счётчиков кэша службы анализа. Данная статистика накапливается в формате CSV в директориях **[INSTALLDIR]\data\statistics\YYYY-MM-DD\cache** и включает в себя следующие параметры:

- Временная метка события;
- Счётчики обрабатываемых объектов кэша службы анализа.

Тег Analysers

Тег **Analysers** является вложенным в тег **Counters** и содержит флаг накопления показаний счётчиков детектирования сообщений. Данная статистика накапливается в формате CSV в директориях **[INSTALLDIR]\data\statistics\YYYY-MM-DD\analyser** и включает в себя следующие параметры:

- Временная метка события;
- Счётчики детектирования сообщений службой анализа.

Тег Filters

Тег **Filters** является вложенным в тег **Counters** и содержит флаг накопления показаний счётчиков фильтра HTTP-запросов и фильтра сообщений. Данная статистика накапливается в формате CSV в директориях **[INSTALLDIR]\data\statistics\YYYY-MM-DD\filters** и включает в себя следующие параметры:

- Временная метка события;
- Счётчики фильтров службы анализа (RAW-фильтр HTTP-запросов, фильтр сообщений).

Тег Quotas

Тег **Quotas** является вложенным в тег **Counters** и содержит флаг накопления показаний счётчиков дисковых квот. Данная статистика накапливается в формате CSV в директориях **[INSTALLDIR]\data\statistics\YYYY-MM-DD\quotas** и включает в себя следующие параметры:

- Временная метка события;
- Счётчики использования дисковых квот.

Тег Transports

Тег **Transports** является вложенным в тег **Counters** и содержит флаг накопления показаний счётчиков транспортировки сообщений. Данная статистика накапливается в формате CSV в директориях **[INSTALLDIR]\data\statistics\YYYY-MM-DD\transports** и включает в себя следующие параметры:

- Временная метка события;
- Счётчики транспортировки сообщений.

Примеры конфигурации службы EtherSensor Watcher

Пример 1:

```
<LogRule output="file://example.log"
         maxsize="10Mb"
         encoding="utf-8"
         endline="CR,LF">
  <Channel name="ETHCAP"
           loglevels="criterr" />
  <Channel name="ICAP"
           loglevels="error" />
  <Channel name="ANALYSER"
           loglevels="warning" />
  <Channel name="TRANSFER"
           loglevels="warning" />
  <Channel name="WATCHER"
           loglevels="all" />
</LogRule>
```

Данный вариант конфигурации создаст файл с именем **example.log** и сохранит в нем сообщения для следующих каналов:

- Служба **EtherSensor EtherCAP** - сообщения основного канала **ETHCAP** с уровнем журналирования "критические ошибки";
- Служба **EtherSensor ICAP** - сообщения основного канала **ICAP** с уровнем журналирования "некритические ошибки службы";
- Служба **EtherSensor Analyser** - сообщения основного канала **ANALYSER** с уровнем журналирования "предупреждения";
- Служба **EtherSensor Watcher** - сообщения основного канала **WATCHER** с уровнем журналирования "все сообщения".

Пример 2:

```
<LogRule output="file://error.log"
         maxsize="10Mb"
         encoding="utf-8"
         endline="CR,LF">

  <Channel name="ETHCAP"
           loglevels="error" />
  <Channel name="ICAP"
           loglevels="error" />
  <Channel name="ANALYSER"
           loglevels="error" />
  <Channel name="TRANSFER"
           loglevels="error" />
  <Channel name="WATCHER"
           loglevels="error" />
</LogRule>
```

Данный вариант конфигурации создаст файл с именем **error.log** и сохранит в нем сообщения всех служб **Microolap EtherSensor** с уровнем журналирования "некритические ошибки".

Пример 3:

```
<LogRule output="file://ethercap.log"
         maxsize="10Mb"
         encoding="utf-8"
         endline="CR,LF">

  <Channel name="ETHCAP"
           loglevels="all" />
  <Channel name="CAPERR"
           loglevels="error" />
  <Channel name="CAPMAIN"
           loglevels="error" />
</LogRule>
```

В данном файле будут сохранены сообщения со следующими тегами каналов: **ETHCAP** - все сообщения от службы, **CAPERR** - только ошибки перехвата, **CAPMAIN** - только ошибки обрабатываемых сообщений.

Формат файлов журналов

Файлы журналов представляют собой XML-файлы с содержанием, аналогичным следующему:

```
<Message time="2010-07-12T15:22:27.5390000" level="info">
  <Client channelname="WATCHER"
          processname="watcher.exe"
          modulename="watcher.exe"
          processId="5252" />
  <Text>Start of the application work.</Text>
</Message>
<Message time="2010-07-12T15:22:27.5390000" level="info">
  <Client channelname="WATCHER"
          processname="watcher.exe"
          modulename="watcher.exe"
          processId="5252" />
</Message>
<Message time="2010-07-12T15:28:52.4670000" level="info">
  <Client channelname="WATCHER"
          processname="watcher.exe"
          modulename="watcher.exe"
          processId="5252" />
  <Text>Finish of the application work.</Text>
</Message>
```

Тег Message

Является корневым тегом сообщения, записанного в файл журнала. Атрибут **time** - время отправки сообщения, **level** - под каким приоритетом отправлено сообщение (например, **info** - информационное сообщение, **error** - сообщение о ошибке).

Тег Client

Данный тег описывает отправителя сообщения. Есть следующие атрибуты: **channelname** - имя канала сообщения, **processname** - имя процесса отправителя, **modulename** - имя модуля внутри процесса, создавшего сообщение, **processId** - ID процесса в ОС среды выполнения **Microolap EtherSensor**.

Тег Text

Текст сообщения.

Кроме того, при возникновении критических ситуаций могут встречаться следующие теги:

Тег AdditionalDotNet

Тег описывает **dotNet** сообщение об ошибке (включает в себя информацию об исключительной ситуации, возникшей в результате работы **Microolap EtherSensor** в среде .Net Framework).

Тег AdditionalWin32

Тег описывает Win32 сообщение о ошибке (включает в себя информацию об исключительной ситуации возникшей в результате работы **Microolap EtherSensor** в нативном коде).

3.4. EtherSensor Agent

ПО "EtherSensor Agent" - служба Windows, устанавливаемая на рабочие станции. **EtherSensor Agent** решает две задачи:

- На сервер **Microolap EtherSensor** Агент по UDP-протоколу передаёт информацию о процессе, который создаёт внешние TCP-соединения. Это позволяет решить задачу привязки TCP-сессии к конкретной рабочей станции в случае работы пользователей в терминальной сессии, за NAT и других аналогичных случаях.
- На сервер **EtherStat** Агент по TCP-протоколу на указанный в конфигурации порт и адрес сервера передает информацию о событиях на рабочей станции. При временной невозможности отправки данных (отсутствие соединения и т.п.) происходит их накапливание в локальной базе данных. Как только Агент обнаружит возможность отправить данные, он пакует пакеты по 64Кб и отправляет на сервер.

3.4.1. Условия функционирования Агента

Все специализированные компоненты **ПО "EtherSensor Agent"** функционируют на рабочих станциях, удовлетворяющих следующим системным требованиям:

- ОС (Windows 7, Windows 2008, Windows 8, Windows 8.1, Windows 2012, Windows 10) 32/64 бита.
- Размер необходимого свободного пространства на жестком диске не менее 10 МБ.
- Должны быть выполнены требования по работе со сторонними СЗИ.

Работа со сторонними СЗИ

Для обеспечения стабильной работы **ПО "EtherSensor Agent"** следует учитывать совместимость со сторонними средствами защиты информации (СЗИ) и другими компонентами инфраструктуры:

- **ПО "EtherSensor Agent"** по умолчанию устанавливается в директорию **C:\Program Files\Microolap EtherSensor Agent**. Возможна также установка и в другие директории по выбору администратора. В директории, где установлен **EtherSensor Agent**, расположены рабочие директории. Следует исключать данный путь и все его поддиректории от контроля средств, аналогичных антивирусам, поисковым индексаторам, а также средствам контроля изменения файлов. Подобное ПО не должно блокировать файлы в данной директории и ее поддиректориях от создания, удаления, перемещения и изменения;
- **ПО "EtherSensor Agent"** содержит службу **ethersensor_agent.exe**, которая должна быть разрешена к запуску и работать с правами локальной системы;
- Служба **EtherSensor Agent** требует для нормальной работы возможность обмена информацией по протоколам UDP и TCP с удаленным сервером. СЗИ не должны проверять, модифицировать или ограничивать соединения на сервер, на который **ПО "EtherSensor Agent"** отправляет данные. Аналогично, СЗИ не должны препятствовать службе **EtherSensor Agent** открывать соединения на порты, используемые для передачи информации на сервер **Microolap EtherSensor**.
- **EtherSensor Agent** требует для своей работы регистрации ***Layered Service Provider*** модуля **ethersensor_lsp.dll**. Сторонние СЗИ не должны препятствовать регистрации **ethersensor_lsp.dll** и его работе.
- При установке и функционировании процессы **EtherSensor Agent** используют вызовы, требующие высоких привилегий. Политика безопасности ОС должна позволять операции над драйверами, управление процессами и доступ к сетевым интерфейсам для **ПО "EtherSensor Agent"**.

3.4.2. Установка Агента

Установку **ПО "EtherSensor Agent"** можно производить как в ручном режиме на каждой рабочей станции, так и при помощи групповых политик (GPO) Active Directory.

Для установки Агента в ручном режиме необходимо запустить MSI-инсталлятор (32 или 64 bit), входящий в комплект поставки.

> **Внимание:**
> Для корректной установки **ПО "EtherSensor Agent"** требуются права администратора в том виде, в каком они устанавливаются по умолчанию при установке ОС Windows. Введение искусственных ограничений прав администратора может привести к некорректной работе ПО.

В процессе установки Агента будет установлена служба **EtherSensor Agent** (процесс **ethersensor_agent.exe**), а также в системе будет зарегистрирован ***Layered Service Provider*** - модуль **ethersensor_lsp.dll.**

По умолчанию установка Агента выполняется в директорию **C:\Program Files\Microolap EtherSensor Agent**.

> **Внимание:**
> Для корректной работы установленных экземпляров **EtherSensor Agent** необходимо настроить DNS-сервер сети организации таким образом, чтобы имя сервера, указанное в настройках **EtherSensor Agent**, соответствовало IP-адресу сервера **Microolap EtherSensor**.

Установку также можно произвести через утилиту Windows Installer **msiexec.exe** в командной строке с правами администратора и указать следующие параметры:

INSTALLDIR:
Путь к директории, куда будет установлен **EtherSensor Agent**.

ETHERSTATSERVER:
IP адрес и порт сервера, на котором находится **EtherStat** в формате "адрес:порт".

KEY:
ключ протокола ZeroMQ для безопасного соединения с сервером **EtherStat**, должен содержать 40 символов.

ETHERSENSORSERVER:
IP адрес и порт сервера, на котором находится Microolap EtherSensor в формате "адрес:порт".

Пример:

```
msiexec /i [путь к MSI-дистрибутиву EtherSensor Agent] INSTALLDIR="C:\Program Files\Microolap EtherSensor Agent" ETHERSTATSERVER="etherstat:44445" KEY="0123456789ABCDEFGabcdefg!@#$%^&*<>?-+=^" ETHERSENSORSERVER="ethersens:44444"
```

3.4.3. Состав файлов Агента

Файлы, входящие в пакет установки EtherSensor Agent:

[INSTALLDIR]\config\agent.xml
Текстовый файл конфигурации в формате XML для назначения параметров соединения с серверами **EtherStat** и **Microolap EtherSensor**, периода опроса данных в системе рабочейстанции, а также фильтра приложений, для которых данные о TCP-соединениях не следует отправлять на сервер **Microolap EtherSensor**.

[INSTALLDIR]\syslog.dll
Библиотека, необходимая для создания и ведения всех ***.log** файлов **EtherSensor Agent**.

[INSTALLDIR]\ethersensor_agent.exe
Исполняемый файл **ПО "EtherSensor Agent"**, реализует основные функции Агента. При запуске сервиса необходимо указать один из следующих параметров командной строки:

/service
Запуск в режиме службы Windows;

/process
Запуск в режиме процесса Windows;

/install
Установка службы в ОС;

/remove
Удаление службы ОС.

Если ни один из параметров не был указан, то в файле **[INSTALLDIR]\log\svcagent.log** будет сделана запись о некорректной командной строке с соответствующей подсказкой, и сервис прекратит свою работу.

Файлы, генерируемые в процессе работы:

[INSTALLDIR]\log\svcagent.log
Текстовый файл в формате XML, в который ведется журналирование основных действий и ошибок **ПО "EtherSensor Agent"**.

[INSTALLDIR]\log\ethersensor_agent.exe.log
Текстовый файл для записи информации о событиях, генерируемых внутри подсистемы журналирования **EtherSensor Agent**.

[INSTALLDIR]\log\processinfo.log
Текстовый файл, содержащий информацию о текущих процессах, соединения которых отслеживает **ПО "EtherSensor Agent"**.

[INSTALLDIR]\data.db
Файл базы данных сообщений о событиях, которые не удалось отправить по TCP-соединению на сервер **EtherStat**. При установке соединения с сервером данные будут повторно отправлены, и в случае успешной доставки удалены из базы.

3.4.4. Логические модули Агента

Модуль отслеживания соединений и маркировки HTTP соединений (ethersensor_lsp.dll).

Данный модуль выполнен как ***Layered Service Provider.*** Это означает, что при установке модуля он встраивается в сетевой стек приложений и прозрачно проксирует (при этом отслеживая) все TCP-соединения, создаваемые локальными процессами. Модуль имеет настройки, хранящиеся в реестре Windows:

- UDP порт службы **EtherSensor EtherCAP**. По умолчанию используется порт **44444**.
- Флаг маркировки HTTP-трафика, значение по умолчанию **1**. Если флаг выставлен в состояние **1**, то каждый HTTP-запрос помечается заголовком вида **X-Sensor-UID**: 554E4B4E-4F57-4E20-5555-494400000000, где 554E4B4E-4F57-4E20-5555-494400000000 - уникальный идентификатор пользователя, привязанный к конкретной машине, к конкретному пользователю на данной машине, и являющийся глобальным в контексте сети организации.

В процессе своей работы модуль **ethersensor_lsp.dll** *локально* коммуницирует по протоколу UDP со вторым основным модулем **EtherSensor Agent** - службой **EtherSensor Agent** (процесс **ethersensor_agent.exe**), - и передает ей информацию о процессах, создающих TCP-соединения.

Модуль взаимодействия с сервером Microolap EtherSensor (служба EtherSensor Agent).

Данный модуль выполнен как системная служба Windows, в которой реализованы следующие функции:

- Сбор и передача данных о событиях рабочей станции по шифрованному TCP-соединению на сервер мониторинга и статистики **EtherStat**. Если данные не удалось отправить, то служба **EtherSensor Agent** помещает их в локальную базу данных **[INSTALLDIR]\data.db**.
- Передача по протоколу UDP серверу **Microolap EtherSensor** данных о TCP-соединениях процессов рабочей станции. Настройки позволяют учесть список процессов, соединения которых отслеживать не требуется.
- Учет логов службы и запись их в файл **[INSTALLDIR]\log\svcagent.log**

Настройки конфигурации модуль **ethersensor_agent.exe** берет из **[INSTALLDIR] \config\agent.xml**. При изменении настроек необходимо произвести перезапуск службы **EtherSensor Agent.**

3.4.5. Данные, передаваемые на EtherStat

Агент передает данные на сервер **EtherStat** в двух случаях:

1. Периодически, в соответствии с конфигурацией.

2. При возникновения события, данные о котором **EtherSensor Agent** должен передать в соответствии с конфигурацией.

Периодически отправляемые данные:

Список оборудования
Пересылается только при старте службы **EtherSensor Agent**, далее пересылаются только изменения (по событию изменения). Список содержит структуры данных по установленным устройствам на рабочей станции. Все данные по устройствам получены из их **Свойств**, полученных из **Диспетчера устройств** Windows с помощью соответствующих функций **WinAPI**, и имеют вид:

- Наименование устройства;
- Описание устройства;
- Наименование производителя;
- Соответствующий **Device Id;**

- **GUID Class** устройства в формате {xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx};
- Список **Hardware Ids** устройства;
- Наименование службы, с которой взаимодействует устройство.

Список установленных приложений и служб
Пересылается только при старте службы **EtherSensor Agent**, далее пересылаются только по событию изменения. Список содержит структуры данных по установленному программному обеспечению на рабочей станции. Все данные об установленном ПО извлекаются из реестра Windows с помощью **WinAPI** и имеют вид:

- Наименование продукта;
- Наименование производителя;
- Текущая версия продукта;
- Путь инсталляции продукта.

Ветки реестра, из которых берется информация:

- HKML\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
- HKML\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
- HKEY_USERS**<Просмотр в каждой вкладке>**\Software\Microsoft\Windows\CurrentVersion\Uninstall

Информация об ОС
Пересылается в соответствии с тегом конфигурации **OSMonitor**. Это - данные об ОС Windows на рабочей станции, извлечённые с помощью **WinAPI**:

- Наименование, текущая версия, тип и состояние операционной системы;
- Серийный номер в формате XXXXX-XXXXX-XXXXX-XXXXX;
- Тип архитектуры (x86 или x64);
- Имя компьютера в системе и/или домене;
- Раздел физического диска и директория операционной системы;
- Дата и время последней перезагрузки системы и дата последнего обновления системы (если обновлений не было, то дата установки ОС). Также передается текущее время на рабочей станции;
- Модель и наименование производителя материнской платы;
- Количество запущенных физических и логических процессов;
- Размер файла подкачки операционной системы.

Информация о сетевых адаптерах
Пересылается в соответствии с тегом конфигурации **NETMonitor**. Для каждого адаптера создается отдельное сообщение с его описанием и настройками. Данные по сетевому адаптеру и его конфигурации получаются с помощью функций **WinAPI** и имеют вид:

- Наименование адаптера;
- Наименование производителя;
- MAC-адрес, IP-адреса, маска подсети, настройки DNS-адресов и т.д.;
- Наименование компьютера в в сети и/или домене;
- Флаг использование DHCP;
- **GUID** сетевого адаптера;
- Максимальная скорость передачи данных в сетевом адаптере в битах в секунду.

Данные по текущей загрузке компьютера
Извлекаются с помощью **WinAPI** и содержат:

- Текущую нагрузку на CPU в процентах;
- Текущее использование RAM в процентах;
- Текущее заполнение HDD в процентах;
- Свободное место на HDD.

Данные, отправляемые по событию:

Изменение списка установленного ПО
Создается при обнаружении новых или удалении уже установленных приложений на рабочей станции. Все данные об установленном или удаленном ПО извлекаются из реестра Windows с помощью **WinAPI** и имеют вид:

- Наименование продукта;
- Наименование производителя;
- Текущая версия продукта;
- Путь инсталляции продукта.

Изменение списка установленного оборудования
Создается при обнаружении нового или удаленного устройства на рабочей станции. Все данные по устройствам получены из их **Свойств**, полученных из **Диспетчера устройств** Windows с помощью соответствующих функций **WinAPI** и имеют вид:

- Наименование устройства;
- Описание устройства;
- Наименование производителя;
- Соответствующий **Device Id;**
- **GUID Class** устройства в формате {xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx};
- Список **Hardware Ids** устройства;

- Наименование службы, с которой взаимодействует устройство.

Запуск и завершение процесса с привязкой к TCP-сессии
Создается при обнаружении нового процесса или его завершении. При обнаружении нового процесса будет отправлена структура данных по процессу, содержащая:

- Название процесса;
- Командная строка с аргументами запуска процесса;
- Путь к директории запущенного процесса;
- Время использования пользователем;
- Идентификаторы **ProcessID**, **SessionID** и **ParentID.**

При завершении процесса отправляются идентификаторы **ProcessID** и **SessionID** порождённой процессом сессии.

Данные, отправляемые на сервер при совершении пользователем действий в системе:

При входе пользователя в систему:

- Наименование домена, в который входит пользователь;
- Наименование учетной записи пользователя;
- **SID** - уникальный идентификатор пользователя в ОС;
- **SessionID** - номер сессии на компьютере;
- Наименование способа работы пользователя с рабочей станцией: **console** или **rdp**;
- Дата и время входа пользователя в систему.

При выходе пользователя из системы:

- **SID** - уникальный идентификатор пользователя в ОС;
- **SessionID** - номер сессии на компьютере;
- Дата и время выхода пользователя.

При блокировке или разблокировке учетной записи пользователя:

- **SID** - уникальный идентификатор пользователя в ОС;
- **SessionID** - номер сессии на компьютере.

При изменении активного окна

- Текущий заголовок окна;
- Идентификатор процесса, который владеет этим окном.

3.4.6. Данные, передаваемые на EtherSensor

EtherSensor Agent доставляет полученную информацию на сервер **Microolap EtherSensor** по протоколу UDP.

Агент отправляет на сервер **Microolap EtherSensor** информацию о процессе, который создаёт внешние TCP-соединения:

- Идентификатор процесса;
- Имя процесса;
- Имя пользователя, под которым выполняется процесс;
- Имя компьютера;
- Идентификатор пользователя.

и информацию о самом TCP соединении:

- Идентификатор процесса;
- Идентификатор пользователя;
- Характеристики соединения.

Основываясь на данных, переданных Агентом, сервер **Microolap EtherSensor** будет помечать реконструированные объекты трафика в зависимости от настроек следующими признаками:

- Имя пользователя, под которым выполняется процесс;
- Имя компьютера;
- Идентификатор пользователя вида **X-Sensor-UID**: 554E4B4E-4F57-4E20-5555-494400000000.

3.4.7. Работа с Агентом

Перед запуском в работу **ПО "EtherSensor Agent"** следует произвести следующие настройки:

1. Произвести необходимые настройки конфигурации в файле **[INSTALLDIR] \config\agent.xml** с помощью любого текстового редактора.

2. Запустить **cmd.exe** с правами Администратора**.**

3. Остановить службу **EtherSensor Agent** командой **sc stop "EtherSensor Agent".**

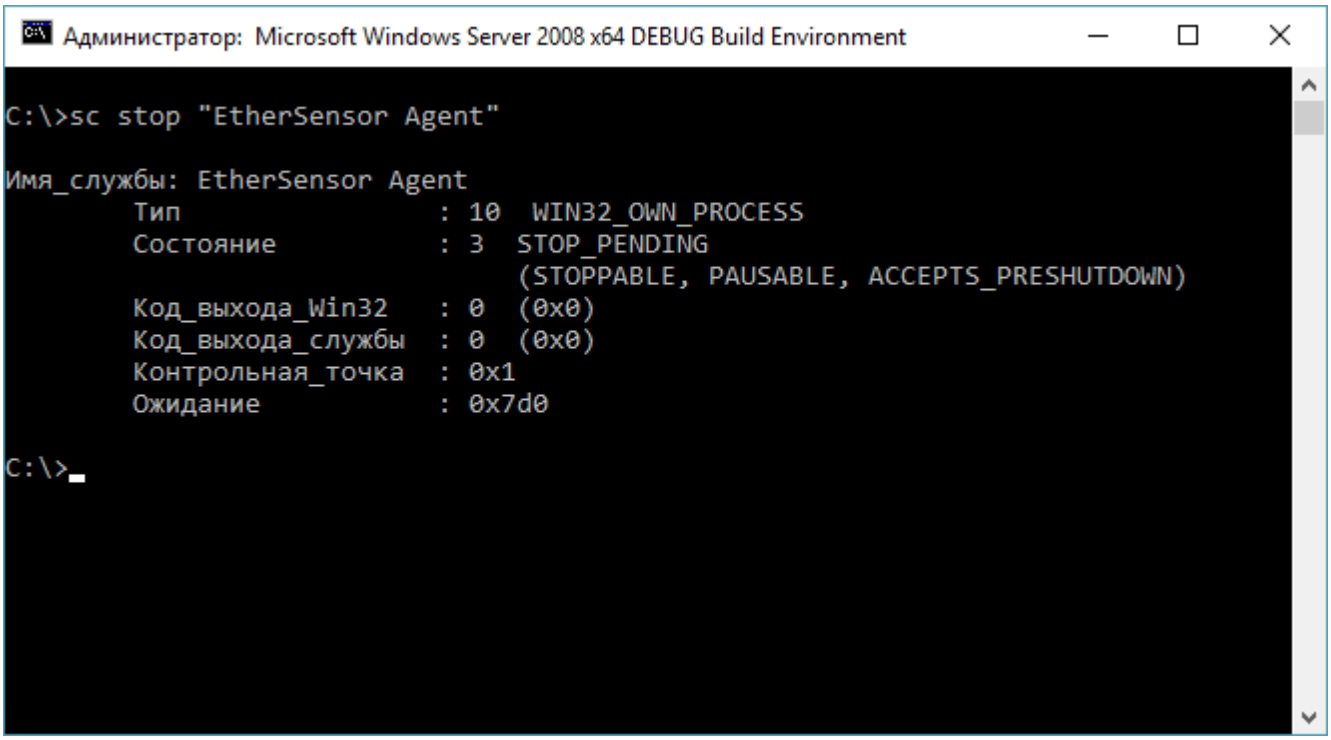

Рис.37. Остановка службы "EtherSensor Agent".

4. Запустить службу **EtherSensor Agent** командой **sc start "EtherSensor Agent".**

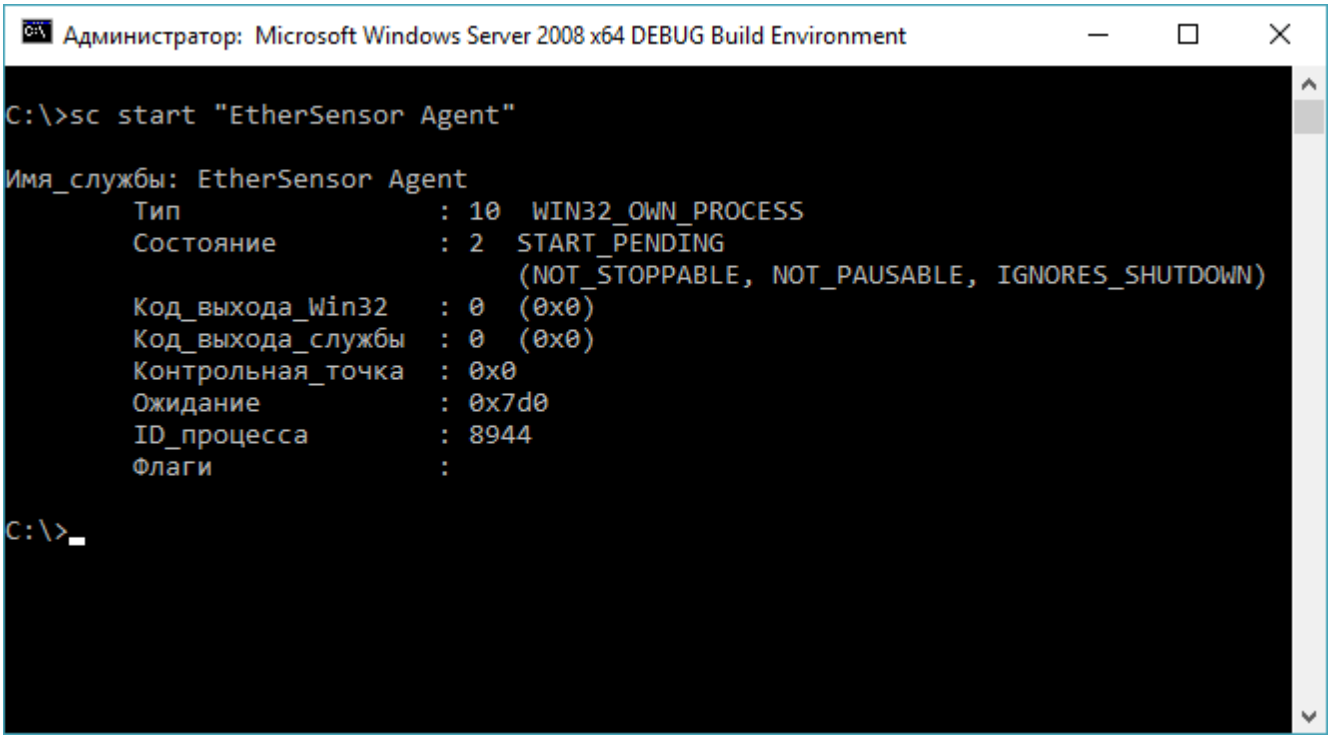

Рис.38. Запуск службы "EtherSensor Agent"

5. Убедиться, что служба запустилась, набрав команду **sc query "EtherSensor Agent"**. Состояние службы должно быть **RUNNING**.

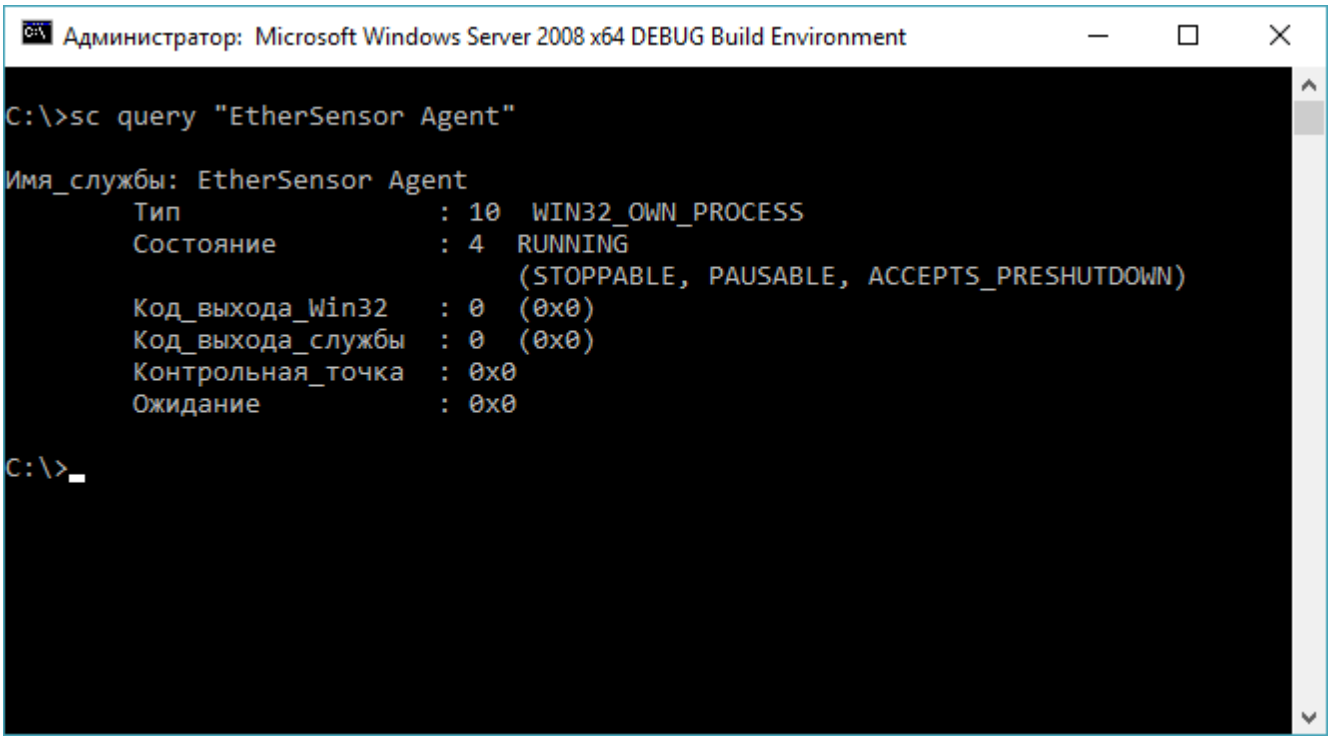

Рис.39. Проверка работы службы "EtherSensor Agent"

3.4.7.1. Возможные варианты работы Агента

Режим работы с сервером EtherStat

Для работы с сервером **EtherStat** необходимо, чтобы рабочие станции, на которых установлено **ПО "EtherSensor Agent"**, находились в одной локальной сети. Сервер **EtherStat** с помощью шифрованного TCP-соединения собирает информацию с рабочих станций, а потом анализирует ее. Для идентификации рабочих станций Агент генерирует уникальный UHID и отправляет в составе сообщения серверу **EtherStat**.

Режим работы прозрачного проксирования без маркировки трафика с сервером Microolap EtherSensor

В данном режиме Агент прозрачно проксирует соединения приложений, запущенных на компьютере пользователя. При успешной установке приложением соединения Агент отправляет на сервер **Microolap EtherSensor** информацию об установлении TCP соединения конкретным приложением, выполняющимся под конкретным пользователем сети.

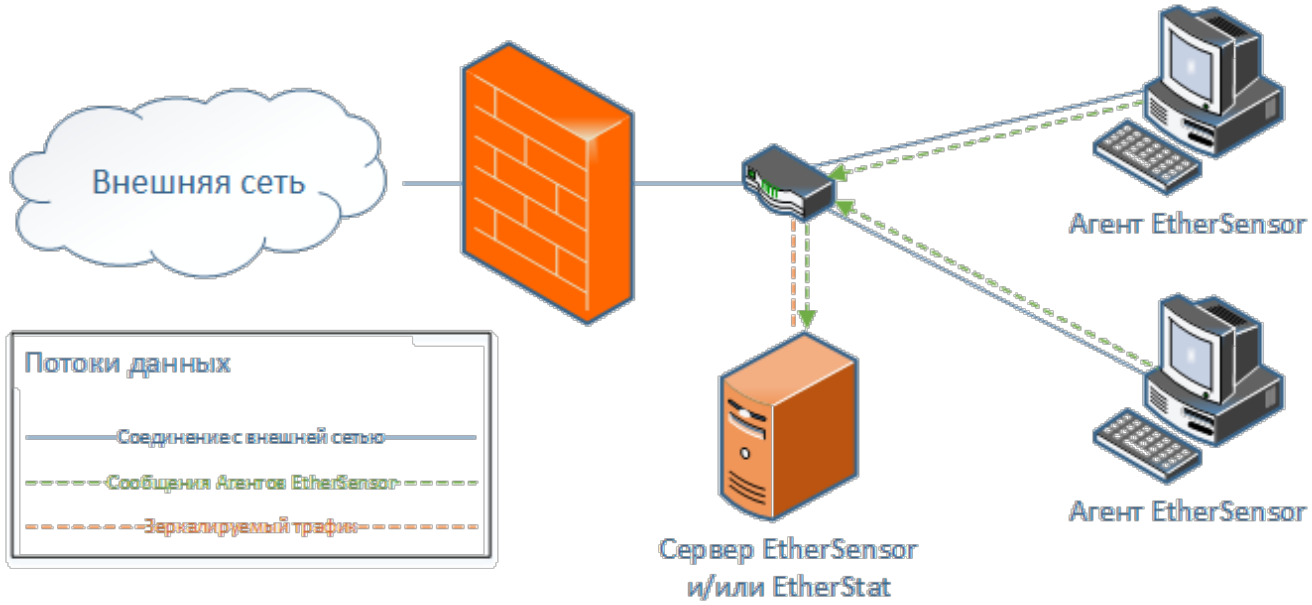

Рис.40. Прозрачное проксирование без маркировки трафика

Таким образом **Microolap EtherSensor** при реконструкции сообщения получает возможность полностью идентифицировать пользователя, отправившего данное сообщение посредством любого поддерживаемого на данный момент протокола (ICQ, MSN, MRA, IRC, XMPP, SMTP, POP3, LOTUS, HTTP, FTP и т.п.).

При этом обязательно должно выполняться условие отвода анализируемого трафика: трафик должен отводиться на **Microolap EtherSensor** до того, как произойдут изменения в параметрах соединений.

Например:

- до прокси-сервера;
- до NAT;
- до межсетевого экрана.

Режим прозрачного проксирования с маркировкой HTTP трафика с сервером Microolap EtherSensor

Данный режим работы Агента отличается от режима без маркировки трафика только тем, что Агент модифицирует на клиентской рабочей станции отправляемые приложениями HTTP-запросы, добавляя в них заголовок **X-Sensor-UID: <GUID>**, где **<GUID>** - уникальный идентификатор пользователя на конкретном компьютере внутри локальной сети. Эти действия выполняются в полном соответствии с HTTP-протоколом, не нарушая его работу.

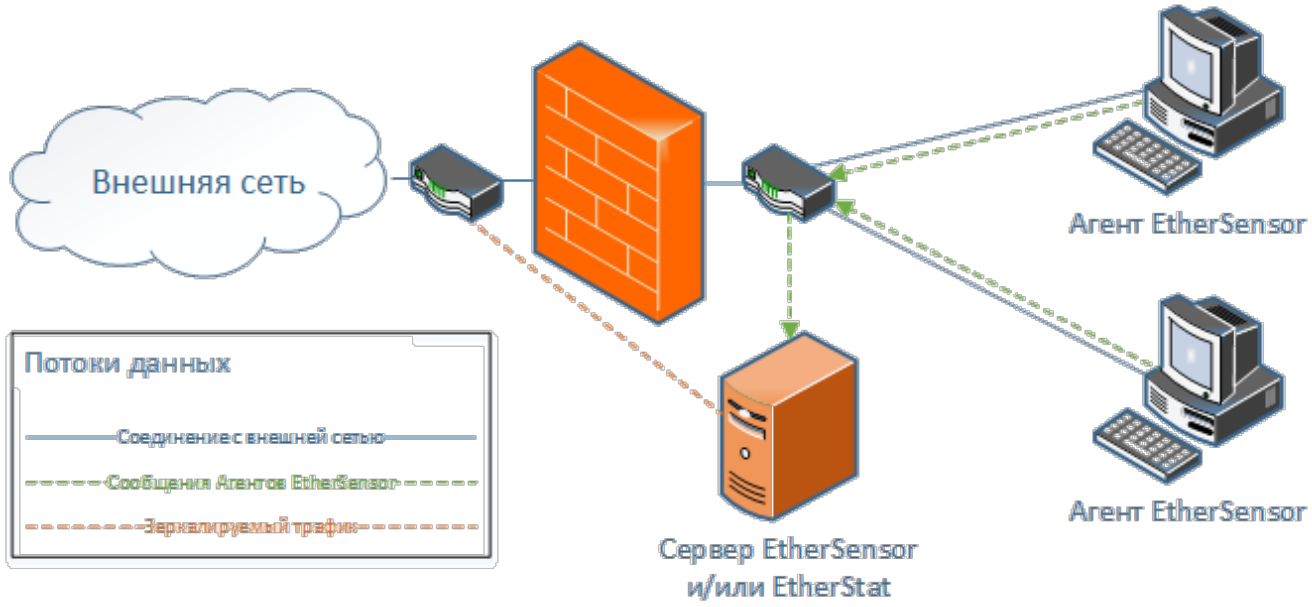

Рис.41. Проксирование с маркировкой трафика

Такой режим работы может использоваться, когда **Microolap EtherSensor** получает отведённый для анализа трафик после модификации параметров соединений. Например, после прохождения соединениями прокси-сервера, NAT или межсетевого экрана.

В этом случае **Microolap EtherSensor** при реконструкции сообщения полностью идентифицирует пользователя сети, отправившего данное сообщение, используя HTTP-протокол.

3.4.7.2. Конфигурирование службы EtherSensor Agent

ПО "EtherSensor Agent" настраивается через внесение изменений в конфигурационный файл **EtherSensor Agent [INSTALLDIR]\config\agent.xml.**

Данные о конфигурации службы **EtherSensor Agent** хранятся в формате XML в файле **agent.xml** в директории **[INSTALLDIR]\config**:

```
<?xml version="1.0" encoding="UTF-8"?>
<Config version="1.1">
  <Local port="44444" markhttp="true" />

  <EtherSensor protocol="2">
    <server address="ethersensor.server1:44444" transport="udp" />
  </EtherSensor>
  <Filter>
    <Excludes>
      <application name="ethersensor_agent.exe" />
      <application name="mstsc.exe" />
      <application name="wmplayer.exe" />
      <application name="uTorrent.exe" />
      <application name="skype.exe" />
      <application name="wmpnetwk.exe" />
      <application name="winlogon.exe" />
      <application name="svchost.exe" />
      <application name="spoolsv.exe" />
      <application name="nissrv.exe" />
    </Excludes>
  </Filter>

  <EtherStat address="127.0.0.1:44445" ZMQKEY="" />
  <DataCollectionSetup>
    <Hardware duration_ms="10000" />
    <Software duration_ms="30000" />
    <OperatingSystem duration_ms="60000" />
    <Processes duration_ms="1000" />
    <Performance duration_ms="60000" />
    <Network duration_ms="60000" />
    <UserMonitor duration_ms="1000" />
    <DatabaseStore size="1" />
  </DataCollectionSetup>
</Config>
```

Тег Config

Является основным тегом конфигурации. Атрибут **version** внутри тега **Config** определяет версию конфигурации.

Тег Local

Тег **Local** является вложенным в тег **Config** и определяет настройки для модуля отслеживания соединений (**ethersensor_lsp.dll**). После загрузки конфигурации служба **EtherSensor Agent** сохраняет данные настройки в реестре Windows.

Атрибут **port** определяет локальный UDP-порт для коммуникации модуля **ethersensor_lsp.dll** со службой **EtherSensor Agent**.

Атрибут-флаг **markhttp** разрешает/запрещает маркировку HTTP-трафика модулем **ethersensor_lsp.dll**.

Тег **Local** является вложенным в тег **Config** и определяет настройки для модуля отслеживания соединений (**ethersensor_lsp.dll**). После загрузки конфигурации служба **ethersensor_agent.exe** сохраняет данные настройки в реестре Windows.

Атрибут **port** определяет локальный UDP-порт для коммуникации модуля **ethersensor_lsp.dll** со службой **EtherSensor Agent**.

Атрибут-флаг **markhttp** разрешает/запрещает маркировку HTTP-трафика модулем **ethersensor_lsp.dll**.

Тег **Local** является вложенным в тег **Config** и определяет настройки для модуля отслеживания соединений (**ethersensor_lsp.dll**). После загрузки конфигурации служба **ethersensor_agent.exe** сохраняет данные настройки в реестре Windows.

Атрибут **port** определяет локальный UDP-порт для коммуникации модуля **ethersensor_lsp.dll** со службой **EtherSensor Agent**.

Атрибут-флаг **markhttp** разрешает/запрещает маркировку HTTP-трафика модулем **ethersensor_lsp.dll**.

Тег EtherSensor

Тег **EtherSensor** является вложенным в тег **Config** и определяет список адресов серверов **Microolap EtherSensor**, с которыми коммуницирует **EtherSensor Agent** для передачи информации по протоколу UDP о процессах, создающих TCP-соединения для привязки рабочей станции к TCP-сессии.

Атрибут **protocol** определяет максимальную версию протокола, используемую **ПО "EtherSensor Agent"** для отправки сообщений на сервер **Microolap EtherSensor**. На сегодняшний день доступна **3** версия протокола. Для поддержки данной версии протокола необходимо использовать **Microolap EtherSensor** версии **4.3.3** или старше. Для совместимости с предыдущими версиями **Microolap EtherSensor** необходимо выставить данное поле в значение **2**.

Тег server

Тег **server** является вложенным в тег **EtherSensor** и определяет адрес и транспортный протокол сервера **Microolap EtherSensor**.

Атрибут **address** определяет адрес и порт для связи с сервером **Microolap EtherSensor**. Возможные варианты адресов - **IP:Port** или **DNSNAME:Port**.

Атрибут **transport** определяет тип транспортного протокола для связи с сервером **Microolap EtherSensor**. Возможные варианты - **udp**.

Тег Filter

Тег **Filter** является вложенным в тег **Config** и определяет настройки фильтра сообщений, отправляемых на сервер **Microolap EtherSensor**.

Тег Excludes

Тег **Excludes** является вложенным в тег **Filter** и определяет список приложений, информацию о TCP-соединениях которых не следует отправлять на сервер **Microolap EtherSensor**.

Тег application

Тег **application** является вложенным в тег **Excludes** и определяет приложение, информация о TCP-соединениях которого не будет отправлена на сервер **Microolap EtherSensor**.

Атрибут **name** определяет точное имя отслеживаемого процесса.

Таким образом, в процессе работы **EtherSensor Agent** сообщает серверу **Microolap EtherSensor** только о TCP-соединениях, которые создаются для связи с другими рабочими станциями и серверами в локальной сети и сети Интернет, причем настройки позволяют учесть список процессов, соединения которых отслеживать не требуется.

Тег EtherStat

Является вложенным в тег **Config** и определяет настройки для соединения к системе мониторинга и статистики **EtherStat**.
Атрибут **address** определяет адрес сервера в формате **"IP-адрес:порт"**.
Атрибут **ZMQKEY** должен содержать ключ для конечной работы в режиме шифрования соединения.

Тег DataCollectionSetup

Является вложенным в тег **Config** и определяет настройки таймеров опроса данных для службы **EtherSensor Agent**.

Тег Hardware

Является вложенным в тег **DataCollectionSetup** и определяет с помощью атрибута **duration_ms** настройки таймера в секундах для опроса текущего оборудования.

Тег Software

Является вложенным в тег **DataCollectionSetup** и определяет с помощью атрибута **duration_ms** настройки таймера в секундах для опроса текущего установленного программного обеспечения.

Тег OperatingSystem

Является вложенным в тег **DataCollectionSetup** и определяет с помощью атрибута **duration_ms** настройки таймера в секундах для опроса данных об ОС.

Тег Processes

Является вложенным в тег **DataCollectionSetup** и определяет с помощью атрибута **duration_ms** настройки таймера в секундах для мониторинга текущих процессов.

Тег Network

Является вложенным в тег **DataCollectionSetup** и определяет с помощью атрибута **duration_ms** настройки таймера в секундах для опроса данных о сетевых адаптерах и их настройках.

Тег Performance

Является вложенным в тег **DataCollectionSetup** и определяет с помощью атрибута **duration_ms** настройки таймера в секундах для опроса данных о производительности ОС.

Тег Users

Является вложенным в тег **DataCollectionSetup** и определяет с помощью атрибута **duration_ms** настройки таймера в секундах для мониторинга действий пользователя.

Тег DatabaseSetup

Является вложенным в тег **DataCollectionSetup** и определяет настройки лимита размера базы данных в процентах от свободного места на HDD, на котором установлен **EtherSensor Agent**.

3.4.7.3. Журналирование работы Агента

EtherSensor Agent ведёт журналирование своих действий в файлы в директории **[INSTALLDIR]\log**, помещая данные в следующие файлы:

- В файл **svcagent.log** заносится информация об основных действиях, выполняемых службой **EtherSensor Agent**.
- В файл **ethersensor_agent.exe.log** заносится информация о событиях, генерируемых внутри службы журналирования **EtherSensor Agent**.
- В файл **processinfo.log** заносится информация о текущих процессах, соединения которых отслеживает **EtherSensor Agent**.

Файлы журналов (**svcagent.log**, **ethersensor_agent.exe.log**) представляют собой XML-файлы следующего содержания:

```
<Message time="2012-03-23T17:47:48.148+04:00" level="information">
  <Client channelname="MICROOLAPAGENT"
          processname="ethersensor_agent.exe"
          modulename="ethersensor_agent.exe" />
  <Text>Start of the application.</Text>
</Message>
```

Тег Message

Является корневым тегом сообщения, записанного в файл журнала. Атрибут **time** - время отправки сообщения, **level** - под каким приоритетом отправлено сообщение (например, **information** - информационное сообщение, **error** - сообщение об ошибке).

Тег Client

Данный тег описывает отправителя сообщения. Есть следующие атрибуты: **channelname** - имя канала сообщения, **processname** - имя процесса отправителя, **modulename** - имя модуля внутри процесса, создавшего сообщение.

Тег Text

Текст сообщения.

Файл **processinfo.log** представляет собой XML-файл следующего содержания:

```
<?xml version="1.0" encoding="UTF-8"?>
<Processes>

  <Process pid="4136" name="chrome.exe">
    <User uuid="32014294-5bbf-11e1-b8f5-005056c00808"
          name="Home-PC\Home"/>
    <Sessions local="0" remote="311"/>
  </Process>

  <Process pid="636" name="svchost.exe">
    <User uuid="3a45de5b-5be6-11e1-b8f5-005056c00808"
          name="HOME\HOME-PC$"/>
    <Sessions local="0" remote="3"/>
  </Process>

  <Process pid="948" name="firefox.exe">
    <User uuid="32014294-5bbf-11e1-b8f5-005056c00808"
          name="Home-PC\Home"/>
    <Sessions local="2" remote="741"/>
  </Process>

  <Process pid="1584" name="googletalk.exe">
    <User uuid="32014294-5bbf-11e1-b8f5-005056c00808"
          name="Home-PC\Home"/>
    <Sessions local="0" remote="89"/>
  </Process>

  <Process pid="2860" name="uTorrent.exe">
    <User uuid="32014294-5bbf-11e1-b8f5-005056c00808"
          name="Home-PC\Home"/>
    <Sessions local="100" remote="27084"/>
  </Process>

  <Process pid="3076" name="vmware.exe">
    <User uuid="32014294-5bbf-11e1-b8f5-005056c00808"
          name="Home-PC\Home"/>
    <Sessions local="4" remote="1"/>
  </Process>

  <Process pid="3908" name="NisSrv.exe">
    <User uuid="fb91c5e7-5eec-11e1-b226-005056c00808"
          name="NT AUTHORITY\LOCAL SERVICE"/>
    <Sessions local="0" remote="1"/>
  </Process>
</Processes>
```

Тег Processes

Является основным тегом отображаемого списка отслеживаемых процессов.

Тег Process

Тег **Process** является вложенным в тег **Processes**. Данный тег описывает отслеживаемый процесс. Есть следующие атрибуты: **pid** - идентификатор процесса в ОС среды выполнения, **name** - имя отслеживаемого процесса.

Тег User

Тег **User** является вложенным в тег **Process**. Данный тег описывает пользователя в локальной системе, под чьими правами выполняется отслеживаемый процесс. Есть следующие атрибуты: **uuid** - идентификатор пользователя, **name** - имя пользователя.

Тег Sessions

Тег **Sessions** является вложенным в тег **Process**. Данный тег описывает отслеживаемые соединения процесса. Есть следующие атрибуты: **local** - количество локальных соединений, выполненных внутри процесса или между процессами, **remote** - количество удалённых соединений, выполненных данным процессом.

3.4.7.4. Проблемы и решения

Не стартует служба EtherSensor Agent.

- Проверить в конфигурации **EtherSensor Agent** настройку портов для серверов **Microolap EtherSensor**, **EtherStat,** а так же настройку локального порта: теги **Local**, **EtherSensor** и **EtherStat**. Порты не должны совпадать. Из-за этого служба не может продолжать корректно работать и завершает свой процесс.
- Необходимо проверить файлы журналов (**svcagent.log**, **ethersensor_agent.exe.log**) на наличие в них сообщений об ошибках работы **EtherSensor Agent**.
- Необходимо проверить журналы Windows на наличие в них сообщений об ошибках работы **EtherSensor Agent**.
- Сообщить об инцидентах в службу поддержки.

После старта EtherSensor Agent файл processinfo.log не отображает ни одного отслеживаемого процесса.

- Не подключена сетевая карта или отключен стек TCP/IP. Убедитесь, что система создаёт TCP-оединения, например загрузив браузер и открыв любую страницу. После этих действий в файле **processinfo.log** должна отобразиться информация о процессе браузера.
- Данный компьютер входит в домен. В таком случае модули **EtherSensor Agent**, загруженные в процессы, которые создают TCP-соединения, пытаются получить имя пользователя в домене, с чьими правами выполняется процесс. В данном случае очень важно, чтобы были правильно выставлены настройки DNS отслеживаемой ОС, так как системное API, которое предоставляет информацию об имени пользователя в домене, использует настройки DNS.

Ни одно приложение в системе не может создать удалённого соединения, но до инсталляции EtherSensor Agent в систему таких проблем не было.

- Перейдите в директорию инсталляции **EtherSensor Agent** и выполните команду **ethersensor_instlsp.exe -p > log.txt**. Данная команда запишет в файл **log.txt** список установленных провайдеров сетевого стека ОС.
- Проанализируйте самостоятельно файл **log.txt** и при необходимости вышлите в службу поддержки.

- Выполните команду **ethersensor_instlsp.exe -f -c b**. Данная команда отключит модуль слежения **EtherSensor Agent ethersensor_lsp.dll**. Запустите новую копию браузера и откройте удалённую страницу. Если страница открылась, значит проблемы действительно в модуле слежения **ethersensor_lsp.dll**. В противном случае проблема не связана с модулем слежения **EtherSensor Agent**.

Microolap EtherSensor не идентифицирует пользователя перехваченного сообщения

- Проверьте конфигурацию **EtherSensor Agent**: тег **EtherSensor**, затем тег **server**. Атрибут **address** тега **server** должен содержать корректное DNS-имя сервера **Microolap EtherSensor**, которое правильно определяется на данной рабочей станции. Если указан IP-адрес, проверьте доступность IP-адреса сервера **Microolap EtherSensor** (например, при помощи утилиты **ping**).

Сервер EtherStat не получает сообщения от EtherSensor Agent:

- Необходимо проверить файл **svcagent.log** на наличие в них сообщений об ошибках **EtherSensor Agent**.
- Проверить конфигурацию соединения с сервером **EtherStat**: тег **EtherStat**. Атрибут **address** тега должен содержать IP-адрес, по которому происходит соединение. Атрибут **key** содержит открытый ключ для шифрованного соединения. Этот ключ должен совпадать с открытым ключом сервера **EtherStat.**
- Проверить доступность IP-адреса сервера **EtherStat** (например, при помощи утилиты **ping**).
- Проверить конфигурацию времени обработки информации в тегах **OSMonitor**, **HWMonitor**, **SWMonitor**, **UserMonitor**, **NetMonitor** и **ProcMonitor**. Если атрибут **timer** установлен в **0**, то сообщения соответствующих событий обрабатываться не будут, следовательно, не будут отправляться и на сервер **EtherStat**.

4. Анализ событий и объектов

Служба **EtherSensor Analyser** предназначена для детектирования, фильтрации и анализа извлечённых из трафика объектов.

Служба анализирует объекты протоколов уровня приложений согласно модели OSI, полученные от служб **EtherSensor EtherCAP, EtherSensor ICAP** и **EtherSensor LotusTXN** с целью детектирования сообщений, передаваемых пользователями сети с распознаванием их принадлежности к определённым Интернет-сервисам. Извлечённые из трафика сообщения проходят этап анализа, в результате которого проверяются их следующие параметры:

- Сетевые адреса участников коммуникации;
- Доменные адреса участников коммуникации;
- Адреса электронной почты (**from, to, cc, bcc**);
- Идентификаторы пользователей клиентов мгновенных сообщений (**ICQ, MRA, MSN, IRC, XMPP**);

- Идентификаторы пользователей социальных сетей;
- Содержимое текстовых полей сообщений (**subject, body**);
- Имена передаваемых вложений;
- Размеры сообщений.

На основе заранее заложенной в правилах фильтрации логики, фильтрующий механизм службы принимает решение:

1. о прекращении обработки сообщения;

2. о транспортировке сообщения системе-потребителю (DLP, UEBA, архив, eDiscovery-система, Enterprise Search и т.п.);

3. о формировании произвольной строки на основе данных, извлечённых из сообщения (как правило, syslog-строка для SIEM-системы).

Общая схема работы службы **EtherSensor Analyser:**

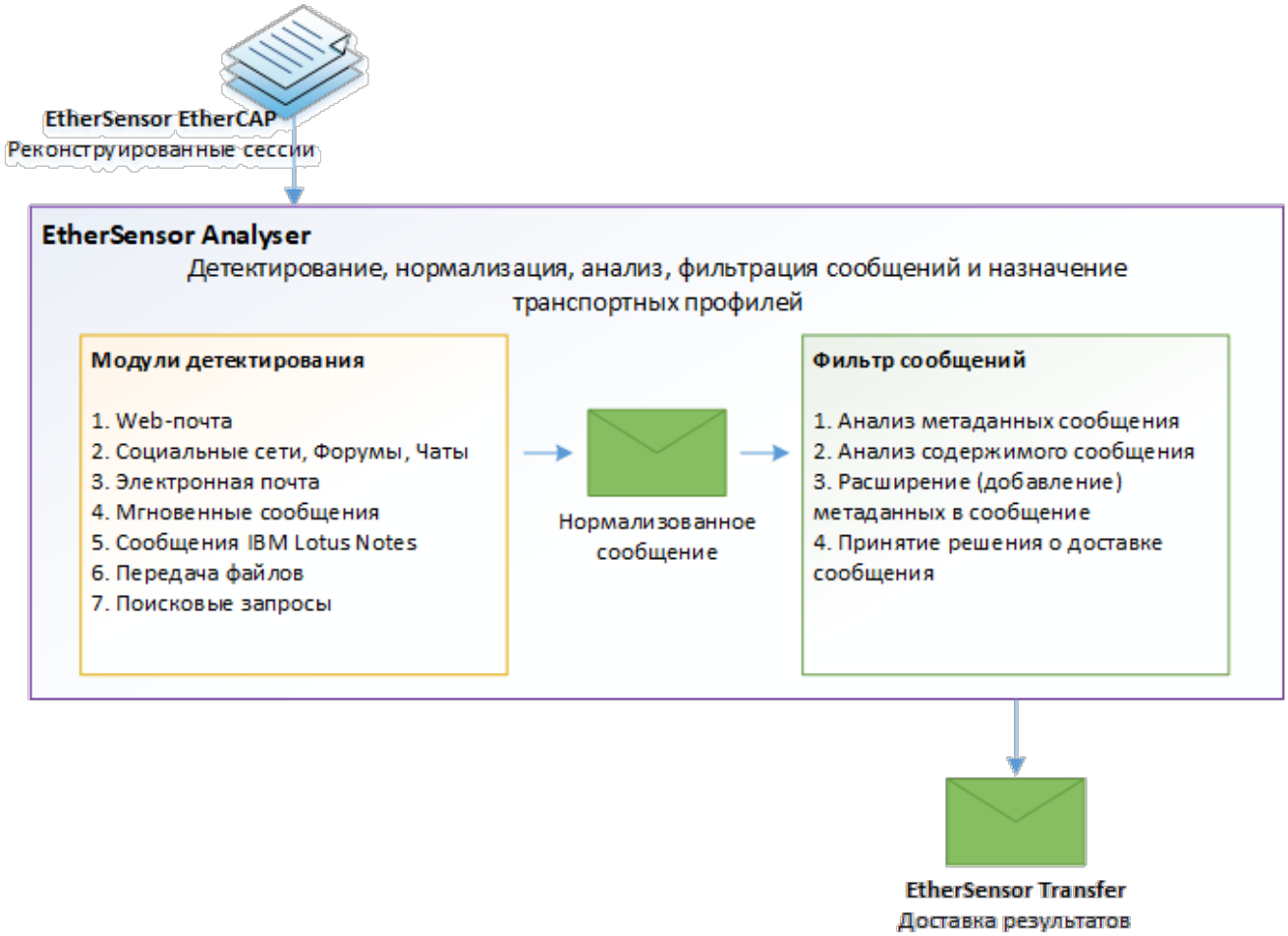

Рис.42. Схема работы службы EtherSensor Analyser.

Фильтрующий механизм службы настраивается с помощью отдельного файла конфигурации, в котором описывается логика обработки распознанных сообщений. Идеология обработки сообщений строится на формировании цепочек правил, которые объединяются в таблицы.

Сообщение проходит проверку правилами, которые в зависимости от того, подпадает сообщение под действие правила или нет, могут изменять содержимое сообщения, его метаданные или ход его дальнейшей обработки. Такая идеология схожа с правилами фильтрации, используемыми в утилите UNIX-систем **iptables**.

Общая схема обработки сообщения механизмом фильтрации:

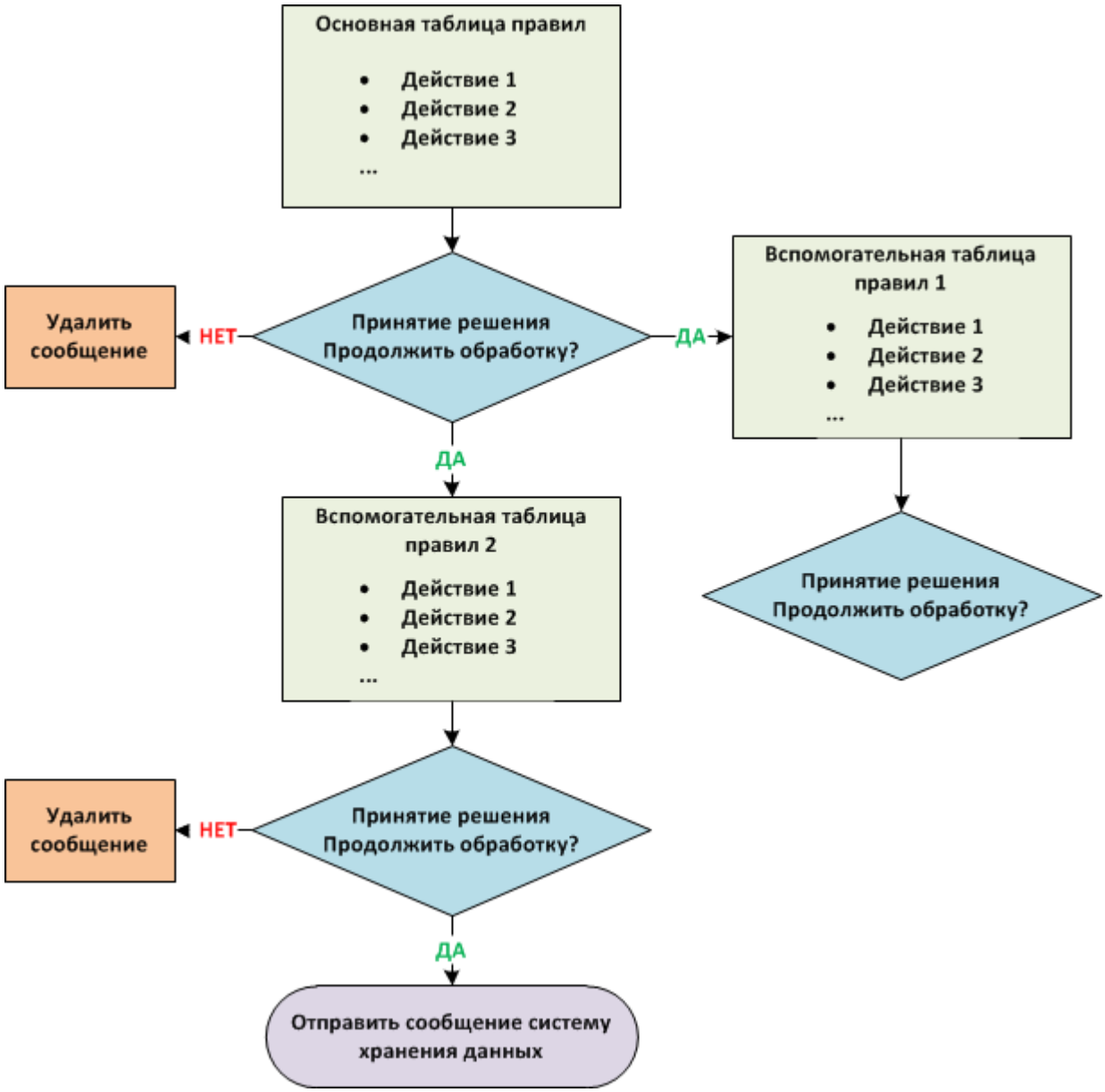

Рис.43. Схема обработки сообщения службой EtherSensor Analyser.

Параметры командной строки

Служба Windows **EtherSensor Analyser** в ходе инсталляции **Microolap EtherSensor** устанавливается с автоматическим запуском. Однако, при необходимости процесс **ethersensor_analyser.exe** можно запустить как приложение Windows со следующими параметрами командной строки:

/process

Запускает процесс **ethersensor_analyser.exe** как обычный Windows Win32-процесс (возможно использовать для отладки).

/service

Запускает как службу Windows.

/config

Сохраняет конфигурацию службы по умолчанию.

4.1. Настройка в конфигураторе

Помимо прямого редактирования файла конфигурации службы **EtherSensor Analyser**, возможна ее настройка посредством графического интерфейса утилиты конфигурирования **Microolap EtherSensor** (файл **ethersensor_console.exe** из поставки).

Дисковые квоты сохранения перехваченных объектов

Перехваченные объекты могут сохраняться службой **EtherSensor Analyser** на файловой системе для последующего анализа. Для настройки выделенных для хранения таких объектов дисковых квот используется форма в левом окне конфигуратора (файл **ethersensor_console.exe** из поставки **Microolap EtherSensor**):

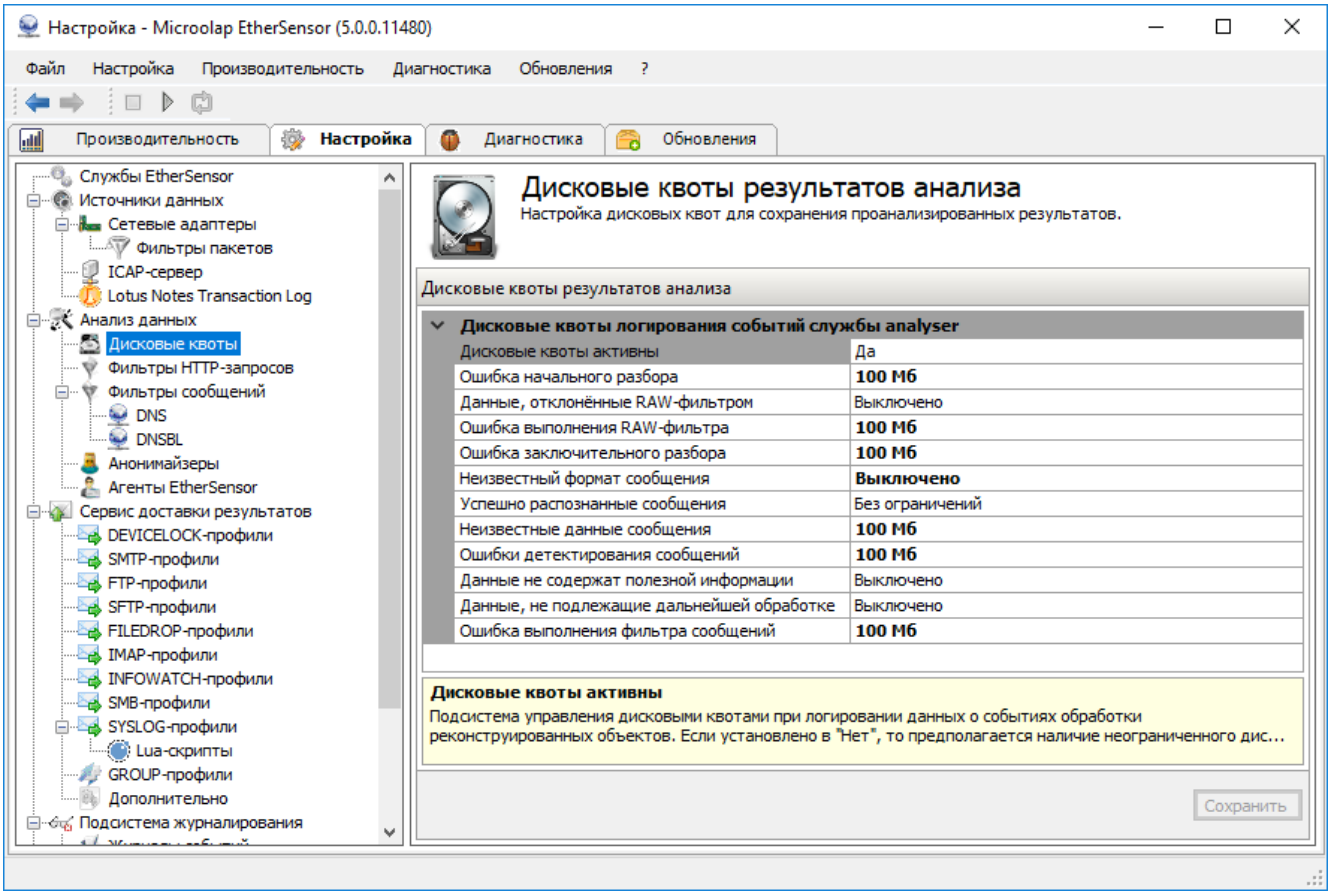

Рис.44. Настройки службы EtherSensor Analyser.

Дисковые квоты активны:

Разрешение/запрещение использования квот. Если установлено в **Нет**, то предполагается наличие неограниченного дискового пространства.

Ошибка начального разбора:

Журналирование ошибок предварительного разбора извлечённых объектов: TCP-сессия успешно реконструирована, но при разборе объекта произошла ошибка, вызванная, как правило, нарушениями протокола (например, add-on к браузеру в POST запросе устанавливает в конце строки байт **00** вместо **0D0A**). Объекты помещаются в директорию **[INSTALLDIR]\data\results\errors\preparse**.

Данные, отклонённые RAW-фильтром

Журналирование данных, отклонённых RAW-фильтром. Используется для отладки или тестирования логики работы RAW-фильтра. Объекты помещаются в директорию **[INSTALLDIR]\data\results\errors\rawfiltered**.

Ошибка выполнения RAW-фильтра

Журналирование ошибок выполнения RAW-фильтра. Объекты помещаются в директорию **[INSTALLDIR]\data\results\errors\rawfilter.**

Ошибка заключительного разбора

Журналирование ошибок разбора извлечённых объектов: TCP-сессия успешно реконструирована, но при разборе объекта произошла ошибка, вызванная, как правило, нарушениями протокола (например, add-on к браузеру в POST запросе устанавливает в конце строки байт **00** вместо **0D0A**). Объекты помещаются в директорию **[INSTALLDIR] \data\results\errors\parse**.

Неизвестный формат сообщения

Журналирование ошибок, вызванных тем, что системе неизвестен формат объекта: данные TCP-сессии успешно реконструированы, но в текущей версии отсутствует детектор сообщений такого типа. Объекты помещаются в директорию **[INSTALLDIR] \data\results\unknown**.

Успешно распознанные сообщения

Журналирование событий об успешно распознанных объектах: данные TCP-сессии успешно реконструированы, сообщение распознано и передано службе **EtherSensor Transfer** для доставки системе-потребителю. Объекты помещаются в директорию **[INSTALLDIR]\data\results\detect\ok**.

Неизвестные данные сообщения

Журналирование ошибок, касающихся объектов распознанных, но содержащих неизвестные данные: TCP-сессия успешно реконструирована, детектор, соответствующий данному типу сообщений, отработал, но ему не удалось извлечь все данные - скорее всего, изменился формат сообщения. Объекты помещаются в директорию **[INSTALLDIR] \data\results\detect\unknown**.

Ошибки детектирования сообщений

Журналирование ошибок детектирования сообщений. Объекты помещаются в директорию **[INSTALLDIR]\data\results\errors\detect**.

Данные не содержат полезной информации

Журналирование данных, которые были успешно распознаны, но не содержат полезных данных для дальнейшей обработки. Объекты помещаются в директорию **[INSTALLDIR] \data\results\detect\noobjects**.

Данные, не подлежащие дальнейшей обработке

Журналирование данных, которые изначально не несут полезной информации, так как являются служебными данными, передаваемыми в процессе взаимодействия пользователя с интернет сервисом. Такие данные не подлежат дальнейшей обработке. Объекты помещаются в директорию **[INSTALLDIR]\data\results\detect\filtered**.

Ошибка выполнения фильтра сообщений

Журналирование ошибок обработки фильтром сообщений. Объекты помещаются в директорию **[INSTALLDIR]\data\results\errors\msgfilter.**

Предварительная фильтрация HTTP-объектов

Управление фильтрацией перехваченных HTTP-запросов происходит в окне **Фильтры HTTP-объектов** конфигуратора:

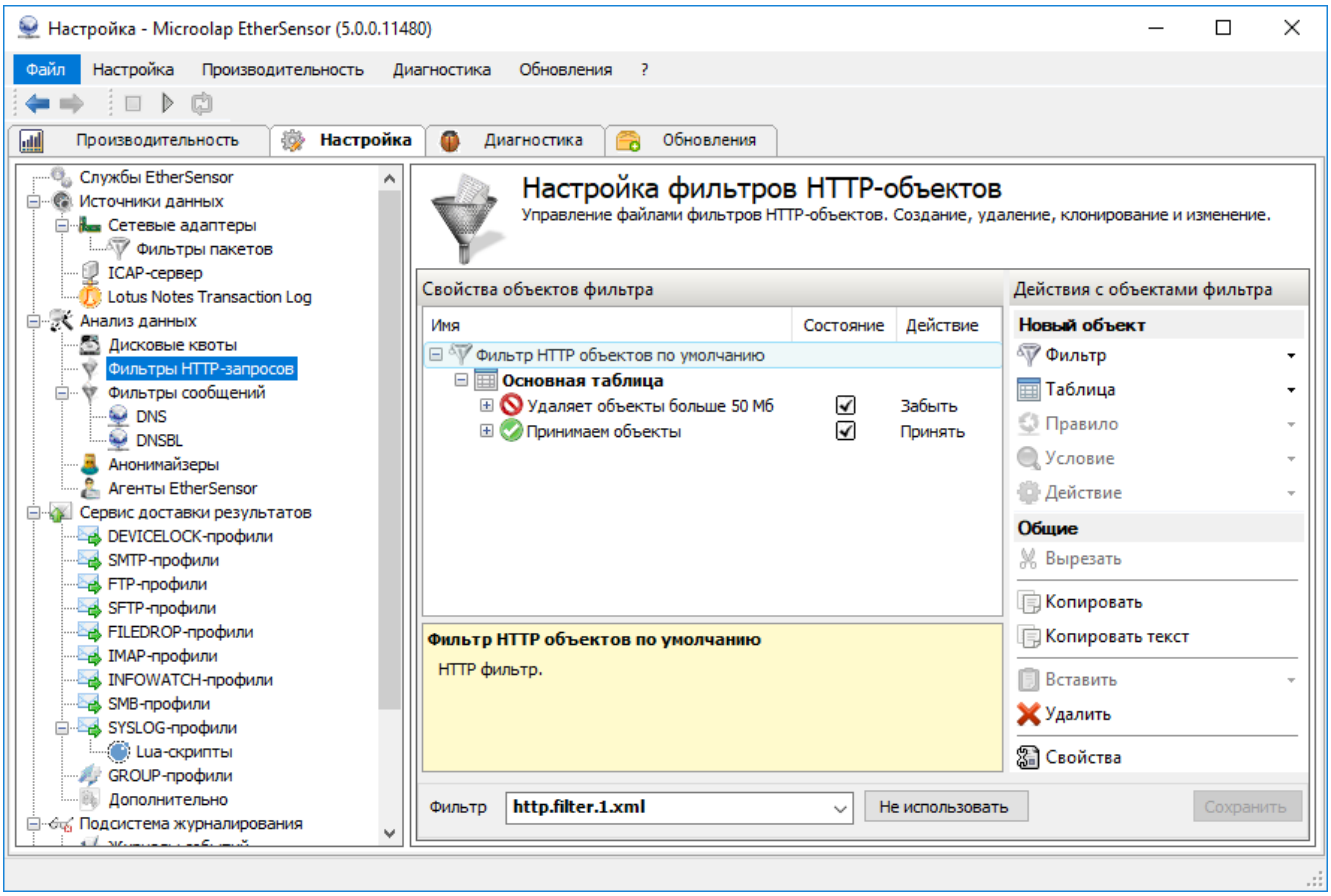

Рис.45. Управление фильтрацией HTTP-объектов.

Предварительная фильтрация HTTP-объектов применяется в основном для снижения нагрузки на сенсор, подробнее ознакомиться с работой этой функции можно в разделе "Префильтрация HTTP-запросов".

Фильтрация реконструированных сообщений

Управление фильтрацией перехваченных сообщений происходит в окне **Фильтры сообщений** конфигуратора. Правила фильтрации перехваченных объектов хранятся в XML-файлах, находящихся в директории **[INSTALLDIR]\data\statistics\YYYY-MM-DD\filters**.

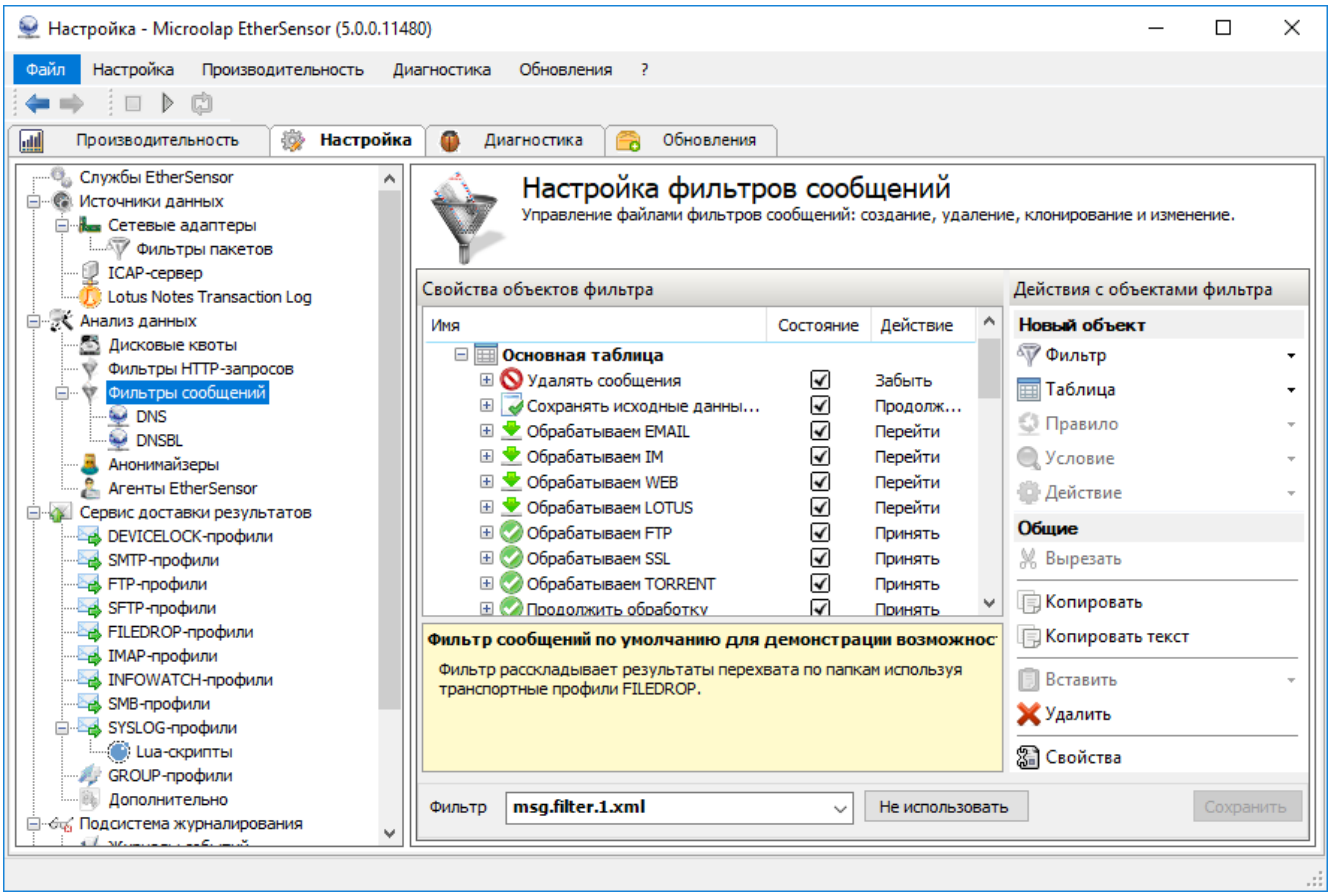

Рис.46. Управление фильтрацией сообщений.

Редактирование фильтра происходит в правом окне, допускается редактирование активного фильтра. Для того, чтобы служба **EtherSensor Analyser** начала использовать измененный фильтр, этот фильтр следует сделать активным и перезапустить службу.

Подробнее о создании фильтров можно ознакомиться в разделе "Фильтрация сообщений".

DNS

При создании правил фильтрации может потребоваться возможность использовать доменные имена, в то время, как в атрибутах перехваченных объектов доступны только IP-адреса.

Для того, чтобы в процессе фильтрации реализовать такую возможность в реальном времени (стоит также учитывать динамическое назначение IP-адресов по DHCP), в секции **DNS** следует определить и настроить доступные DNS-серверы.

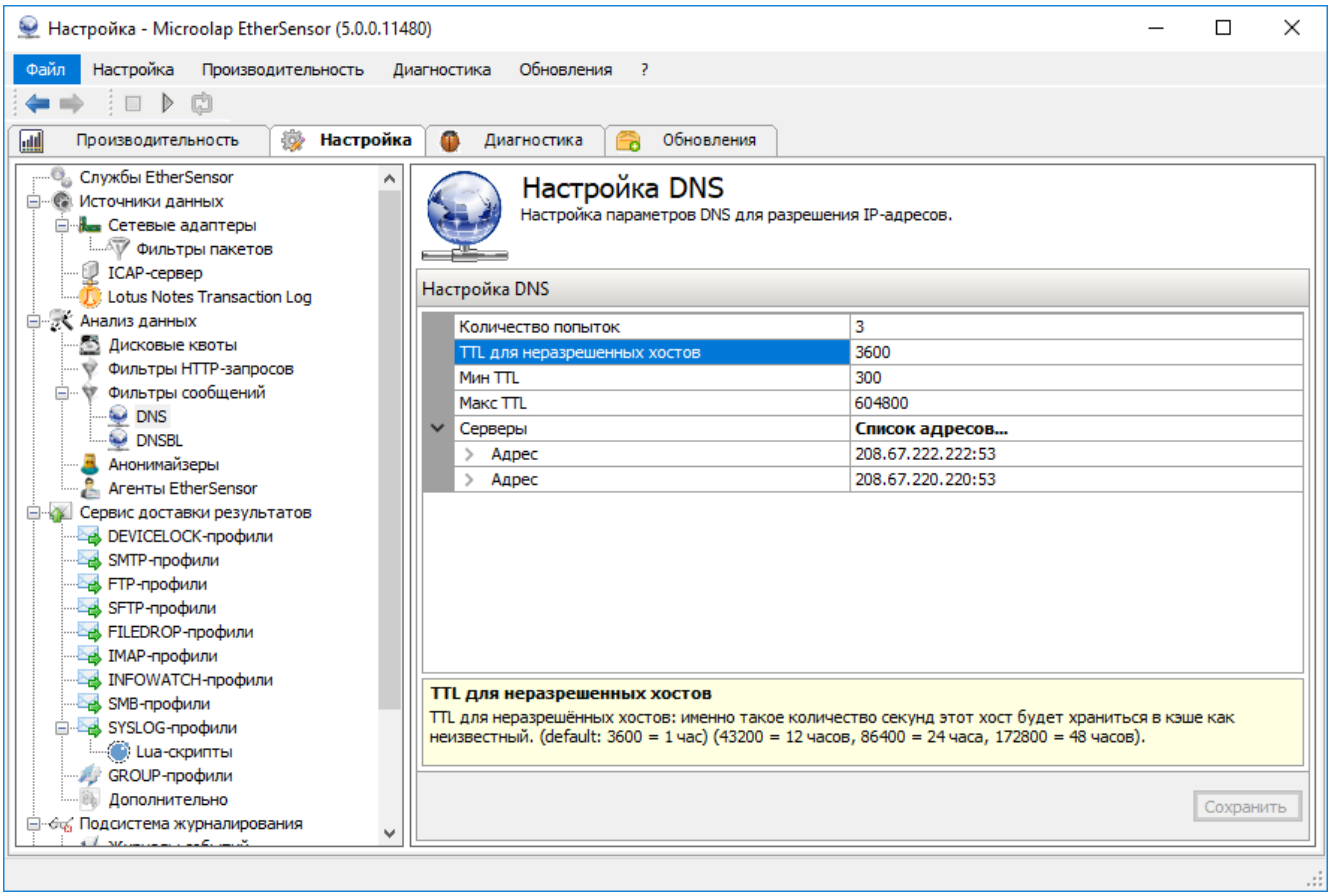

Рис.47. Настройка DNS.

Для того, чтобы добавить, удалить или отредактировать свойства DNS-серверов, а также изменить порядок обращения к ним, нажмите кнопку справа от **Список адресов...**:

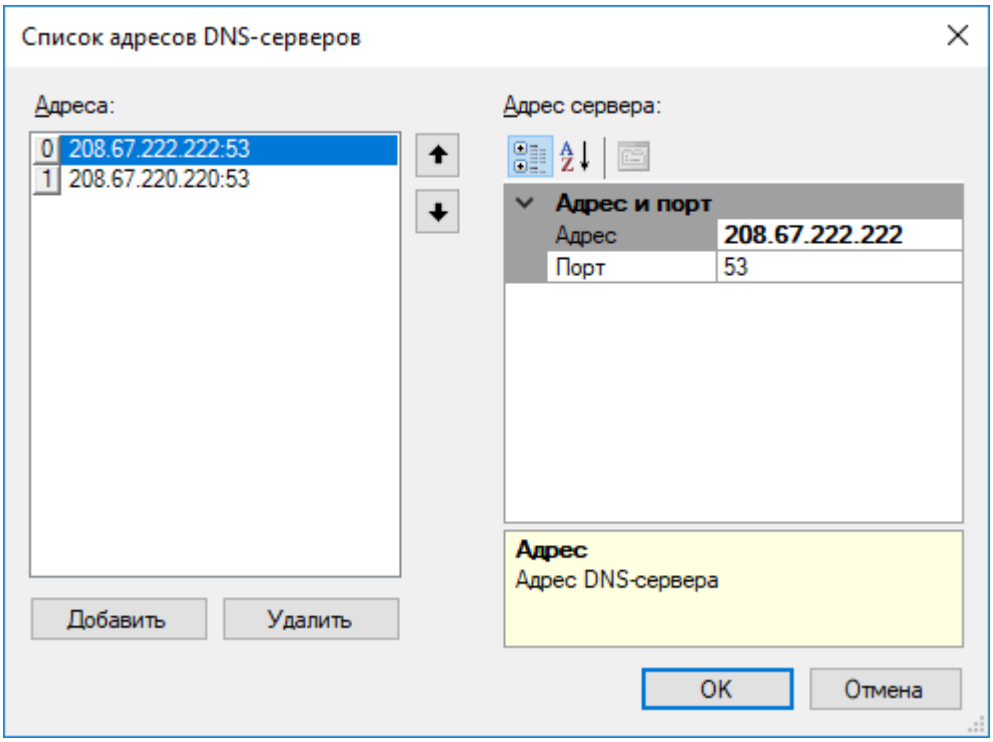

Рис.48. Детальная настройка DNS.

DNSBL

В процессе фильтрации сообщений также может потребоваться категоризация сообщений, для этого в **Microolap EtherSensor** реализована работа с DNSBL-серверами для детектирования спам-сообщений в SMTP-потоке. Настройка этой функции полностью идентична настройке работы с DNS-серверами.

Анонимайзеры

Работа с анонимайзерами в текущей версии **Microolap EtherSensor** (5.1.0.13519) происходит на уровне отслеживания доменов таких сервисов. Для формирования списка доменов следует указать каждый домен на отдельной строке или перечислять несколько доменов в одной строке через запятую.

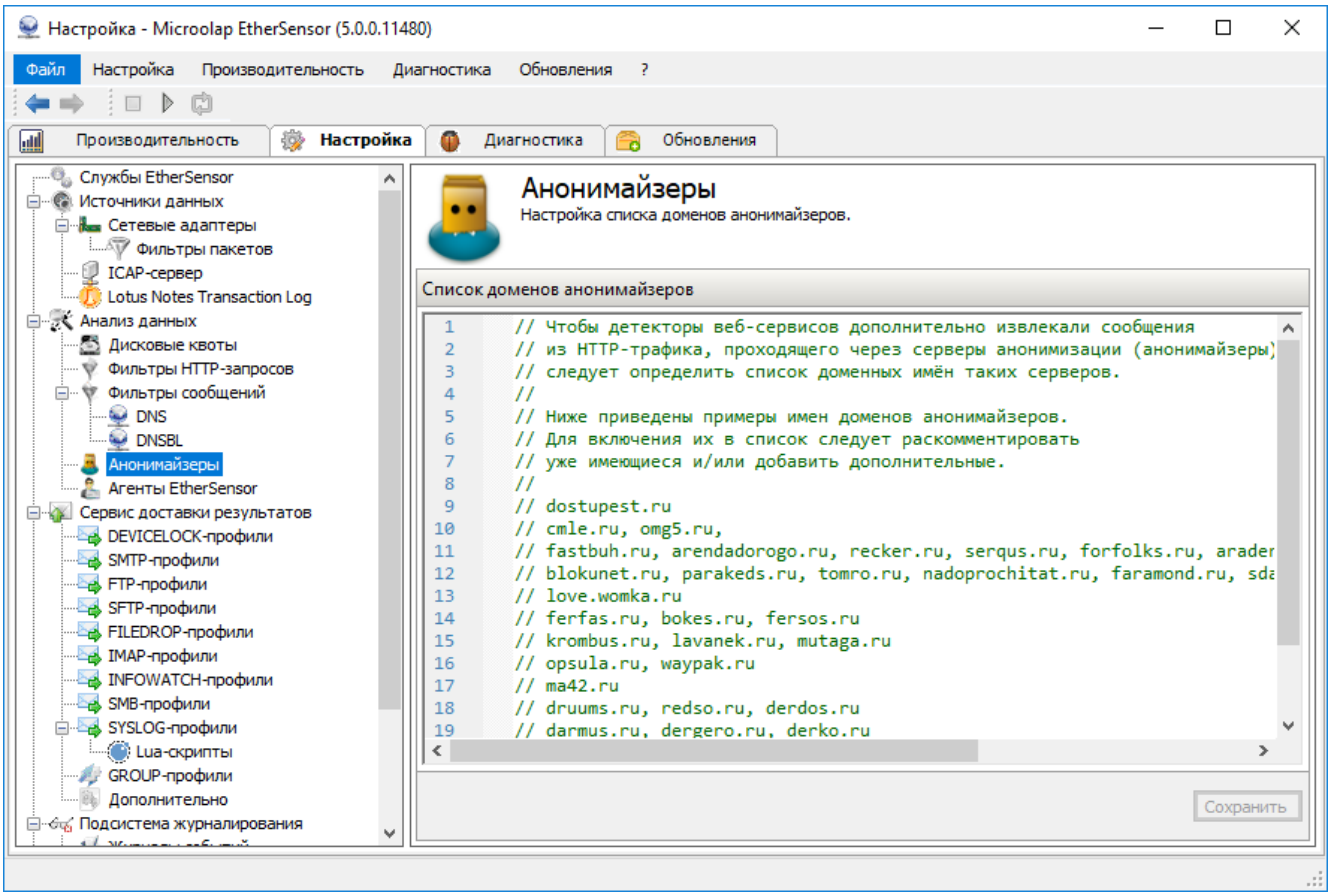

Рис.49. Настройка списка доменов анонимайзеров.

Microolap EtherSensor и EtherSensor Agent

Сервис **EtherSensor Agent** предназначен для привязки TCP-соединений, создаваемых локальными процессами на рабочих станциях пользователей, к их текущим именам и IP-адресам, в том числе и на терминальных серверах.

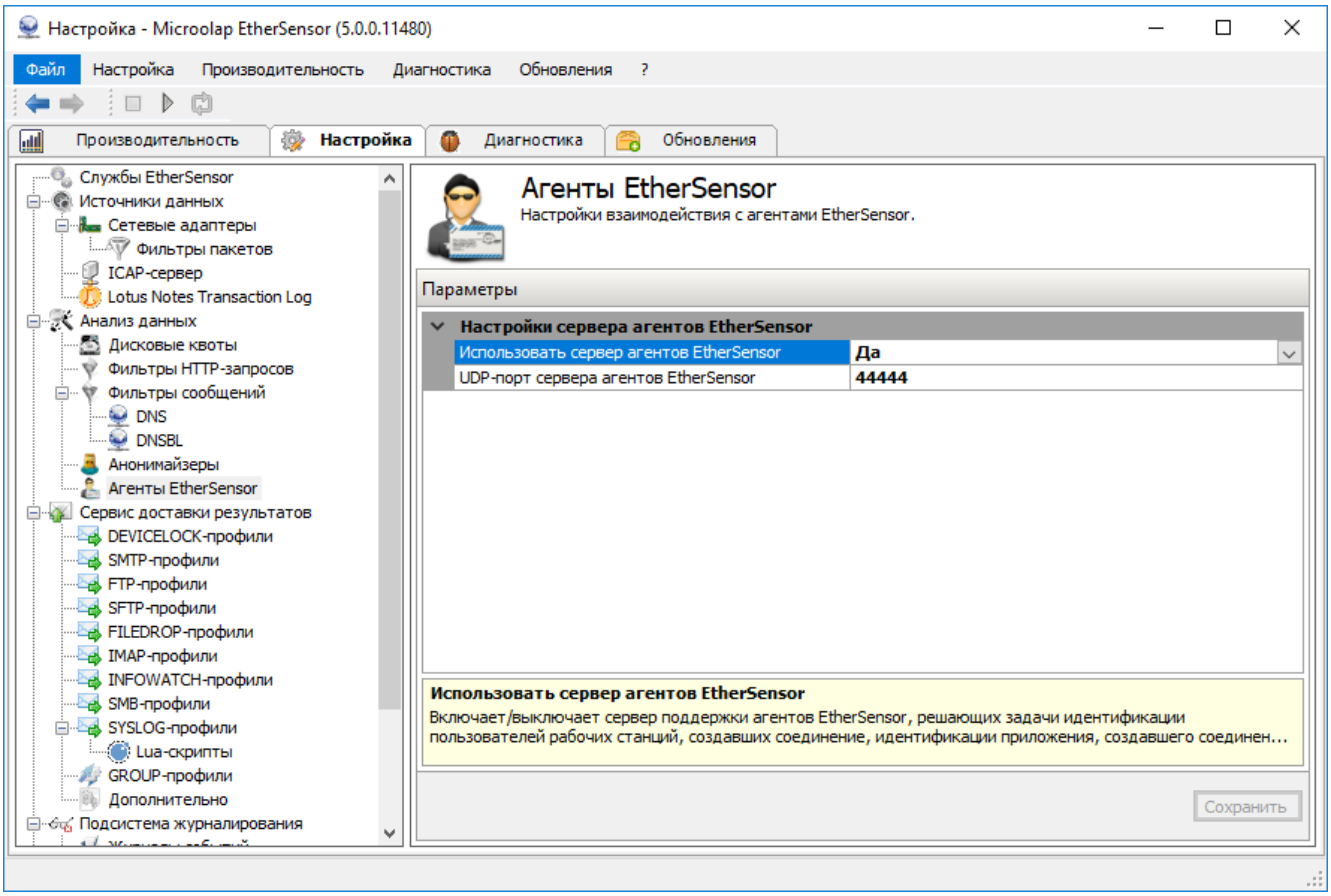

Рис.50. Настройка взаимодействия Microolap EtherSensor с EtherSensor Agent.

4.2. Ручная настройка (файл конфигурации)

Конфигурация службы **EtherSensor Analyser** хранится в XML-файлах **analyser.xml** и **quotas.xml,** расположенных в общей директории конфигураций **Microolap EtherSensor [INSTALLDIR] \config**.

Пример файла конфигурации **analyser.xml**:

```
<?xml version="1.0" encoding="utf-8"?>
<AnalyserConfig version="4.5">
  <MaxFileSizeInMemory>10485760</MaxFileSizeInMemory>
  <AgentsServer enabled="false">
    <UdpPort>44444</UdpPort>
    <SessionTimeOut>10</SessionTimeOut>
  </AgentsServer>
  <RawFilter enabled="false" filename="" />

  <MessageFilter enabled="false" filename="">
    <Dns>
      <AttemptsCount>3</AttemptsCount>
      <TtlForUnknown>3600</TtlForUnknown>
      <MinTtl>300</MinTtl>
      <MaxTtl>604800</MaxTtl>
      <Server ipaddress="208.67.220.220" port="53" />
    </Dns>

    <DnsBl>
      <AttemptsCount>3</AttemptsCount>
      <TtlForUnknown>3600</TtlForUnknown>
      <MinTtl>300</MinTtl>
      <MaxTtl>604800</MaxTtl>
      <Server ipaddress="208.67.222.222" port="53" />
    </DnsBl>
  </MessageFilter>

  <Anonymous>
    <Host />
  </Anonymous>
</AnalyserConfig>
```

Тег AnalyserConfig

Является корневым тегом конфигурации службы. В его атрибуте **version** указывается версия конфигурации.

Тег MaxFileSizeInMemory

Тег **MaxFileSizeInMemory** является вложенным в тег **AnalyserConfig** и указывает на размер объекта кэша в байтах, сохраняемого в памяти ОС. Объекты кэша - это объекты протоколов уровня приложений в модели OSI, полученные от служб **EtherSensor EtherCAP** и **EtherSensor ICAP**. Служба анализирует объекты кэша с целью детектирования сообщений, передаваемых участниками сети. Используйте данный параметр, чтобы минимизировать нагрузку на файловую систему. Все объекты, поступающие в кэш, размер которых меньше указанного в данной настройке, будут обрабатываться без использования файловой системы.

Тег AgentsServer

Тег **AgentsServer** является вложенным в тег **AnalyserConfig** и указывает на настройки сервера **Microolap EtherSensor**, который взаимодействует с экземплярами **EtherSensor Agent**.

ПО "EtherSensor Agent" доставляет информацию о соединениях, которые создают пользователи сети. Таким образом сервер **Microolap EtherSensor** использует эту информацию для идентификации пользователя при обработке перехваченного сообщения.

Тег UdpPort

Тег **UdpPort** является вложенным в тег **AgentsServer** и указывает номер прослушиваемого UDP порта сервером **Microolap EtherSensor**.

Тег SessionTimeOut

Тег **SessionTimeOut** является вложенным в тег **AgentsServer** и указывает время простоя отслеживаемого соединения. По истечении данного времени соединение будет удалено из кэша отслеживаемых соединений. Значение данного параметра указывается в минутах и может быть в диапазоне от 1 до 59.

Тег RawFilter

Тег **RawFilter** является вложенным в тег **AnalyserConfig** и указывает на описание настроек механизма фильтрации HTTP-запросов. В атрибуте **enabled** указывается статус использования механизма фильтрации HTTP-запросов, если данный атрибут выставлен в значение **false**, то фильтр HTTP-запросов не участвует в процессе обработки сообщений. Атрибут **filename** используется для указания имени файла используемых настроек механизма фильтрации. Конфигурация механизма фильтрации хранится в XML-файле **<name>.xml**, расположенном в директории конфигураций **Microolap EtherSensor [INSTALLDIR]\config\filter\http**.

Тег MessageFilter

Тег **MessageFilter** является вложенным в тег **AnalyserConfig** и указывает на описание настроек механизма фильтрации сообщений. В атрибуте **enabled** указывается статус использования механизма фильтрации сообщений, если данный атрибут выставлен в значение **false**, то фильтр сообщений не участвует в процессе обработки сообщений. Атрибут **filename** используется для указания имени файла используемых настроек механизма фильтрации. Конфигурация механизма фильтрации хранится в XML-файле **<name>.xml**, расположенном в директории конфигураций **Microolap EtherSensor [INSTALLDIR]\config\filter**.

Тег Dns

Тег **Dns** является вложенным в тег **Filter** и служит для настройки модуля DNS, используемого механизмом фильтрации, для получения DNS-имён участников сетевого взаимодействия.

Пример настройки модуля DNS:

```
<Dns>
  <AttemptsCount>3</AttemptsCount>
  <TtlForUnknown>3600</TtlForUnknown>
  <MinTtl>300</MinTtl>
  <MaxTtl>604800</MaxTtl>
  <Server ipaddress="208.67.220.220" port="53"/>
  <Server ipaddress="208.67.222.222" port="53"/>
</Dns>
```

Свойства модуля DNS:

AttemptsCount

Определяет количество попыток запроса DNS-имени хоста. Пример: **3**;

TtlForUnknown

Определяет время хранения статуса неопределённого DNS-имени в локальном DNS-кэше в секундах в случае, когда не удалось получить DNS-имя хоста за отведённое количество попыток. Пример: **3600**;

MinTtl

Определяет минимальное время хранения записи DNS-имени в локальном DNS-кэше, в секундах. Пример: **300**;

MaxTtl

Определяет максимальное время хранения записи DNS-имени в локальном DNS-кэше, в секундах. Пример: **604800**;

Server

Определяет адрес и порт сервера DNS. Пример: **ipaddress="208.67.222.222" port="53"**;

Тег DnsBl

Тег **DnsBl** является вложенным в тег **Filter** и служит для настройки модуля **DnsBl**, используемого механизмом фильтрации для получения информации от службы DNSBL (DNS blacklist) об участниках сетевого взаимодействия.

Пример настройки модуля DNSBL:

```
<DnsBl>
  <AttemptsCount>3</AttemptsCount>
  <TtlForUnknown>3600</TtlForUnknown>
  <MinTtl>300</MinTtl>
  <MaxTtl>604800</MaxTtl>
  <Server ipaddress="192.68.0.20" port="53"/>
  <Server ipaddress="192.68.0.21" port="53"/>
</DnsBl>
```

Свойства модуля DNSBL:

AttemptsCount

Определяет количество попыток запроса к службе DNSBL. Пример: **3**;

TtlForUnknown

Определяет время хранения статуса неопределённого ответа, полученного от службы DNSBL в локальном DNSBL-кэше в секундах в случае, когда не удалось получить результат запроса от службы DNSBL за отведённое количество попыток. Пример: **3600**;

MinTtl

Определяет минимальное время хранения записи результата, полученного от службы DNSBL в локальном DNSBL-кэше в секундах. Пример: **300**;

MaxTtl

Определяет максимальное время хранения записи результата, полученного от службы DNSBL в локальном DNSBL-кэше в секундах. Пример: **604800**;

Server

Определяет адрес и порт сервера службы DNSBL. Пример: **"192.68.0.20" port="53"**;

Тег Anonymous

Тег **Anonymous** является вложенным в тег **AnalyserConfig** и указывает на настройки списка доменов анонимайзеров.

Тег Host

Тег **Host** является вложенным в тег **Anonymous** и через запятую указывает имя или список имён отслеживаемых доменов анонимизирующих серверов.

Пример настройки модуля **Anonymous**:

```
<Anonymous>
  <Host>dostupest.ru</Host>
  <Host>fastbuh.ru, arendadorogo.ru, recker.ru</Host>
</Anonymous>
```

Пример файла конфигурации **quotas.xml**:

```
<?xml version="1.0" encoding="utf-8"?>
<QuotasConfig version="1.0" enabled="true">
  <NotProcessed>0</NotProcessed>
  <PreParseError>10</PreParseError>
  <RawFiltered>0</RawFiltered>
  <RawFilterError>10</RawFilterError>
  <ParseError>10</ParseError>
  <UnknownObject>10</UnknownObject>
  <DetectOk>-1</DetectOk>
  <DetectUnknown>10</DetectUnknown>
  <DetectError>10</DetectError>
  <DetectNoObjects>0</DetectNoObjects>
  <DetectFiltered>0</DetectFiltered>
  <MessageFilterError>10</MessageFilterError>
  <SendError>1000</SendError>
</QuotasConfig>
```

Тег QuotasConfig

Является корневым тегом конфигурации дисковых квот. В его атрибуте **version** указывается версия конфигурации. В атрибуте **enabled** указывается статус использования дисковых квот, если данный атрибут выставлен в значение **false**, то значения дисковых квот не учитываются в процессе обработки сообщений.

Тег PreParseError

Тег **PreParseError** является вложенным в тег **Quotas** и указывает на значения дисковой квоты для сохранения результатов, во время обработки которых произошла ошибка, связанная с разбором данных используемого интернет-протокола. Предварительная фильтрация данных выполняется перед вызовом RAW-фильтра.

Тег **RawFiltered** является вложенным в тег **Quotas** и указывает на значения дисковой квоты для сохранения результатов, отклонённых RAW-фильтром. Основная цель использования данного параметра - это отладка (проверка) логики работы RAW-фильтра.

Тег **RawFilterError** является вложенным в тег **Quotas** и указывает на значения дисковой квоты для сохранения объектов, которые вызвали ошибку в процессе работы фильтра.

Тег ParseError

Тег **ParseError** является вложенным в тег **Quotas** и указывает на значения дисковой квоты для сохранения результатов, во время обработки которых произошла ошибка, связанная с разбором данных используемого интернет-протокола. Данные TCP-сессии такого результата успешно перехвачены, но при разборе произошла ошибка, вызванная, как правило, нарушениями протокола. Например, расширение к браузеру в POST-запросе передает в конце строки байт **00** вместо **0D0A**.

Тег UnknownObject

Тег **UnknownObject** является вложенным в тег **Quotas** и указывает на значения дисковой квоты для сохранения объектов неизвестного формата. Данные TCP-сессии такого результата успешно перехвачены, но в текущей версии **Microolap EtherSensor** (5.1.0.13519) отсутствует детектор сообщений такого типа.

Тег DetectOk

Тег **DetectOk** является вложенным в тег **Quotas** и указывает на значения дисковой квоты для сохранения успешно распознанных объектов. Данные TCP-сессии успешно перехвачены, сообщение распознано и передано службе доставки перехваченных сообщений.

Тег DetectUnknown

Тег **DetectUnknown** является вложенным в тег **Quotas** и указывает на значения дисковой квоты для сохранения распознанных объектов, содержащих неизвестные данные. Данные TCP-сессии успешно перехвачены, детектор, соответствующий данному типу сообщений, отработал, но ему не удалось извлечь все данные (скорее всего, изменился формат сообщения).

Тег DetectError

Тег **DetectError** является вложенным в тег **Quotas** и указывает на значения дисковой квоты для сохранения объектов, содержащих данные, приводящие к ошибкам детектирования сообщений.

Тег DetectNoObjects

Тег **DetectNoObjects** является вложенным в тег **Quotas** и указывает на значения дисковой квоты для сохранения объектов, которые были успешно распознаны, но не содержат необходимых данных для дальнейшей обработки.

Тег DetectFiltered

Тег **DetectFiltered** является вложенным в тег **Quotas** и указывает на значения дисковой квоты для сохранения объектов, которые изначально не несут полезной информации, т.к. являются служебными данными, передаваемыми в процессе взаимодействия пользователя с интернет-сервисом.

Тег MessageFilterError

Тег **MessageFilterError** является вложенным в тег **Quotas** и указывает на значения дисковой квоты для сохранения объектов, которые вызвали ошибку в процессе работы фильтра сообщений.

Тег SendError

Тег **SendError** является вложенным в тег **Quotas** и указывает на значения дисковой квоты для сохранения перехваченных сообщений, которые вызвали непредвиденную ошибку в процессе их отправки внешнему потребителю.

4.3. Формируемые сообщения

Результатом работы **Microolap EtherSensor** являются сообщения, сформированные из объектов уровня приложения (сообщений), извлеченных из трафика. Для дальнейшей обработки **Microolap EtherSensor** передает такие сообщения системам-потребителям с помощью службы доставки результатов.

Для передачи данных о реконструированной коммуникации применяются следующие механизмы:

1. Перехваченное сообщение формируется в XML-паспорт, где описаны известные данные о характере перехваченных данных, отправителях, получателях. В процессе обработки паспорт наполняется собираемыми данными.

2. На момент передачи в службу доставки результатов **Microolap EtherSensor** заканчивает обрабатывать объект, и он в виде паспорта и других файлов данных передается на отправку.

3. Служба доставки результатов, в зависимости от требуемого типа транспорта и его настроек, формирует из паспорта передаваемый объект.

Например, для передачи по протоколу SMTP формируется сообщение электронной почты, где в адреса отправителя и получателя (FROM, TO, CC, BCC) подставляются перехваченные данные об источнике и назначении сообщения, если такие данные есть. Текст сообщения становится текстом email-сообщения, передаваемые файлы - вложениями к сообщению. Прочие данные, накопленные **Microolap EtherSensor** при обработке соединения, сохраняются в виде MIME-заголовков сообщения.

Оформление сообщения для доставки результата

Передаваемые службой доставки результатов сообщения должны соответствовать требованиям к сообщениям, передаваемым по протоколу SMTP в соответствии с RFC. Длинные

заголовки могут разбиваться и кодироваться, основной кодировкой является UTF-8. Типы данных объектов выясняются на основе обрабатываемых заголовков протокола.

> **Помните:**
> **1.** Для ряда веб-сервисов возможен перехват нескольких сообщений на одну операцию пользователя в интерфейсе - это реакция **Microolap EtherSensor** на отправку в сервис черновиков или прикладываемых файлов.
> **2.** Допустима ситуация, когда текст и вложение доставляются как отдельные сообщения.
> **3.** Допустима ситуация, когда для нескольких сообщений передается один контейнер с содержимым этих сообщений (в основном для IM-протоколов для минимизации трафика и связанных с ним накладных расходов).

Служебные MIME-заголовки Microolap EtherSensor с примерами значений

X-Sensor-Version: 5.1.0.13519

Текстовая строка. Идентифицирует текущую версию **Microolap EtherSensor**.

X-Sensor-Id: sensor-01

Текстовая строка. Идентификатор сенсора, позволяет отличить сообщения от одного сенсора от сообщений другого сенсора или сгруппировать по этому значению. Может быть любой ASCII идентификатор, по умолчанию прописывается UHID.

X-Sensor-Session-Id: 6612456

Целое число. Внутренний идентификатор соединений, обработанных **Microolap EtherSensor**. Выдается источником сообщений (службами **EtherSensor ICAP** или **EtherSensor EtherCAP**). Регистрируется в журнале **capture.log.**

X-Sensor-Net-Interface-Id: 00-21-28-10-58-80

Текстовая строка. В случае если сообщение перехвачено службой **EtherSensor EtherCAP**, то значение - MAC адрес интерфейса или **capdrop** - виртуальный идентификатор драйвера разбора PCAP-файлов.

В случае ICAP-сервера будет приведен идентификатор из конфигурации ICAP-сервера. Этот заголовок позволяет проследить источник сообщения: с какого именно интерфейса, сервиса были получены данные для обработки.

X-Sensor-Session-Level: 0

Целое число. Показывает, сколько потребовалось разобрать различных протоколов, чтобы добраться до сообщения. Протоколом может быть, например, соединение HTTP, HTTP-proxy соединение через это соединение, а также и GRE-инкапсуляция.

X-Sensor-Src-Address: 10.31.90.22:47016

X-Sensor-Dst-Address: 193.203.100.139:8080

IP-адреса и порты соединения, исходящие и назначения. Могут быть не определены, если идёт обработка ICAP-трафика, в котором нет заголовков **X-Client-IP** и, **X-Server-IP**. Пример ICAP -заголовков: **X-Client-IP:** 192.168.3.67, **X-Server-IP:** 123.45.67.89.

X-Sensor-Src-Host: pc-test.msk.su

X-Sensor-Dst-Host: nns-team.ru

Текстовые строки. Имена хостов, соответствующие заголовкам **X-Sensor-Src-Address** и **X-Sensor-Dst-Address**. Так как многие сети выдают внутренние адреса по DHCP, следует выяснять имя хоста именно в момент перехвата сообщения. **Microolap EtherSensor** делает это, используя обратный DNS-запрос к указанному в конфигурации службы **EtherSensor Analyser** DNS-серверу. В случае если распознать не удалось, значение будет **<not resolved>**.

X-Sensor-Protocol: HTTP

Текстовая строка. Название детектора, который был использован для разбора данных. Возможны SMTP, ICQ, MRA и другие.

X-Sensor-Detector: phpBB

Текстовая строка. Название детектора **Microolap EtherSensor**, который определил наличие данных в соединении.

X-Sensor-Attachments-Count: 0

Целое число. Если в сообщении был перехвачен файл или файлы, их количество указывается в этом значении.

X-Sensor-Object-Date: Fri, 17 Sep 2010 17:30:24 +0400

Текстовая строка. Время перехвата соединения (время создания объекта в **Microolap EtherSensor**). Таймзона выбирается по настройкам ОС сенсора.

X-Sensor-Object-Size: 2735

Целое число. Размер перехваченного объекта до обработки в байтах.

X-Sensor-Object-MD5Hash: c326230de58279229862b18e818a3912

Текстовая строка, **md5** хэш от перехваченного объекта. Если у сообщений одинаковый текст, но разные размер, хэш, дата объекта или адреса и порты источника и назначения - то это не дубликаты, а сильно похожие объекты. Совпадения объектов по **md5** не должно быть в нормальной ситуации. Если оно происходит, значит одно и то же соединение обрабатывается **Microolap EtherSensor** несколько раз (петля).

X-Sensor-Via: 1.1 off:1080 (squid/2.6.STABLE18)

X-Sensor-Forwarded-For: 10.255.241.31

Текстовые строки. Заголовки из соединения HTTP, подставляются их значения, если присутствуют. По данным значениям можно выяснить, что клиент соединения работает за прокси-сервером, а также иногда узнать его адрес на момент регистрации сообщения.

X-Sensor-Icap-Client-Username: user1

X-Sensor-Icap-Subscriber-Id: mike.smith@mycompany.com

X-Sensor-Icap-Authenticated-User:
TERBUDovLzE5Mi4xNjguMTIuMTAwL289bXljb21wYW55LCBvdT1lbmdpbmVlcmluZywgY249bWlrZS5zbWl0aA==

X-Sensor-Icap-Authenticated-Group:
TERBUDovLzE5Mi4xNjguMTIuMTAwL289bXljb21wYW55LCBvdT1lbmdpbmVlcmluZw==

Значения данных заголовков формируются при обработке ICAP-трафика. Для этого используются соответствующие заголовки ICAP-протокола (**X-Client-Username, X-Subscriber-ID, X-Authenticated-User, X-Authenticated-Groups)**.

X-Sensor-Filter-Name: TEST

X-Sensor-Tags: Filtered=1

X-Sensor-Labels: filter-begin-time="2010-09-17T17:30:24.6318125+04:00",

dns-begin="2010-09-17T17:30:24.6318125+04:00",

dns-end="2010-09-17T17:30:24.6318125+04:00",

Filtered="true",

filter-end-time="2010-09-17T17:30:24.6318125+04:00"

Служебные заголовки службы **EtherSensor Analyser**. Позволяют определить сработавший фильтр, характер содержимого сообщения, установленные теги и метки, а также отследить обработку сообщения в фильтре. Результирующий состав этих заголовков сильно зависит от политики фильтра.

Date: Fri, 17 Sep 2010 17:30:24 +0400

В данный заголовок дублируется значение **X-Sensor-Object-Date**.

From: anonymous@nns-team.ru

To: forum@nns-team.ru

CC, BCC и другие заголовки

Subject: Re: World of Tanks

Если удается, в заголовки отправителя и получателя подставляются адреса или идентификаторы пользователей, извлеченные из сообщений, заголовков запросов и т.д.

Могут быть не определены, а также зависят от детектора - например, если протокол не имеет возможности задавать тему сообщения, она может быть использована для информации от сенсора.

X-Sensor-RawSource-Type: LotusMail

Все сообщения помечаются заголовком - "**X-Sensor-RawSource-Type**" для того, чтобы было известно из какого именно источника данных было получено конечное сообщение.

Значениями этого заголовка в текущей версии **Microolap EtherSensor** (5.1.0.13519) могут быть:

HttpGetRequest

Означает, что первичным источником данных был HTTP-запрос GET;

HttpPostRequest

Означает, что первичным источником данных был HTTP-запрос POST;

HttpPutRequest

Означает, что первичным источником данных был HTTP-запрос PUT;

FtpFile

Означает, что первичным источником данных был FTP-файл;

SmtpEml

Означает, что первичным источником данных было SMTP-сообщение в формате EML;

Pop3Eml

Означает, что первичным источником данных было POP3-сообщение в формате EML;

IcqContactList

Означает, что первичным источником данных был список контактов ICQ;

IcqMessageList

Означает, что первичным источником данных был список сообщений ICQ;

IcqFile

Означает, что первичным источником данных был файл, переданный между ICQ-клиентами;

IcqLoginInfo

Означает, что первичным источником данных была ICQ-информация о пользователе;

MraUserInfo

Означает, что первичным источником данных была MRA-информация о пользователе;

MraContactList

Означает, что первичным источником данных был список контактов MRA;

MraMessageList

Означает, что первичным источником данных был список сообщений MRA;

MraFile

Означает, что первичным источником данных был файл, переданный между MRA-клиентами;

MsnContactList

Означает, что первичным источником данных был список контактов MSN;

MsnMessageList

Означает, что первичным источником данных был список сообщений MSN;

MsnFile

Означает, что первичным источником данных был файл, переданный между MSN-клиентами;

XmppContactList

Означает, что первичным источником данных был список контактов XMPP;

XmppMessageList

Означает, что первичным источником данных был список сообщений XMPP;

XmppFile

Означает, что первичным источником данных был файл, переданный между XMPP-клиентами;

IrcMessageList

Означает, что первичным источником данных был список сообщений IRC;

IrcFile

Означает, что первичным источником данных был файл, переданный между IRC-клиентами;

SkypeVersionRequest

Означает, что первичным источником данных был запрос последней версии к **ui.skype.com**;

SslSessionsList

Означает, что первичным источником данных был список SSL-сессий;

LotusMail

Означает, что первичным источником данных было сообщение протокола LOTUS;

LotusAttachment

Означает, что первичным источником данных был файл вложения (аттачмент) сообщения LOTUS.

X-Sensor-LicOption: Lotus

Все сообщения помечаются заголовком "**X-Sensor-LicOption**", для того, чтобы было известно, каким модулем было обработано данное сообщение. Значениями этого заголовка в текущей версии **Microolap EtherSensor** (5.1.0.13519) могут быть:

WebMail

Означает, что сообщение было обработано модулем с лицензионной опцией "Веб-почта";

WebSocial

Означает, что сообщение было обработано модулем с лицензионной опцией "Социальные сети";

Email

Означает, что сообщение было обработано модулем с лицензионной опцией "Электронная почта";

IM

Означает, что сообщение было обработано модулем с лицензионной опцией "Мгновенные сообщения";

FT

Означает, что сообщение было обработано модулем с лицензионной опцией "Передача файлов";

WebMailRead

Означает, что сообщение было обработано модулем с лицензионной опцией "Чтение входящей веб-почты";

Lotus

Означает, что сообщение было обработано модулем с лицензионной опцией "Перехват сообщений системы **Lotus Notes**";

LotusTxn

Означает, что сообщение было обработано модулем с лицензионной опцией "Извлечение сообщений из **Lotus Notes Transaction Log"**.

X-Sensor-UID: 0e515c8c-61eb-11e1-a529-000c29ff0707

Данный заголовок формируется при взаимодействии сервера **Microolap EtherSensor** и экземпляров **EtherSensor Agent**, установленных на рабочих станциях пользователей сети. Значение заголовка уникально идентифицирует пользователя организации на конкретном компьютере внутри организации.

X-Sensor-UID-UserName: CN=Administrator,CN=Users,DC=bigbrother,DC=foo

Данный заголовок формируется при взаимодействии сервера **Microolap EtherSensor** и экземпляров **EtherSensor Agent**, установленных на рабочих станциях пользователей сети. Значение заголовка уникально идентифицирует пользователя внутри организации.

X-Sensor-UID-UserSID: S-1-5-21-86032015-1269853868-1024056280-1001

Данный заголовок формируется при взаимодействии сервера **Microolap EtherSensor** и экземпляров **EtherSensor Agent**, установленных на рабочих станциях пользователей сети. Значение заголовка уникально идентифицирует пользователя внутри организации и описывает идентификатор безопасности текущего пользователя.

X-Sensor-UID-ComputerName: WS325-LOCK.bigbrother.foo

Данный заголовок формируется при взаимодействии сервера **Microolap EtherSensor** и экземпляров **EtherSensor Agent**, установленных на рабочих станциях пользователей сети. Значение заголовка уникально идентифицирует компьютер внутри организации.

X-Sensor-UID-AdapterType: if_type_ethernet_csmacd

Данный заголовок формируется при взаимодействии сервера **Microolap EtherSensor** и экземпляров **EtherSensor Agent**, установленных на рабочих станциях пользователей сети. Значение заголовка содержит тип сетевого адаптера, через который было отправлено сообщение. Полный список возможных вариантов значений данного поля доступен на сайте компании Microsoft.

X-Sensor-UID-MacAddress: 00-1F-C6-2D-EA-40

Данный заголовок формируется при взаимодействии сервера **Microolap EtherSensor** и экземпляров **EtherSensor Agent**, установленных на рабочих станциях пользователей сети. Значение заголовка содержит MAC-адрес сетевого адаптера, через который было отправлено сообщение.

X-Sensor-UHID: UO2D-RNVO-JRN7-R1EN-91C0-61TA-1HP7-YRVF

Содержит уникальный идентификатор для каждого экземпляра **Microolap EtherSensor** и набора оборудования (Unique Hardware IDentifier).

X-Sensor-Lotus-MessageId: <OF4D026078.B21F0C4F-ON44257C15.002E1625-44257C15.002E2225@LocalDomain>

Содержит уникальный идентификатор сообщения, передаваемого по протоколу Lotus Notes.

X-Sensor-Lotus-Form: Reply

Содержит имя формы передаваемого по протоколу Lotus сообщения.

X-Sensor-Lotus-Mailer: Lotus Notes Release 8.5.2FP2 SHF236 October 24, 2011

Содержит строку, идентифицирующую тип клиента системы **Lotus Notes**.

X-Sensor-Lotus-INetPrincipal: UserName/OU/O@ServerName.Domain.com

Содержит расширенную информацию об отправителе сообщения.

X-Sensor-Lotus-RouteServers: CN=lotus1/O=Company

Содержит список серверов Lotus, которые участвовали в передаче сообщения.

X-Sensor-Lotus-References: <OF02B9DAC2.33CDF581-ON44257C15.002DF8CD@LocalDomain>

Содержит список идентификаторов сообщений, на которые ссылается текущее сообщение.

4.4. Фильтрация результатов перехвата

Начиная с версии **3.0** в **Microolap EtherSensor** добавлен фильтр распознанных сообщений.

Идеология обработки сообщений строится на формировании цепочек правил, которые объединяются в таблицы. Сообщение проходит проверку правилами, которые, в зависимости от попадания сообщения под действие правила, могут изменять содержимое сообщения, его метаданных, или ход его дальнейшей обработки.

Эта идеология очень схожа с правилами фильтрации, используемыми в утилите **iptables**.

Использование фильтров позволяет управлять процессом обработки сообщений, направлять сообщения в различные средства для дальнейшего анализа, а также удалять заведомо не интересные сообщения с целью снижения нагрузки на **Microolap EtherSensor** и среду выполнения.

4.4.1. Основы фильтрации

Ключевыми понятиями фильтрации являются:

Критерий (match)

Логическое выражение, состоящее из одного или более условий (**condition**) объединённых логическими операторами **OR**, **AND**, **XOR** и **NOT**, анализирующее содержимое и/или метаданные сообщения и определяющее, подпадает ли данное конкретное сообщение под действие текущего правила.

Условие (condition)

Элементарное условие проверки сообщения и/или его метаданных. Проверяет одно или несколько полей сообщения или его метаданных единообразным способом на соответствие некому условию (равенству, неравенству, соответствию шаблону и т.д.).

Действие (action)

Описание действия, которое необходимо выполнить над сообщением в том случае, если сообщение подпадает под действие этого правила. Более подробно о возможных действиях над сообщениями указано в разделе Действия.

Правило (rule)

Состоит из условий и действий. Если сообщение соответствует условиям, к нему применяются действия. Условий может и не быть — тогда неявно предполагается критерий "все сообщения" или "любое сообщение".

Таблица (table)

Упорядоченная последовательность правил. Таблица обязана иметь уникальное имя. Существует одна системная таблица с именем "**main**". Она является точкой входа для проверки сообщения фильтром. Таблица "**main**" обязана присутствовать в каждом фильтре. Более подробно таблицы рассматриваются в разделе Таблицы.

Принципы работы фильтров

Все сообщения проходят через таблицы фильтра, начиная с таблицы "**main**". При прохождении сообщением таблицы к нему последовательно применяются все правила этой таблицы в порядке их следования.

Под применением правила понимается:

- проверка сообщения (включая метаданные) на соответствие условиям;
- применение к нему действий правила, если сообщение соответствует этому условию.

Под действием может подразумеваться как базовая операция (встроенное действие, например, **ACCEPT, DROP, JUMP** или **RETURN**), так и ориентированное на пользователя действие (это действия установки меток, тегов, изменения сообщения и/или его метаданных и т.п.). Базовые операции могут быть как терминирующими, то есть прекращающими обработку сообщения фильтром (это **ACCEPT, DROP**), так и нетерминирующими, то есть не прерывающими процесса обработки (это **JUMP** и **RETURN**).

Таблица "**main**" обязана всегда заканчиваться правилом с критерием **"все сообщения"** и одним из терминирующих действий (**ACCEPT** или **DROP**). Остальные таблицы всегда обязаны заканчиваться правилом с условием **"все сообщения"** и терминальным действием (**ACCEPT** или **DROP**) или действием **RETURN**.

Для организации перехода сообщения из текущей таблицы в другую используется действие **JUMP**. В случае применения в этой таблице к сообщению действия **RETURN**, сообщение вернется в исходную таблицу и продолжит ее прохождение, начиная со следующего правила. Другие таблицы, кроме "**main**", и переходы в них могут понадобиться для минимизации количества правил, через которые необходимо пройти сообщению, чтобы для него было принято решение **ACCEPT** или **DROP**.

Также это может быть полезно при объединении групп правил для обработки сообщений, объединяемых некими "глобальными" категориями, которые невозможно описать в контексте критерия одного правила.

Внимание!
Исходя из этого следует, что таблица **main** не может заканчиваться правилом с действием **RETURN**, так как из неё просто некуда возвращаться. Также в таблицу **main** невозможно сделать переход **JUMP**.

Следует особо подчеркнуть, что **запрещено** использовать явные или неявные "циклические" переходы, и это проверяется на этапе компиляции правил. Например, сценарий "таблица "**main**" -> **jump** -> таблица **"boss-messages**" -> таблица "**shopping**" -> таблица "**spam**" -> таблица "**boss-messages**"" будет заблокирован при попытке компиляции фильтра.

4.4.1.1. Конфигурация фильтра

Настройки фильтра хранятся в виде XML-файла, имеющего определённую структуру.

Файл настроек начинается со стандартного тега начала XML-документа с указанием версии XML 1.0 и кодировки документа.

Например:

```
<?xml version="1.0" encoding="utf-8"?>
```

Далее указывается корневой тег **filter**, который содержит настройки фильтра. Корневой тег имеет атрибуты **name** - краткое имя фильтра, и **version** - версия фильтра. На текущий момент версия только "**1.0**".

Например:

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="main filter" version="1.0">
    ...
</filter>
```

Если есть необходимость, для фильтра возможно указать комментарий - некое текстовое описание для пояснения содержания фильтра. Комментарии могут содержать любой текст и при работе фильтра игнорируются. Комментарий добавляется в качестве отдельного тега **<comment>.**

Например:

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="main filter" version="1.0">
    <comment>This is a comment.</comment>
    ...
</filter>
```

Аналогичным образом комментарии можно указывать для таблиц и правил.

4.4.1.2. Таблицы

Фильтр всегда состоит из таблицы "**main**" и, возможно, других таблиц. Проверка сообщения фильтром всегда начинается с таблицы "**main**". Таблица определяется в фильтре тегом **<table>**. Каждая таблица обязана иметь уникальное имя, указываемое в атрибуте **name** XML-тега **<table>**. Таблица может иметь в качестве необязательного комментария XML-тег **<comment>**.

Например:

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="main filter" version="1.0">
  <comment>This is a comment.</comment>
    <table name="main">
      <comment>This is a comment for the table "main".</comment>
        ...
    </table>

    <table name="spam">
        ...
    </table>

</filter>
```

В данном фильтре указаны две таблицы - обязательная таблица **main** и дополнительная таблица **spam**.

4.4.1.3. Правила

Правила состоят из критерия, состоящего из одного или более условий, и одного или нескольких действий, выполняемых в случае соответствия сообщения данному критерию.

Правила определяются внутри таблиц при помощи XML-тега <**rule**>.

Правило может иметь необязательное имя, указываемое в атрибуте **name** XML-тега <**rule**>.

Правило может иметь необязательный комментарий - XML-тег <**comment**>.

Правило может быть включенным - будет выполняться в текущей конфигурации, или выключенным - в ходе выполнения текущей конфигурации оно будет игнорироваться. Активность правила определяется обязательным атрибутом **enabled** XML-тега <**rule**>. Атрибут **enabled** может принимать следующие значения:

1 или **true**:
Правило включено, участвует в фильтрации сообщений;

0 или **false**:
Правило выключено, не участвует в фильтрации сообщений, игнорируется.

Критерий правила описывается XML-тегом <**match**> внутри тега правила. Действия правила описывается последовательностью XML-тегов <**action**> внутри тега правила.

Например:

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="main filter" version="1.0">
  <comment>This is a comment.</comment>

  <table name="main">
    <comment>This is a comment for the table "main".</comment>
    <rule enabled="1">
      <match ...> ... </match>
      <action ...> ... </action>
    </rule>

    <rule name="spam" enabled="1">
      <comment>The rule for the messages of the SPAM category.</comment>
      <match ...> ... </match>
      <action ...> ... </action>
      <action ...> ... </action>
      <action ...> ... </action>
    </rule>

    <rule enabled="1">
      <action name="drop" />
    </rule>

  </table>
</filter>
```

В этом примере в таблице **"main"** есть три правила, все правила включены. Второе правило (в отличие от первого) имеет имя, комментарий и несколько действий. Третье правило - это обязательно терминирующее правило - отклонить все сообщения, не принятые в правилах выше.

Если критерий **<match>** отсутствует в правиле или является пустым (**<match />**), то неявно подразумевается критерий **"все сообщения"** - **<c name="all"/>**.

4.4.1.3.1. Критерии и условия

Критерий (**match**) в правиле описывается XML-тегом **<match>** и определяет, будут ли выполняться действия правила для данного сообщения.

Критерий в правиле состоит из одного или нескольких условий (**conditions**), которые связаны логическими операциями **AND**, **OR**, **XOR** или **NOT**. Это позволяет строить критерий на основе логических выражений, состоящих из условий.

Пример:

```
<rule>
  <match>
    <c name="all" />
  </match>
  <action name="drop" />
</rule>
```

Данный критерий состоит из одного условия "**все сообщения**".

Условия в критериях

Условие (**condition**) - это элементарная проверка сообщения или его метаданных на соответствие чему-либо. Условие описывается XML-тегом **<condition>** или **<c>**. Сообщение либо удовлетворяет условию и в этом случае условие имеет значение **TRUE** - истина, либо не удовлетворяет условию, и в таком случае результатом проверки условия будет **FALSE** - ложь.

Для условия (**condition**) указывается его имя в атрибуте **name**, которое определяет, что и как проверять в сообщении. В прочих атрибутах тега указываются параметры для выполнения действия. Имена атрибутов дополнительных параметров зависят от конкретных условий.

Общая структура XML-тега, описывающего условие:

```
<condition name="The name of the condition." [additional parameters] />
```

или

```
<condition name="The name of the condition." [additional parameters] >
</condition>
```

или

```
<c name="The name of the condition." [additional parameters] />
```

или

```
<c name="The name of the condition." [additional parameters] ></c>
```

Большинство **условий (conditions)** использует атрибут **value="…",** в котором указываются значения для проверки на соответствие условию, или атрибут **data="…",** в котором можно указывать внешний файл для загрузки данных для такой проверки (это могут быть наборы слов, списки доменных имён и другие параметры). Какие атрибуты и как именно проверяются, описано в разделах соответствующих **условий (conditions)**.

Логические выражения в критериях

В случае, когда необходимо создать для правила сложный критерий, состоящий из нескольких условий, эти условия можно объединять в логические выражения с использованием логических операций **AND**, **OR**, **XOR**, **NOT**. Логические операции в виде XML-тегов выглядят следующим образом:

<and> … </and>:

Соответствует **(… & … & … & …)** - все условия, находящиеся внутри тега <and>, объединяются логической операцией **AND**.

<or> … </or>:

Соответствует **(… | … | … | …)** - все условия, находящиеся внутри тега <or>, объединяются логической операцией **OR**.

<xor> … </xor>:

Соответствует **(… ^ … ^ … ^ …)** - все условия, находящиеся внутри тега <xor>, объединяются логической операцией **XOR**.

<not> … </not>:

Соответствует **!(…)** - к условию применяется операция отрицания.

Например:

```
<and>
  <c name="ccc1"/>
  <c name="ccc2"/>
</and>
```

означает результат **(ccc1 & ccc2),**

а критерий:

```
<not><c name="ccc1"/></not>
```

означает результат **не (ccc1)**.

Любые теги логических операций могут быть вложенными.

Например:

```
<and>
  <c name="ccc1"/>
  <or>
    <c name="ccc2">
    <c name="ccc3">
  </or>
  <or>
    <c name="ccc4">
    <c name="ccc5">
    <not><c name="ccc6"></not>
  </or>
</and>
```

означает результат **(ccc1 & (ccc2 | ccc3) & (ccc4 | ccc5 | !ccc6))**. То есть, сообщение будет удовлетворять указанному в примере критерию, если: удовлетворяет условию **ccc1**, а также удовлетворяет (условию **ccc2** или условию **ccc3**), а также (удовлетворяет (условию **ccc4** или условию **ccc5**) или не удовлетворяет условию **ccc6**).

Для наглядности можно разбить данный критерий на блоки условий, которые обязательно должны возвращать **TRUE** при следующих проверках:

1) сообщение должно удовлетворять условию **ccc1**;

И

2) сообщение должно удовлетворять одному из условий (**ccc2** или **ccc3**);

И

3) сообщение должно удовлетворять одному из условий (**ccc4** или **ccc5**) ИЛИ не удовлетворять условию **ccc6**.

4.4.1.3.1.1. Условие ALL, *

Специальное условие, под которое попадают все фильтруемые объекты.

Описание

Условие является истинным для любых объектов. Данное условие неявно подразумевается, если критерий **<match>…</match>** является пустым или отсутствует в правиле (правило содержит только **<actions>**).

Формат

```
<c name="all" />
<c name="*" />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="all"** или **name="*"**.

Пример

Правило принимает для дальнейшей обработки все сообщения.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">
  <comment>HTTP filter.</comment>

  <table name="main">

    <rule enabled="1">
      <comment>This rule accepts all messages for further processing.</comment>
      <match>
        <c name="all" />
      </match>
      <action name="accept" />
    </rule>
  </table>

</filter>
```

Пример (неявное условие all)

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">
  <comment>HTTP filter comment.</comment>
  <table name="main">
    <rule enabled="1">
      <action name="accept" />
    </rule>
  </table>
</filter>
```

4.4.1.3.1.2. Условие DETECTOR

Установить имя детектора, который идентифицировал сообщение.

Описание

При срабатывании детектора система сохраняет его имя в метаданных сообщения. Условие DETECTOR позволяет выяснить на этапе фильтрации сообщения, какой именно детектор на него среагировал (он может быть только один).

Формат

```
<c name="detector" value="[detector-name(s)]" />
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="detector"**.

Атрибут value:

В атрибуте **value="..."** указывается имя, с которым сравнивается имя детектора, сработавшего на сообщение. Имён может быть несколько, в этом случае они перечисляются через запятую '**,**'. Для читаемости позволяется после запятой ставить пробелы.

Пример:

Сообщения от детекторов mail.ru, yandex.ru.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Messages filter.</comment>
  <table name="main">

    <rule enabled="1">
      <comment>
        Messages from detectors mail.ru,
        yandex.ru.
      </comment>
      <match>
        <c name="detector" value="mail.ru, yandex.ru" />
      </match>
      <action name="drop" />
    </rule>

  </table>
</filter>
```

4.4.1.3.1.3. Условие PROTOCOL

Проверить, по какому протоколу было получено сообщение.

Описание

Это условие проверяет, по какому протоколу было получено сообщение.

Формат

```
<c name="protocol" value="[protocol-name(s)]" />
```

Атрибут name:

В атрибуте **name** указывается имя действия - **name="protocol"**.

Атрибут value:

В атрибуте **value="..."** указывается имя, с которым сравнивается имя протокола, по которому получено сообщение.

Проверяемых протоколов может быть несколько. В этом случае они перечисляются через запятую ','. Для читаемости позволяется после запятой ставить пробелы.

Пример:

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Messages filter.</comment>
  <table name="main">
    <rule enabled="1">
      <comment>
        Drop messages received by SMTP or IMAP.
      </comment>
      <match>
        <c name="protocol" value="smtp, imap" />
      </match>
      <action name="drop" />
    </rule>
    </table>
</filter>
```

4.4.1.3.1.4. Условие MSG-SIZE, TOTAL-SIZE

Проверить размер сообщения.

Описание

Это условие проверяет размер сообщения.

условие **msg-size** - учитывает размер извлечённых текстов и размер извлечённых вложений (аттачментов);

условие **total-size** - учитывает суммарный размер извлечённых текстов, размер извлечённых вложений (аттачментов) и размер исходных данных, из которых они получены.

Формат

```
<c name="msg-size" op="<operation>" value="<compare pattern>" />
<c name="total-size" op="<operation>" value="<compare pattern>" />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="msg-size"** или **name="total-size"**.

Атрибут value:

В атрибуте **value="..."** указывается число, с которым сравнивается размер сообщения:

<число> или <число>B

Указывает размер в байтах;

<число>K

Указывает размер в килобайтах;

<число>M

Указывает размер в мегабайтах;

<число>G

Указывает размер в гигабайтах.

Атрибут op:

Атрибут **op="..."** указывает на тип операции сравнения и может принимать значения:

eq или = или ==

Условие выполняется, если размер **РАВЕН** указанному числу;

ne или != или <>

Условие выполняется, если размер **НЕ РАВЕН** указанному числу;

lt или <

Условие выполняется, если размер **МЕНЬШЕ** указанного числа;

gt или >

Условие выполняется, если размер **БОЛЬШЕ** указанного числа;

le или <=

Условие выполняется, если размер **МЕНЬШЕ ИЛИ РАВНО** указанного числа;

ge или >=

Условие выполняется, если размер **БОЛЬШЕ ИЛИ РАВНО** указанного числа.

Пример:

Правило прекращает обработку сообщений, у которых размер без учёта исходных данных больше 100 килобайт или размер с учётом исходных данных больше 1 мегабайта.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Messages filter.</comment>

  <table name="main">

      <rule enabled="1">
        <match>
          <or>
            <c name="msg-size" op=">" value="100K"/>
            <c name="total-size" op="gt" value="1M"/>
          </or>
        </match>
        <action name="drop" />
      </rule>

    </table>
</filter>
```

4.4.1.3.1.5. Условие CHECK-MD5

Проверить MD5-хэш сообщения на повторное появление в течение определённого интервала времени (отслеживание дублей сообщений).

Описание

Это условие проверяет, не встречалось ли уже (в течение указанного периода времени) сообщение с таким же MD5 хэшем, как и у текущего проверяемого сообщения.

Формат

```
<c name="check-md5" time="<timeout>" />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="check-md5"**.

Атрибут "time":

В атрибуте **time="..."** указывается время ожидания в миллисекундах.

Время ожидания не может быть меньше **1** миллисекунды и больше **5** минут, т.е. 5*60*1000 = 300000 миллисекунд.

Пример:

Если в течение двух секунд были повторные сообщения с таким же MD5, то удалять их.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">
      <rule enabled="1">
        <match>
          <c name="check-md5" time="2000" />
        </match>
        <action name="drop" />
      </rule>

  </table>
</filter>
```

4.4.1.3.1.6. Условие CHECK-MESSAGE-ID

Проверить заголовок **Message-ID** (для протокола LOTUS проверяется заголовок **X-Sensor-Lotus-MessageId**) сообщения на повторное появление в течение определённого интервала времени (отслеживание дублей сообщений).

Описание

Это условие проверяет, не встречалось ли уже (в течение указанного периода времени) сообщение с таким же заголовком **Message-ID** (для протокола LOTUS проверяется заголовок **X-Sensor-Lotus-MessageId**), как и у текущего проверяемого сообщения.

Формат

```
<c name="check-message-id" time="<timeout>" />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="check-message-id"**.

Атрибут "time":

В атрибуте **time="..."** указывается время ожидания в миллисекундах.

Время ожидания не может быть меньше **1** миллисекунды и больше **5** минут, т.е. 5*60*1000 = 300000 миллисекунд.

Пример:

Если в течение двух секунд были повторные сообщения с таким же заголовком Message-ID - удалять их.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">
    <rule enabled="1">
      <match>
        <c name="check-message-id" time="2000" />
      </match>
      <action name="drop" />
    </rule>

  </table>
</filter>
```

4.4.1.3.1.7. Условие HOSTNAME

Проверить имена хостов источника и назначения в сообщении.

Описание

Это условие проверяет имена хостов источника или назначения на соответствие строке или на соответствие шаблону wildcard или regexp. Для корректной полнофункциональной работы условия необходимо произвести разрешения имён хостов (см. раздел "Действие DNS").

> **Совет:**
> Если необходимо проверить только хост назначения и только для протокола HTTP, то

разрешение имён через действие DNS не имеет смысла, так как имя хоста назначения будет доступно из заголовка Host в HTTP-запросе.

Формат

```
<c name="hostname"
  address="<address type>"
  op="<operation>"
  value="<compare pattern>" />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="hostname"**.

Атрибут "address":

В атрибуте **address="..."** указывается тип адреса для проверки. Возможные значения:

src или client

Проверять только адрес источника;

dst или server

Проверять только адрес назначения;

both или all или *

Проверять оба адреса (и источника и назначения).

Если этот атрибут отсутствует, то подразумевается **"both"** - проверять оба адреса.

Атрибут "op":

Атрибут **op="..."** указывает на тип операции сравнения и может принимать значения:

eq или = или ==

Условие выполняется, если проверяемое значение **СОДЕРЖИТ** указанное значение;

ne или != или <>

Условие выполняется, если проверяемое значение **НЕ СОДЕРЖИТ** указанное значение;

wc или wildcard

Условие выполняется, если проверяемое значение **соответствует** указанному **wildcard**-шаблону;

re или regex или regexp

Условие выполняется, если проверяемое значение **соответствует** указанному **regexp**-шаблону;

Атрибут "value":

В атрибуте **value="..."** указывается строка, с которой сравнивается значение, или шаблон для проверки.

Пример:

Сообщения, отправляемые на хосты *.yandex.ru, забывать.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">
    <rule enabled="1">
      <match>
        <c name="hostname" address="server" op="wc" value="*.yandex.ru" />
      </match>
      <action name="drop" />
    </rule>

  </table>
</filter>
```

4.4.1.3.1.8. Условие IP

Проверить IP-адреса клиента или сервера на вхождение в диапазон или на принадлежность к подсети.

Описание

Это условие проверяет IP-адреса клиента или сервера на вхождение в диапазон или на принадлежность к подсети.

> **Внимание!**
> **1.** Нежелательный трафик нужно отсекать как можно раньше. От этого зависит производительность **Microolap EtherSensor** и среды выполнения.
> **2.** Весь трафик с некоторого IP лучше всего отсекать в IP-фильтре службы ethercap.
> **3.** Определённый трафик HTTP с некоторого IP (если возможно выделить такие критерии) лучше всего отсекать в HTTP-фильтре.
> **4.** Определённые сообщения с некоторого IP-адреса необходимо обрабатывать в фильтре сообщений.

Формат

```
<c name="ip" address="<address type>" value="<ip-range>" />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="ip"**.

Атрибут "address":

В атрибуте **address="..."** указывается тип адреса для проверки. Возможные значения:

src или client

Проверять адрес источника;

dst или server

Проверять адрес назначения;

any или *

Соответствие любого из адресов.

Если атрибут пропущен, то подразумевается по умолчанию - **"*"**.

Атрибут "value":

В атрибуте **value="..."** значение для сравнения. Возможные значения:

ipaddress

Проверяет IP-адрес на равенство. Например, **value="192.168.0.10"**;

ip1-ip2

Проверяет на вхождение IP-адреса в диапазон. Например, **value="192.168.0.1-192.168.0.10"**;

ip/netmask

Проверяет на принадлежность IP-адреса указанной подсети. Например, **value="192.168.0.1/255.255.255.0"**;

ip/netmaskbits

Проверяет на принадлежность IP-адреса указанной подсети. Например, **value="192.168.0.1/24"**.

Пример

Сообщения от клиента с машины 192.168.0.15 забывать.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">

      <rule enabled="1">
        <match>
          <c name="ip" address="client" value="192.168.0.15" />
        </match>
        <action name="drop" />
      </rule>

      <rule enabled="1">
        <action name="accept" />
      </rule>

  </table>
</filter>
```

4.4.1.3.1.9. Условие HEADER

Проверяет значение одного из заголовков сообщения.

Описание

Это условие проверяет значение заголовка сообщения на наличие подстроки в строке или на соответствие шаблону wildcard или regexp. Заголовки сообщения - это любые генерируемые детекторами заголовки метаданных вида **"X-Sensor-…"**.

Также это заголовки из почтовых сообщений, кроме заголовков:

From

To

Cc

Bcc

Subject

Date

Content-Type

Content-Transfer-Encoding

Следует помнить, что для более эффективной фильтрации не стоит фильтровать заголовки метаданных **"X-Sensor-…",** для которых есть специализированные условия проверки. Например, для заголовка **"X-Sensor-Detector"** более эффективно проверять не значение этого заголовка через условие **header**, а использовать специальное условие **<c name="detector" value="…" />**

Формат

```
<c name="header"
   headername="<header name>"
   op="<operation>"
   value="<compare pattern>" />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="header"**.

Атрибут "headername":

В атрибуте **headername="..."** указывается имя проверяемого заголовка.

Атрибут "op":

Атрибут **op="..."** указывает на тип операции сравнения и может принимать значения:

eq или = или ==

Условие выполняется, если проверяемое значение **СОДЕРЖИТ** указанное значение;

ne или != или <>

Условие выполняется, если проверяемое значение **НЕ СОДЕРЖИТ** указанное значение;

wc или wildcard

Условие выполняется, если проверяемое значение **соответствует** указанному **wildcard**-шаблону;

re или regex или regexp

Условие выполняется, если проверяемое значение **соответствует** указанному **regexp**-шаблону;

Атрибут "value":

В атрибуте **value="..."** указывается строка, с которой сравнивается значение, или шаблон для проверки.

Примеры

```
<c name="header" headername="X-Priority" op="eq" value="3" />
```

Условие выполняется, если в сообщении присутствует заголовок **X-Priority** и его значение содержит строку **"3"**.

```
<c name="header" headername="X-Mailer" op="!=" value="Outlook" />
```

Условие выполняется, если в сообщении присутствует заголовок **X-Mailer** и его значение не содержит строку **"Outlook"**.

```
<c name="header"
   headername="X-Sensor-Net-Interface-Id"
   op="eq"
   value="01-icap" />
```

Условие выполняется, если в сообщении присутствует заголовок **X-Sensor-Net-Interface-Id** и его значение содержит строку **"01-icap"**.

```
<c name="header"
   headername="X-Sensor-Net-Interface-Id"
   op="wc"
   value="*-icap" />
```

или

```
<c name="header"
   headername="X-Sensor-Net-Interface-Id"
   op="wildcard"
   value="*-icap" />
```

Условие выполняется, если в сообщении присутствует заголовок **X-Sensor-Net-Interface-Id** и его значение соответствует **wildcard**-шаблону **"*-icap"**.

Пример

Сообщения, отправляемые через Outlook, забывать.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">
    <rule enabled="1">
      <match>
        <c name="header"
           headername="X-Mailer"
           op="=="
           value="Outlook" />
      </match>
      <action name="drop" />
    </rule>

  </table>
</filter>
```

4.4.1.3.1.10. Условие ATTACH-NAME

Проверить имена вложений (аттачментов) в сообщении.

Описание

Это условие проверяет имена вложений (аттачментов) на соответствие строке или на соответствие шаблону wildcard или regexp.

Формат

```
<c name="attach-name" op="<operation>" value="<compare pattern>" />
```

Атрибут name:

В атрибуте **name** указывается имя условия - **name="attach-name"**.

Атрибут op:

В атрибуте **op="..."** указывает тип операции сравнения и может принимать значения:

eq или = или ==

Условие выполняется, если проверяемое значение **СОДЕРЖИТ** указанное значение;

ne или != или <>

Условие выполняется, если проверяемое значение **НЕ СОДЕРЖИТ** указанное значение;

wc или wildcard

Условие выполняется, если проверяемое значение **соответствует** указанному **wildcard**-шаблону;

re или regex или regexp

Условие выполняется, если проверяемое значение **соответствует** указанному **regexp**-шаблону;

Атрибут "value":

В атрибуте **value="..."** указывается строка, с которой сравнивается значение, или шаблон для проверки.

Пример

```
<c name="attach-name" op="eq" value="instruction.doc" />
```

Условие выполняется, если какое-либо имя вложения (аттачмент) сообщения содержит **"instruction.doc"**.

```
<c name="attach-name" op="eq" value="instruction.doc" />
```

Условие выполняется если какое-либо имя вложения (аттачмент) сообщения не содержит **"instruction.doc"**.

```
<c name="attach-name" op="wc" value="*.doc" />
```

или

```
<c name="attach-name" op="wildcard" value="*.doc" />
```

Условие выполняется, если какое-либо имя вложения (аттачмент) сообщения соответствует wildcard-шаблону **"*.doc"**.

```
<c name="attach-name" op="re" value=".+\.doc" />
```

или

```
<c name="attach-name" op="regexp" value=".+\.doc" />
```

Условие выполняется, если какое-либо имя вложения (аттачмент) сообщения соответствует regex-шаблону **".+\.doc"**.

```
<c name="attach-name" op="re" value=".+((\.doc)|(\.exe)|(\.zip))" />
```

Условие выполняется если какое-либо имя вложения (аттачмент) сообщения соответствует regex-шаблону **".+((\.doc)|(\.exe)|(\.zip))"**.

Пример

Сообщения с вложениями ***.exe** забывать.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">
    <rule enabled="1">
      <match>
        <c name="attach-name" op="re" value=".+\.exe" />
      </match>
      <action name="drop" />
    </rule>

  </table>
</filter>
```

4.4.1.3.1.11. Условие ATTACH-EXIST

Проверить сообщение на наличие вложений (аттачментов).

Описание

Это условие, под которое попадают сообщения, содержащие любые вложения (аттачменты).

Формат

```
<c name="attach-exist" />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="attach-exist"**.

Пример

Сообщения с любыми вложениями забывать.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">
    <rule enabled="1">
      <match>
        <c name="attach-exist" />
      </match>
      <action name="drop" />
    </rule>

  </table>
</filter>
```

4.4.1.3.1.12. Условие TAG

Проверяет наличие установленного тега и значение его счётчика (см. раздел "Действие TAG").

Описание

Это условие проверяет существование тега или значение счётчика тега.

Если тег отсутствует - условие не выполняется.

Формат

```
<c name="tag" op="<operation>" value="<compare value>" />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="tag"**.

Атрибут "op":

Атрибут **op="..."** указывает на критерий проверки:

eq или = или ==

Условие выполняется, если значение счётчика **РАВНО** указанному числу;

ne или != или <>

Условие выполняется, если значение счётчика **НЕ РАВНО** указанному числу;

lt или <

Условие выполняется, если значение счётчика **МЕНЬШЕ** указанного числа;

gt или >

Условие выполняется, если значение счётчика **БОЛЬШЕ** указанного числа;

le или <=

Условие выполняется, если значение счётчика **МЕНЬШЕ ИЛИ РАВНО** указанного числа;

ge или >=

Условие выполняется, если значение счётчика **БОЛЬШЕ ИЛИ РАВНО** указанного числа;

exist

Условие выполняется, если тег **существует** (уже установлен ранее для этого объекта);

По умолчанию (если атрибут **op** отсутствует) принимается значение **"exist"**. Для операции "**exist**" указывать атрибут **value** не обязательно.

Атрибут "value":

В атрибуте **value="..."** указывается число, с которым сравнивается значение счётчика тега.

Пример

```
<c name="tag" tag="SPAM" op="exist" />
```

или

```
<c name="tag" tag="SPAM" />
```

Условие выполняется, если для объекта установлен тег "**SPAM**".

```
<c name="tag" tag="SPAM" op="eq" value="1" />
```

Условие выполняется, если для сообщения установлен тег "**SPAM**" и его счётчик равен **1**.

```
<c name="tag" tag="SPAM" op=">" value="1" />
```

Условие выполняется, если для сообщения установлен тег "**SPAM**" и его значение его счётчика больше **1**.

```
<c name="tag" tag="SPAM" op=">=" value="3" />
```

Условие выполняется, если для сообщения установлен тег "**SPAM**" и его значение его счётчика больше или равно **3**.

Пример

Сообщения, помеченные тегом **SPAM** со значением больше **1**, забывать.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">
    <rule enabled="1">
      <match>
        <c name="tag" tag="SPAM" op=">" value="1" />
      </match>
      <action name="drop" />
    </rule>

  </table>
</filter>
```

4.4.1.3.1.13. Условие FROM, TO, CC, BCC, ADDRESS, SUBJECT

Проверить значение одного из полей **from, to, cc, bcc, subject, address**.

Описание

Это условие проверяет значение поля на содержание указанной подстроки или на соответствие шаблону wildcard или regexp.

from

Проверяет поле FROM (адрес отправителя);

to

Проверяет поле TO (адрес получателя);

cc

Проверяет поле CC;

bcc

Проверяет поле BCC;

address

Проверяет все поля адресов (**from, to, cc, bcc**). Если в любом из них найдено соответствие, то условие выполняется;

subject

Проверяет поле SUBJECT.

Формат

```
<c name="from" op="<operation>" value="<compare pattern>" />
<c name="to" op="<operation>" value="<compare pattern>" />
<c name="cc" op="<operation>" value="<compare pattern>" />
<c name="bcc" op="<operation>" value="<compare pattern>" />
<c name="subject" op="<operation>" value="<compare pattern>" />
<c name="address" op="<operation>" value="<compare pattern>" />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="from"**, **name="to"**, **name="cc"**, **name="bcc"**, **name="subject"** или **name="address"**

Атрибут "op":

Атрибут **op="..."** указывает на тип операции сравнения и может принимать значения:

eq или = или ==

Условие выполняется, если значение поля **СОДЕРЖИТ** указанное значение;

ne или != или <>

Условие выполняется, если значение поля **НЕ СОДЕРЖИТ** указанное значение;

wc или wildcard

Условие выполняется, если значение поля **соответствует** указанному **wildcard**-шаблону;

re или regex или regexp

Условие выполняется, если значение поля **соответствует** указанному **regexp**-шаблону.

Атрибут value:

В атрибуте **value="..."** указывается строка, с которой сравнивается значение, или шаблон для проверки.

Пример

```
<c name="from" op="eq" value="xxx@mail.ru" />
```

Условие выполняется, если поле **FROM** сообщения содержит строку **"xxx@mail.ru"**.

```
<c name="to" op="!=" value="xxx@mail.ru" />
```

Условие выполняется, если поле **TO** сообщения не содержит строку **"xxx@mail.ru"**.

```
<c name="cc" op="wc" value="*@mail.ru" />
```

или

```
<c name="cc" op="wildcard" value="*@mail.ru" />
```

Условие выполняется, если поле **CC** сообщения соответствует wildcard-шаблону **"*@mail.ru".**

```
<c name="address" op="re" value=".+@mail.ru" />
```

или

```
<c name="address" op="regexp" value=".+@mail.ru" />
```

Условие выполняется, если любое из адресных полей сообщения (**FROM, TO, CC** или **BCC**) соответствует regex-шаблону **"+@mail.ru".**

```
<c name="subject" op="re" value=".*((badword1)|(badword2)|(badword3)).*" />
```

Условие выполняется, если в теме сообщения найдено соответствие regex-шаблону **".*((badword1)|(badword2)|(badword3)).*"**.

Проще говоря - условие выполняется, если в теме есть слова **badword1**, **badword2** или **badword3**.

```
<c name="subject" op="re"
   value="(\+?\d([ \-\(])?\d{3}([ \-\)])?)?([ -])?((\d{7})|
          (\d{3}([ \-])?\d{2}([ \-])?\d{2})|
          (\d{2}([ \-])?\d{3}([ \-])?\d{2}))" />
```

Условие выполняется, если в теме сообщения найден номер телефона (строка, соответствующая regexp).

Телефонный номер в этом случае может соответствовать одному из следующих форматов:

1234567

123 45 67

12 345 67

89031234567

8(903)1234567

8-903-123-45-67

8 903 123 45 67

+79031234567

+7(903)1234567

+7-903-123-45-67

+7 903 123 45 67

Пример

Письма с/на адреса ***@mail.ru** продолжить обрабатывать, всё остальное забыть.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">

    <rule enabled="1">
      <match>
        <c name="address" op="wildcard" value="*@mail.ru" />
      </match>
      <action name="accept" />
    </rule>

    <rule enabled="1">
      <action name="drop" />
    </rule>

  </table>
</filter>
```

4.4.1.3.1.14. Условие TEXT

Проверить наличие ключевых слов в тексте сообщения или в его теме.

Описание

Это условие проверяет наличие ключевых слов в тексте сообщения или теме.

Проверка наличия происходит по общему вхождению ключевого слова в текст, а не только как отдельные слова.

Это можно выразить, как будто для каждого ключевого слова ищется wildcard-шаблон "*ключевое слово*".

Например, под критерий ключевого слова **"secret"** будут попадать слова **"secret"**, **"sECrEt"**, **"secretary"**, **"insecretory"** и т.п.

При поиске ключевых слов регистр символов не учитывается.

Формат

```
<c name="text" op="<operation>" value="<compare pattern>" />
<c name="text" op="<operation>" data="<data source>" />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="text"**.

Атрибут op:

Атрибут **op="..."** указывает на критерий проверки:

all

В сообщении должны быть установлены все указанные метки;

one

Достаточно, чтобы в сообщении была установлена хотя бы одна метка.

По умолчанию (если атрибут **op** отсутствует) принимается значение **"one"**.

Атрибут "value":

В атрибуте **value="..."** перечисляются ключевые слова. Если ключевых слов несколько, они перечисляются через запятую ',**'**. Также ключевые слова могут быть указаны в значении самого тега **<c>key-word-list</c>**

Атрибут "data":

В атрибуте **data="..."** может указываться другой источник ключевых слов. Это позволяет указывать большие наборы слов, когда это неудобно делать в атрибуте **value="..."**.

Возможные значения:

data="<extern data name>"

Загрузить список ключевых слов из внешнего блока в фильтре (тег **<data name="extern-data-name">...</data>**);

data="extern://<extern data name>"

Загрузить список ключевых слов из внешнего блока в фильтре (тег **<data name="extern-data-name">...</data>**). Ключевые слова перечисляются через запятую;

data="file://<full-file-path>"

Загрузить список ключевых слов из указанного файла. Ключевые слова перечисляются каждое на отдельной строке (запятые не нужны).

Пример

```
<c name="text" op="one" value="secret1, secret2, secret3, secret4" />
```

или

```
<c name="text" op="one">secret1, secret2, secret3, secret4</c>
```

Условие выполняется, если в теме сообщения или в его тексте найдётся хотя бы одно из указанных ключевых слов: как самостоятельных слов, либо как часть другого слова.

Примеры текстов:

1. Тема письма - "**RE: secret 1 secret2**" - условие ВЫПОЛНЯЕТСЯ.

2. Тема письма - "**RE: secret3 secret4**" - условие ВЫПОЛНЯЕТСЯ.

3. Текст письма - "**посылаю вам наш secret 1 secret2**" - условие ВЫПОЛНЯЕТСЯ.

4. Тема письма - "**Съешь ещё этих мягких французских булок**" - условие НЕ ВЫПОЛНЯЕТСЯ.

```
<c name="text" op="all" value="secret1, secret2" />
```

или

```
<c name="text" op="all">secret1, secret2</c>
```

Условие выполняется, если в теме сообщения или в его тексте найдутся оба указанных ключевых слова как самостоятельные слова, или же, как части других слов.

Примеры текстов:

1. Тема письма - "**RE: secret1 secret2**" - условие ВЫПОЛНЯЕТСЯ.

2. Тема письма - "**RE: secret1 от буха**" - условие НЕ ВЫПОЛНЯЕТСЯ.

3. Текст письма - "**посылаю вам наш secret2**" - условие НЕ ВЫПОЛНЯЕТСЯ.

4. Текст письма - "**посылаю вам наш secret1 от secret2**" - условие ВЫПОЛНЯЕТСЯ.

```
<c name="text" op="one" data="dictionary.txt" />
```

Загрузить список ключевых слов для проверки из файла **"dictionary.txt"**.

Пример

Письма, содержащие ключевые слова из списка **keywords**, взять на дальнейшую обработку. Всё остальное забыть.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">

    <rule enabled="1">
      <comment></comment>
      <match>
        <c name="text" data="extern://keywords" />
      </match>
      <action name="accept" />
    </rule>

    <rule enabled="1">
      <action name="drop" />
    </rule>

  </table>

  <data name="keywords">
        secret1,
        secret2,
        secret3,
        secret4
  </data>

</filter>
```

4.4.1.3.2. Действия

Все **действия (actions)** описываются в XML-тегах **<action>**. Для каждого действия указывается его имя в атрибуте **name**, которое определяет, какая операция будет выполнена над сообщением. В прочих атрибутах тега указываются параметры для выполнения действия. Имена атрибутов дополнительных параметров зависят от конкретных действий.

Общая структура XML-тега, описывающего действие:

```
<action name="action name" [parameters] />
```

или

```
<action name="action name" [parameters]></action>
```

Большинство **действий (actions)** использует атрибут **value="…"**, в котором указываются значения для выполнения действия, или атрибут **data="…"**, в котором можно указывать внешний файл для загрузки данных для выполнения действия (это могут быть наборы слов, списки доменных имён и другие параметры). Описание атрибутов и их действий подробно указано в разделах соответствующих **действий (actions)**.

Базовые действия

Базовые действия - это действия, изменяющие порядок прохождения сообщения через фильтр. К базовым действиям относятся **ACCEPT, DROP, JUMP** и **RETURN.**

Пользовательские действия

Пользовательские действия - это действия, изменяющие сообщение или его метаданные, а также выполняющие обработку сообщения через внешние сервисы (антивирусы, URL-категоризаторы, DNS-blacklist и т.п.).

4.4.1.3.2.1. Действие ACCEPT

Пропустить сообщение к дальнейшей обработке.

Описание

Действие **ACCEPT** прекращает работу фильтров с текущим сообщением и немедленно пропускает его к дальнейшей обработке (то есть, транспортировке согласно предопределенному транспортному профилю или профилю по умолчанию).

Формат

```
<action name="accept" />
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="accept"**.

Пример:

Сообщения, достигшие этого правила, принимаются к дальнейшей обработке.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">
    <rule enabled="1">
      <match ...> ... </match>
      <action ...> ... </action>
    </rule>

    <rule enabled="1">
      <comment>
        All the messages reaching this rule are accepted for
        further processing.
      </comment>
      <action name="accept" />
    </rule>
  </table>
</filter>
```

4.4.1.3.2.2. Действие DROP

Забыть сообщение без продолжения дальнейшей обработки.

Описание

Это действие прекращает обработку текущего сообщения и сообщает **Microolap EtherSensor**, что данные о нем необходимо уничтожить ("забыть").

Формат

```
<action name="drop" />
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="drop"**.

Пример:

Данные и метаданные сообщений, достигших этого правила, уничтожить ("забыть").

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">
    <rule enabled="1">
      <comment>
        Details/metadata of any message reaching this point
        are destroyed (discarded).
      </comment>
      <action name="drop" />
    </rule>
  </table>
</filter>
```

4.4.1.3.2.3. Действие JUMP

Продолжить обработку сообщения в другой таблице.

Описание

Это действие продолжает обработку сообщения в другой таблице.

Формат

```
<action name="jump" value="<table name>" />
```

<action name="jump" value="<table name>" />

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="jump"**.

Атрибут "value":

В атрибуте **value="..."** указывается имя таблицы, в которую необходимо перейти для дальнейшей обработки сообщения.

Внимание!
Следует помнить, что переход в таблицу **main** запрещён.

Также запрещены переходы, которые могут привести к явной или неявной цикличности.

Пример:

Из таблицы **main** переход в таблицу **yandex** для обработки сообщений от mail.ru и yandex.ru. Таблица **yandex**: единственное правило уничтожает сообщения больше 100 kb. После этого происходит возврат в таблицу **main**.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">
    <rule enabled="1">
      <comment>
        Processing of messages from the mail.ru,
        yandex.ru detectors in the yandex table.
      </comment>
      <match>
        <c name="detector" value="mail.ru, yandex.ru" />
      </match>
      <action name="jump" value="yandex"/>
    </rule>

    <rule enabled="1">
      <action name="drop" />
    </rule>
  </table>

  <table name="yandex">
    <comment>
      The table processes messages from the mail.ru,
      yandex.ru detectors.
    </comment>

    <rule enabled="1">
      <comment>
        Discard messages larger than 100 Kb.
      </comment>
      <match>
        <c name="size" op=">" value="100K"/>
      </match>
      <action name="drop" />
    </rule>

    <rule enabled="1">
      <comment>
        Returning to the main table for further processing.
      </comment>
      <action name="return" />
    </rule>
  </table>

</filter>
```

4.4.1.3.2.4. Действие RETURN

Вернуться в предыдущую (вызвавшую) таблицу и продолжить выполнение в ней со следующего правила.

Описание

Это действие возвращает обработку сообщения в предыдущую (вызвавшую) таблицу и продолжить выполнение в ней со следующего правила.

Формат

```
<action name="return" />
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="return"**.

Внимание!
Действие не может применяться в таблице **main**.

Примеры:

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">
    <rule enabled="1">
      <comment>
        Processing of messages from the mail.ru,
        yandex.ru detectors in the yandex table.
      </comment>
      <match>
        <c name="detector" value="mail.ru, yandex.ru" />
      </match>
      <action name="jump" value="yandex"/>
    </rule>

    <rule enabled="1">
      <action name="drop" />
    </rule>
  </table>

  <table name="yandex">
    <comment>
      The table processes messages from the mail.ru,
      yandex.ru detectors.
    </comment>

    <rule enabled="1">
      <comment>
        Discard messages larger than 100 Kb.
      </comment>
      <match>
        <c name="size" op=">" value="100K"/>
      </match>
      <action name="drop" />
    </rule>

    <rule enabled="1">
    <comment>
      Returning to the main table for further processing.
    </comment>
    <action name="return" />
    </rule>
  </table>
</filter>
```

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="main filter" version="1.0">

  <table name="main">

    <rule enabled="1">
      <match ...> ... </match>
      <action ...> ... </action>
    </rule>

    <rule name="spam" enabled="1">
      <match ...> ... </match>
      <action name="jump" value="spam"/>
    </rule>

    <rule enabled="1">
      <action name="drop" />
    </rule>

  </table>

  <table name="spam">
    <rule enabled="1">
      <match ...> ... </match>
      <action ...> ... </action>
    </rule>

    <rule enabled="1">
      <match ...> ... </match>
      <action ...> ... </action>
    </rule>

    <rule name="return-to-main" enabled="1">
      <action name="return" />
    </rule>

  </table>
</filter>
```

В данном примере в таблице **main** происходит некая обработка сообщения. При обработке сообщения вторым правилом стоит правило с именем **spam:** если сообщение проходит критерий этого правила, то оно передаётся на дальнейшую обработку во вторую таблицу **spam**.

После прохождения в таблице **spam**, если обработка сообщения не будет прервана предыдущими правилами, то дойдя до правила с именем **return-to-main**, обработка сообщения снова продолжится в таблице **main** с правила, следующего за правилом **spam**.

4.4.1.3.2.5. Действие LABEL

Добавляет к метаданным сообщения строковую метку.

Описание

Это действие устанавливает ярлык (строковую метку) в метаданных текущего обрабатываемого сообщения.

Если данный ярлык уже был ранее установлен для сообщения (или HTTP-объекта, из которого получено сообщение), то его значение заменяется более новым.

Используется для добавления описаний к сообщениям.

Формат

```
<action name="label" label="<label name>" value="<label value>" />
```

или

```
<action name="label" label="<label name>" > label value </action>
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="label"**.

Атрибут "label":

В атрибуте **label="..."** указывается имя устанавливаемой строковой метки.

Атрибут "value":

В атрибуте **value="..."** указывается значение (строка) для метки.

Значение также можно перечислять в самом теге **<action>**.

Пример

```
<action name="label"
        label="VIRUS-DESCR"
        value="Win.32.BlackHorse.trojan.virus - mail worm, very dangerous!!!" />
```

или

```
<action name="label"
        label="VIRUS-DESCR">
          Win.32.BlackHorse.trojan.virus -
          mail worm, very dangerous!!!
</action>
```

Устанавливает для сообщения строковую метку с именем "VIRUS-DESCR" и записывает в неё строку *"Win.32.BlackHorse.trojan.virus - mail worm, very dangerous!!!"*.

Пример

Пометить сообщения, обработанные детекторами mail.ru, yandex.ru меткой CONTENT-DESCR.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="TEST" version="1.0">
  <comment>This is the comment for the filter.</comment>
  <table name="main">

    <rule enabled="true">
      <comment>
        Mark messages detected by the mail.ru,
        yandex.ru detectors with the CONTENT-DESCR label.
      </comment>
      <match>
        <c name="detector" value="mail.ru, yandex.ru" />
      </match>
      <action name="label"
              label="CONTENT-DESCR"
              value="Russian mail services"/>
    </rule>

    <rule enabled="true">
      <match><c name="all"/></match>
      <action name="accept" />
    </rule>

  </table>
</filter>
```

4.4.1.3.2.6. Действие TAG

Добавляет к метаданным сообщения тег (числовую метку).

Описание

Это действие устанавливает в метаданных сообщения тег (числовую метку). Тегов может быть несколько. В этом случае они перечисляются через запятую '**,**' или точку с запятой '**;**'. Если один и тот же тег устанавливать для объекта несколько раз, то у тега повышается "уровень" (его числовое значение). Иначе говоря, у каждого тега есть внутренний счётчик, показывающий, сколько раз он был установлен для этого объекта.

Установлен тег или нет, а также значение его счётчика (сколько раз он был установлен для текущего объекта) можно впоследствии проверять в условиях фильтров для принятия решений.

По умолчанию значение счётчика при установке тега увеличивается на **1**. Если счётчик тега необходимо увеличить более чем на **1**, то можно задавать значение на которое необходимо увеличить счётчик после имени тега в круглых скобках: **"TAG(...)"**. Например, **SPAM(3)** - увеличивает значение счётчика для тега **SPAM** на **3**, а **SPAM(1)** равносильно просто **SPAM**. Это может быть необходимо в случаях, когда условия, устанавливающие один и тот же тег, имеют разную значимость, важность или приоритет.

Значение для изменения счётчика может быть отрицательным. **SPAM(-3)** - уменьшает значение счётчика для тега **SPAM** на **3**.

Формат

```
<action name="tag" value="<tag list>" />
```

или

```
<action name="tag" > tag list </action>
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="tag"**.

Атрибут "value":

В атрибуте **value="..."** перечисляются имена тегов.

Имена тегов также можно перечислять в самом теге **<action>**.

Пример

```
<action name="tag" value="SPAM" />
```

Устанавливает тег с именем "SPAM".

```
<action name="tag" value="SPAM(3)" />
```

Устанавливает тег с именем "SPAM" и увеличивает его счётчик на 3.

```
<action name="tag" value="SPAM, shopping" />
```

Устанавливает теги с именами "SPAM" и "shopping".

```
<action name="tag" value="SPAM(3), shopping(2)" />
```

Устанавливает теги с именами "SPAM" и "shopping" и увеличивает их счётчики на 3 и 2 соответственно.

```
<action name="tag" value="SPAM, shopping">VIP-OFFICE</action>
```

Также устанавливает теги с именами "SPAM" и "shopping".

```
<action name="tag" value="SPAM, shopping">VIP-OFFICE</action>
```

Устанавливает теги с именами "SPAM", "shopping", "VIP-OFFICE".

Пример

Пометить запросы на популярные российские почтовые сервисы тегом RUS_MAIL.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="TEST" version="1.0">
  <comment>This is the comment for the filter.</comment>
  <table name="main">

    <rule enabled="true">
      <comment>
        Mark requests to popular Russian mail services
        with the RUS_MAIL tag.
      </comment>
      <match>
        <c name="req-header"
           headername="Host"
           op="eq"
           value="win.mail.ru" />
        <c name="req-header"
           headername="Host"
           op="eq"
           value="mail.yandex.ru" />
        <c name="req-header"
           headername="Host" op="eq"
           value="mail.rambler.ru" />
      </match>
      <action name="tag" value="RUS_MAIL"/>
    </rule>

    <rule enabled="true">
      <match><c name="all"/></match>
      <action name="accept" />
    </rule>

  </table>
</filter>
```

4.4.1.3.2.7. Действие DATETIME

Установить для сообщения строковую метку со значением текущих даты и времени.

Описание

Это действие устанавливает строковую метку (**label**) для сообщения, её значением становится строка текущих даты и времени. Если данная строковая метка уже была ранее установлена для сообщения, то её значение заменяется более новым. Используется для отслеживания времени прохождения сообщения по фильтру.

Формат

```
<action name="datetime" value="label-name" />
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="datetime"**.

Атрибут "value":

В атрибуте **value="..."** указывается имя устанавливаемой строковой метки.

Пример:

Добавить метку начала обработки FILTER-BEGIN и метку конца обработки FILTER-END во все сообщения.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">
    <rule enabled="1">
      <comment>
        Set the FILTER-BEGIN processing start label
        for all the messages.
      </comment>
      <action name="datetime" value="FILTER-BEGIN" />
    </rule>

    <rule enabled="1">
      <comment>
        Set the FILTER-END processing end label
        for all the messages.
      </comment>
      <action name="datetime" value="FILTER-END" />
      <action name="accept" />
    </rule>
  </table>
</filter>
```

4.4.1.3.2.8. Действие DNS

Проводит разрешение имён DNS в IP-адреса и IP-адреса в имена для неизвестных адресов хостов.

Описание

Это действие производит разрешение имён хостов и IP-адресов сессии.

В каждой сессии есть источник (клиент) и приёмник (сервер) со своими именами или IP-адресами. Возможна ситуация, когда для сообщения известно имя хоста клиента или сервера, но не известен его IP-адрес или наоборот. Действие **DNS** производит разрешение недостающей информации об адресе клиента или сервера.

Если известен IP-адрес, но не известно имя хоста, соответствующее этому IP, то оно находится (если возможно). То же самое делается и если известно имя хоста, но не известен его IP-адрес. Если в сообщении уже присутствует и имя хоста и его IP, то никаких действий не производится.

Также в случае успешного получения имён в метаданные добавляются заголовки **X-Sensor-Src-Host**, **X-Sensor-Dst-Host** и становится возможным их использование в условии **"header"** (проверка значения заголовка).

Следует также помнить, что условие типа **"hostname"** (проверка имени хоста) имеет смысл применять только после выполнения действия **DNS**.

Формат

```
<action name="dns" address="<address type for resolving>" />
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="dns"**.

Атрибут address:

В атрибуте **address="..."** указывается тип адреса для разрешения имен. Возможные значения:

src или client

Проводить разрешение имен только для адреса источника;

dst или server

Проводить разрешение имен только для адреса назначения;

both или all или *

Проводить разрешение имен для обоих адресов (и источника и назначения).

Если этот атрибут отсутствует, то подразумевается действие **"both"** - проводить разрешение имен для обоих адресов.

Пример

Провести разрешение имен для сообщения.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="TEST" version="1.0">
  <comment>This is the comment for the filter.</comment>
  <table name="main">

    <rule enabled="true">
      <comment>
        Resolve names for the message.
      </comment>
      <action name="dns" address="server"/>
    </rule>

    <rule enabled="true">
      <match><c name="all"/></match>
      <action name="accept" />
    </rule>

  </table>
</filter>
```

4.4.1.3.2.9. Действие DNSBL-LH, DNSBL-RH

Проверяет вхождение адресов сообщения в DNSBL списки, и при вхождении устанавливает указанный тег.

Описание

dnsbl-rh - проверка IP-адреса в DNSBL-RHSBL.

dnsbl-lh - проверка имени хоста в DNSBL-LHSBL.

При попадании одного из адресов в один из DNSBL это действие увеличивает значение указанного тега на **1**.

Список проверяется всегда полностью.

Попадание каждого адреса (или имени хоста) в каждый DNSBL увеличивает тег на **1**. То есть, если в один и тот же DNSBL попадают и адрес источника и адрес назначения, то на каждое попадание происходит увеличение тега.

В дальнейшем значение тега можно проверять в условиях фильтров и принимать решение на основании вхождения адресов сообщения в DNSBL.

Формат

```
<action name="dnsbl-rh"
        address="<address-type>"
        tag="<tag-name>"
        value="<dns-bl domains list>" />
<action name="dnsbl-rh"
        address="<address-type>"
        tag="<tag-name>"
        data="<dns-bl domains list source>" />
<action name="dnsbl-lh"
        address="<address-type>"
        tag="<tag-name>"
        value="<dns-bl domains list>" />
<action name="dnsbl-lh"
        address="<address-type>"
        tag="<tag-name>"
        data="<dns-bl domains list source>" />
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="dns"**.

Атрибут "address":

В атрибуте **address="..."** указывается тип адреса для разрешения имен. Возможные значения:

src или client

Проверять только адрес источника;

dst или server

Проверять только адрес назначения;

both или all или *

Проверять оба адреса (и источника и назначения).

Если этот атрибут отсутствует, то подразумевается действие **"both"** - проверять оба адреса.

Атрибут "tag":

В атрибуте **tag="..."** указывается имя увеличиваемого тега.

Атрибут "value":

В атрибуте **value="..."** перечисляются домены DNSBL.

Если доменов несколько, они перечисляются через запятую ','.

Также домены могут быть указаны в значении самого тега **<action >dns-bl-domains-list</action>**

Атрибут "data":

В атрибуте **data="..."** может указываться другой источник списка DNSBL доменов. Это позволяет указывать длинные списки, когда это неудобно делать в атрибуте **value="..."**.

Возможные значения:

data="<extern data name>"

Загрузить список из внешнего блока в фильтре (тег **<data name="extern-data-name">...</data>**)

data="extern://<extern data name>"

Загрузить список из внешнего блока в фильтре (тег **<data name="extern-data-name">...</data>**). Домены DNSBL перечисляются через запятую.

data="file://<full-file-path>"

Загрузить список из указанного файла. Домены DNSBL перечисляются на отдельных строках (запятые не нужны).

Пример

```
<action name="dnsbl-rh" tag="SPAM">
  bl.spamcop.net, vote.drbl.sandy.ru,
  sbl.spamhaus.org, cblplus.anti-spam.org.cn
</action>
```

Увеличивает тег "**SPAM**", если адреса сообщения попадают в один из DNSBL. Если какой либо адрес попадает в только один список - "**SPAM**" будет равен **1**. Если адрес попадает в два списка - "**SPAM**" будет равен **2** и т.д.

В дальнейшем можно проверить, если ("**SPAM**" > **3**), то это точно спам, а если меньше - то просто подозрительно. Если оба адреса попадают в один DNSBL, то тег увеличивается на **2**.

```
<action name="dnsbl-rh" address="src" tag="SPAM">
  bl.spamcop.net, vote.drbl.sandy.ru,
  sbl.spamhaus.org, cblplus.anti-spam.org.cn
</action>
```

Проверяет только IP-адрес источника.

```
<action name="dnsbl-lh" address="dst" tag="SPAM">
  bl.spamcop.net, vote.drbl.sandy.ru,
  sbl.spamhaus.org, cblplus.anti-spam.org.cn
</action>
```

Проверяет только **hostname** назначения.

Пример

Проверить все адреса сообщения через DNS-BL list. Положительные срабатывания пометить тегом SPAM. Сообщения с тегом SPAM удалить, остальные принять.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">
    <rule enabled="1">
      <comment>
        Checks all message addresses against the DNS-BL list. Hits
        are to be marked with the SPAM tag.
      </comment>
      <action name="dnsbl-rh"
              address="both" tag="SPAM"
              data="extern://dns-bl-list" />
    </rule>

    <rule enabled="1">
      <comment>Delete spam.</comment>
      <match>
        <c name="tag-exist" value="SPAM" />
      </match>
      <action name="drop" />
    </rule>

    <rule enabled="1">
      <comment>Accept the rest.</comment>
      <action name="accept" />
    </rule>

  </table>

  <data name="dns-bl-list">
    bl.spamcop.net,
    vote.drbl.sandy.ru,
    sbl.spamhaus.org,
    cblplus.anti-spam.org.cn
  </data>

</filter>
```

4.4.1.3.2.10. Действие SAVE RAW DATA

Включить/выключить для сообщения сохранение исходных данных, из которых оно было получено.

Описание

Это действие включает/выключает для сообщения сохранение исходных данных, из которых оно было получено. В случае если сообщение получено из перехвата HTTP-трафика, то исходными данными будут два файла, содержащие HTTP-запрос и HTTP-ответ. В случае если сообщение получено из SMTP- или POP3-перехвата, то исходными данными будет файл ,содержащий исходный email в формате EML.

По умолчанию для каждого сообщения сохранение исходных данных **отключено**. Если включить сохранение исходных данных для сообщения, то файлы с исходными данными будут приложены к сообщению в качестве вложений (аттачментов).

Стоит помнить, что включение сохранения исходных данных более чем в 2 раза увеличивает объем сохраняемых данных, поэтому данной возможностью стоит пользоваться только для отладочных целей, или же когда наличие исходных данных крайне необходимо.

Формат

```
<action name="save-raw-data" value="<true/false/1/0>" />
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="save-raw-data"**.

Атрибут "value":

В атрибуте **value="..."** указывается активность действия.

true или 1

Включить сохранение исходных данных для сообщения.

false или 0

Отключить сохранение исходных данных для сообщения (если ранее в фильтре оно было включено).

Пример:

Включить сохранение исходных данных сообщений, полученных по HTTP-протоколу.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">
    <rule enabled="1">
      <comment>
        Enable saving source data for messages
        intercepted over the HTTP protocol.
      </comment>
      <match>
        <c name="protocol" value="http" />
      </match>
      <action name="save-raw-data" value="true" />
    </rule>

  </table>
</filter>
```

4.4.1.3.2.11. Действие TRANSPORT

Установить транспортный профиль для сообщения, которым оно должно быть доставлено в случае его успешной обработки фильтром с действием **ACCEPT**.

Описание

Если такой транспортный профиль уже был ранее установлен для сообщения, то действие ничего не выполняет.

Для сообщения можно указывать несколько транспортных профилей, для этого указываются несколько действий **transport**.

Если в ходе фильтрации для сообщения не было применено ни одного транспортного профиля, то сообщение в случае принятия будет доставлено **профилем по умолчанию**.

Формат

```
<action name="transport" value="<transport-profile-name>" />
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="transport"**.

Атрибут "value":

В атрибуте **value="..."** указывается имя устанавливаемого транспортного профиля.

Пример:

Установить транспортные профили "smtp-archive" и "smtp-archive-rezerv" для всех сообщений. Если сообщение будет принято фильтром, то оно будет доставлено с помощью ОБОИХ профилей.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">
  <comment>Message filter.</comment>

  <table name="main">

    <rule enabled="1">
      <comment>
        Set the "smtp-archive" and "smtp-archive-rezerv"
        transport profiles for all messages. If the message
        is accepted by the filter, it will be delivered by
        BOTH profiles.
      </comment>
      <action name="transport" value="smtp-archive" />
      <action name="transport" value="smtp-archive-rezerv" />
    </rule>

    </table>
</filter>
```

4.4.1.3.2.12. Действие HEADER

Добавляет к метаданным объекта пользовательский заголовок **X-Sensor-...** или изменяет значение существующего **X-Sensor-...** заголовка.

Описание

Это действие добавляет в сообщение пользовательский заголовок **X-Sensor-...**

Если заголовок с таким именем уже существует в сообщении, то его значение заменяется более новым.

Формат

```
<action name="header" headername="<UserHeader>" value="<user header value>" />
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="header"**.

Атрибут "headername":

В атрибуте **headername="..."** указывается имя устанавливаемой строковой метки.

Атрибут "value":

В атрибуте **value="..."** указывается значение заголовка.

Пример

Добавляет к сообщению заголовок: **X-Sensor-UserHeader: user header value.**

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="TEST" version="1.0">
  <comment>This is the comment for the filter.</comment>
  <table name="main">

    <rule enabled="true">
      <comment>
        Adds the following header to the message:
        X-Sensor-UserHeader: user header value.
      </comment>
      <action name="header"
              headername="UserHeader"
              value="user header value" />
    </rule>

    <rule enabled="true">
      <match><c name="all"/></match>
      <action name="accept" />
    </rule>

  </table>
</filter>
```

4.4.1.3.2.13. Действие HEADER_EX

Добавляет к метаданным объекта пользовательский заголовок или изменяет значение существующего заголовка, за исключением заголовков **From, To, Cc, Bcc, Subject, Date**.

Описание

Это действие добавляет в сообщение пользовательский заголовок.

Если заголовок с таким именем (независимо от регистра написания) уже существует в сообщении, то его значение заменяется более новым.

Имя заголовка не может быть:

From

To

Cc

Bcc

Subject

Date

Формат

```
<action name="header_ex"
        headername="<UserHeader>"
        value="<user header value>" />
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="header_ex"**.

Атрибут "headername":

В атрибуте **headername="..."** указывается имя устанавливаемой строковой метки.

Атрибут "value":

В атрибуте **value="..."** указывается значение заголовка.

Пример

Adds the following header to the message: **X-SomethingElse-UserHeaderEx: user header value.**

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="TEST" version="1.0">
  <comment>This is the comment for the filter.</comment>
  <table name="main">

    <rule enabled="true">
      <comment>
        Adds the following header to the message:
        X-SomethingElse-UserHeaderEx: user header value.
      </comment>
      <action name="header_ex"
              headername="X-SomethingElse-UserHeaderEx"
              value="user header value" />
    </rule>

    <rule enabled="true">
      <match><c name="all"/></match>
      <action name="accept" />
    </rule>

   </table>
</filter>
```

4.4.1.3.2.14. Действие LOG

Делает запись в журнал в соответствии с определенными каналом и приемником, используется в целях отладки фильтров.

Описание

Это действие отправляет в указанный приёмник (файл, **syslog**-сервер) строку текста, значение тегов сообщения, значение меток сообщения или метаданные сообщения.

Запись происходит в формате:

```
[<timestamp>] <value>
```

В журнал можно отправить:

- строку, указываемую в атрибуте **value="..."**;
- список меток и их значений, указываемых в атрибуте **field="#labels"**;
- список тегов и их значений, указываемых в атрибуте **field="#tags";**
- значение заголовка метаданных сообщения. Для этого в атрибуте **field="X-Sensor-..."** указывается имя заголовка.

Действие **LOG** полезно использовать для отладки фильтров. Расставляя его в нужных правилах фильтра, можно получить детальный отчёт о том, как сообщения проходят обработку, и как при этом меняется значение метаданных, тегов и меток.

> **Внимание!**
> Следует помнить, что это действие применяется для целей отладки фильтров и их

поведения при фильтрации сообщений. Постоянное его применение может привести к снижению общей производительности **Microolap EtherSensor** и среды выполнения, если будет происходить интенсивная запись на диск.

Формат

```
<action name="log" dst="<log-destination>" value="<user string value>" />
<action name="log" dst="<log-destination>" field="<field type>" />
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="log"**.

Атрибут "dst":

В атрибуте **dst="..."** указывается приёмник записи в журнал. Это может быть:

dst="syslog://<syslog-server-ip:port>"

Отправляет сообщение на **syslog**-сервер по протоколу UDP (RFC-3164);

dst="channel://<channel-name>"

Отправляет сообщение в канал, предварительно настроенный в службе **Watcher**;

dst="file://<full-file-path>"

Сохраняет сообщение в файл.

Атрибут "field":

В атрибуте **field="..."** указывается тип поля сообщения, которое необходимо отправить в журнал. Возможные значения:

#labels

Вывод списка меток сообщения и их значений;

#tags

Вывод списка тегов сообщения и их значений;

#from

Вывод списка адресов FROM;

#to

Вывод списка адресов TO;

#subject

Вывод темы сообщения;

X-Sensor-...

Вывод значения заголовка метаданных сообщения.

Атрибут "value":

В атрибуте **value="..."** указывается строка сообщения, которая будет отправлена в журнал.

Пример

```
<action name="log" dst="file://d:\file\path.log.txt"
        value="user string value" />
```

Сохраняет в файл журнала **d:\file\path.log.txt** строку:

```
"[<timestamp>] user string value".
```

Действие:

```
<action name="log" dst="file://d:\file\path.log.txt" field="#tags" />
```

Сохраняет в файл журнала **d:\file\path.log.txt** строку:

```
"[<timestamp>] Tags:"
"                   <TAG = value>"
"                   <TAG = value>"
"                   <TAG = value>"
```

Каждый тег сохраняется в отдельной строке.

Действие:

```
<action name="log" dst="channel://debug.log.txt" field="#labels" />
```

Отправляет в канал **debug.log.txt** строку:

```
"[<timestamp>] Labels:"
"                   <LABEL = "value">"
"                   <LABEL = "value">"
"                   <LABEL = "value">"
```

Каждая метка сохраняется в отдельной строке.

Действие:

```
<action name="log"
        dst="syslog://192.168.0.1:514"
        field="X-Sensor-Src-Address" />
```

Отправляет на **syslog**-сервер с адресом **192.168.0.1:514** строку:

```
"[<timestamp>] X-Sensor-Src-Address: <metadata header value>"
```

Пример

Отослать данные сообщения на syslog-сервер.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="TEST" version="1.0">
  <comment>This is the comment for the filter.</comment>
  <table name="main">

    <rule enabled="true">
      <comment>
        Sending message details to syslog.
      </comment>
      <action name="log"
              dst="syslog://192.168.0.1:514"
              value="Message info dump:" />
      <action name="log"
              dst="syslog://192.168.0.1:514"
              field="X-Sensor-Src-Address" />
      <action name="log"
              dst="syslog://192.168.0.1:514"
              field="X-Sensor-Dst-Address" />
      <action name="log" dst="syslog://192.168.0.1:514"
              field="#labels" />
      <action name="log"
              dst="syslog://192.168.0.1:514"
              field="#tags" />
    </rule>

    <rule enabled="true">
      <match><c name="all"/></match>
      <action name="accept" />
    </rule>

  </table>
</filter>
```

4.4.1.4. Краткие правила написания фильтров

1. Фильтр всегда должен содержать таблицу **main**, с неё начинается выполнение фильтра.

2. Таблица не может быть пустой. Каждая таблица фильтра обязана заканчиваться правилом, под условие которого попадают все сообщения, и выполняется одно из действий: **ACCEPT**, **DROP** или **RETURN**. Это правило обязательно должно быть включено.

Например:

```
<rule name="end" enabled="1">
  <match>
    <c name="all"/>
  </match>
  <action name="drop" />
</rule>
```

или

```
<rule enabled="1">
  <action name="accept" />
</rule>
```

3. RETURN может применяться в любых таблицах, кроме **main**.

4. Переходы (**JUMP**) в таблицу **main** делать запрещено (во избежание циклических ссылок).

5. JUMP-переходы, образующие циклические ссылки (явные или неявные), запрещены.

4.4.1.5. Советы

В этом разделе описаны различные приёмы, которые помогут отлаживать и тестировать фильтры.

Метки времени

Метки времени (**<action name="datetime" value="label-name">**) можно использовать не только в конце и начале обработки сообщения, но и в каждом правиле - тогда можно будет узнать, когда оно было обработано относительно начала фильтрации всего сообщения в целом. Для этого действие **datetime** можно указывать непосредственно перед терминирующим действием.

Например:

```
<rule name="rule2" enabled="1">
  <match>
    <c name="attach-exist"/>
  </match>
  <action name="datetime" value="rule2-end" />
  <action name="accept" />
</rule>
```

В данном примере после обработки сообщения правилом у сообщения будет установлена метка **"rule2-end"**, показывающая время, когда сообщение было принято (**ACCEPT**) этим правилом.

Выполнение некоторых действий может занимать довольно длительное время (например, DNS-разрешение имён, проверка сообщения внешними антивирусами и т.п.). Так как все действия выполняются последовательно, то можно замерить время выполнения этого длительного действия, обрамив его действиями **datetime**.

Например:

```
<rule name="rule2" enabled="1">
  <match>
    <c name="attach-exist"/>
  </match>
  <action name="datetime" value="rule2-dns-start" />
  <action name="dns" />
  <action name="datetime" value="rule2-dns-end" />
</rule>
```

В примере после обработки сообщения правилом можно будет сравнить значение меток **"rule2-dns-start"** и **"rule2-dns-end"** и узнать время, которое занимала операция **dns**.

Теги правил

Можно использовать **action** установки тега во всех правилах, и при этом имя тега ставить таким же, как имя правила. Тогда после прохождения сообщения через фильтр в нём будет "история" того, через какие правила прошло сообщение. Это может быть полезно для тестирования фильтров и отслеживания "путей" их прохождения, когда фильтр достаточно сложный и содержит множество правил и таблиц.

Например:

```
<rule name="rule-attach" enabled="1">
  <match>
    <c name="attach-exist"/>
  </match>
  <action name="tag" value="rule-attach" />
</rule>

<rule name="rule-bad-words" enabled="1">
  <match>
    <c name="text" op="all" value="tel, respect" />
  </match>
  <action name="tag" value=" rule-bad-words" />
</rule>

<rule name="rule-only-for-dns" enabled="1">
  <action name="dns" />
  <action name="tag" value=" rule-only-for-dns" />
</rule>

<rule name="accept-all" enabled="1">
  <action name="tag" value="accept-all" />
  <action name="accept" />
</rule>
```

Так же можно поступить и с метками времени, в этом случае будет видно не только через какие правила прошло сообщение, но и в какое время.

"От простого к сложному"

Выполнение некоторых действий может занимать довольно длительное время (DNS-разрешение имён, проверка сообщения внешними антивирусами и т.п.). Следует размещать такие действия как можно ближе к концу обработки сообщения, чтобы было как можно меньше ситуаций, когда выполняется длительная операция, а потом применяется для сообщения действие **DROP** из-за того, что поле **FROM** не прошло проверку. Лучше сначала проверить **FROM** и отсеять на нём часть сообщений, и лишь потом выполнять для них **dns** или другие длительные операции вроде проверки антивирусами.

4.4.2. Префильтрация HTTP запросов

Начиная с версии **4.0** в **Microolap EtherSensor** был добавлен механизм предварительной фильтрации HTTP-запросов, призванный решать следующие задачи:

1. Отфильтровывание ненужного HTTP-трафика для снижения нагрузки на **Microolap EtherSensor** и среду выполнения на этапе анализа сообщений (действия ACCEPT и DROP);

2. Накопление информации о возможных новых тенденциях в HTTP-трафике для предоставления службе поддержки и/или разработчику **Microolap EtherSensor** (действие COPY).

3. Журналирование информации о HTTP-запросах в формате SQUID-ACCESS-LOG (действие ACCESS-LOG);

4. Манипуляции с тегами и метками на этапе препроцессинга с целью использования накопленной в них информации при анализе сообщений (действия TAG и LABEL).

Конфигурация HTTP-фильтра содержится в XML-файле, хранящемся в поддиректории **[INSTALLDIR]\config\filter\http.**

Для редактирования фильтра воспользуйтесь любым внешним текстовым/XML редактором, либо используйте встроенный в утилиту конфигурирования **Microolap EtherSensor** (файл **ethersensor_console.exe** из поставки), специально разработанный для целей редактирования фильтров редактор:

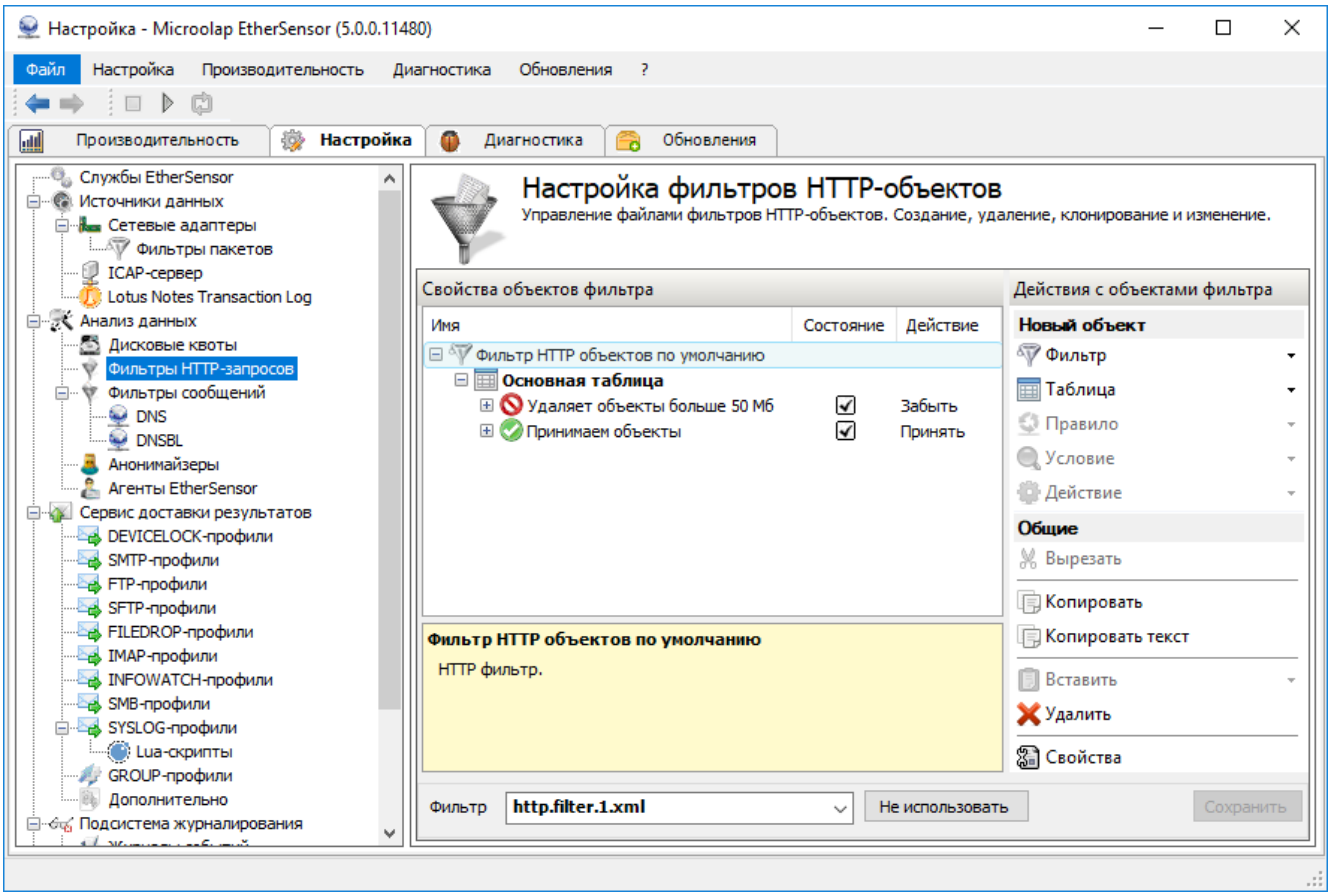

Рис.51. Редактирование HTTP-фильтра.

4.4.2.1. Условия

Ниже приведены условия, использующиеся в правилах префильтрации HTTP запросов.

4.4.2.1.1. Условие ALL, *

Специальное условие, под которое попадают все фильтруемые объекты.

Описание

Условие является истинным для любых объектов. Данное условие неявно подразумевается, если критерий **<match>…</match>** является пустым или отсутствует в правиле (правило содержит только **<actions>**).

Формат

```
<c name="all" />
<c name="*" />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="all"** или **name="*"**.

Пример

Правило принимает все сообщения к дальнейшей обработке.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">
  <comment>HTTP filter.</comment>

  <table name="main">

    <rule enabled="1">
      <comment>
        This rule accepts all messages for further processing.
      </comment>
      <match>
        <c name="all" />
      </match>
      <action name="accept" />
    </rule>

  </table>

</filter>
```

Пример (неявное условие all)

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">
  <comment>HTTP filter.</comment>
  <table name="main">

    <rule enabled="1">
      <action name="accept" />
    </rule>

  </table>
</filter>
```

4.4.2.1.2. Условие METHOD

Условие проверяет метод HTTP-запроса.

Это условие (**condition**) проверяет название метода HTTP-запроса. Если имя метода совпадает - условие выполняется.

Формат

```
<c name="method" value="<HTTP method>" />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="method"**.

Атрибут "value":

В атрибуте **value="..."** указывается имя метода для сравнения.

Пример

Правило прекращает обработку всех GET-запросов.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">
  <comment>HTTP filter.</comment>

  <table name="main">
    <rule enabled="1">
      <match ...> ... </match>
      <action ...> ... </action>
    </rule>

    <rule enabled="1">
      <comment>
        The rule stops further processing of GET requests.
      </comment>
      <match>
        <c name="method" value="GET"/>
      </match>
      <action name="drop" />
    </rule>
  </table>
</filter>
```

4.4.2.1.3. Условие IP

Проверить IP-адреса клиента или сервера на вхождение в диапазон или на принадлежность к подсети.

Описание

Это условие проверяет IP-адреса клиента или сервера на вхождение в диапазон или на принадлежность к подсети.

> **Внимание!**
> Нежелательный трафик нужно отсекать как можно раньше: от этого зависит производительность **Microolap EtherSensor** и среды выполнения.
> **1.** Весь трафик с конкретного IP-адреса или диапазона лучше всего отсекать в IP-фильтре службы EtherSensor EtherCAP.
> **2.** Определённый трафик HTTP с конкретного IP-адреса или диапазона (если возможно выделить такие критерии) лучше всего отсекать в HTTP-префильтре, а не на этапе анализа сообщений.
> **3.** Определённые сообщения с определенного IP-адреса лучше отфильтровывать в фильтре сообщений.

Формат

```
<c name="ip" address="<address type>" value="<ip-range>" />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="ip"**.

Атрибут "address":

В атрибуте **address="..."** указывается тип адреса для проверки. Возможные значения:

src или client

Проверять адрес источника;

dst или server

Проверять адрес назначения.

Атрибут "value":

В атрибуте **value="..."** указывается значение для сравнения. Возможные значения:

ipaddress

Проверяет IP-адрес на равенство. Например, **value="192.168.0.10"**;

ip1-ip2

Проверяет на вхождение IP-адреса в диапазон. Например, **value="192.168.0.1-192.168.0.10"**;

ip/netmask

Проверяет на принадлежность IP-адреса к указанной подсети. Например, **value="192.168.0.1/255.255.255.0"**;

ip/netmaskbits

Проверяет на принадлежность IP-адреса к указанной подсети. Например, **value="192.168.0.1/24"**.

Пример

Забывать все сообщения с адреса 192.168.0.15.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">
  <comment>HTTP filter.</comment>

  <table name="main">

    <rule enabled="1">
      <comment>
        Discard messages from 192.168.0.15.
      </comment>
      <match>
        <c name="ip" address="client" value="192.168.0.15" />
      </match>
      <action name="drop" />
    </rule>

    <rule enabled="1">
      <action name="accept" />
    </rule>

    </table>
</filter>
```

4.4.2.1.4. Условие REQ-SIZE, RESP-SIZE, SIZE

Условие проверяет полный (включая заголовки) размер HTTP-объекта.

Описание

Условия группы **size** проверяют полный (включая заголовки) размер HTTP-запроса/ответа.

req-size

Условие выполняется, если размер HTTP-запроса соответствует условию;

resp-size

Условие выполняется, если размер HTTP-ответа соответствует условию;

size

Условие выполняется, если размер HTTP-запроса **или** размер HTTP-ответа соответствуют условию.

Формат

```
<c name="req-size" op="<operation>" value="<compare pattern>" />
<c name="resp-size" op="<operation>" value="<compare pattern>" />
<c name="size" op="<operation>" value="<compare pattern>" />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="req-size"** или **name="resp-size"** или **name="size"**.

Атрибут "value":

В атрибуте **value="..."** указывается число, с которым сравнивается размер HTTP-объекта.

<число> или <число>B

Указывает размер в байтах;

<число>K

Указывает размер в килобайтах;

<число>M

Указывает размер в мегабайтах;

<число>G

Указывает размер в гигабайтах.

Атрибут "op":

В атрибуте **op="..."** указывает тип операции сравнения и может принимать значения:

eq или = или ==

Условие выполняется, если размер **РАВЕН** указанному числу;

ne или != или <>

Условие выполняется, если размер **НЕ РАВЕН** указанному числу;

lt или <

Условие выполняется, если размер **МЕНЬШЕ** указанного числа;

gt или >

Условие выполняется, если размер **БОЛЬШЕ** указанного числа;

le или <=

Условие выполняется, если размер **МЕНЬШЕ ИЛИ РАВНО** указанного числа;

ge или >=

Условие выполняется, если размер **БОЛЬШЕ ИЛИ РАВНО** указанного числа.

Пример

Правило прекращает обработку всех HTTP-объектов запроса размером более 100KB или HTTP-объектов ответа размером более 1MB.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">
  <comment>HTTP filter.</comment>
  <table name="main">

    <rule enabled="1">
      <comment>
        The rule stops processing HTTP objects with the request size
        over 100KB or the response size over 1MB.
      </comment>
      <match>
        <or>
          <c name="req-size" op=">" value="100K"/>
          <c name="resp-size" op="gt" value="1M"/>
        </or>
      </match>
      <action name="drop" />
    </rule>
  </table>
</filter>
```

4.4.2.1.5. Условие REQ-HEADER, RESP-HEADER

Проверяет значение одного из заголовков HTTP-запроса или ответа.

Описание

Это условие проверяет значение заголовка HTTP-запроса на наличие подстроки в строке или на соответствие шаблону wildcard или regexp.

Формат

```
<c name="req-header" headername="..." op="..." value="..." />
```

или

```
<c name="resp-header" headername="..." op="..." value="..." />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="req-header"** или **name="resp-header"**.

req-header

Проверяет заголовки HTTP-запроса;

resp-header

Проверяет заголовки HTTP-ответа

Атрибут "headername":

В атрибуте **headername="..."** указывается имя проверяемого заголовка.

Атрибут "headername":

Строка, с которой сравнивается значение или шаблон для проверки, указывается в атрибуте **value="..."**.

Атрибут "op":

В атрибуте **op="..."** указывает тип операции сравнения и может принимать значения:

eq или = или ==

Условие выполняется, если значение поля **СОДЕРЖИТ** указанное значение;

ne или != или <>

Условие выполняется, если значение поля **НЕ СОДЕРЖИТ** указанное значение;

wc или wildcard

Условие выполняется, если значение поля **соответствует** указанному **wildcard** шаблону;

re или regex или regexp

Условие выполняется, если значение поля **соответствует** указанному **regexp** шаблону;

Для заголовка **Content-Length** доступны операции:

eq или = или ==

Условие выполняется, если значение поля **СОДЕРЖИТ** указанное значение;

ne или != или <>

Условие выполняется, если значение поля **НЕ СОДЕРЖИТ** указанное значение;

lt или <

Условие выполняется, если размер **МЕНЬШЕ** указанного числа;

gt или >

Условие выполняется, если размер **БОЛЬШЕ** указанного числа;

le или <=

Условие выполняется, если размер **МЕНЬШЕ ИЛИ РАВНО** указанного числа;

ge или >=

Условие выполняется, если размер **БОЛЬШЕ ИЛИ РАВНО** указанного числа.

Эти операции выполняются со значением заголовка как с ЧИСЛОМ, а не как со строкой.

Атрибут "value":

В атрибуте **value="..."** указывается проверяемое значение (строка, wildcard или regexp шаблон).

Внимание!
Для заголовка **Content-Length** указывается числовое значение для сравнения.

Число, с которым сравнивается размер, указывается в виде:

<число> или <число>B

Указывает размер в байтах.

<число>K

Указывает размер в килобайтах.

<число>M

Указывает размер в мегабайтах.

<число>G

Указывает размер в гигабайтах.

Пример

Игнорировать запросы с Content-Length более 100K. Принимать запросы на win.mail.ru и *.yandex.ru.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">
  <comment>HTTP filter.</comment>
  <table name="main">

    <rule enabled="1">
      <comment>
        Ignore requests where Content-Length is more than 100K.
      </comment>
      <match>
        <c name="req-header"
           headername="Content-Length"
           op=">" value="100K" />
      </match>
      <action name="drop" />
    </rule>

    <rule enabled="1">
      <comment>
        Accept requests to win.mail.ru and *.yandex.ru.
      </comment>
      <match>
        <or>
          <c name="req-header"
             headername="Host" op="eq"
             value="win.mail.ru" />
          <c name="req-header"
             headername="Host"
             op="wc"
             value="*.yandex.ru" />
        </or>
      </match>
      <action name="accept" />
    </rule>
  </table>
</filter>
```

4.4.2.1.6. Условие URL

Проверяет значение URL HTTP-запроса.

Описание

Это условие проверяет значение URL HTTP-запроса на наличие подстроки в строке или на соответствие шаблону wildcard или regexp.

Следует помнить, что проверяется полный URL запроса, т.е. в виде http://www.server.com/script-or-page-path.htm.

> **Помните:**
> Если необходимо проверять только имя хоста, то следует пользоваться условием "**HEADER**". Это повысит скорость проверки и сэкономит ресурсы.

Формат

```
<c name="url" op="..." value="..." />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="url"**.

Атрибут "op":

В атрибуте **op="..."** указывает тип операции сравнения и может принимать значения:

eq или = или ==

Условие выполняется, если значение поля **СОДЕРЖИТ** указанное значение;

ne или != или <>

Условие выполняется, если значение поля НЕ **СОДЕРЖИТ** указанное значение;

wc или wildcard

Условие выполняется, если значение поля **соответствует** указанному **wildcard** шаблону;

re или regex или regexp

Условие выполняется, если значение поля **соответствует** указанному **regexp** шаблону;

Атрибут value:

В атрибуте **value="..."** указывается проверяемое значение (строка, wildcard или regexp шаблон).

Пример

```
<c name="url" op="eq" value="game" />
```

Условие выполняется, если в URL присутствует подстрока "game".

```
<c name="url" op="wc" value="http://*.mail.ru/*send*" />
```

Условие выполняется, если URL соответствует wildcard шаблону "http://*.mail.ru/*send*".

```
<c name="url" op="re" value="satan|shopping|dating|movies|hexogen" />
```

Условие выполняется, если URL соответствует regexp шаблону "satan|shopping|dating|movies|hexogen".

Пример

Детектировать запросы с нехорошими словами (satan|shopping|dating|movies|hexogen), метить тегом **shopping**. Игнорировать запросы, помеченные тегом **shopping**.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">
  <comment>HTTP filter.</comment>
  <table name="main">

    <rule enabled="1">
      <comment>
        Detect requests possibly related to bad content.
      </comment>
      <match>
        <c name="url"
           op="re"
           value="satan|shopping|dating|movies|hexogen" />
      </match>
      <action name="tag" value="shopping"/>
    </rule>

    <rule enabled="1">
      <comment>
        Ignore requests tagged as "shopping".
      </comment>
      <match>
        <c name="tag" tag="shopping"/>
      </match>
      <action name="drop" />
    </rule>

    <rule enabled="1">
      <action name="accept" />
    </rule>
  </table>
</filter>
```

4.4.2.1.7. Условие TAG

Проверяет наличие установленного тега и значение его счётчика (см. раздел "Действие TAG").

Описание

Это условие проверяет активность указанного тега для объекта, а также его уровень.

Формат

```
<c name="tag" tag="<tag name>" op="<operation>" value="<compare value>" />
```

Атрибут "name":

В атрибуте **name** указывается имя условия - **name="tag"**.

Атрибут "tag":

В атрибуте **tag="..."** указывается имя проверяемого тега.

Атрибут "op":

В атрибуте **op="..."** указывается тип операции сравнения и может принимать значения:

eq или = или ==

Условие выполняется, если значение **РАВНО** указанному числу;

ne или != или <>

Условие выполняется, если значение **НЕ РАВНО** указанному числу;

lt или <

Условие выполняется, если значение **МЕНЬШЕ** указанного числа;

gt или >

Условие выполняется, если значение **БОЛЬШЕ** указанного числа;

le или <=

Условие выполняется, если значение **МЕНЬШЕ ИЛИ РАВНО** указанного числа;

ge или >=

Условие выполняется, если значение **БОЛЬШЕ ИЛИ РАВНО** указанного числа;

exist

Условие выполняется, если тег **существует** (уже установлен ранее для этого HTTP-объекта);

По умолчанию (если атрибут **op** отсутствует) принимается значение **"exist"**. Для операции **"exist"** указывать атрибут **"value"** не обязательно.

Атрибут "value":

В атрибуте **value="..."** указывается проверяемое значение, если проверяется значение счётчика тега.

Пример

```
<c name="tag" tag="SPAM" op="exist" />
```

или

```
<c name="tag" tag="SPAM" />
```

Условие выполняется, если для объекта установлен тег **SPAM**.

```
<c name="tag" tag="SPAM" op=">=" value="3" />
```

Условие выполняется, если для объекта установлен тег **SPAM** и значение его счётчика больше или равно **3**.

Пример

Детектировать запросы с нехорошими словами (satan|shopping|dating|movies|hexogen), метить тегом **shopping**. Игнорировать запросы, помеченные тегом **shopping**.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">
  <comment>HTTP filter.</comment>
  <table name="main">

    <rule enabled="true">
      <comment>
        Detect requests possibly related to bad things.
      </comment>
      <match>
        <c name="url"
           op="re"
           value="satan|shopping|dating|movies|hexogen" />
      </match>
      <action name="tag" value="shopping"/>
    </rule>

    <rule enabled="true">
      <comment>
        Ignore a request tagged as "shopping".
      </comment>
      <match>
        <c name="tag" tag="shopping"/>
      </match>
      <action name="drop" />
    </rule>

    <rule enabled="1">
      <action name="accept" />
    </rule>
  </table>
</filter>
```

4.4.2.2. Действия

Ниже приведены варианты действий, исполняемых правилами HTTP префильтрации.

4.4.2.2.1. Действие ACCEPT

Пропустить HTTP-объект к дальнейшей обработке.

Описание

Действие **ACCEPT** прекращает работу фильтров с текущим HTTP-объектом и пропускает его к дальнейшей обработке детекторами.

Формат

```
<action name="accept" />
```

Атрибут name:

В атрибуте **name** указывается имя действия - **name="accept"**.

Пример:

Все сообщения, достигшие этого правила, принимать к дальнейшей обработке.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">
  <comment>HTTP filter.</comment>
  <table name="main">

    <rule enabled="1">
      <match ...> ... </match>
      <action ...> ... </action>
    </rule>

    <rule enabled="1">
      <comment>
        All messages that reach this rule are accepted for
        further processing.
      </comment>
      <action name="accept" />
    </rule>
  </table>
</filter>
```

4.4.2.2.2. Действие DROP

Проигнорировать HTTP-объект без продолжения дальнейшей обработки.

Описание

Это действие прекращает обработку текущего HTTP-объекта в **Microolap EtherSensor** и сообщает ему, что сообщение необходимо проигнорировать ("забыть") и уничтожить все накопленные о нем данные.

Формат

```
<action name="drop" />
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="drop"**.

Пример:

Все сообщения, достигшие этого правила, забыть.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">
  <comment>HTTP filter.</comment>
  <table name="main">

    <rule enabled="1">
      <comment>
        All messages that reach this rule will be discarded.
      </comment>
      <action name="drop" />
    </rule>
  </table>
</filter>
```

4.4.2.2.3. Действие JUMP

Продолжить обработку HTTP-объекта в другой таблице.

Описание

Это действие продолжает обработку HTTP-объекта в другой таблице.

Формат

```
<action name="jump" value="<table name>" />
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="jump"**.

Атрибут value:

В атрибуте **value="..."** указывается имя таблицы, в которую необходимо перейти для дальнейшей обработки HTTP-объекта.

Внимание!
Следует помнить, что переход в таблицу **main** запрещён для исключения зацикливания.

Также запрещены переходы, которые могут привести к явной или неявной цикличности.

Пример:

GET-запросы передаются на обработку в таблицу **get-process**. GET-запросы обрабатываются в таблице **get-process**. ACCEPT для запросов на win.mail.ru. Возврат в таблицу **main** для дальнейшей обработки.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">
  <comment>HTTP filter.</comment>
  <table name="main">
    <rule enabled="1">
      <comment>
        Processing of GET requests is passed to the "get-process" table.
      </comment>
      <match>
        <c name="method" value="GET"/>
      </match>
      <action name="jump" value="get-process"/>
    </rule>

    <rule enabled="1">
      <action name="drop" />
    </rule>
  </table>

  <table name="get-process">
    <comment>
      GET requests are processed in the table get-process.
    </comment>

    <rule enabled="1">
      <comment>
        ACCEPT for requests for win.mail.ru.
      </comment>
      <match>
        <c name="req-header"
           headername="Host"
           op="eq"
           value="win.mail.ru" />
      </match>
      <action name="accept" />
    </rule>

    <rule enabled="1">
      <comment>
        Return to "main" table for further processing.
      </comment>
      <action name="return" />
    </rule>
  </table>

</filter>
```

4.4.2.2.4. Действие RETURN

Вернуться в предыдущую (вызвавшую) таблицу и продолжить выполнение в ней со следующего правила.

Описание

Это действие возвращает обработку HTTP-объекта в предыдущую (вызвавшую) таблицу и продолжает выполнение в ней со следующего правила.

Формат

```
<action name="return" />
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name**="**return**".

Внимание!
Действие не может применяться в таблице **main**.

Пример:

GET-запросы передаются на обработку в таблицу **get-process**. GET-запросы обрабатываются в таблице **get-process**. ACCEPT для запросов на win.mail.ru. Возврат в таблицу **main** для дальнейшей обработки.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">
  <comment>HTTP filter.</comment>
  <table name="main">

    <rule enabled="1">
      <comment>
        Processing of GET requests is passed to the "get-process" table.
      </comment>
      <action name="jump" value="get-process"/>
    </rule>

    <rule enabled="1">
      <action name="drop" />
    </rule>
  </table>

  <table name="get-process">
    <comment>
      GET requests are processed in the table.
    </comment>

    <rule enabled="1">
      <comment>
        ACCEPT for requests for win.mail.ru.
      </comment>
      <match>
        <c name="req-header"
           headername="Host"
           op="eq"
           value="win.mail.ru" />
      </match>
      <action name="accept" />
    </rule>

    <rule enabled="1">
      <comment>
        Return to "main" table for further processing.
      </comment>
      <action name="return" />
    </rule>
  </table>

</filter>
```

4.4.2.2.5. Действие COPY

Копировать текущий обрабатываемый HTTP-объект (запрос и ответ, если есть) и паспорт в указанную директорию.

Описание

Это действие копирует текущий обрабатываемый HTTP-объект (запрос и ответ, если есть) и паспорт в указанную директорию.

Формат

```
<action name="copy" value="<folder path>"/>
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="copy"**.

Атрибут value:

В атрибуте **value="..."** указывается путь к директории, в которую следует копировать данные.

Если директория не существует - она будет создана.

Пример:

Копировать запросы на win.mail.ru в папку **d:\data_from_mail.ru**.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="TEST" version="1.0">
  <comment>This is a comment for the filter.</comment>
  <table name="main">

    <rule enabled="true">
      <comment>
        Copy requests for win.mail.ru to d:\data_from_mail.ru.
      </comment>
      <match>
        <c name="req-header"
           headername="Host"
           op="eq"
           value="win.mail.ru" />
      </match>
        <action name="copy" value="d:\data_from_mail.ru"/>
    </rule>

    <rule enabled="true">
      <match><c name="all"/></match>
      <action name="accept" />
    </rule>

  </table>
</filter>
```

4.4.2.2.6. Действие ACCESS-LOG

Сохранить информацию о текущем HTTP-объекте в канал журналирования в формате SQUID-ACCESS-LOG.

Описание

Действие **access-log** сохраняет информацию о текущем HTTP-объекте в канал журналирования в формате SQUID-ACCESS-LOG.

Формат

```
<action name="access-log" value="<log-channel-name>" />
```

Атрибут name:

В атрибуте **name** указывается имя действия - **name="access-log"**.

Атрибут value:

В атрибуте **value="..."** имя канала журналирования. Этот канал должен быть предварительно настроен в службе **EtherSensor Watcher**.

Пример

Логировать все запросы в канал **all-log-channel**, а запросы на win.mail.ru ещё и в **mail-ru-log-channel.**

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="TEST" version="1.0">
  <comment>This is a comment for the filter.</comment>
  <table name="main">

    <rule enabled="true">
      <comment>
        Log requests for win.mail.ru to mail-ru-log-channel.
      </comment>
      <match>
        <c name="req-header"
           headername="Host"
           op="eq"
           value="win.mail.ru" />
      </match>
      <action name="access-log" value="mail-ru-log-channel"/>
    </rule>

    <rule enabled="true">
      <comment>
        Log all requests to all-log-channel.
      </comment>
      <action name="access-log" value="all-log-channel"/>
      <action name="accept" />
    </rule>

  </table>
</filter>
```

4.4.2.2.7. Действие TAG

Добавляет к метаданным объекта тег (числовую метку).

Описание

Это действие устанавливает в метаданных объекта тег (числовую метку). Тегов может быть несколько. В этом случае они перечисляются через запятую '**,**' или точку с запятой '**;**'. Если один и тот же тег устанавливать для объекта несколько раз, то у тега повышается "уровень" (его числовое значение). У каждого тега есть внутренний счётчик, показывающий, сколько раз он был установлен для этого объекта.

Существование тега, а также значение его счётчика (сколько раз он был установлен для текущего объекта) можно впоследствии проверять в условиях фильтров для принятия решений.

По умолчанию значение счётчика при установке тега увеличивается на **1**. Если счётчик тега необходимо увеличить более чем на **1**, то можно задавать значение, на которое необходимо увеличить счётчик, после имени тега в круглых скобках: **"TAG(...)"**. Например, **SPAM(3)** - увеличивает значение счётчика для тега **SPAM** на **3**, а **SPAM(1)** равносильно просто **SPAM**. Это может быть необходимо в случаях, когда условия, устанавливающие один и тот же тег, имеют разную значимость / важность / приоритет.

Значение для изменения счётчика может быть отрицательным. **SPAM(-3)** - уменьшает значение счётчика для тега **SPAM** на **3**.

> **Помните:**
> Установленные теги в дальнейшем будут доступны в условиях фильтра сообщений , если из данного HTTP-объекта будет извлечено сообщение.

Формат

```
<action name="tag" value="<tag list>" />
```

или

```
<action name="tag" > tag list </action>
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="tag"**.

Атрибут "value":

В атрибуте **value="..."** перечисляются имена тегов.

Имена тегов также можно перечислять в самом теге **<action>**.

Пример 1:

```
<action name="tag" value="SPAM" />
```

Устанавливает тег с именем "SPAM".

```
<action name="tag" value="SPAM(3)" />
```

Устанавливает тег с именем "SPAM" и увеличивает его счётчик на 3.

```
<action name="tag" value="SPAM, shopping" />
```

Устанавливает теги с именами "SPAM" и "shopping".

```
<action name="tag" value="SPAM(3), shopping(2)" />
```

Устанавливает теги с именами "SPAM" и "shopping" и увеличивает их счётчики на 3 и 2.

```
<action name="tag">SPAM, shopping</action>
```

Также устанавливает теги с именами "SPAM" и "shopping".

```
<action name="tag" value="SPAM, shopping">VIP-OFFICE</action>
```

Устанавливает теги с именами "SPAM", "shopping", "VIP-OFFICE".

Пример 2:

Помечать запросы на популярные российские почтовые сервисы тегом RUS_MAIL.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="TEST" version="1.0">
  <comment>Filter comment.</comment>
  <table name="main">

    <rule enabled="true">
      <comment>
        Mark requests to popular Russian mail services
        with RUS_MAIL tag.
      </comment>
      <match>
        <c name="req-header"
           headername="Host"
           op="eq"
           value="win.mail.ru" />
        <c name="req-header"
           headername="Host"
           op="eq"
           value="mail.yandex.ru" />
        <c name="req-header"
           headername="Host"
           op="eq"
           value="mail.rambler.ru" />
      </match>
      <action name="tag" value="RUS_MAIL"/>
    </rule>

    <rule enabled="true">
      <match><c name="all"/></match>
      <action name="accept" />
    </rule>

  </table>
</filter>
```

4.4.2.2.8. Действие LABEL

Добавляет к метаданным объекта строковую метку.

Описание

Это действие устанавливает ярлык (строковую метку) в метаданных текущего обрабатываемого HTTP-объекта. Если данный ярлык уже был ранее установлен для HTTP-объекта, то его значение заменяется более новым. Используется для добавления описаний к HTTP-объектам.

> **Помните:**
> Установленные метки в дальнейшем будут доступны в фильтре сообщений (если из данного HTTP-объекта было извлечено сообщение).

Формат

```
<action name="label" label="<label name>" value="<label value>" />
```

или:

```
<action name="label" label="<label name>" > label value </action>
```

Атрибут "name":

В атрибуте **name** указывается имя действия - **name="label"**.

Атрибут "label":

В атрибуте **label="..."** указывается имя устанавливаемой строковой метки.

Атрибут "value":

В атрибуте **value="..."** указывается строковое значение для метки.

Значение также можно перечислять в самом теге **<action>**.

Пример

```
<action name="label"
        label="VIRUS-DESCR"
        value="Win.32.BlackHorse.trojan.virus -
               mail worm, extremely dangerous!!!" />
```

или:

```
<action name="label"
        label="VIRUS-DESCR">Win.32.BlackHorse.trojan.virus -
                            mail worm, extremely dangerous!!!
</action>
```

Устанавливает для сообщения строковую метку с именем "VIRUS-DESCR" и записывает в неё строку "Win.32.BlackHorse.trojan.virus - mail worm, extremely dangerous!!!".

Пример

Помечать запросы на популярные российские почтовые сервисы меткой CONTENT-DESCR.

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="TEST" version="1.0">
  <comment>This is a comment for the filter.</comment>
  <table name="main">

    <rule enabled="true">
      <comment>
        Mark requests for popular Russian mail services
        with CONTENT-DESCR label.
      </comment>
      <match>
        <or>
          <c name="req-header"
             headername="Host"
             op="eq"
             value="win.mail.ru" />
          <c name="req-header"
             headername="Host"
             op="eq"
             value="mail.yandex.ru" />
          <c name="req-header"
             headername="Host"
             op="eq"
             value="mail.rambler.ru" />
        </or>
      </match>
      <action name="label"
              label="CONTENT-DESCR"
              value="Russian mail services"/>
    </rule>

    <rule enabled="true">
      <match><c name="all"/></match>
      <action name="accept" />
    </rule>

  </table>
</filter>
```

4.4.3. Примеры применения фильтров

Ниже описаны примеры применения фильтров для обработки результатов перехвата.

4.4.3.1. Добавление имени хоста

Задача

Необходимо, чтобы в реконструированных сообщениях вместе с IP-адресами содержались доменные имена хостов отправителя и получателя.

Описание логики решения

Для этого необходимо, чтобы **Microolap EtherSensor** производил разрешение доменных имён через службу DNS.

Для этого следует:

1. В конфигурации службы **EtherSensor Analyser** указать, через какие DNS-серверы необходимо производить разрешение имён;

2. Написать фильтр сообщений, в котором будет находиться правило с действием, указывающим, что для текущего обрабатываемого сообщения необходимо произвести DNS-разрешение имён хостов.

Решение

1. Настройка в конфигурации службы EtherSensor Analyser параметров DNS-серверов для разрешения имён.

Настройку можно производить в конфигураторе или в конфигурационном файле.

В файле конфигурации службы **EtherSensor Analyser**:

Корневой тег **<AnalyserConfig>**, далее вложенный тег настроек фильтров **<Filter>** (включается фильтр сообщений), далее вложенный тег **<Dns>** - настройки DNS-серверов для разрешения имён в фильтре сообщений.

```
<?xml version="1.0" encoding="utf-8"?>
<AnalyserConfig version="3.2">

<!-- specify other settings for the service here -->

  <Filter enabled="true" filename="msg_filter.xml">

<!-- specify other filter settings here -->

    <Dns>
      <AttemptsCount>3</AttemptsCount>
      <TtlForUnknown>3600</TtlForUnknown>
      <MinTtl>300</MinTtl>
      <MaxTtl>604800</MaxTtl>
      <Server ipaddress="127.0.0.1" port="53" />
    </Dns>

  </Filter>
</AnalyserConfig>
```

В данном случае предполагается, что DNS-сервер располагается по адресу **127.0.0.1:53**.

2. Настройка фильтра сообщений

Например, файл **msg_filter.xml**:

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="DNS resolve" version="1.0">

  <table name="main">

    <rule enabled="true">
      <comment>
        Resolve the sender and the recipient host names
        for the message.
      </comment>
      <action name="dns" address="both"/>
    </rule>

    <rule enabled="true">
      <comment>
        Accept all message that reached this point.
      </comment>
      <action name="accept" />
    </rule>

  </table>
</filter>
```

Комментарии и общие рекомендации

1. После выполнения действия **DNS** в метаданные сообщения будут добавлены заголовки **X-Sensor-Src-Host**, **X-Sensor-Dst-Host** со значениями доменных имён или со значением **"<not resolved>",** если получить какое-то из доменных имён не удалось.

2. Для более быстрого разрешения имён DNS в конфигурации службы **EtherSensor Analyser** желательно указывать как можно более быстрые DNS-серверы. Это могут быть как серверы Интеернет-провайдера, так и собственные DNS-серверы.

3. Действие **DNS** (разрешение имён DNS) является относительно длительной операцией, в связи с этим старайтесь выполнять его в фильтре только для тех сообщений, для которых это необходимо.

4. Старайтесь применять действие **DNS** в конце фильтра и непосредственно в том месте, где понадобятся результаты его работы.

Например, если необходимо, чтобы на выходе в сообщении адреса хостов отправителя и получателя просто содержали доменные имена, достаточно применять действие **DNS** прямо перед окончанием фильтрации сообщения и действием **ACCEPT**. Нет необходимости делать это в начале фильтра, так как в ходе фильтрации часть сообщений может быть отклонена действием **DROP** и для этих сообщений действие **DNS** (если оно в установлено начале фильтра) будет производить лишнюю нагрузку на **Microolap EtherSensor** и среду выполнения.

Если же требуется полученные DNS-имена отправителя и получателя использовать далее в условиях фильтра для отсеивания сообщений по именам хостов, то разрешение имён DNS следует делать в правиле, которое расположено непосредственно перед правилом, в условиях которого будут использоваться полученные DNS-имена.

Поиск неисправностей

Если разрешение DNS-имён для IP-адресов отправителя или получателя не происходит:

1. Проверьте доступность DNS-сервера непосредственно с машины-сенсора при помощи утилиты **ping** (например, **ping <IP-адрес-dns-сервера>**) и **telnet** (например, **telnet <IP-адрес-dns-сервера>**).

2. Убедитесь, что используемый DNS-сервер может производить разрешение имён для машины-сенсора. Это можно сделать утилитой **nslookup**.

- В командной строке запустите утилиту **nslookup**.
- В запущенной утилите выполните команду **server <IP-адрес-dns-сервер>**, чтобы установить DNS-сервер, через который будет проводиться разрешение имён.
- Введите IP-адрес, имя которого не удаётся разрешить.

Если **nslookup** может разрешить имя хоста, то необходимо проверить ход выполнения фильтрации:

1. Убедитесь, что правило в фильтре, в котором находится действие **DNS,** включено и условия этого правила соответствуют сообщениям.

2. Убедитесь, что правило в фильтре, в котором находится действие **DNS**, вообще будет выполняться, то есть не возникает ситуации, когда сообщения принимаются правилами выше и процесс фильтрации не доходит до этого правила (например, выше этого правила нет правил с действием **ACCEPT** или **DROP**).

3. Убедитесь, что при старте **Microolap EtherSensor** в журналах службы **EtherSensor Analyser** отсутствуют сообщения о неправильной загрузке фильтра сообщений и ошибках.

Если ничего не помогло, отправьте разработчику **Microolap EtherSensor**:

- Несколько примеров сообщений, для которых разрешение имён не происходит.
- Используемый фильтр сообщений.
- Диагностический отчет работе **Microolap EtherSensor**, генерируемый утилитой **ethersensor_console.exe** из поставки **Microolap EtherSensor**.
- Свои комментарии и соображения по вышеперечисленным действиям.

4.4.3.2. Фильтрация по хостам

Задача

Необходимо в случае выполнения запросов на сайты **<*baender*.com, benderlog.ru, banderlog.biz>** прекратить обрабатывать такое сообщение и удалить накопленные данные о нем.

Описание логики решения

Возможны два варианта решения задачи:

1. Полностью игнорировать трафик на хосты с указанными именами в фильтре протокола HTTP. Для этого необходимо написать условие фильтрации по заголовку HTTP-запроса "**Host**".

2. В фильтре сообщений удалять сообщения, отправляемые на указанные хосты. Для этого необходимо произвести разрешение DNS-имён и написать условие фильтрации "**hostname**".

Вариант **1** является более предпочтительным, так как позволяет отфильтровывать ненужные данные на более раннем этапе, что значительно снижает нагрузку на **Microolap EtherSensor**, увеличивая его общую производительность.

Решение

1. Вариант 1 - игнорирование трафика на ранней стадии при помощи фильтра протокола HTTP.

Например, файл фильтра HTTP-протокола может выглядеть так:

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">
  <table name="main">

    <rule enabled="true">
      <match>
        <or>
          <c name="req-header"
             headername="Host"
             op="wc"
             value="*baender*.com*"/>
          <c name="req-header"
             headername="Host"
             op="eq"
             value="benderlog.ru"/>
          <c name="req-header"
             headername="Host"
             op="eq"
             value="banderlog.biz"/>
        </or>
      </match>
      <action name="drop" />
    </rule>

    <rule enabled="true">
      <action name="accept" />
    </rule>

  </table>
</filter>
```

Подробное описание условия фильтрации **"req-header"** смотрите в разделе "Условие REQ-HEADER, RESP-HEADER".

2. Вариант 2 - удаление сообщений в фильтре сообщений.

Необходимо включить разрешение DNS-имён, файл фильтра сообщений может выглядеть так:

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">

  <table name="main">

    <rule enabled="1">
      <match>
        <or>
          <c name="hostname"
             address="server"
             op="wc"
             value="*baender*.com*" />
          <c name="hostname"
             address="server"
             op="eq"
             value="benderlog.ru" />
          <c name="hostname"
             address="server"
             op="eq"
             value="banderlog.biz" />
        </or>
      </match>
      <action name="drop"/>
    </rule>

    <rule enabled="1">
      <action name="accept" />
    </rule>

  </table>
</filter>
```

Подробное описание условия фильтрации **"hostname"** смотрите в разделе "Условие HOSTNAME".

Комментарии и общие рекомендации

1. В варианте **1** обратите внимание, что проверка имени хоста из заголовка **Host** по wildcard-маске "***baender*.com***" содержит "*****" в начале и в конце маски. В начале маски это необходимо потому, что в начале имени хоста могут идти имена доменов верхнего уровня (например, **www.baender.com** или **123.baender.com**). В конце маски это необходимо потому, что в конце имени хоста в заголовке **Host** может быть указан порт назначения (например, **baender.com:80**).Проверка на равенство (операция в условии "**eq**") подразумевает просто поиск подстроки в строке. Поэтому "**eq**" со значением "**benderlog.ru**" будет срабатывать и для **www.benderlog.ru** и для **benderlog.ru:80**.

2. Для варианта **2** в общем случае для работы условия **hostname** необходимо предварительно произвести разрешение имён DNS. Однако, в указанном случае (мы проверяем только хост назначения и только для протокола HTTP) этого делать не обязательно, так как значение хоста будет доступно из заголовка **Host** HTTP-протокола.

4.4.3.3. Фильтрация по URL

Задача

Необходимо в случае присутствия в URL слов **<forum, phorum, post, submit>** для метода **get** установить на сообщение пометку **"user reads forums"**.

Описание логики решения

Проверить URL и метод HTTP-запроса, используя фильтр HTTP-протокола. Для проверки URL следует использовать условие **"url"**, для проверки метода HTTP-протокола следует использовать условие **"method"**.

Решение

Например, файл фильтра HTTP-протокола может выглядеть так:

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">

  <table name="main">

    <rule enabled="true">
      <comment>
        Detect requests possibly related to forums.
      </comment>
      <match>
        <and>
          <c name="method"
             value="GET"/>
          <c name="url"
             op="re"
             value="http://.*/.*(forum|phorum|post|submit).*" />
        </and>
      </match>
        <action name="tag" value="USER_READS_FORUMS"/>
    </rule>

    <rule enabled="true">
      <action name="accept" />
    </rule>
  </table>
</filter>
```

Подробное описание условий фильтрации "**url**" и "**method**" смотрите в разделах **"Условие URL"** и **"Условие METHOD"**.

Комментарии и общие рекомендации

1. Следует помнить, что на этапе фильтрации HTTP-протокола ещё не существует сообщений, проверка на их наличие в трафике будет выполнена позже. Однако, метки и теги, установленные для запросов на этом этапе будут сохранены и в сообщении (если оно будет извлечено из этих запросов). Эти метки и теги будут доступны для проверки в фильтре сообщений и в дальнейшем в виде заголовков **X-Sensor-Tags** и **X-Sensor-Labels**.

2. Следует помнить, что в условие **"url"** попадает полный URL запроса, включая имя хоста (т.е. в виде **http://www.mail.ru/mail/read.php?some=parameter&param2**), это необходимо учитывать в условии проверки.

4.4.3.4. Фильтрация по HTTP+DNSBL

Задача

Если сообщение получено или передано методом GET HTTP-протокола и адрес сервера есть в списке **dnsbl** (например, **dnsbl.sorbs.net**), то необходимо пометить сообщение меткой **"possible malware or proxy"**.

Описание логики решения

Проверить метод HTTP-запроса, используя фильтр HTTP-протокола. Чтобы убедиться, что адрес сервера присутствует в некотором DNSBL-списке, необходимо использовать фильтр сообщений. Таким образом для решения общей задачи будут использованы два фильтра: фильтр HTTP-протокола и фильтр сообщений. В фильтре HTTP-протокола будет проверен метод GET и поставлена некоторая метка на все GET-запросы (например "HTTP_GET").

Эта метка останется и в сообщениях, которые будут извлечены из этих запросов и будет доступна далее в фильтре сообщений. В фильтре сообщений, для сообщений, содержащих метку "**HTTP_GET**", будет проверено вхождение адреса сервера в DNSBL-список через выполнение действия "**dnsbl**". Если адрес сервера будет входить в DNSBL-список, то на это сообщение будет установлена метка (например, "**DNSBL_EXIST**"). Далее в фильтре сообщений необходимо будет проверить для сообщения уже две метки - "**HTTP_GET**" и "**DNSBL_EXIST**" и уже для сообщений с обеими метками установить метку "**possible malware or proxy**".

Также для корректной работы действия "**dnsbl**" необходимо в конфигурации службы **EtherSensor Analyser** настроить DNS-серверы для проверки DNSBL.

Решение

1. Настройка DNS-серверов в конфигурации службы EtherSensor Analyser для проверки DNSBL.

Настройку можно производить в конфигураторе или в конфигурационном файле.

В файле конфигурации службы **EtherSensor Analyser**:

Корневой тег **<AnalyserConfig>**, далее вложенный тег **<RawHttpFilter>** - включаем фильтр HTTP-протокола. Тег настроек фильтров **<Filter>** (включаем фильтр сообщений). Далее вложенный тег **<DnsBl>** - настройки DNS-серверов для проверок адресов в DNSBL-списках в фильтре сообщений.

```
<?xml version="1.0" encoding="utf-8"?>
<AnalyserConfig version="3.2">

<!-- other service settings -->
  <RawHttpFilter enabled="true" filename="http-filter.xml" />
  <Filter enabled="true" filename="msg_filter.xml">

<!-- other filter settings -->

    <DnsBl>
      <AttemptsCount>3</AttemptsCount>
      <TtlForUnknown>3600</TtlForUnknown>
      <MinTtl>300</MinTtl>
      <MaxTtl>604800</MaxTtl>
      <Server ipaddress="127.0.0.1" port="53" />
    </DnsBl>

  </Filter>
</AnalyserConfig>
```

В данном случае предполагается, что DNS-сервер располагается по адресу **127.0.0.1:53**.

2. Файл фильтра HTTP-протокола может выглядеть так (http-filter.xml):

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">

  <table name="main">

    <rule enabled="true">
      <match>
        <c name="method" value="GET"/>
      </match>
      <action name="tag" value="HTTP_GET"/>
    </rule>

    <rule enabled="true">
      <action name="accept" />
    </rule>
  </table>
</filter>
```

Подробное описание условия фильтрации "**method**" и действия "**tag**" смотрите в разделах **"Условие METHOD"** и **"Действие TAG"**.

3. Файл фильтра сообщений может выглядеть так (msg_filter.xml):

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="Message filter" version="1.0">

  <table name="main">

    <rule enabled="true">
      <match>
        <c name="tag" tag="HTTP_GET"/>
      </match>
      <action name="dnsbl-rh"
              address="both"
              tag="DNSBL_EXIST"
              value="dnsbl.sorbs.net" />
    </rule>

    <rule enabled="true">
      <match>
        <and>
          <c name="tag" tag="HTTP_GET"/>
          <c name="tag" tag="DNSBL_EXIST"/>
        </and>
      </match>
      <action name="tag" value="MALWARE_OR_PROXY"/>
    </rule>

  </table>
</filter>
```

Подробное описание условия "**tag**", действия "**tag**" и действия "**dnsbl**" смотрите в разделах "**Условие TAG**", "**Действие TAG**" и "**Действие DNSBL-LH, DNSBL-RH**".

Комментарии и общие рекомендации

1. Для более быстрого разрешения имён DNS в конфигурации службы **EtherSensor Analyser** желательно указывать как можно более быстрые DNS-сервера. Это могут быть как серверы Интернет-провайдера, так и собственные DNS-серверы.

2. Действие "**dnsbl**" (разрешение имён DNS для DNSBL) является относительно длительной операцией (особенно если указано использование нескольких DNSBL-сервисов), в связи с этим старайтесь выполнять его в фильтре только для тех сообщений, для которых это необходимо.

3. Старайтесь применять действие "**dnsbl**" в конце фильтра, в месте, где понадобятся результаты его работы.

4. Следует помнить, что на этапе фильтрации HTTP-протокола ещё не существует сообщений, проверка на их наличие в трафике будет выполнена позже. Однако метки и теги, установленные для запросов, на этом этапе будут сохранены в сообщении (если оно будет извлечено из этих запросов).

4.4.3.5. Фильтрация больших объектов HTTP

Задача

Иногда по протоколу HTTP происходит передача очень больших объектов (закачка файлов, просмотр фильмов онлайн). При большом количестве таких объектов, передаваемых одновременно, **Microolap EtherSensor** может потреблять большое количество оперативной

памяти. Такая ситуация может приводить к общей деградации производительности **Microolap EtherSensor** и среды выполнения.

Необходимо с помощью фильтров отсекать большие HTTP-объекты и удалять их до начала анализа.

Описание логики решения

Для удаления больших HTTP-объектов до их полного анализа (и загрузки для этого в память целиком) необходимо применить HTTP-фильтр. Для проверки размера HTTP-запроса или ответа следует использовать условие **"size"**, которое оно проверяет размер и запроса и ответа.

Решение

Например, файл фильтра HTTP-протокола может выглядеть так:

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">

  <table name="main">

    <rule enabled="1">
      <comment>
        The rule stops processing HTTP objects for which
        the request or response size is greater than 1MB.
      </comment>
      <match>
        <c name="size" op="gt" value="1M"/>
      </match>
        <action name="drop" />
    </rule>

    <rule enabled="true">
      <action name="accept" />
    </rule>
  </table>
</filter>
```

Подробное описание условий фильтрации HTTP-запросов "**size**" смотрите в разделе **"Условие REQ-SIZE, RESP-SIZE, SIZE"**.

Комментарии и общие рекомендации

1. Вместо условия **"size"**, которое проверяет и размер запроса и размер ответа, возможно применять условия **"req-size"** (для проверки размера только HTTP-запроса) или **"resp-size"** (для проверки размера только HTTP-ответа).

5. Служба обновления Microolap EtherSensor

Служба обновления **EtherSensor Updater** (процесс **ethersensor_updater.exe**) предназначена для автоматизированной загрузки и установки файлов обновлений и патчей. **EtherSensor Updater** является частью сервиса разработчика по поддержке работы **Microolap EtherSensor** в штатном режиме и обновлению его функций.

Функции EtherSensor Updater:

- Проверка наличия обновлений и патчей для **Microolap EtherSensor**, их загрузка и установка.
- Оперативное обновление файла лицензии продукта при его изменении.
- Создание архивной копии предыдущей версии продукта и помещение в неё всех необходимых файлов.
- Восстановление предыдущей версии из архива при возникновении ошибки установки обновления.

Вы можете указать интервал проверки обновлений или использовать настройки по умолчанию. **EtherSensor Updater** также позволяет гибко настраивать сетевое подключение, поддерживает работу с прокси сервером.

Принцип работы:

Служба обновлений проверяет как наличие новых версий ПО, так и наличие обновлённых версий лицензий. Для этого она через заданные в настройках интервалы времени устанавливает соединение с сервером обновлений и передаёт ему информацию о версии и лицензии **Microolap EtherSensor**.

Если для установленного программного обеспечения доступны более новые версии, сервер отправляет службе ответный файл-манифест, в котором указаны файлы, которые необходимо загрузить и установить. Служба загружает с сервера обновлений эти файлы и помещает их в очередь на установку. Во время, указанное в конфигурации службы, эти файлы запускаются, и происходит обновление программного обеспечения.

Установка EtherSensor Updater:

Первоначальная установка **EtherSensor Updater** выполняется запуском файла **ethersensor_updater_X.X.X.XXXX_x64.msi** из состава дистрибутива. В дальнейшем служба будет обновляться самостоятельно при выходе новых версий.

Для установки в директорию, отличную от директории по умолчанию следует применить утилиту **msiexec.exe** ОС Windows.

Например:

```
msiexec.exe /i ethersensor_updater_4.6.3.12232_x64.msi INSTALLDIR="C:\Program Files\Microolap Ether
```

Технические требования:

- Служба **EtherSensor Updater** должна иметь доступ в Интернет через порт 80 или 443 к серверам серверами **license.microolap.com** и **kpps-downloads.microolap.com**
- Если используется прокси-сервер, он должен обеспечивать корректную работу SOAP-протокола.
- Операционная система Windows Server 2008, Windows Server 2012 R2 или Windows Server 2016.

EtherSensor Updater состоит из следующих частей:

Служба EtherSensor Updater (процесс **ethersensor_updater.exe**)

Запускается в фоновом режиме и выполняет все действия, необходимые для проверки наличия доступных обновлений и их дальнейшей установки. В процессе работы создаётся статус-файл **status.xml**, в котором содержится информация о текущем состоянии службы.

Раздел "Обновления" конфигуратора **Microolap EtherSensor** (приложение **ethersensor_console.exe**)

Служит для настройки конфигурации и отображения статуса службы**,** в отдельной закладке отображается основной файл журнала обновлений.

Примечание:
1. Конфигуратор **Microolap EtherSensor** соединяется со службой **ethersensor_updater.exe** по TCP/IP-протоколу, порт 52076.
2. Если конфигуратор **Microolap EtherSensor** обнаруживает, что служба **ethersensor_updater.exe** не запущена, попытка установить соединение не происходит. Если необходимо установить соединение со службой, работающей в консольном режиме, можно воспользоваться параметром командной строки **/ignore-service-status**
3. Также можно использовать параметр командной строки **/no-connect**, который запрещает любые попытки связаться со службой. В этом случае конфигуратор **Microolap EtherSensor** получает информацию о состоянии службы только через файл **status.xml**.

Директория [INSTALLDIR]\config

Содержит конфигурационные файлы службы (настройка службы).

Директория [INSTALLDIR]\downloads

При настройке по умолчанию в эту директорию выполняется загрузка файлов, необходимых для обновления ПО.

Директория [INSTALLDIR]\log

Содержит файлы журналов и статус-файл:

status.xml

Статус-файл, содержащий информацию о текущем состоянии службы.

log.txt

Основной журнал работы службы.

uupdater_log.txt

Журналы специальной программы **ethersensor_uupdater.exe**, которая вызывается при необходимости установить новую версию **ПО "Служба обновления EtherSensor"**.

5.1. Настройка в конфигураторе

Конфигурация **EtherSensor Updater** хранится в файле **system.xml**, расположенном в директории **[INSTALLDIR]\config**.

Служба считывает файл конфигурации при запуске. После изменения файла конфигурации необходимо выполнить перезапуск службы, чтобы применить внесённые изменения.

Текущее состояние

В разделе **Текущее состояние** отображается информация из статус-файла **EtherSensor Updater**, касающаяся работы самой службы обновления.

Также отображается список обнаруженного на сенсоре ПО, для которого возможна проверка обновлений, список загружаемых файлов (если что-то загружается прямо сейчас) и список готовых к установке обновлений.

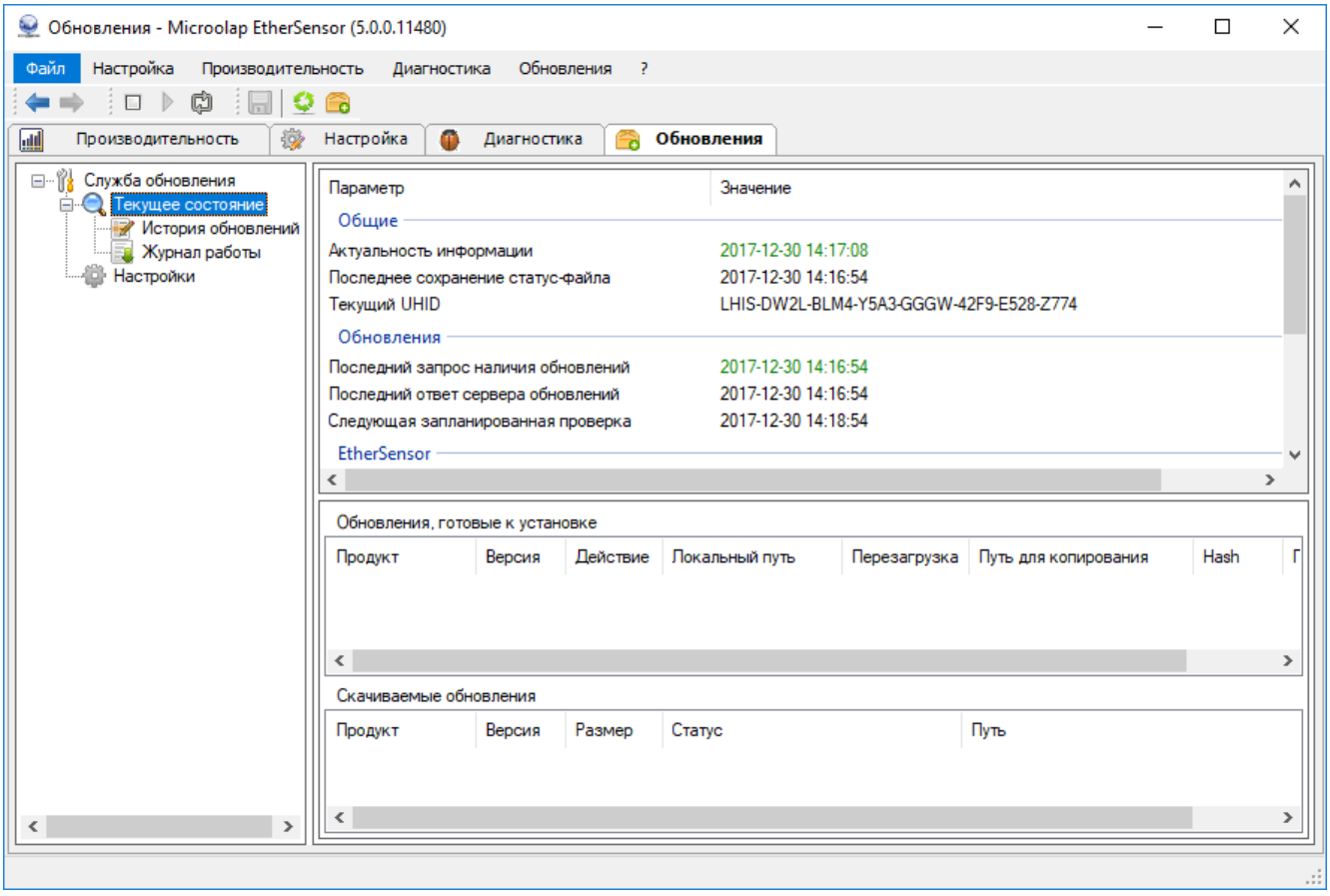

Рис.52. Раздел "Текущее состояние"

Настройки, вкладка **Загрузка обновлений**

В разделе **Загрузка обновлений** устанавливаются режимы работы **EtherSensor Updater** и частота проверок наличия обновлений. Также в этом разделе можно включить тестовый

режим, в котором в файлы журналов добавляются более подробные сообщения о работе службы.

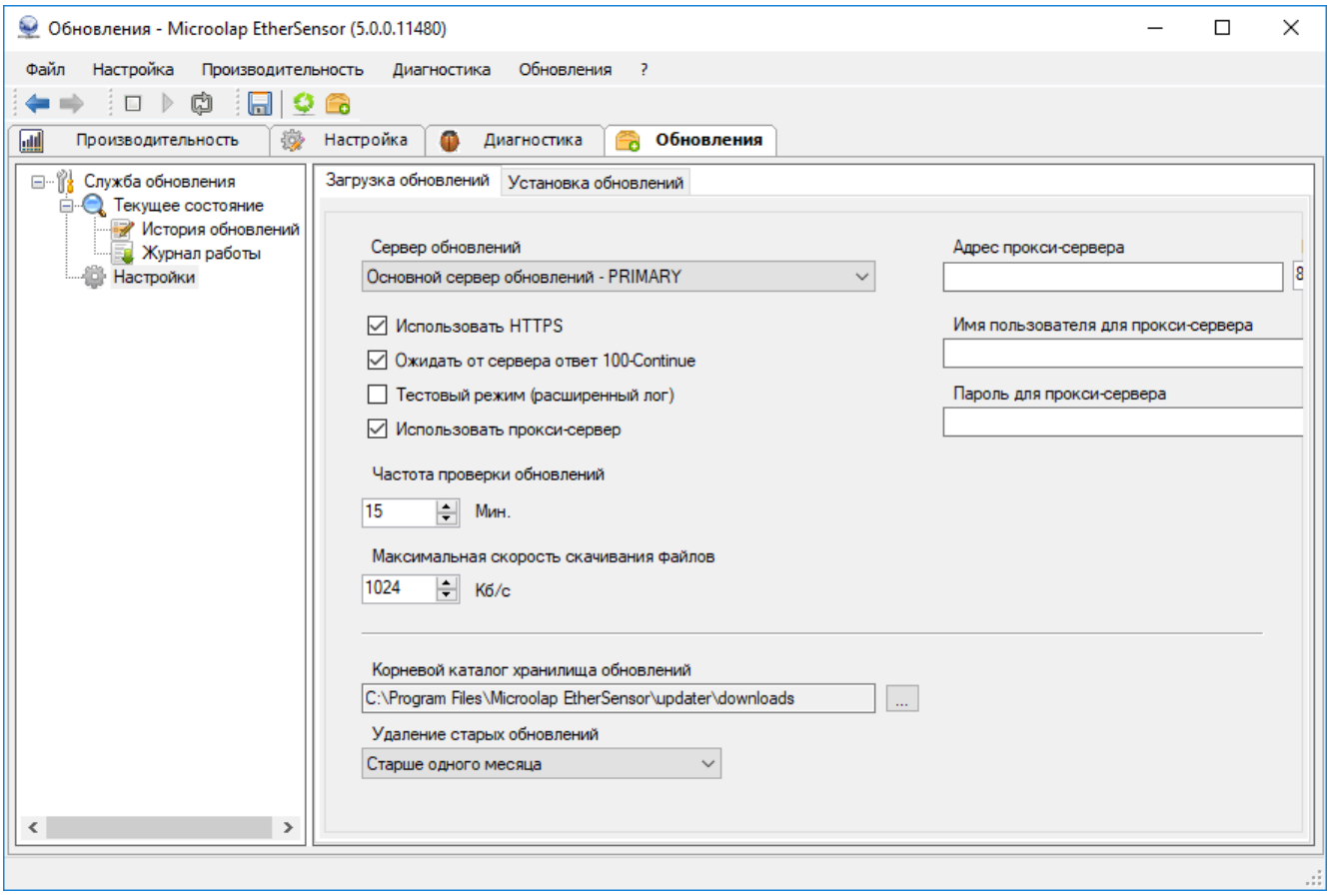

Рис.53. Раздел "Загрузка обновлений"

Более подробно параметры режимов работы **EtherSensor Updater** описаны в разделе Конфигурационный файл system.xml

Настройки, вкладка **Установка обновлений**

В разделе **Установка обновлений** настраивается время автоматической установки обновлений. После установки обновлений происходит перезагрузка ОС, если таковая потребовалась.

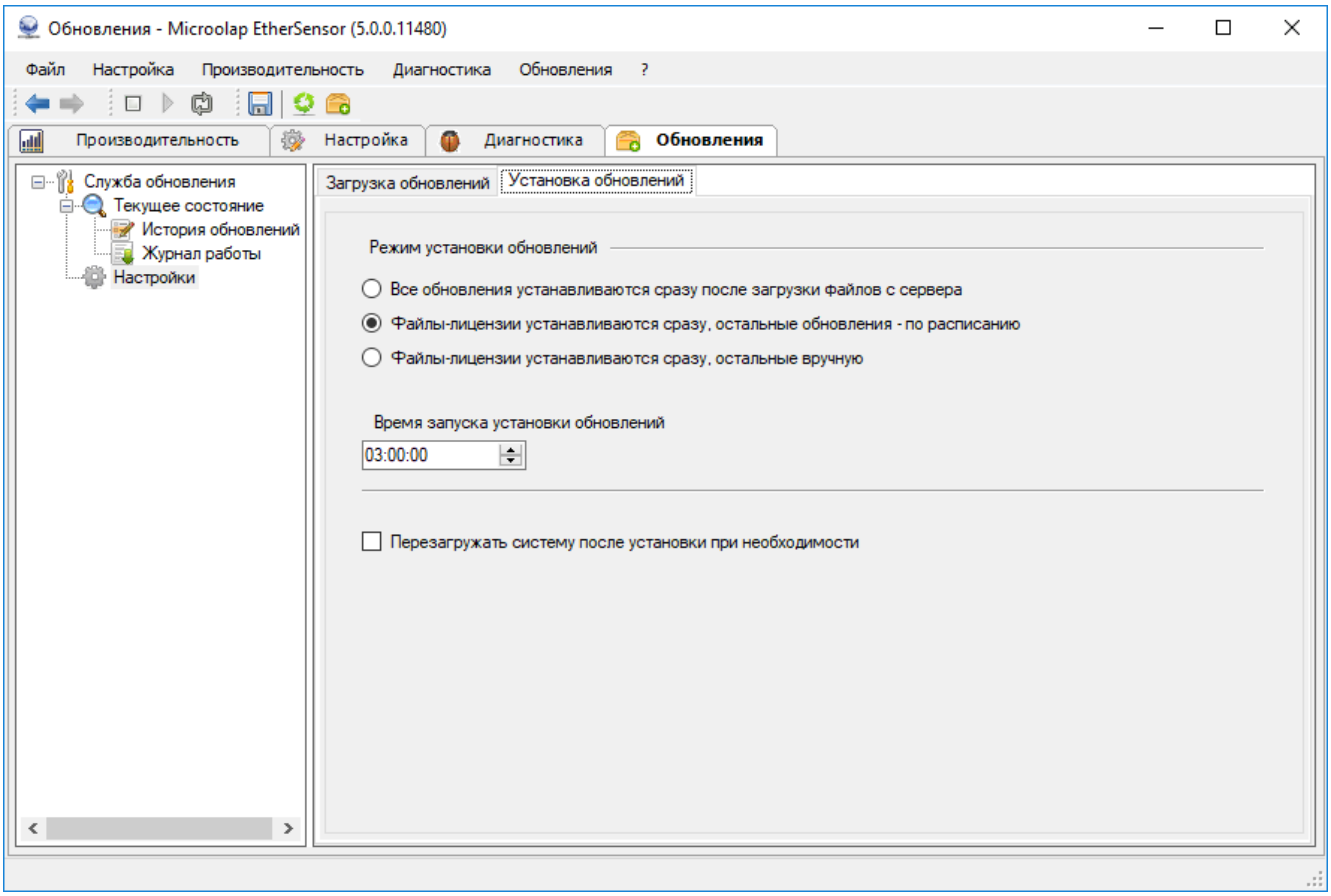

Рис.54. Раздел "Установка обновлений"

Журнал работы

В разделе **Журнал работы** отображаются последние записи файлов журналов **EtherSensor Updater**.

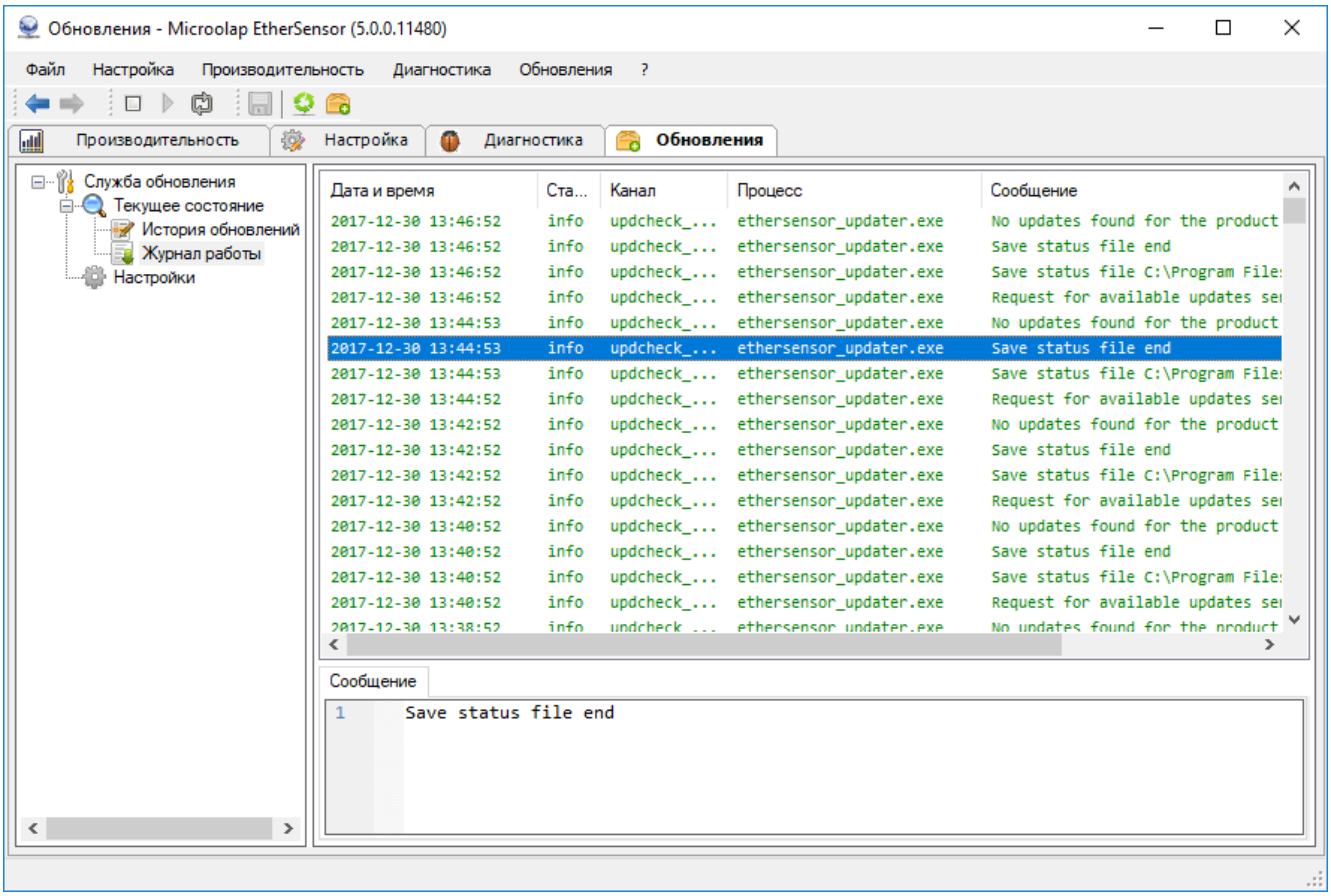

Рис.55. Раздел "Журнал работы"

История обновлений

В разделе **История обновлений** отображается список установленных ранее обновлений.

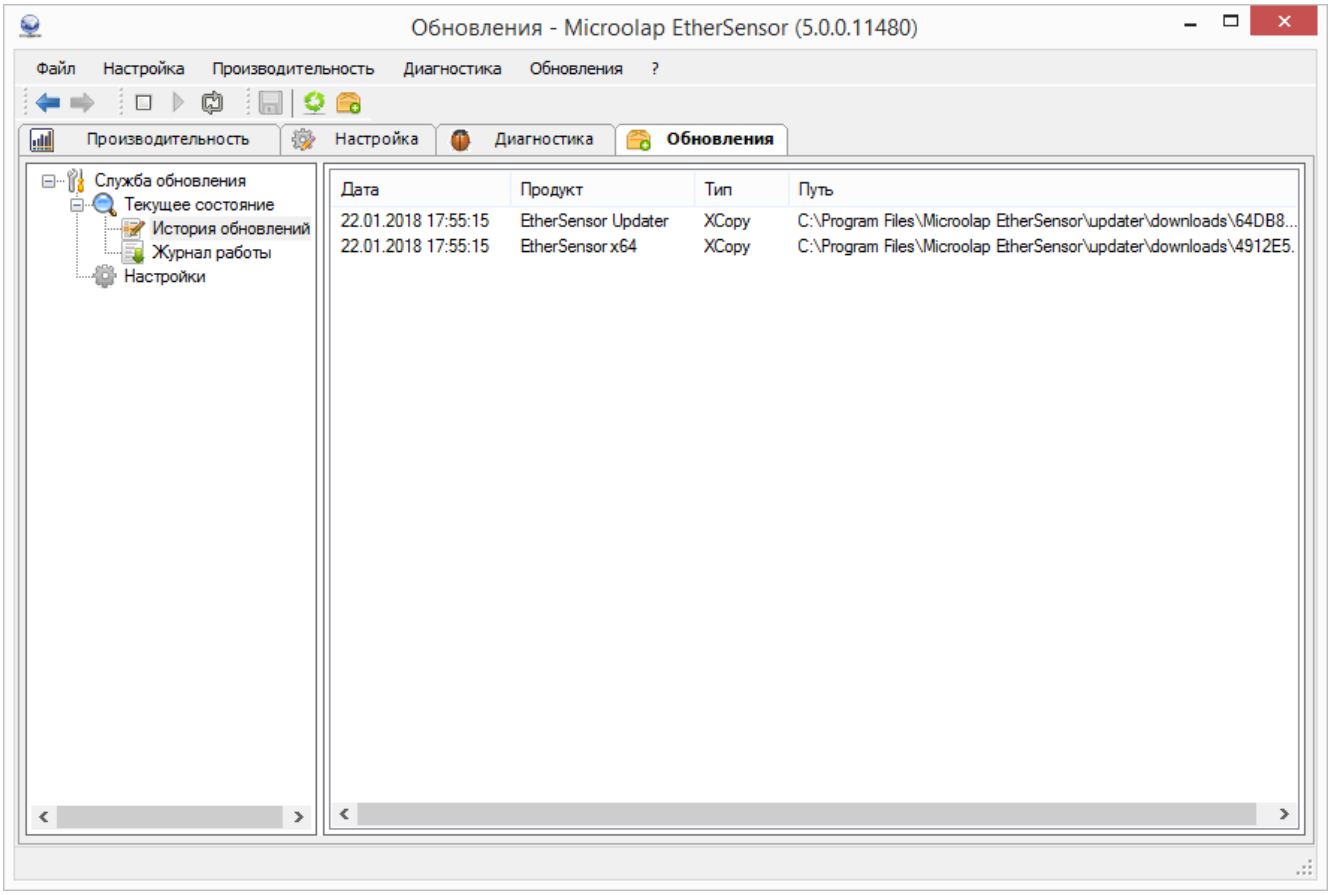

Рис.56. Раздел "История обновлений"

5.2. Ручная настройка (файл конфигурации)

Конфигурация **EtherSensor Updater** хранится в файле **system.xml**, расположенном в директории **[INSTALLDIR]\config**.

Пример файла конфигурации **system.xml**:

```
<?xml version="1.0"?>
<UpdaterConfig xmlns:xsd="http://www.w3.org/2001/XMLSchema"
               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Store>
    <Location>c:\Program Files\Microolap DLP SUS\Downloads\</Location>
    <Rate>SixMonth</Rate>
  </Store>
  <Version>1.0</Version>
  <UpdatesServer>PRIMARY</UpdatesServer>
  <UseHTTPS>false</UseHTTPS>
  <UseWebProxy>false</UseWebProxy>
  <WP_Address>192.168.10.2</WP_Address>
  <WP_Port>3128</WP_Port>
  <WP_Username>test</WP_Username>
  <WP_Password>TscOFRJHHBwXOM5QgazQ8w==</WP_Password>
  <CheckRate>30</CheckRate>
  <mode>wm_standard</mode>
  <InstallationTime>3:00</InstallationTime>
  <AutoReboot>false</AutoReboot>
  <MaxDownloadRate>128</MaxDownloadRate>
</UpdaterConfig>
```

Ниже описаны XML-теги, используемые в файле конфигурации:

CheckRate

Частота опроса обновлений в минутах. Задаёт интервал в минутах, через который будет происходить периодическая проверка обновлений. Первая проверка наличия обновлений происходит через **5** минут после запуска службы. После этого дальнейшие проверки происходят с заданной периодичностью. Для немедленной проверки наличия доступных обновлений можно использовать действие **Проверить обновления** в конфигураторе **Microolap EtherSensor**.

InstallationTime

Время суток, в которое будет автоматически запускаться установка загруженных обновлений. По умолчанию - **3:00**. Для немедленной установки обновлений используйте действие **Установить готовые обновления** в конфигураторе **Microolap EtherSensor**.

AutoReboot

Перезагружать ОС после установки при необходимости. Если какое-либо из установленных обновлений требует перезагрузки операционной системы, конфигуратор **Microolap EtherSensor** выводит сообщение об этом. Если разрешить данную опцию, то операционная система будет перезагружена автоматически после установки всех обновлений, если хотя бы одно из них потребовало перезагрузки.

mode

Режим работы. На данный момент поддерживается только один режим работы: **wm_standard**.

UseHTTPS

Использовать протокол HTTPS для соединения с сервером обновлений. Значение **true** разрешает использования протокола HTTPS для соединения с сервером обновлений. Значение **false** означает, что все соединения будут устанавливаться по протоколу HTTP.

UseWebProxy

Соединяться через прокси-сервер. Данная опция указывает на необходимость соединения через прокси-сервер при работе в стандартном режиме.

WP_Address

Адрес прокси-сервера.

WP_Port

Номер порта прокси-сервера.

WP_Username

Имя пользователя для прокси-сервера. Параметры для установки соединения через прокси-сервер. Если прокси-сервер не требует авторизации, поля **Имя пользователя для прокси-сервера** и **Пароль для прокси-сервера** следует оставить пустыми.

WP_Password

Пароль для прокси-сервера в зашифрованном виде. Для его изменения следует использовать конфигуратор **Microolap EtherSensor**.

<Store><Location>

Корневая директория хранилища. Путь к директории, в которую будет происходить загрузка файлов при работе в стандартном режиме, а также в котором будут сохраняться файлы из директории обновлений при работе в локальном режиме. В этой директории создаются поддиректории, содержащие в имени ID продукта, для которого предназначены обновления, а также дату и время, когда это обновление было получено. По умолчанию это поддиректория **downloads** директории установки службы обновлений.

<Store><Rate>

Интервал очистки хранилища. Период времени, после которого сохранённые в хранилище файлы удаляются. Допустимые значения тега:

None

Не удалять файлы;

OneMonth

Удалять файлы старше одного месяца;

TwoMonth

Удалять файлы старше двух месяцев;

ThreeMonth

Удалять файлы старше трёх месяцев;

SixMonth

Удалять файлы старше полугода;

Year

Удалять файлы старше года.

<MaxDownloadRate>

Максимальная скорость загрузки файлов. Максимальная скорость в килобайтах в секунду, с которой загрузчик будет выполнять загрузку файлов обновлений с сервера. Рекомендуется ограничивать эту скорость, чтобы не допустить полной загрузки интернет-канала Службой обновления.

6. Регламентное обслуживание сенсора

В целях поддержания оптимального рабочего состояния сенсора и обнаружения проблем на ранних этапах их развития, рекомендуется регулярно выполнять следующие основные операции.

1. Проверка журналов событий сенсора на предмет наличия предупреждений и ошибок служб.

2. Выполнение резервного копирования. Необходимо убедиться в том, что конфигурационный файл сенсора регулярно резервируется на внешний носитель информации.

3. Проверка индикаторов производительности сервера, на котором функционирует **Microolap EtherSensor**, таких как свободное место на диске, утилизация процессора, использование оперативной памяти. Для этой цели может быть использовано средство Windows Performance Monitor и приложение **ethersensor_console.exe**, установленное в директории установки **Microolap EtherSensor**. Использование механизма уведомлений позволяет уведомлять сотрудников группы поддержки **Microolap EtherSensor** о внезапных изменениях или проблемах с производительностью сервера.

4. Проверка журнальных файлов на сетевом устройстве. Следует проводить анализ журнальных файлов на предмет корректности работы транспортной службы, а также оценить объемы ответвляемого трафика с целью недопущения перегрузки его потребителей.

5. Проверка доступности потребителей перехваченных сообщений со стороны сенсора. Следует убедиться, что сообщения, формируемые службами сенсора, доставляются на серверы потребителей сообщений. В случае невозможности доставки сообщений потребителям возможно переполнение дискового пространства на сенсоре (зависит от установленных администратором дисковых квот).

6.1. Вопросы по обслуживанию сенсора

Как удалить сервисы Microolap EtherSensor вручную?

1. В командной строке выполнить следующие команды:

```
sc delete "EtherSensorEtherCAP"
sc delete "EtherSensorICAP"
sc delete "EtherSensorLotusTXN"
sc delete "EtherSensorAnalyser"
sc delete "EtherSensorTransfer"
sc delete "EtherSensorWatcher"
```

2. Запустить утилиту **regedit** и удалить ветки реестра:

```
HKLM/System/CurrentControlSet/EtherSensorAnalyser
HKLM/System/CurrentControlSet/EtherSensorEtherCAP
HKLM/System/CurrentControlSet/EtherSensorICAP
HKLM/System/CurrentControlSet/EtherSensorLotusTXN
HKLM/System/CurrentControlSet/EtherSensorTransfer
HKLM/System/CurrentControlSet/EtherSensorWatcher
```

3. Удалить файлы старой версии.

4. Перезагрузить сервер.

Почему много дубликатов в письмах?

1. Веб сервисы могут отправлять формы более одного раза, например при сохранении черновиков или добавлении вложений (аттачментов).

2. В некоторых сложных сетевых условиях (например, при использовании цепочки прокси-серверов или балансировщиков нагрузки) возможна ситуация, когда сенсор видит одно и тоже соединение несколькими интерфейсами одновременно. В таком случае следует использовать фильтр **check-md5**, это позволит принять решение - обрабатывать или не обрабатывать данное сообщение еще раз.

Я вижу трафик из mirror порта <другим сниффером>, а ваш сенсор ничего не ловит.

Счетчики трафика крутятся, но сенсор ничего не ловит.

В записи перехвата не видно обратных пакетов от HTTP-сервисов, т.е. пакеты от клиентского IP на удаленный сервер/порт видны, а ответы от удаленного сервера/порта - нет. От клиента при этом летят пакеты ACK, FIN/ACK, т.е. это означает, что это рабочие сессии с реальным трафиком, который доходит до клиента.

Проверка производится в следующем порядке:

1. Убедиться, что службы запущены и работают.

2. Проверить правила IP-фильтрации, помня о том, что для применения правил необходимо перезапустить службы.

3. Проверить счетчики трафика. Не должно быть количество **Получено** равно количеству **Отклонено**.

4. Проверить наличие перехваченных данных в поддиректории **data** директории установки **Microolap EtherSensor**. Если используются фильтры, проверить также содержимое **[INSTALLDIR]\data\filter.**

5. Проверить директорию **[INSTALLDIR]\data\result** - есть ли перехваченные сообщения, которые не отправлены?

6. Проверить журналы и счетчики на предмет ошибок. Если их нет, то службы работают нормально.

7. Проверить настройки mirror-порта. Например, на оборудовании компании Cisco по умолчанию зеркалируются пакеты либо **RX**, либо **TX**. Нужно указать в настройке ключевое слово **both**:

```
monitor session 1 source interface <interface-id> both
```

8. Проверить, настроен ли профиль в настройках службы транспорта, правильный ли профиль указан в качестве профиля по умолчанию.

9. В случае если выяснить причину самостоятельно не удается, обратиться в техническую поддержку.

7. Лицензирование Microolap EtherSensor

Ниже описан порядок лицензирования **Microolap EtherSensor**.

7.1. Лицензионный файл

Информация о лицензиях **Microolap EtherSensor** содержится в файле **license.licx**, который должен находиться в корневой директории установки **Microolap EtherSensor**.

> **Внимание!**
> Версии **Microolap EtherSensor** начиная с **4.0.15** не работают с лицензиями, выписанными до марта 2012г.
> Пожалуйста, убедитесь, что Вы обновили файл **license.licx** перед тем, как обновлять **Microolap EtherSensor** до версий **4.0.15** и выше.
> (Если открыть файл **license.licx** текстовым редактором, он должен содержать XML-тег **<UPDSUBEND></UPDSUBEND>**)

Лицензия содержит информацию о модулях, лицензированных для данной инсталляции, сроках действия лицензии для каждого модуля, дату истечения подписки на обновления и другие данные. Содержимое файла лицензии открыто для просмотра, но защищено контрольной суммой и цифровой подписью. Лицензия выдается для инсталляции **Microolap EtherSensor** на конкретном оборудовании, для чего предусмотрена специальная проверка.

Состояние лицензии можно просмотреть с помощью конфигуратора (секция **Лицензирование**).

В зависимости от наличия в корневой директории файла **license.licx** и типов лицензий на **Microolap EtherSensor**, все модули работают в одном из режимов:

Демо-режим

В этом режиме детектируются все сообщения, но только каждое пятое сообщение передается службе транспортировки в полном оригинальном виде. Срок работы **Microolap EtherSensor** в демо-режиме не ограничен. В полный режим **Microolap EtherSensor** переводится помещением в корневую директорию корректного файла **license.licx** (без перезапуска служб).

Полный режим

В полном режиме ПО сенсора работает в течение неограниченного периода времени, обеспечивая работу всех доступных в соответствии с лицензией модулей. После даты окончания подписки на обновления, указанной в файле лицензии **license.licx**, ПО перестанет обновляться автоматически. Установка вручную версии ПО, выпущенной после даты окончания подписки на обновления, приведёт к запуску ПО в демонстрационном режиме, в котором ПО будет оставаться до тех пор, пока не получит файл лицензии **license.licx** с обновленными лицензионными данными. При запуске в демо-режиме версии ПО, выпущенной после даты окончания подписки на обновления, в файл журнала будет выдано сообщение о последней версии, работа с которой допускается текущей лицензией.

В отдельных случаях (например, в целях тестирования) в лицензию могут быть включены модули с указанными сроками их действия. В таком случае после окончания сроков действия модулей перехват сообщений, соответствующих этим модулям, будет происходить в демонстрационном режиме.

Microolap EtherSensor записывает факт окончания лицензии в журналы **Microolap EtherSensor**.

Файл лицензии может быть передан на работающий сенсор автоматически, через систему обновлений.

Файл лицензии **license.licx** генерируется разработчиком **Microolap EtherSensor** на основе файла запроса на лицензию **request.licx**, созданного на конкретном экземпляре оборудования сенсора. При переносе **Microolap EtherSensor** на другой сервер или замене вышедшего из строя оборудования, если **Microolap EtherSensor** будет распознавать лицензию как нерабочую, следует отправить новый запрос на лицензию и получить новый файл лицензии **license.licx**.

> **Внимание!**
>
> Каждая лицензия привязывается к оборудованию среды выполнения, для которой она выписывалась.
>
> Поэтому для исключения проблем с изменением UHID в процессе эксплуатации перед созданием файла **request.licx** необходимо привести всё оборудование среды

выполнения в то состояние, в котором оно будет эксплуатироваться, то есть отключить все временные устройства (флеш-карты, USB-HDD и т.п.), отключить все временные, виртуальные или неиспользуемые сетевые карты, настроить MAC-адреса и т.п.

Более подробно с понятием UHID можно ознакомиться в разделе UHID (HardwareID) среды выполнения.

Для создания файла **request.licx** следует в конфигураторе открыть секцию **Запрос лицензии** и заполнить в появившемся окне соответствующие поля, затем нажать кнопку **Сохранить**:

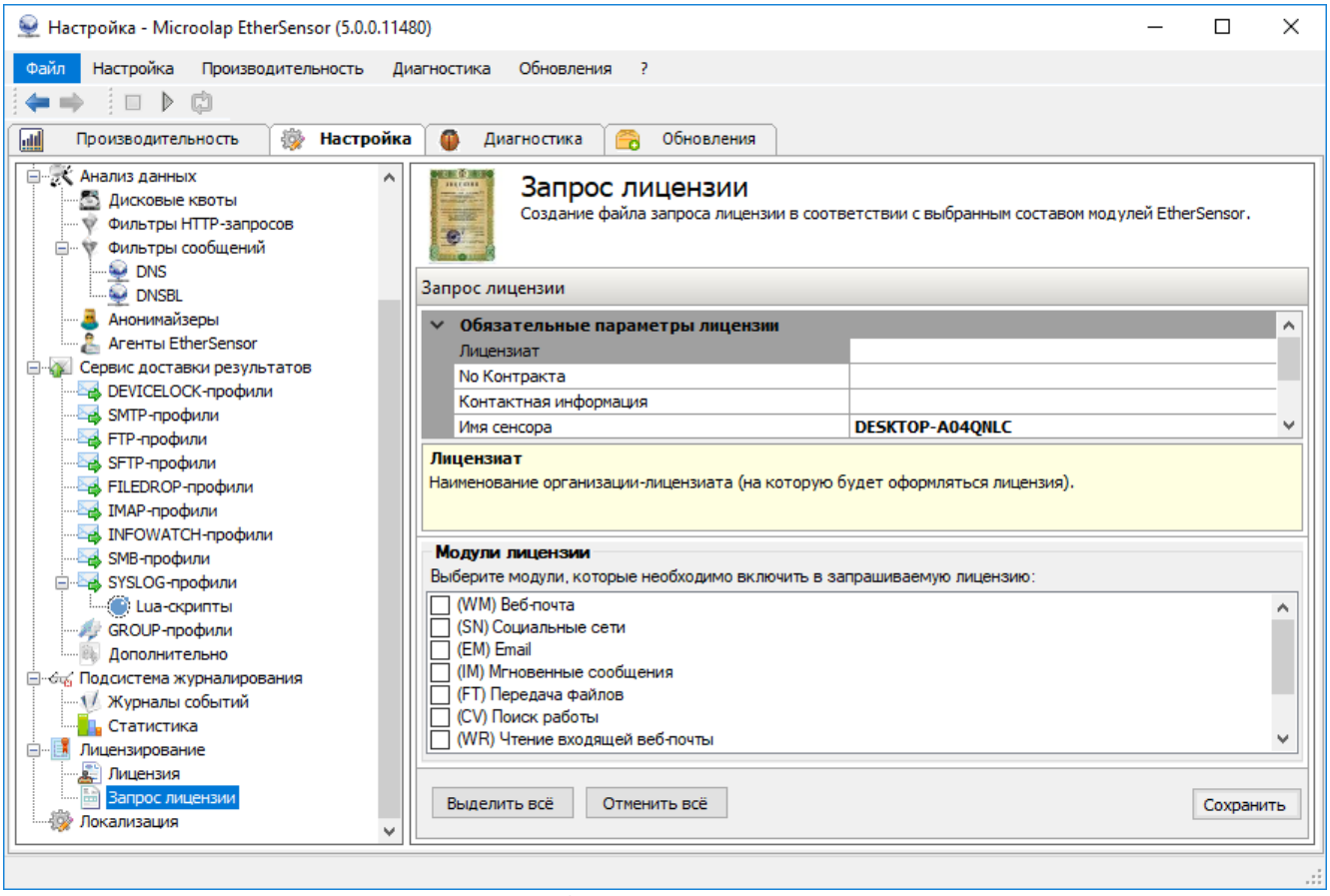

Рис.57. Форма запроса лицензии.

Файл запроса лицензии будет сохранен в директории установки **Microolap EtherSensor** с именем **request.licx**.

Лицензиат:

Полное название организации-лицензиата.

No Контракта:

Реквизиты договора, по которому предоставляются лицензии, название контрагента обязательно.

Контактная информация:

Достаточные контактные данные лица, отвечающего за эксплуатацию **Microolap EtherSensor** (имя, номер телефона, электронный адрес и т.п.).

Имя сенсора:

Наименование сенсора (физической станции). Используется, чтобы отличать разные сенсоры в пределах одной организации. Сюда можно ввести имя хоста или какое-либо условное наименование сенсора, однозначно идентифицирующее его в пределах организации-лицензиата.

Модули лицензии:

Модули **Microolap EtherSensor**, подлежащие лицензированию.

После нажатия кнопки **"Сохранить"** в корневой директории установки **Microolap EtherSensor** появится файл **request.licx.** Его следует отправить поставщику **Microolap EtherSensor** для создания на его основе нового файла лицензии **license.licx**.

7.2. UHID (HardwareID) среды выполнения

Каждая лицензия на продукт (файл **license.licx**) привязывается к оборудованию среды выполнения **Microolap EtherSensor**, для которой предназначается эта лицензия. Эта привязка делается через т.н. **UHID** - специальный код, уникальный для каждой системы и набора оборудования (**U**nique **H**ardware **ID**entifier). UHID добавляется в файл-лицензию, и затем **Microolap EtherSensor** проверяет соответствие UHID системы и UHID в лицензии.

Если UHID в лицензии не соответствует текущему UHID системы, то Microolap EtherSensor автоматически переходит в Демо-режим (подробнее см. раздел "Лицензионный файл").

При вычислении текущего UHID в том числе используется и список сетевых карт системы, а также список устройств хранения системы. Это означает, что при изменении списка сетевых карт или списка устройств хранения системы текущий UHID также может измениться.

> **Внимание!**
> Для исключения проблем с изменением UHID в процессе эксплуатации перед созданием файла request.licx необходимо привести всё оборудование среды выполнения **Microolap EtherSensor** в то состояние, в котором оно будет эксплуатироваться, т.е. отключить все временные устройства (флеш-карты, USB-HDD и т.п.), отключить все временные, виртуальные или неиспользуемые сетевые карты, настроить MAC-адреса и т.п.
>
> После этого в созданном файле **request.licx** будет выполнена привязка к оборудованию, и при наличии этого оборудования в среде выполнения **Microolap EtherSensor** нарушение работы лицензии происходить не будет.

После получения лицензии (файл **license.licx**) **Microolap EtherSensor** проверяет UHID, указанный в лицензии, на соответствие UHID среды выполнения.

В процессе эксплуатации **Microolap EtherSensor** может выполняться временное подключение устройств хранения (флеш-карта, переносной HDD и т.п.). ПО умеет отслеживать такие ситуации и продолжит работать корректно с лицензионным файлом даже несмотря на временную смену UHID.

Однако при запланированной замене или добавлении оборудования UHID может измениться на постоянной основе. В этой ситуации необходимо заново сгенерировать файл **request.licx** (подробнее см. раздел "Лицензионный файл"), и отправить его на адрес license@microolap.com с объяснением того, какое именно оборудование изменилось. Оператор разработчика **Microolap EtherSensor** проверит данные и изменит лицензию, чтобы она соответствовала новому UHID среды выполнения **Microolap EtherSensor**.

Посмотреть текущий UHID среды выполнения, а также UHID, заданный в лицензии, и проверить их соответствие можно в конфигураторе (утилита **ethersensor_console.exe**):

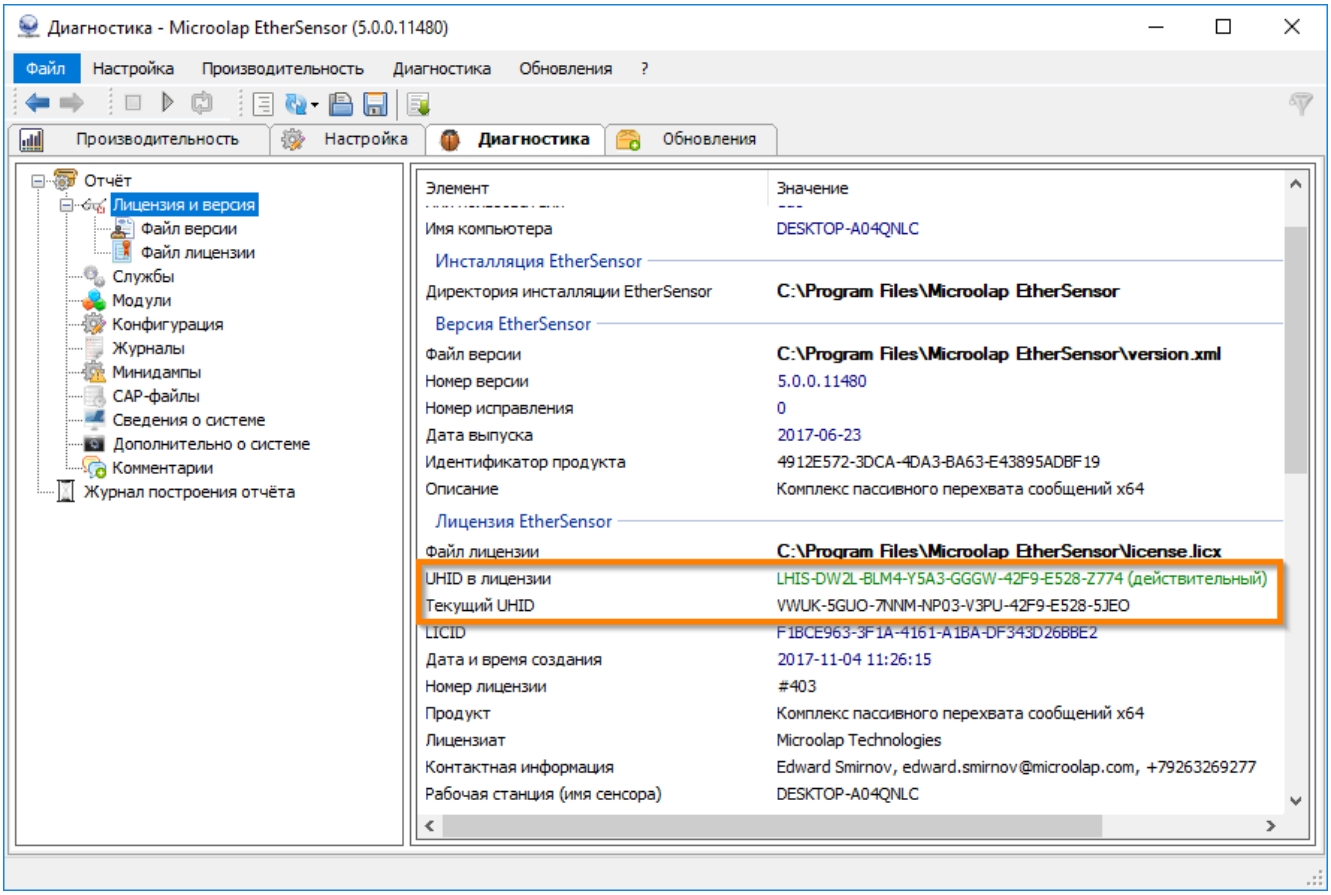

Рис.58. Информация об UHID среды выполнения и лицензии в утилите ethersensor_console.exe

Видно, что текущий UHID среды выполнения отличается от UHID лицензии (так как было подключено дополнительное устройство хранения). Однако **Microolap EtherSensor** по-прежнему признаёт UHID в лицензии действительным.

7.3. Работа с системой лицензирования

Невозможно выписать лицензию до момента установки **Microolap EtherSensor** на сервер для данной инсталляции, так как для генерации лицензии системе лицензирования необходимы данные о среде выполнения. Лицензии привязаны к оборудованию среды выполнения и на других платформах работать не должны.

После установки Microolap EtherSensor следует используя конфигуратор (файл **ethersensor_console.exe** из поставки **Microolap EtherSensor**) создать запрос на лицензию, который содержит данные о среде выполнения. Запрос сохраняется в виде файла **request.licx** в корневой директории установки **Microolap EtherSensor**. Более подробно о генерации файла **request.licx**: Лицензионный файл

На основании данного запроса разработчик **Microolap EtherSensor** выдает тот или иной тип лицензии. Данный файл можно передать по email, на съемном носителе, а также можно воспользоваться веб-интерфейсом системы лицензирования, доступным сервисным инженерам.

Интерфейс расположен по адресу https://license.microolap.com

Генерация лицензии требует подтверждения разработчика **Microolap EtherSensor** для того, чтобы инженер смог получить ее с интерфейса или по почте. Получение подтверждения занимает не менее 3 часов.

Доступ к системе лицензирования предоставляется инженерам поддержки по запросу на адрес license@microolap.com.

> **Внимание!**
> Следует помнить, что от состояния лицензии напрямую зависит работа системы обновления **Microolap EtherSensor** - с истекшей лицензией обновления получить невозможно, от данных лицензии зависит, когда и какие обновления получит **Microolap EtherSensor**. Так, в частности, система обновления позволяет заменить лицензионный файл для инсталляции, так что не потребуется ручных операций по замене лицензии.

Экспресс-лицензии

Если требуется быстро запустить **Microolap EtherSensor**, инженер может получить для новой инсталляции **экспресс-лицензию**. Она представляет собой полную лицензию на **Microolap EtherSensor**, однако время ее действия ограничивается одной неделей с даты выписки, и ее можно загрузить из интерфейса лицензирования сразу после выписки, без подтверждения разработчика **Microolap EtherSensor**. Для каждой инсталляции возможно выписать одну экспресс-лицензию - следующие лицензии должны быть полными и подтвержденными разработчиком **Microolap EtherSensor**.

> **Внимание!**
> Экспресс-лицензии стоит использовать только в крайних случаях, когда необходимо действительно срочно запустить работу **Microolap EtherSensor**.
>
> Запрещается использование экспресс лицензирования для выписки временных, тестовых и т.п. лицензий. Для таких лицензий необходимо отправлять файл **request.licx** на адрес license@microolap.com с пояснением, для чего и на какой срок необходимо сгенерировать лицензию.

Если инженер выписал экспресс-лицензию для площадки, он **должен** обратиться с письмом на license@microolap.com с просьбой заменить лицензию на полную лицензию. Оператор разработчика **Microolap EtherSensor** проверит данные о сервисном контракте и выпустит лицензию для данной инсталляции через Службу обновлений.

Важно: Служба обновлений автоматически применяет обновления раз в сутки. Получение обновлений и замены для лицензий в автоматическом режиме следует ожидать не ранее, чем на следующий день после обращения, или же вручную инициировать установку обновлений, полученных Службой обновления.

> **Внимание!**
> Для штатной работы **Microolap EtherSensor** требуется доступ сервера установки ПО к Службе обновлений, в отсутствие такого доступа корректная работа ПО не гарантируются и поддержка не предоставляется.

Бета-лицензии

Лицензионная система позволяет определить некоторые лицензии как бета-лицензии. Инсталляции с бета-лицензиями получают обновления до того, как они будут выпущены для всех прочих инсталляций. Это позволяет иметь тестовые инсталляции продукта для проверки работы новых версий.

8. Действия в аварийных ситуациях

Ниже описан порядок действий в аварийных ситуациях.

8.1. Отказ технических средств

Ниже перечислены возможные виды отказа технических средств, на которых работает **Microolap EtherSensor**, действия по их устранению и последующему восстановлению работы сенсора.

Невозможность запуска служб Microolap EtherSensor в случае некорректной перезагрузки или остановки сервера.

Симптомом данной аварийной ситуации является системное сообщение (Error 1053) о невозможности запуска службы.

В случае если не удается запустить какую-либо службу **Microolap EtherSensor**, необходимо выполнить следующие действия:

- Попробовать запустить службы повторно, при этом необходимо помнить, что для успешного запуска служб **Microolap EtherSensor** необходим запуск службы **EtherSensor Watcher**;
- Если повторный запуск служб не был выполнен успешно, необходимо обратиться в службу технической поддержки.

Переполнение дискового пространства, выделенного под спулы перехвата сообщений.

Симптомами данной аварийной ситуации являются:

- Оповещения операционной системы об отсутствии свободного места на диске;
- Записи в системном журнале операционной системы об отсутствии свободного места на диске.

Системный администратор должен установить причину отсутствия свободного пространства. Для этого нужно воспользоваться оснасткой **Disk Management**. Если причиной является переполнение спулов (директория **[INSTALLDIR]\data**), необходимо удалить или перенести данные спулов на свободный дисковый раздел. Также причинами переполнения могут быть:

- Недоступность сервера, на который сенсор должен передавать сообщения - в таком случае требуется устранить неполадки связи;
- Слишком большой объем трафика, обрабатываемый сенсором - в таком случае необходима установка дополнительных сенсоров и разделением нагрузки между сенсорами.

Аварийное выключение питания сервера, на котором работает Microolap EtherSensor.

После возобновления питания и включения сервера, на котором работает **Microolap EtherSensor**, системный администратор должен убедиться в том, что все службы успешно запущены.

При возникновении отклонений от нормального запуска следует просмотреть журналы служб. Если там обнаруживаются сообщения об ошибках, необходимо обратиться в службу технической поддержки.

Обрыв сетевого подключения сервера, на котором функционирует Microolap EtherSensor.

Симптомами данной аварийной ситуации являются:

- Сетевая карта сервера, на котором функционирует сенсор, сигнализирует о механическом нарушении канала связи;
- Возврат пакетов, отправленных по протоколу ICMP на серверы дальнейшей обработки сообщений, не выполняется или выполняется частично;

Системный администратор должен проверить и восстановить канал связи сервера, на котором функционирует **Microolap EtherSensor**. Затем следует проверить настройки сети в операционной системе. После устранения проблем с сетевым подключением необходимо убедиться в том, что все службы **Microolap EtherSensor** работают.

8.2. Несанкционированный доступ к ПО или ОС

Несанкционированное вмешательство в **Microolap EtherSensor** или ОС можно определить по следующим признакам:

- В журнале безопасности Windows присутствуют записи о попытках несанкционированного доступа в систему;
- В системе происходит самопроизвольное удаление или создание файлов, запуск произвольных служб.

В случае обнаружения подобных признаков необходимо выполнить следующие действия:

1. Отключить доступ сенсора к сети.

2. Остановить функционирование **Microolap EtherSensor** посредством остановки всех служб.

3. Устранить причины несанкционированного вмешательства в систему.

4. Восстановить работоспособность **Microolap EtherSensor**.

9. Локализация GUI

В рабочем режиме узел **Локализация** конфигуратора **Microolap EtherSensor** спрятан. Чтобы он появился, в поддиректории **lang** директории установки **Microolap EtherSensor** необходимо создать файл с именем **!.xml** (содержимое не имеет значения).

После перезапуска **ethersensor_console.exe** в дереве функций слева появится узел **Локализация.** Если кликнуть по нему, то откроется окно локализации элементов GUI:

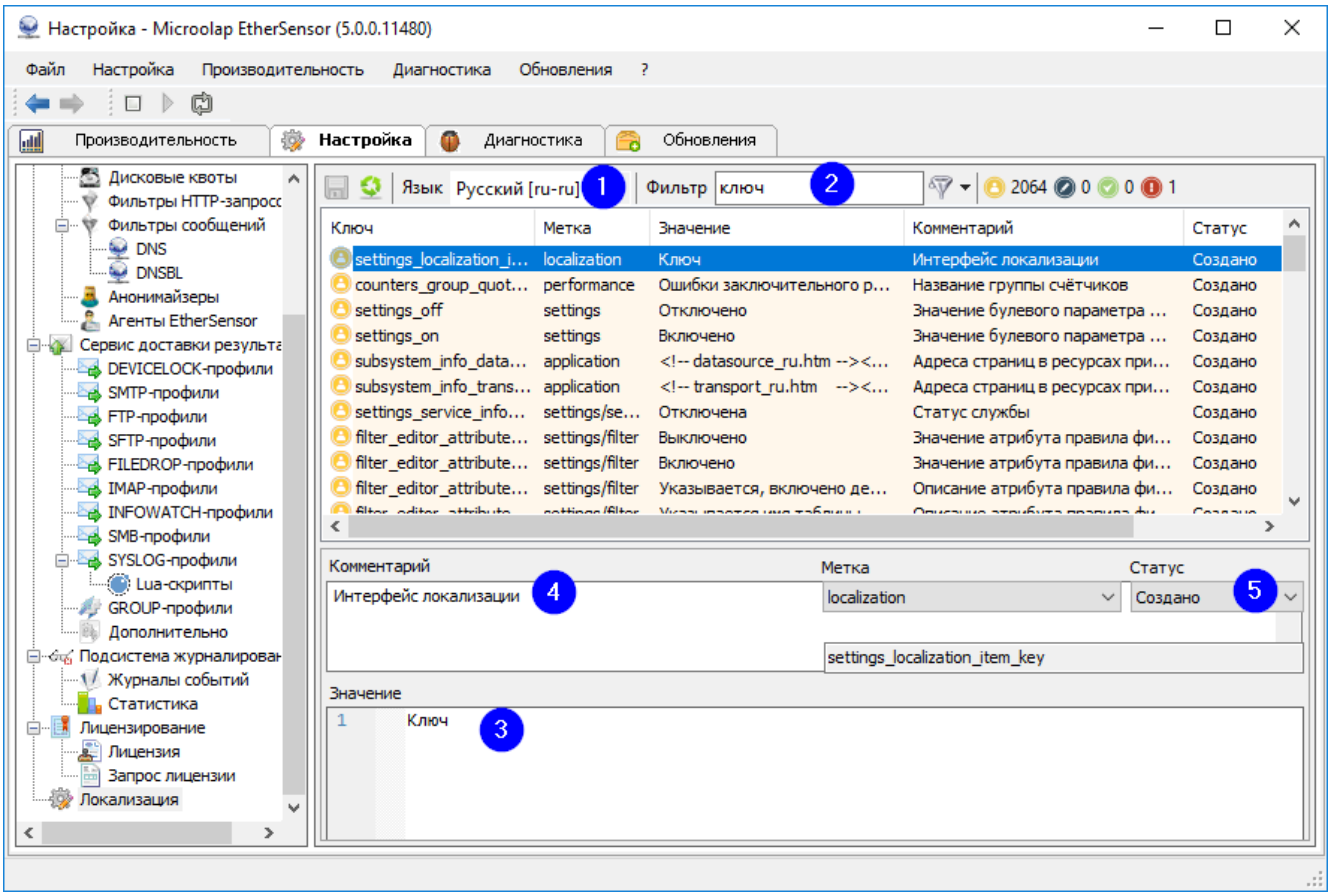

Рис.59. Окно узла Локализация

Текстовые строки элементов GUI хранятся в языковых XML-файлах, находящихся в поддиректории **lang** директории установки **Microolap EtherSensor.** Эти файлы редактируются непосредственно в окне узла **Локализация**.

Для того, чтобы сохранить изменённый текст в языковом XML-файле, нажмите **Ctrl-S**. Чтобы увидеть обновлённые элементы GUI, нажмите **Ctrl-R.** Эти же действия можно произвести кнопками на тулбаре слева от выпадушки **Язык** (1).

Основные элементы управления окна локализации:

1. Язык:
Переключатель редактируемого языкового XML-файла (не путать с языком GUI, переключаемым по **Настройка -- Изменить язык**). Надписи на этом элементе определяются названием и содержимым языковых XML-файлов.

2. Фильтр:
Фильтр для поиска строковых значений. Поиск может происходить в колонках **Ключ**, **Метка**, **Значение**, **Комментарий**, **Статус** или же во всех сразу. Область поиска устанавливается в выпадушке около значка воронки справа от элемента **Фильтр.**

3. Значение:
Окно редактирования поля **Значение**. Содержимое именно этого окна используется при отображении элемента интерфейса.

4. Комментарий:
Окно редактирования поля **Комментарий**. Предназначено для произвольного текста - напоминаний, пояснений: **Что они имели в виду?**, **Погуглить термин**, **Укоротить** и т.п.

5. Статус:
Переключатель статуса элемента интерфейса. По умолчанию значения статусов: **Создано**, **Отредактировано**, **Утверждено, Ошибка**, но могут быть изменены на ваше усмотрение здесь же. Каждому статусу соответствует свой фоновый цвет строки элемента интерфейса. Справа вверху окна интерфейса локализации расположены счетчики элементов с различными статусами, что позволяет оценить объем оставшейся работы.

Поля **Ключ** и **Метка**:

Ключ:
Текстовые элементы GUI хранятся в XML-файлах по принципу "ключ-значение", где поле **Ключ** является уникальным ключом, а поле **Значение** содержит отображаемый в элементе GUI текст. Все остальные поля являются вспомогательными и используются только для удобства работы.

Метка:
Хотя разработчики и стремились сделать значения поля **Ключ** понятными и иерархичными, им показалось это недостаточным и они ввели поле **Метка** для более точного обозначения, к какой именно группе элементов относится данный текстовой элемент GUI. Введя соответствующую строку в фильтре можно ограничить список показываемых элементов заданным меткой разделом.

Текстовые элементы также можно перегруппировывать по принадлежности к группе с помощью элемента **Метка**. Список меток жестко зашит в **ethersensor_console.exe** и в текущей версии изменён быть не может.

Поле **Связи** нужно ***только*** разработчикам для контроля неиспользуемых элементов GUI: "осиротевших" или же заготовленных на будущее.

> **Советы:**
> **1.** Строки таблицы текстовых элементов GUI можно сортировать по возрастанию и по убыванию: для этого нужно кликнуть по названию соответствующего столбца. Такая сортировка помогает быстро найти нужные элементы: по статусу, по принадлежности к группе, по алфавиту и т.д.
> **2.** Если какое-либо из полей не пригождается в работе, столбец с этим полем можно скрыть, сузив его до минимальной ширины.

9.1. Языковые файлы

Текстовые строки элементов GUI хранятся в языковых XML-файлах, находящихся в поддиректории **lang** директории установки **Microolap EtherSensor**. Языковые файлы поименованы по принципу **<язык>-<культура>.xml,** например **en-us.xml**, **pt-br.xml** и т.п.

Внутри языковой XML-файл выглядит так:

Рис.60. Содержание языкового XML-файла GUI.

Значение атрибута **lang** тега **root** вместе с именем файла используются при отображении текущего языкового файла в элементе **Язык.**

Для того, чтобы начать локализацию GUI на новый язык, нужно сделать следующее:

1. Скопировать существующий языковой файл, например, **en-us.xml** в новый, например, **pt-br.xml**;

2. Открыть только что созданный файл **pt-br.xml** любым текстовым редактором и исправить **English** на, например, **Português brasileiro**.

3. Закрыть и заново запустить конфигуратор **ethersensor_console.exe**. В выпадушке **Язык** появится новый язык и новый файл.

Теперь можно начинать редактировать текстовые элементы GUI в файле **pt-br.xml**.

> **Совет:**
> Некоторые элементы GUI содержат HTML, поэтому редактировать языковые XML-файлы в текстовом редакторе следует только в том случае, если вы точно знаете, что делаете. Наиболее безопасным является редактирование текстовых элементов GUI в окне узла **Локализация**.

9.2. Редактирование элементов GUI

Для того, чтобы отредактировать текст элемента GUI, кликните по окошку **Значение**, измените текст, нажмите **Ctrl-S** - новое значение элемента сохранится в языковом файле, затем **Ctrl-R** - новое значение элемента прочитается из языкового файла и отобразится в соответствующем элементе. Эти же действия можно произвести кнопками на тулбаре слева от выпадушки **Язык**.

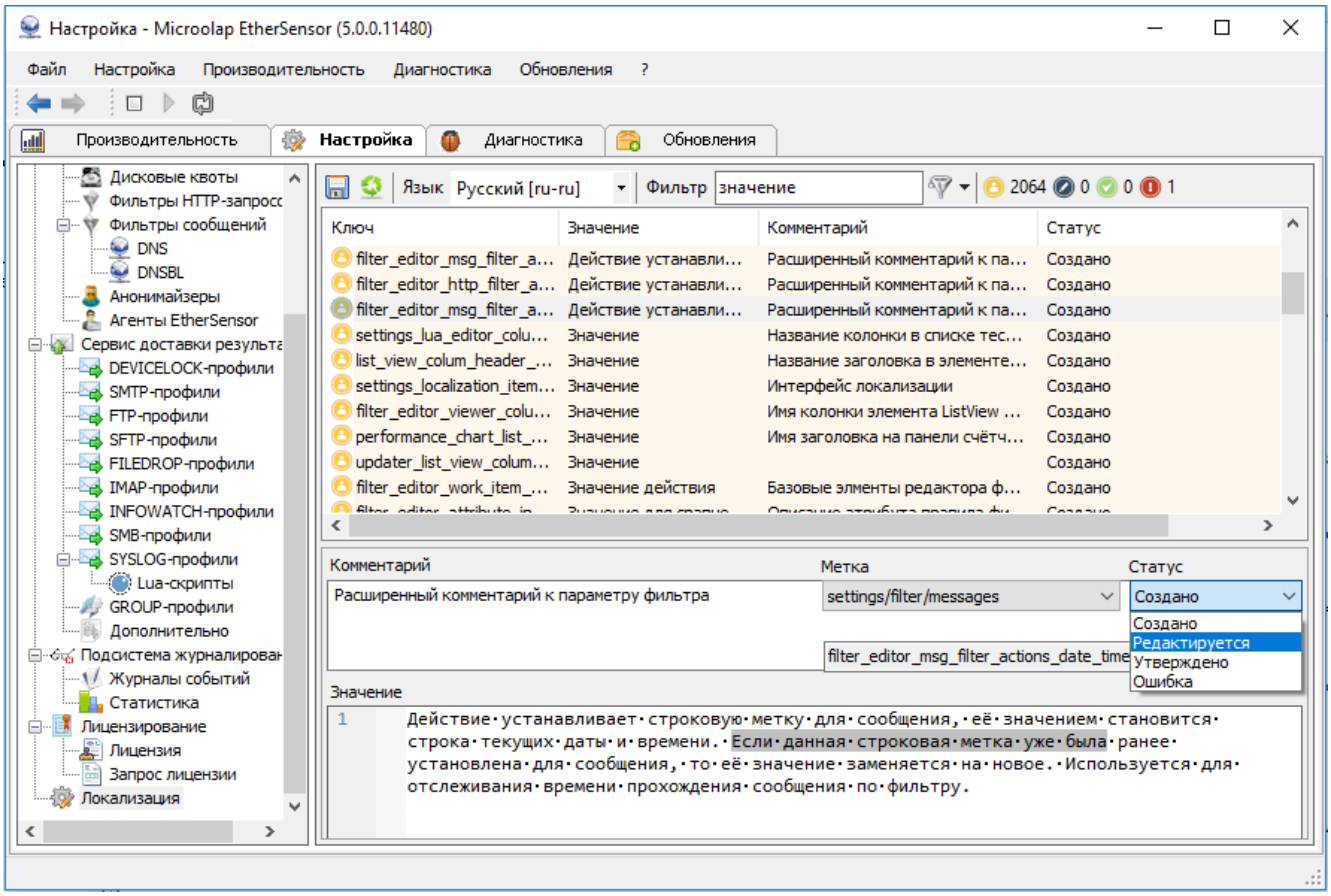

Рис.61. Редактирование текста элемента GUI.

Не забудьте сразу же поменять статус элемента, если это необходимо.

> **Совет:**
> Можно одновременно изменить или удалить комментарии в любом количестве элементов, а так же изменить им статусы. Для этого нужно выделить элементы клавишами **Shift-Down/Up**, и затем вписать нужное значение в поле **Комментарий** или установить нужный статус.

Редактирование больших элементов.

Некоторые элементы GUI представляют собой целые HTML-страницы, например, описание узла **Источники данных**:

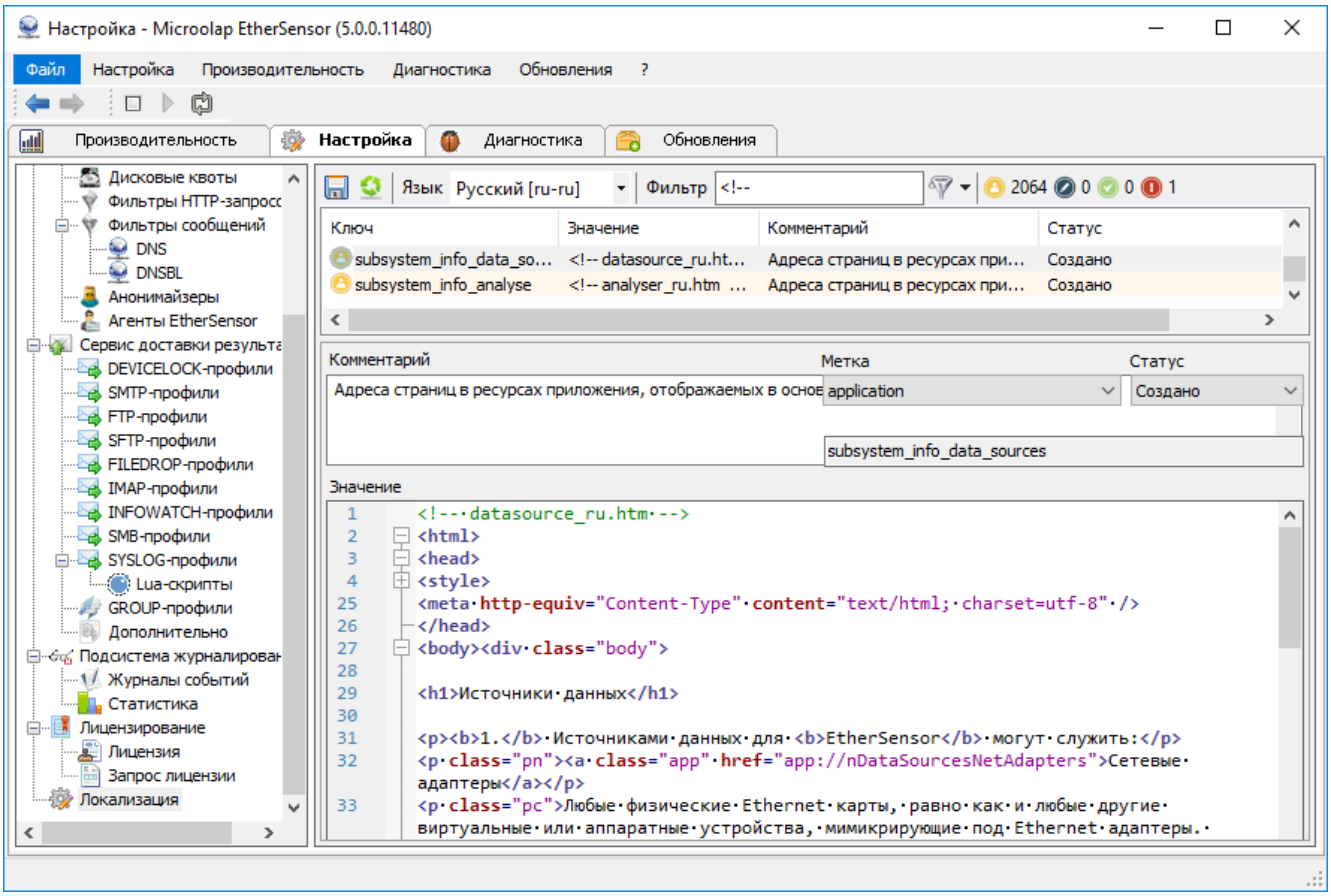

Рис.62. Пример элемента GUI, содержащего довольно много HTML.

Такой элемент можно отредактировать прямо в окошке **Значение**, но иногда бывает удобно скопировать весь текст такого элемента во внешний редактор, там отредактировать, а потом вернуть в окошко **Значение.**

> **Совет:**
> HTML-элементы GUI, подобные приведённому выше, могут содержать ссылки на окна приложения конфигуратора, разделы файла справки и т.п., будьте осторожны со ссылками.

Одновременная работа с двумя языками GUI.

Чтобы не переключаться постоянно между двумя языками языковой пары GUI, лучше иметь открытыми одновременно два окна конфигуратора. Для этого проделайте следующее:

1. Создайте папку для работы с первым языком, например, **en-us.xml**. Назовём её **C:\Ethersensor-en-us**;

2. Создайте папку для работы со вторым языком, например, **pt-br.xml**. Назовём её **C:\Ethersensor-pt-br**;

3. Скопируйте в эти папки файлы приложения конфигуратора, оставив в первой папке в поддиректории **lang** только файл **en-us.xml**, а во второй - только **pt-br.xml.**

Теперь можно открыть одновременно два окна приложения конфигуратора и редактировать файлы, избежав возможных ошибок и путаницы.

Использование регулярных выражений при поиске в полях элементов (Фильтр).

Если строку с искомым текстом в элементе **Фильтр** предварить комбинацией символов **re.** ("**r**", "**e**" и "**.**"), то она будет интерпретироваться как регулярное выражение.

Например:
re.[а-яА-Я] - найти все элементы, в которых есть хотя бы одна ***русская буква***;
re.[0-9]$ - найти все элементы, в которых значение оканчивается на ***цифру***;
re.: $ - найти все элементы, в которых значение оканчивается на ***двоеточие пробел***;
re.^.{4,6}$ - найти все элементы, состоящие из строк длиной от **4** до **6** символов.

10. История изменений Microolap EtherSensor

2018-09-08 Версия 5.1.0.13519

Среда выполнения
Windows Server 2008, Windows Server 2012, Windows Server 2016.
Источники данных и реконструкция объектов
Служба EtherSensor EtherCAP:
[+] Реализована поддержка протокола IPv6.
[+] Улучшена обработка TCP/UDP трафика с различной глубиной инкапсуляции, например:
eth -> vlan -> ip4 -> ip6 - > ip4 -> gre -> ppp -> ip4 -> tcp/udp -> application data.
[+] Метаданные обрабатываемых событий теперь содержат информацию о VLAN.
[+] Реализован перехват FTP over IPv6 (активный и пассивный режимы).
[+] Реализована работа IPC-каналов TCP-SESSIONS и UDP-SESSIONS для доставки результатов анализа по протоколу NETFLOW.
[+] Сокращено на 30% потребление ресурсов при перехвате трафика.
[-] Исправлена ошибка распаковки socks-тоннелей.
Анализ перехваченных объектов:
[+] Изменён внутренний формат представления обрабатываемых событий, на основе этого реализована строгая типизация результатов анализа.
Теперь все детектируемые события (сообщения) укладываются в следующую схему:

```
registration <- событие регистрации в системе
login        <- событие входа в систему
profile      <- событие изменения профиля в системе

send_msg     <- событие отправки сообщения
recv_msg     <- событие получения сообщения

send_file    <- событие отправки файла
recv_file    <- событие получения файла

conversation <- событие перехвата беседы
contacts     <- событие пересылки контактов
search_query <- событие поискового запроса
```

[+] Сокращено на 15% потребление ресурсов при детектировании сообщений.
Доставка результатов анализа системам-потребителям:

[+] Выполнена интеграция с DLP-решением FALCONGAZE Secure Tower.
[+] Реализована прямая доставка результатов анализа из IPC-канала по протоколу SYSLOG, в том числе и объектов, получаемых при RAW-фильтрации в службе анализа. Результаты анализа доставляются в формате CEF-HTTP или SQUID ACCESS LOG. Количество потребителей не ограничено. Также реализована возможность доставки результатов анализа с использованием TCP over SSL.
[+] Реализована прямая доставка результатов анализа из IPC-канала по протоколу NETFLOW версий 1, 5 и 9. Теперь информация о всех TCP/UDP сессиях, обработанных платформой EtherSensor может быть доставлена на NETFLOW-серверы. Количество потребителей не ограничено. Реализована возможность доставки результатов анализа с использованием TCP over SSL. Примеры потребителей: Splunk(NetFlow Analytics for Splunk), McAfee Security Information and Event Management (SIEM), IBM QRadar Security Intelligence Platform, HP ArcSight.
[+] Обновлён модуль LUA-интеграции для отправки по протоколу SYSLOG в формате CEF. Примеры потребителей: Splunk, HP ArcSight, IBM QRadar, LogRhythm, EMC-RSA NetWitness, McAfee Enterprise Security Manager/NitroView, Symantec Security Information Manager (SSIM).
[+] Обновлён модуль доставки результатов в формате JSON.
[+] Обновлён модуль доставки результатов в формате XML.
[+] Обновлён модуль доставки результатов в формате EML.
[+] Сокращено потребление ресурсов при доставке результатов анализа.

Журналирование:

[+] Добавлено отображение информации об обработанных соединениях с использованием IPv6.

Консоль управления:

[+] Добавлен интерфейс управления транспортными профилями FALCONGAZE.
[+] Добавлен интерфейс управления транспортными профилями SYSLOG при работе напрямую с IPC-каналом.
[+] Добавлен интерфейс управления транспортными профилями NETFLOW при работе напрямую с IPC-каналом.

2018-04-25 Версия 5.0.3.12929

Среда выполнения

Windows Server 2008, Windows Server 2012, Windows Server 2016.

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[+] Обновлен перехват FTP в случае, когда клиент и/или сервер находятся за NAT.
[+] Улучшена работа с фрагментированными IP пакетами.
[+] Интеграция с обновлённым IPC на уровне ядра операционной системы.

Анализ перехваченных объектов:

[+] Обновлены детекторы: odnoklassniki.ru, !generic.
[+] Добавлено поле <PRI> в CEF-лог для HTTP запросов.
[-] Исправлено формирование строки CEF|SquidAccess: возможен был вариант request=/https://r3-- (лишний "/" после "=").

Доставка результатов анализа системам-потребителям:

[+] Обновлены библиотеки iwthrift.dll, libcrypto-1_1-x64.dll, libcurl.dll, libssh2.dll, libssl-1_1-x64.dll, libxml2.dll, libxmlsec-openssl.dll, libxmlsec.dll, libxslt.dll, zlib1.dll.
[+] Добавлено направление скачивания/загрузки для событий SMB в InfoWatch Traffic Monitor.
[+] Добавлено направление скачивания/загрузки для событий FTP в InfoWatch Traffic Monitor.
[-] Исправлена редкая ошибка при конвертировании сообщений в EML: в некоторых случаях неправильно обрабатывались переносы строк в заголовках.
[-] Исправлена незначительная ошибка подсчёта объёма отправленных потребителю данных.
[+] Обновлён Lua-скрипт для SYSLOG-транспорта, входящий в поставку.

[-] Исправлена ошибка в Lua engine для SYSLOG-транспорта: некорректное получение контента тела сообщения в Lua-скрипте.

Журналирование:

[+] Уточнено вычисление и отображение счётчиков производительности.

Консоль управления:

[+] Добавлена возможность удалить квотируемые накопленные результаты.
[+] Добавлена возможность удалить накопленные журналы EtherSensor.
[+] В настройки служб добавлена кнопка "Применить". Действие кнопки - сохранить изменения и перезапустить службу(службы).
[+] Улучшена логика управления запуском и остановкой служб при обновлении EtherSensor.

Служба обновления

[+] Улучшена работа службы обновления через прокси сервер.
[-] Исправлена обработка русских символов в конфигурации службы обновления.

2018-03-20 Версия 5.0.2.12765

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[+] Обновлён движок перехвата трафика.
[+] Поддержка технологии RSS. Поддержка аппаратного ускорения обработки трафика на многоядерных системах с использованием серийного оборудования.
[+] Интеграция с обновлённым IPC на уровне ядра операционной системы.
[+] Обработка потоков трафика до 20 Gbit.
[+] Сокращение потребления ресурсов в 4 раза.
[+] Перехват и обработка протокола WebSocket.
[+] Перехват и обработка протокола SMB1 и SMB2.
[+] Обновление протокола ICQ и MRA.
[+] Декапсуляция WEB туннелей (метод CONNECT, WebSocket).
[+] Декапсуляция SOCKS туннелей, распознавание и обработка протоколов внутри SOCKS.
[-] Исправлены ошибки в обработке протокола IMAP4.

Анализ перехваченных объектов:

[+] Обновлён движок IPC (Inter Process Communications).
[+] Ускорение обработки данных в режиме реального времени.
[+] Сокращение потребления ресурсов в 2 раза.
[+] Расширение обработки видов запросов HTTP, добавлена поддержка методов ACL, AJAX, BAN, BASELINE-CONTROL, BCOPY, BDELETE, BIND, BITS_POST, BMOVE, BPROPFIND, BPROPPATCH, CCM_POST, CHECKIN, CHECKOUT, CONNECT, COPY, DELETE, GET, HEAD, HTML, INVOKE, JSON, LABEL, LINK, LOCK, LOG, MERGE, MKACTIVITY, MKCOL, MKREDIRECTREF, MKWORKSPACE, MOVE, M-SEARCH, NETHCMD, NOTIFY, OPTIONS, ORDERPATCH, PATCH, POLL, POST, PROPFIND, PROPPATCH, PURGE, PUT, REBIND, REPORT, REQMOD, RESPMOD, SEARCH, SCRIPT, SOURCE, SUBSCRIBE, TRACE, UNBIND, UNCHECKOUT, UNLINK, UNLOCK, UNSUBSCRIBE, UPDATE, UPDATEREDIRECTREF, VERSION-CONTROL, X-MS-ENUMATTS.
[+] В фильтр HTTP добавлена возможность генерации лога HTTP запросов в формате CEF для доставки в SIEM-системы.
[+] Детектирование чатов на базе WebSocket (Skype, Mobile Applications, Web Chats).
[+] Обработка событий Web WhatsUp (Списки контактов, Идентификация пользователей).
[+] Детектирование сообщений на базе Google Protobuf (Gmail).
[+] Детектирование сообщений Web Skype.
[+] Детектирование сообщений Web ICQ, MRA (Mail.ru Group).
[+] Детектирование передачи файлов по протоколам SMB1 и SMB2.
[+] Обновление Web детекторов: !generic,!fileupload, accounts, facebook.com, google.com, mail.ru, mamba.ru, odnoklassniki.ru, vkontakte.ru, yandex.ru.

Доставка результатов анализа системам-потребителям:

[+] Интеграция с IPC.
[+] Сокращение потребления ресурсов в 2 раза.
[+] Доставка сообщений по протоколу SYSLOG. Кастомизировано создание сообщений для протокола SYSLOG за счёт интеграции со скриптовым языком Lua. Добавлена возможность формирования сообщений в собственных форматах.
[+] Доставка сообщений по протоколу SYSLOG с использованием TCP, реализована поддержка SSL.
[+] Добавлен модуль LUA-интеграции для отправки по протоколу SYSLOG в формате CEF. Примеры потребителей: Splunk, HP ArcSight, IBM QRadar, LogRhythm, EMC-RSA NetWitness, McAfee Enterprise Security Manager/NitroView, Symantec Security Information Manager (SSIM).

Журналирование:

[+] Записи журналов EtherSensor переведены и ведутся на английском языке.
[+] Добавлен журнал HTTP запросов в формате CEF.

Консоль управления:

[+] Служба обновления интегрирована в инсталляционный пакет Ethersensor.

2016-09-16 Версия 4.5.6.10479

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[+]Добавлен парсер протокола **httpv2**;
[+]Добавлен парсер протокола **skype**: перехват, передача файлов, текстовых сообщений, контакт-листов;
[-]Исправлена ошибка в обработке протоколов http, ftp, pop3;
[-]Исправлена ошибка при обработке конфигурации старой версии;

Служба EtherSensor ICAP:

[+]Значение заголовка X-Sensor-Net-Interface-Id теперь формируется с использованием значения прослушиваемого порта, например: **icap-000-1344.**
[-]Исправлена ошибка в обработке заголовков протокола ICAP, приводившая к некорректному формированию сообщения.

Анализ перехваченных объектов:

[+]Чтобы при обработке сообщений, передаваемых по протоколу httpv2, различать результаты в обработке фильтра HTTP запросов, добавлен заголовок **X-Sensor-Httpv2: Microolap EtherSensor.**
[+]Обработка сообщений, передаваемых по протоколу **skype.**
[+]В HTTP фильтр добавлено условие "Проверить идентификатор сетевого интерфейса (X-Sensor-Net-Interface-Id)".
[+]В фильтр сообщений добавлено действие "Удалить вложение сообщения по имени".
[+]Обновлены детекторы: !generic,!fileupload,cv (careerist.ru, hh.ru, job.ru, job50.ru, job-mo.ru, jobsmarket.ru, rabotavia.ru, rabota.by, rabota.ru, rosrabota.ru, superjob.ru, zarplata.ru), facebook.com, google.com, gorod55, ipboard, linkedin.com, livejournal.com, loveplanet.ru, mail.ru, mamba.ru, mfd.ru, my.mail.ru, mybb, odnoklassniki.ru, phpBB, pochta.ru (qip.ru), rambler.ru, smsmms (skylink.ru, megafon.ru, mts.ru, tele2.ru), twitter.com, vbulletinboard, vkontakte.ru, wordpress.com, yandex.ru, xmpp
[-]Исправлена ошибка в обработке поисковых запросов.
[-]Исправлена ошибка в обработке MIME частей.

Доставка результатов анализа системам-потребителям:

[+]Добавлен DeviceLock Enterprise Server (DLES) транспорт. Позволяет нативным образом доставлять сообщения в DeviceLock Enterprise Server.
[-]Исправлена ошибка в форматировании сообщения в формат EML.
[-]Исправлена ошибка в кодировании аттачмента сообщения в base64.
[-]Исправлена ошибка отправки чатов в INFOWATCH Traffic Monitor.

Журналирование:

[+]Добавлено журналирование счётчиков отладки.

Консоль управления:

[+] В HTTP-фильтр добавлено условие "Проверить идентификатор сетевого интерфейса (X-Sensor-Net-Interface-Id)".
[+] В фильтр сообщений добавлено действие "Удалить вложение сообщения по имени".
[+] Добавлен профиль транспортировки сообщений в DeviceLock Enterprise Server.

2016-05-11 Версия 4.5.5.10199

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*] Профилирование кода, повышение производительности службы EtherSensor EtherCAP на 20%.
[-] Отказ от плагинной системы для парсеров протоколов.

Анализ перехваченных объектов:

[*] Профилирование кода, повышение производительности службы EtherSensor Analyser на 50%.
[+] Добавлена возможность сохранения перехваченных сообщений в формате JSON.
[+] Повышена достоверность детектирования кодировки сообщений.
[+] Повышена достоверность детектирования сообщений.
[+] Обновлены детекторы: !generic, accounts, chanboard, cv (careerist.ru, hh.ru, hotjob.ru, jobsmarket.ru, job.ru, rabotamedikam.ru, rabotavgorode.ru, rabota.mail.ru, rabota.ru, rosrabota.ru, superjob.ru, zarplata.ru), hotmail.com, facebook.com, google.com, gorod55, icq, ipboard, linkedin.com, livejournal.com, loveplanet.ru, lync, mail.ru, mamba.ru, my.mail.ru, mybb, myspace.com, newmail.ru, nextmail.ru, odnoklassniki.ru, phpBB, pochta.ru (qip.ru), rambler.ru, smsmms (beeline.ru, megafone.ru, mts.ru, tele2.ru), twitter.com, vbulletinboard, vkontakte.ru, ukr.net, wordpress.com, yandex.ru, yahoo.com.
[-] Отказ от плагинной системы детекторов сообщений.
[-] Исправлена редко воспроизводимая ошибка, приводящая к утечке памяти.
[-] Исправлена ошибка обработки временных файлов, приводившая к утечке дискового пространства.
[-] Исправлена ошибка обработки сообщений Microsoft Skype For Buisness.

Доставка результатов анализа системам-потребителям:

[+] Добавлен транспортный профиль **INFOWATCH Traffic Monitor**.
[-] Исправлена ошибка форматирования сообщения в формат EML.
[-] Исправлена редко воспроизводимая ошибка, приводящая к утечке памяти при формировании EML-конверта.
[-] Исправлена редко воспроизводимая ошибка: в некоторых случаях при чтении конфигурации было падение службы транспорта.

Консоль управления:

[+] Добавлен профиль транспортировки сообщений INFOWATCH Traffic Monitor транспорт.
[+] В диагностический отчёт **Microolap EtherSensor** добавлено время последнего изменения конфигурационного файла.
[-] Исправлена ошибка обработки атрибутов правил в фильтрах сообщений.

2016-02-09 Версия 4.5.4.9893

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*] Обновлён парсер протокола ICQ.
[*] Обновлён парсер протокола ICAP для интеграции с ICAP-клиентами методом пассивного прослушивания трафика.

Служба EtherSensor ICAP:

[-] Исправлена ошибка записи в лог.

Анализ перехваченных объектов:

[+] Ускорено конвертирование вложений в EML формат.
[+] Добавлен механизм передачи сообщений в транспортную службу в обход дисковой подсистемы.

[+] Повышена достоверность детектирования сообщений.
[+] Обновлены детекторы: !generic, accounts, chanboard, cv (careerist.ru, hh.ru, hotjob.ru, jobsmarket.ru, job.ru, rabotamedikam.ru, rabotavgorode.ru, rabota.mail.ru, rabota.ru, rosrabota.ru, superjob.ru, zarplata.ru), hotmail.com, facebook.com, google.com, gorod55, icq, ipboard, linkedin.com, livejournal.com, loveplanet.ru, mail.ru, mamba.ru, my.mail.ru, mybb, myspace.com, newmail.ru, nextmail.ru, odnoklassniki.ru, phpBB, pochta.ru (qip.ru, borda.ru, pochta.com), plaxo.com, rambler.ru, search-query, smsmms (beeline.ru, megafone.ru, mts.ru, mysmsbox.ru, tele2.ru), twitter.com, vbulletinboard, vkontakte.ru, wordpress.com, yandex.ru, yahoo.com.
[-] Исправлена редко воспроизводимая ошибка, приводившая к утечке памяти.
[-] Исправлена редко воспроизводимая ошибка фильтрации сообщений.

Доставка результатов анализа системам-потребителям:

[*] Распределение нагрузки на системы-потребители результатов анализа реконструированных объектов с использованием DNS Round Robin.
[+] Добавлены счётчики ошибок работы кэша транспортной службы.
[-] Исправлена ошибка в формировании EML-конверта.

Журналирование:

[+] Добавлена запись счётчиков кэша службы Доставки результатов в файл counters.log.

Консоль управления:

[*] Запуск, остановка, пауза и перезапуск выполняются теперь в отдельных потоках.
[*] Изменён пользовательский интерфейс редактирования фильтра сообщений.
[+] Уточнены описания счётчиков.

2015-12-16 Версия 4.5.3.9707

Консоль управления:

[+] Актуализированы названия модулей в системе лицензирования.

2015-12-15 Версия 4.5.2.9700

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*] Улучшена обработка GRE протокола.
[*] Улучшена обработка PCAP-файлов.
[+] Добавлена поддержка Windows 10 (Windows Server 2016 Preview).
[+] При остановке службы добавлено принудительное закрытие потоков после 10 секундного таймаута для отзывчивости при перезагрузке службы.

Служба EtherSensor ICAP:

[+] Подключена возможность создавать отчёты при падениях службы.
[+] При остановке службы добавлено принудительное закрытие потоков после 10 секундного таймаута, для отзывчивости при перезагрузке службы.
[-] Исправлена ошибка работы в среде Windows Server 2003.
[-] Исправлена ошибка работы с Allow 204.
[-] Исправлена ошибка с неправильным месяцем в именах файлов и папок для Raw дампа ICAP.

Анализ перехваченных объектов:

[+] При остановке службы добавлено принудительное закрытие потоков после 10 секундного таймаута, для отзывчивости при перезагрузке службы.
[+] Добавлен принудительный перенос тела - "This is a multipart message in MIME format." в конец списка тел сообщений.
[+] Подключена возможность создавать отчёты при падениях службы.
[+] Расширен лог об ошибках при инициализации контекстов детектирования сообщений.
[-] Исправлена ошибка действия фильтра сообщений ("Выполнить запись в лог").
[-] Исправлена ошибка в обработке данных из директории data\replay.
[-] Исправлена ошибка в обработке данных, поставляемых Агентами EtherSensor.
[-] Исправлена ошибка обработки XML файлов.

[-]Исправлена ошибка в разборе RFC822 EML адресов.

Доставка результатов анализа системам-потребителям:

[+]При остановке службы добавлено принудительное закрытие потоков после 10 секундного таймаута, для отзывчивости при перезагрузке службы.

[-]Исправлена ошибка отправки результата групповым профилем - поток, использующий групповой профиль мог уходить в бесконечный цикл.

[-]Исправлена ошибка формирования EML-конверта.

Журналирование:

[+]При остановке службы добавлено принудительное закрытие потоков после 10 секундного таймаута, для отзывчивости при перезагрузке службы.

Консоль управления:

[+]Уточнено отображение счётчиков.

[-]Исправлена ошибка потери фокуса при переключении между узлами дерева на вкладке "Производительность".

2015-11-11 Версия 4.5.1.9623

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*]Значительно уменьшен расход памяти при захвате трафика.

[*]В библиотеке захвата трафика Packet Sniffer SDK повышена производительность реконструкции TCP соединений.

[+]В библиотеке захвата трафика Packet Sniffer SDK добавлена обработка пакетов VLAN 802.1Q.

[+]В библиотеке захвата трафика Packet Sniffer SDK добавлена установка максимального значения удерживаемых пакетов на один TCP поток.

[+]Добавлен парсер протокола SOCKS4 и SOCKS5. Позволяет отслеживать и перехватывать туннелируемые через протокол SOCKS.

[+]Добавлен парсер ICAP. Позволяет пассивно отслеживать ICAP соединения, не меняя существующей архитектуры.

Служба EtherSensor ICAP:

[+]Добавлен режим работы SECURE ICAP. Теперь ICAP сервер может использовать SSL для создания защищённых соединений с ICAP клиентами.

[+]Добавлен перехват LYNC сообщений на серверах Microsoft Lync (Microsoft Skype for Business). Работает в связке с Microolap LYNC агентом, который работает через ICAP протокол.

Анализ перехваченных объектов:

[*]Значительно уменьшен расход памяти при детектировании и анализе сообщений.

[+]В фильтр сообщений добавлена возможность отправки произвольного (составного) сообщения на SYSLOG-сервер для интеграции с SIEM системами.

[+]Добавлена отправка детектируемых поисковых запросов по протоколу SYSLOG для поисковых систем (google.com, rambler.ru, yandex.ru, mail.ru, aport.ru, bing.com, yahoo.com, wikipedia.org).

[+]Обновлены детекторы сообщений: blogger.com, cv (careerist.ru, hh.ru, job50.ru, job.ru, rabota.ru, superjob.ru, zarpalata.ru), facebook.com, hotmail.com, linkedin.com, livejournal.com, loveplanet.ru, mamba.ru, mail.ru, my.mail.ru, moikrug.ru, odnoklassniki.ru, pochta.ru, rambler.ru, smsmms (beeline.ru, megafon.ru, mts.ru, skylink.ru, tele2.ru, wsms.ru), ukr.net, vkontakte.ru (добавлено чтение входящих сообщений), wordpress.com.

Доставка результатов анализа системам-потребителям:

[*]Значительно уменьшен расход памяти при отправке сообщений.

[+]Добавлен новый транспортный протокол SFTP для отправки сообщений по протоколу SSH.

Консоль управления:

[+]Добавлен транспортный профиль (SFTP).

2015-10-01 Версия 4.5.0.9505

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[+]Добавлены парсеры протоколов ICAP и SOCKS;

Служба EtherSensor ICAP:

[+]ICAP сервер теперь поддерживает защищённые соединения Secure ICAP (SSL);

[+]Добавлен перехват LYNC сообщений на серверах Microsoft Lync. Работает в связке с Microolap LYNC агентом;

[+]Добавлена отправка детектируемых поисковых запросов по протоколу SYSLOG.

Анализ перехваченных объектов:

[*]Значительно уменьшен расход памяти;

[+]Обновлены детекторы протоколов;

[+]Добавлен перехват входящих сообщений vkontakte.ru.

Доставка результатов анализа системам-потребителям:

[+]Добавлен новый транспортный протокол SFTP.

Журналирование:

[+]Для сообщений отправляемых по протоколу SYSLOG, теперь можно назначать имя канала.

Консоль управления:

[+]Добавлена отправка статистки по протоколу SYSLOG.

2014-07-08 Версия 4.4.1.8036

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*]Обновлена библиотека перехвата трафика Packet Sniffer SDK: повышена производительность реконструкции TCP соединений.

[*]Доработан парсер POP3:
добавлена поддержка расширения AUTH с многострочным ответом;
корректно обрабатывается ситуация, когда Login и Password не указаны.**[+]** Добавлен парсер протокола IMAP4.

[+]Добавлен парсер протоколов NMDC и ADC (DC++).

[+]Добавлен детектор протокола TORRENT для TCP соединений.

[+]Доработан детектор протокола SSL (добавлена поддержка TLS 1.1 и TLS 1.2).

[-]Исправлена ошибка в детекторе протокола SSL, в некоторых случаях приводившая к незначительной утечке памяти.

[-]Исправлена ошибка в подсчёте сессий, закрываемых по тайм-ауту.

[-]Исправлена ошибка обработки PCAP-файлов: убран "жесткий" сброс сессий для PCAP-файла при завершении его обработки, теперь соединения закрываются по тайм-ауту.

Служба EtherSensor ICAP:

[-]Исправлена ошибка перекодирования заголовков X-Sensor-Icap-Authenticated-User, X-Sensor-Icap-Authenticated-Group.

[-]Исправлена ошибка передачи запросов в службу анализа: в редких случаях запросы не передавались для дальнейшей обработки.

Анализ перехваченных объектов:

[*]Повышены достоверность распознавания и производительность обработки сообщений в детекторе !generic.

[*]Повышена достоверность распознавания выгрузки (загрузки) файлов в детекторе !file-upload. Сделано более логичным формирование имени файла из URL для случаев, когда в HTTP-запросе его имя явно не указано.

[+]Обновлены детекторы: blogger.com, cv (careerist.ru, hh.ru, job50.ru, job.ru, job-mo.ru, job.ws, jobsmarket.ru, rabotamedikam.ru, rabotavgorode.ru, rabota.mail.ru, rabota.ru, superjob.ru, zarpalata.ru), diary.ru, google.com, gorod55, facebook.com, hotmail.com, linkedin.com, livejournal.com, loveplanet.ru, mamba.ru, mail.ru, my.mail.ru, mfd.ru, moikrug.ru, odnoklassniki.ru, pochta.ru, rambler.ru, smsmms (beeline.ru, megafon.ru, mts.ru, skylink.ru, tele2.ru, wsms.ru), twitter.com, yandex.ru, yahoo.com, ukr.net, vkontakte.ru, wordpress.com.

[+] Добавлен детектор OWA (Outlook Web Access). Детектирует отправляемые, редактируемые и просматриваемые сообщения в системе Outlook Web Access.

[-] В фильтре сообщений исправлена ошибка обработки условий (CHECK-MESSAGE-ID, CHECK-MD5) для фильтрации дубликатов сообщений по полю Message-ID или по хешу MD5 сообщения. В некоторых случаях выполнение данных действий завершалась с ошибкой.

[-] Исправлена ошибка обработки email-сообщений с пустым полем TO. В некоторых случаях обработка таких сообщений завершалась с ошибкой.

[-] Исправлена ошибка обработки имени файла в детекторе FTP. В некоторых случаях обработка таких сообщений завершалась с ошибкой.

[-] Исправлена ошибка декодирования HTTP-запросов, в некоторых случаях параметры HTTP оставались не декодированными.

[-] Исправлена ошибка в детекторах IM, в некоторых случаях декодирование данных в формате BASE64 завершалось с ошибкой.

Доставка результатов анализа системам-потребителям:

[*] Повышена производительность SMTP транспорта.

Журналирование:

[*] Уменьшен размер потребляемых ресурсов процессом сбора и сохранения значений счётчиков Microolap EtherSensor.

[+] Расширен формат записи журнала транспортной службы, в журналируемые сообщения добавлены числовые идентификаторы отправляющих потоков для отслеживания последовательности событий конкретного отправляющего потока.

Консоль управления:

[+] Добавлена проверка работоспособности транспортных профилей (SMTP, FTP, FILEDROP, SMB). Теперь при изменении параметров транспортного профиля можно проверить его работоспособность минуя процесс перехвата и обработки сообщения.

[+] Добавлен вывод ipconfig /all в отчёт о работе Microolap EtherSensor.

[+] Добавлены редактор фильтров HTTP-запросов и редактор фильтра сообщений. Теперь для управления фильтрами используется графическая оболочка.

[+] Редактирование квот обрабатываемых результатов вынесено в файл quotas.xml.

2013-11-12 Версия 4.4.0.7340

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*] Изменен драйвер перехвата трафика pssdk6.sys. В некоторых ситуациях старая версия приводила к BSOD;

[*] Изменен алгоритм разбора URI в парсере протокола HTTP;

[*] Изменен парсер протокола FTP: в некоторых случаях приводило к падению службы ethcapsvc.exe;

[*] Изменен парсер протокола SMTP: некорректно обрабатывались многострочные ответы сервера для ПРИВЕТСТВИЯ и пр. команд.

[*] Теперь TCP соединения, которые не имеют нормального завершения согласно RFC, журналируются со статусом warning.

Анализ перехваченных объектов:

[*] Повышена достоверность распознавания и производительность обработки сообщений Lotus Notes;

[*] В фильтре сообщений обновлено условие (CHECK-MESSAGE-ID) для фильтрации дубликатов сообщений по полю Message-ID;

[+] Теперь для протокола LOTUS проверяется заголовок X-Sensor-Lotus-MessageId;

[*] В фильтре сообщений обновлено условие для фильтрации сообщений по IP-адресу. Добавлен тип проверки адреса any.

```
<rule enabled="true">
  <match>
    <c name="ip"
       address="any"
       value="10.64.40.24" />
    </match>
    <action name="drop" />
</rule>
```

[+] В фильтре сообщений добавлено действие SAVE RAW DATA. Действие позволяет для сообщения сохранять исходные данные, из которых оно было получено;

[+] Добавлена возможность исходные данные прикреплять к сообщению в виде аттачмента:

```
<rule enabled="1">
  <comment>For all HTTP objects save original data.</comment>
  <match>
    <c name="protocol" value="http" />
  </match>
  <action name="save-raw-data" value="true" />
</rule>
```

[+] Обновлены детекторы: CV (hh.ru, job50.ru, job.ru, job.ws, jobsmarket.ru, rabotamedikam.ru, rabotavgorode.ru, rabota.mail.ru, rabota.ru, rabota.by, superjob.ru), diary.ru, google.com (добавлен перехват WEB сообщений Google Hangouts), gorod55, facebook.com, linkedin.com, livejournal.com, loveplanet.ru, mamba.ru, mail.ru, my.mail.ru, mfd.ru, moikrug.ru, pochta.ru, smsmms (mysmsbox.ru, megafon.ru, mts.ru, skylink.ru, tele2.ru, wsms.ru), yandex.ru, yahoo.com, ukr.net, vkontakte.ru, wordpress.com.

[+] Добавлена реконструкция файлов, загружаемых отдельными частями по протоколу HTTP;

[+] Исправлена ошибка перехода в демонстрационный режим с действующей лицензией: некорректно проверялись даты окончания действия лицензии модуля.

Доставка результатов анализа системам-потребителям:

[+] В заголовки сообщений добавлен текущий UHID Microolap EtherSensor: заголовок X-Sensor-UHID;

[-] Исправлена ошибка в транспорте SMTP. Иногда для отправки сообщений в архив использовались уже закрытые соединения.

Журналирование:

[*] Теперь некорректно завершенные TCP соединения журналируются со статусом warning. В конфигурации по умолчанию для службы watcher создаётся правило, которое журналирует такие сообщения в отдельный файл.

```
<LogRule output="file://capstrange.log"
         maxsize="10Mb"
         encoding="utf-8"
         endline="CR,LF">
  <Channel name="CAPMAIN" loglevels="error, warning, criterr" />
</LogRule>
```

[-] В сообщениях системы журналирования исправлена ошибка подсчета оставшегося времени действия модуля;

[-] Исправлена ошибка получения полного пути к файлу журналирования сообщений;

[-] Исправлена ошибка сохранения статистики, в некоторых случаях приводившая к утечке памяти.

Консоль управления:

[*] Утилиты mconsole.exe, kppsreport.exe, perfmonitor.exe объединены в одно приложение для управления Microolap EtherSensor - mconsole.exe;

[+] Для сохранения изменённой конфигурации добавлена горячая клавиша Ctrl+S;

[+] Добавлена возможность остановки, запуска и перезапуска всех служб Microolap EtherSensor разом;
[+] Добавлена возможность распаковки Диагностического отчёта Microolap EtherSensor в отдельную директорию.
[+] Для повышения читаемости фильтров добавлена возможность переформатирования фильтров сообщений и фильтров HTTP-запросов.
[-] Исправлена ошибка отображения фильтров (некорректная кодировка фильтра);
[-] Исправлена ошибка получения полного пути к файлу журналирования сообщений;
[-] Исправлена ошибка обновления счётчиков производительности;
[-] Исправлена ошибка загрузки и отображения лицензии. В некоторых случаях происходил сбой работы приложения;
[-] Исправлена ошибка сохранения настроек профиля filedrop;

2013-07-10 Версия 4.3.9.7149

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[-] Исправлена ошибка в парсере протокола SSL. В некоторых случаях некорректная работа парсера приводила к падению службы ethcapsvc.exe.
[-] Исправлена ошибка подсчёта распознаваемых соединений парсерами протоколов.

Анализ перехваченных объектов:

[*] Обновлён алгоритм восстановления индекса спула директорий. Обновлена библиотека System.Data.SQLite.dll (версия 1.0.86.0).
[+] Добавлена работа с анонимайзерами: если список анонимайзеров не пуст, то детекторы сервисов обрабатывают также и трафик по доменам из списка. Обновлена конфигурация службы EtherSensor Analyser.
[+] Добавлен детектор сервиса gorod55.ru.

Доставка результатов анализа системам-потребителям:

[+] Добавлен транспортный профиль SMB. Данный профиль позволяет писать сообщения на сетевые папки.
[+] Добавлен транспортный профиль GROUP. Данный профиль предназначен для резервирования транспортных профилей и балансировки нагрузки на потребителей сообщений.
[+] В алгоритм работы транспортного профиля SMTP добавлен флаг keep-connection, который позволяет включать/отключать удержание соединения с SMTP-сервером.
[+] Во все транспортные профили добавлена опция profile-fail-timeout, которая позволяет выставлять в секундах время блокировки профиля в случае невозможности отправить сообщение на указанный приёмник.
[+] Во все транспортные профили добавлена опция pgo-profile-reserve, которая позволяет выставлять флаг резервирования профиля. Данная настройка действительна только в составе группового профиля.
[+] Во все транспортные профили добавлена опция profile-fail-timeout, которая позволяет выставлять вес профилю. Данная настройка действительна только в составе группового профиля.

Журналирование:

[-] Исправлена ошибка архивирования статистики работы **Microolap EtherSensor**.

Консоль управления:

[+] Добавлено управление списком доменов анонимайзеров.
[+] Во все типы транспортных профилей добавлены опции profile-fail-timeout, pgo-profile-reserve, profile-fail-timeout;
[+] Добавлено управление транспортными профилями SMB и GROUP.

2013-05-30 Версия 4.3.8.6986

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*] Обновлена библиотека Packet Sniffer SDK (pssdk.dll). В некоторый случаях при обработке перехваченного трафика предыдущая версия библиотеки приводила к падению службы EtherSensor EtherCAP.

Служба EtherSensor ICAP:

[+] Добавлена поддержка новой опции лицензии "ICAP интеграция".

Анализ перехваченных объектов:

[*] Обновлены детекторы: CV (hh.ru, jobsmarket.ru, job.ru, rabota.ru, superjob.ru, zarpalata.ru), blogger.com, chanboard, facebook.com, linkedin.com, livejournal.com, loveplanet.ru, mail.ru, mamba.ru, my.mail.ru, pochta.ru, rambler.ru, twitter.com, vkontakte.ru, yahoo.com, yandex.ru, ukr.net, wordpress.com.

[+] В фильтр сообщений добавлено новое условие проверки для заголовка Message-ID;

[+] В фильтр сообщений добавлено новое действие для добавления/изменения в сообщении произвольного заголовка (за исключением заголовков From, To, Cc, Bcc, Subject, Date).

Доставка результатов анализа системам-потребителям:

[*] Обновлена конфигурация службы: во всех типах транспортных профилей заменена опция save-xheaders на опцию save-headers для сохранения заголовков сообщения в отдельное вложение с именем microolap_msis_headers.txt;

[*] Повышена производительность SMTP транспорта: теперь в текущем соединении выполняется отправка сразу нескольких сообщений.

Журналирование:

[*] Обновлена конфигурация службы EtherSensor Watcher: добавлена возможность управления накоплением статистики работы Microolap EtherSensor;

[*] Повышена производительность архивирования журналов и статистики Microolap EtherSensor, сокращен размер требуемого дискового пространства.

Консоль управления:

[*] Изменён внешний вид отображения счётчиков.

[+] Во все типы транспортных профилей добавлена опция сохранения заголовков в отдельное вложение сообщения save-headers;

[+] Добавлено управление накоплением статистики работы Microolap EtherSensor.

2013-04-08 Версия 4.3.7.6840

Анализ перехваченных объектов:

[*] Обновлён алгоритм детектирования почтовых адресов (From, To, Cc, Bcc);

[*] Профилирование кода с целью уменьшения потребления памяти;

[+] Обновлены детекторы: CV (careerist.ru, hh.ru, job-mo.ru, job50.ru, jobsmarket.ru, job.ru, rabotavgorode.ru, rabota.mail.ru, rabota.ru, superjob.ru, zarpalata.ru), blogger.com, facebook.com, linkedin.com, livejournal.com, loveplanet.ru, mail.ru, mamba.ru, my.mail.ru, odnoklassniki.ru, pochta.ru, rambler.ru, smsmms (beeline.ru, megafon.ru, mts.ru, smste.ru, tele2.ru), twitter.com, vkontakte.ru, yahoo.com, yandex.ru, wordpress.com.

Доставка результатов анализа системам-потребителям:

[+] В службе EtherSensor Transfer добавлена возможность управления количеством отправляющих потоков;

[+] В службе EtherSensor Transfer во все типы транспортных профилей добавлена опция save-xheaders - сохранения заголовков X-Sensor, X-Sensor в отдельное тело сообщения.

Консоль управления:

[*] Изменён внешний вид отображения счётчиков в узлах "Быстродействие", "Сетевые адаптеры", "Кэш перехватываемых объектов", "Дисковые квоты".

[+] Добавлено редактирование Sensor ID при конфигурировании службы EtherSensor Transfer;

[+] Добавлено управление количеством отправляющих потоков службы EtherSensor Transfer, которое зависит от аппаратных ресурсов сенсора и может находится в диапазоне от 1 до CPU * 2.

[+] Во все типы транспортных профилей добавлена опция save-xheaders сохранения заголовков X-Sensor в отдельное тело сообщения.

2013-03-11 Версия 4.3.6.6714

Источники данных и реконструкция объектов

[-]Исправлена ошибка в модуле обработки исключительных ситуаций crashreport.dll.

Анализ перехваченных объектов:

[*]Повышена достоверность детектирования почтовых адресов (From, To, Cc, Bcc);

[*]Профилирование кода с целью уменьшения потребления памяти.

Консоль управления:

[*]Ограничен сбор информации о PCAP файлах и минидампах: не более 50 в списке.

2013-02-21 Версия 4.3.5.6608

Анализ перехваченных объектов:

[+]Обновлены детекторы: blogger.com, hotmail.com, myspace.com, moikrug.ru, rambler.com, twitter.com, ukr.net, yahoo.com.

[-]Исправлена ошибка анализа HTTP-запросов от ICAP-сервера Microolap EtherSensor.

2013-02-14 Версия 4.3.4.6584

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[+]Теперь при обработке исключительных ситуаций служба принудительно перезагружается. Ранее служба пыталась продолжать работать, что приводило к неконтролируемому расходу памяти и другим сбоям (например, большому количеству дампов процесса службы).

[-]Исправлена ошибка в драйвере перехвата трафика, в некоторых случаях приводившая к перезагрузке ОС (Win2008/Win7/Win2012/Win8) при деинсталляции;

Анализ перехваченных объектов:

[*]Уменьшено использование памяти и ресурсов CPU при обработке реконструированных объектов;

[+]Обновлены детекторы: yahoo.com, yandex.com.

[+]Теперь для работы с агентами Microolap EtherSensor лицензия Microolap EtherSensor должна содержать опцию для работы с агентами Microolap EtherSensor;

[-]Исправлена ошибка анализа параметров форм HTTP-запросов;

Консоль управления:

[-]Исправлена ошибка построения диагностического отчёта: в некоторых случаях консоль управления могла расходовать большое количество памяти при построении отчёта о работе Microolap EtherSensor;

[-]Исправлена ошибка проверки файла version.xml системы обновления Microolap EtherSensor.

2013-02-01 Версия 4.3.3.6536

Анализ перехваченных объектов:

[+]Добавлена поддержка нового сообщения от агента Microolap EtherSensor, позволяющая в результат перехвата добавлять заголовки X-Sensor-UID-AdapterType, X-Sensor-UID-MacAddress;

[+]Обновлены детекторы: !generic.

Консоль управления:

[*]Ускорена загрузка приложения;

[*]Скорректировано редактирование пакетных фильтров.

2012-12-26 Версия 4.3.2.6488

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[+]Добавлена поддержка работы с новым драйвером для перехвата трафика. Теперь новый драйвер используется при инсталляции на ОС Windows Vista и старше (до Windows 8/Windows 2012 включительно);

[-] Исправлена ошибка реконструкции TCP соединений. Теперь учитываются флаги ECE и CWR (RFC 3168).

2012-12-07 Версия 4.3.1.6448

Источники данных и реконструкция объектов

Служба EtherSensor LotusTXN

[+] Реализовано получение времени отправки сообщения;

[-] Исправлена ошибка, происходившая при закрытии сетевого ресурса с файлами Lotus Notes Transaction Log.

Анализ перехваченных объектов:

[+] Обновлены детекторы: blogger.com, CV (hh.ru, job-mo.ru, job.ru, rabota.ru, rabota.mail.ru, superjob.ru), facebook.com, livejournal.com, linkedin.com, mail.ru, mamba.ru, my.mail.ru, myspace.com, odnoklassniki.ru, pochta.ru, rambler.ru, smsmms (megafon, mts), twitter.com, vkontakte.ru, yahoo.com, yandex.ru.

[-] Исправлена ошибка распознавания email-адресов;

Консоль управления:

[+] Добавлена настройка SMTP порта в профиле SMTP;

[-] Исправлены ошибки добавления правила журналирования.

2012-11-21 Версия 4.3.0.6413

Источники данных и реконструкция объектов

[+] Релиз службы **EtherSensor LotusTXN**, извлекающей сообщения из **Lotus Notes Transaction Log**.

Анализ перехваченных объектов:

[+] Анализ объектов, поставляемых службой **EtherSensor LotusTXN**.

2012-11-15 Версия 4.2.3.6399

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*] Обновлена библиотека перехвата трафика Packet Sniffer SDK. Повышена производительность реконструкции TCP соединений, уменьшен объём потребления памяти;

[*] Изменено отображение счётчиков производительности захвата трафика.

Служба EtherSensor LotusTXN

[*] Предрелиз службы **EtherSensor LotusTXN**.

Анализ перехваченных объектов:

[*] Выполнена отдельная очередь для анализа больших "сырых" (в контексте фильтрации используется термин "RAW") данных перехвата. Теперь все объекты, которые попадают в кэш и из-за своих объёмов выгружаются на диск, анализируются отдельной очередью с целью экономии памяти.

[+] Обновлены детекторы: blogger.com, CV (hh.ru, job-mo.ru, job.ru, rabota.ru, rabota.mail.ru, superjob.ru), facebook.com (добавлено 210 новых url), google.com, hotmail.com, livejournal.com, linkedin.com, mail.ru, mamba.ru, my.mail.ru, moikrug.ru, myspace.com, odnoklassniki.ru, pochta.ru, rambler.ru, smsmms (megafon, mts, skylink, tele2), taba.ru, twitter.com, vkontakte.ru, ukr.net, wordpress.com, yahoo.com, yandex.ru.

Консоль управления:

[-] Исправлены ошибки при конфигурировании запуска, остановки, перезапуска служб Microolap EtherSensor.

[-] Исправлена ошибка отображения счётчиков детектирования TCP соединений.

[-] Исправлена ошибка отображения журналов.

2012-08-22 Версия 4.2.2.6219

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*]Обновлена библиотека захвата трафика Packet Sniffer SDK. Повышена производительность реконструкции TCP соединений, значительно уменьшен объём потребления памяти;

[+]Добавлена возможность комментировать отдельные правила фильтрации пакетов.

Анализ перехваченных объектов:

[+]Добавлена проверка доступности физической памяти. Если доступной физической памяти оказывается меньше 50Мб, кэш с результатами перехвата постепенно записывается на диск.

[-]Исправлена ошибка распаковки больших архивов, приводившая к большому расходу памяти (ошибка распаковки GZIP данных в HTTP-запросах).

Доставка результатов анализа системам-потребителям:

[-]Исправлена ошибка формата сообщений об исключительных ситуациях.

Консоль управления:

[-]Исправлены ошибки конфигурирования запуска, остановки, перезапуска служб Microolap EtherSensor.

2012-08-14 Версия 4.2.1.6196

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*]Обновлена библиотека захвата трафика Packet Sniffer SDK: повышена производительность реконструкции TCP соединений;

[*]Ускорен парсинг протоколов. Теперь для каждого прослушиваемого сетевого адаптера распознанные TCP сессии анализируются несколькими потоками одновременно (количество потоков равно количеству ядер CPU * 2);

[*]Обновлён алгоритм парсинга XMPP-протокола;

[-]Исправлена ошибка, приводившая к исключительной ситуации во время обработки SSL соединений;

[-]Исправлена ошибка в распаковке LZ1 вложений Lotus Notes;

[-]Исправлена ошибка обработки PCAP-файлов, в которых размер пакета превышал 1514 байт;

[-]Исправлена ошибка генерации BPF-фильтра.

Анализ перехваченных объектов:

[*]Ускорена инициализация дисковых квот во время загрузки службы EtherSensor Analyser;

[*]Увеличен в 4 раза канал передачи реконструированных объектов между службой EtherSensor EtherCAP и службой EtherSensor Analyser.

Внимание!

Это увеличивает пропускную способность и скорость детектирования и анализа сообщений, однако, выросли аппаратные требования для Microolap EtherSensor: оперативной памяти требуется 1 Гбайт. Следует учитывать данное требование при развёртывании Microolap EtherSensor на виртуальных машинах.

[+]Добавлена обработка схемы (GET/PUT/POST) ftp://xxx.xx.xx/, что позволяет обрабатывать/перехватывать файлы, отправляемые/получаемые посредством FTP OVER HTTP;

[+]Обновлены детекторы: CV (hh.ru, job-mo.ru, job.ru, rabota.ru, job50.ru, jobsmarket.ru, rabota.mail.ru, rosrabota.ru, superjob.ru), facebook.com, hotmail.com, linkedin.com, livejournal.com, livejournal.ru, loveplanet.ru, mail.ru, my.mail.ru, mamba.ru, meebo.com, moikrug.ru, myspace.com, odnoklassniki.ru, phpbb, pochta.ru, rambler.ru, smsmms, twitter.com, vkontakte.ru, yahoo.com, yandex.ru.

[+]Выполнена обязательная очистка директории временных файлов \data\temp во время загрузки Microolap EtherSensor;

[-]Исправлена ошибка в MIME парсере. Неправильно искались boundary, состоящие из символов '-';

[-]Исправлена ошибка разархивирования данных в HTTP-запросах/ответах.

Доставка результатов анализа системам-потребителям:

[+] В транспортные профили FTP и FileDrop добавлена опция save-zip, которая позволяет архивировать объекты в формате ZIP.

Журналирование:

[+] Добавлен функционал отслеживания работоспособности службы EtherSensor LotusTXN.

Консоль управления:

[+] Добавлена функция управления службой извлечения сообщений из Lotus Notes Transaction Log (EtherSensor LotusTXN).

[+] Добавлена возможность сохранения в диагностический отчёт файлов лицензий и версий Microolap EtherSensor.

[+] Добавлено отображение счётчиков производительности службы EtherSensor LotusTXN;

[+] Добавлено отображение счётчиков протокола YAHOO;

[-] Исправлена ошибка, приводившая к утечке памяти.

[-] Исправлены ошибки конфигурирования запуска, остановки и перезапуска служб Microolap EtherSensor;

2012-06-20 Версия 4.2.0.6046

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[+] Добавлен парсинг протокола YAHOO.

Служба EtherSensor LotusTXN

[+] Начало ограниченного тестирования службы извлечения сообщений из Lotus Notes transaction Log - EtherSensor LotusTXN. Служба позволяет отслеживать и извлекать сообщения из Lotus Notes transaction Log и передавать для дальнейшего анализа в службу детектирования и анализа сообщений EtherSensor Analyser.

Внимание!

Служба до конца не протестирована для работы с "линейным" стилем ведения транзакций Lotus Notes transaction Log.

2012-04-19 Версия 4.1.5.5923

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*] Обновлена библиотека перехвата трафика Packet Sniffer SDK. Повышена производительность реконструкции TCP соединений.

2012-04-16 Версия 4.1.4.5917

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*] Обновлена библиотека перехвата трафика Packet Sniffer SDK. Повышена производительность реконструкции TCP соединений;

[-] Исправлена ошибка перехвата проксируемых соединений, использующих HTTP метод CONNECT. Некорректно обрабатывались соединения, когда прокси-сервер требовал аутентификацию.

Служба EtherSensor ICAP:

[-] Исправлена ошибка распаковки сжатых (GZIP) запросов.

Анализ перехваченных объектов:

[*] Обновлён протокол взаимодействия с агентом Microolap EtherSensor;

[*] Обновлена конфигурация службы анализа (настройки взаимодействия с агентами Microolap EtherSensor);

[*] Изменён алгоритм детектирования Email адресов в Web сообщениях;

[+] Обновлены детекторы: CV (hh.ru, job-mo.ru, rabota.mail.ru, zarplata.ru), google.com (добавлена поддержка Web GTalk), facebook.com, myspace.com, odnoklassniki.ru, pochta.ru, rambler.ru, smsmms, ukr.net, vbulletinboard, vkontakte.ru, yandex.ru.

Журналирование:

[-]Исправлена ошибка архивирования журналов.

Консоль управления:

[*]Обновлено отображение счётчиков обработки Web-сообщений.

2012-03-27 Версия 4.1.3.5862

[-]Инсталлятор предыдущей сборки содержал некорректную версию agent.server.dll.

2012-03-26 Версия 4.1.2.5859

Источники данных и реконструкция объектов

Служба EtherSensor ICAP:

[-]Исправлена ошибка в обработке HTTP-запросов в режиме непрозрачного проксирования. В некоторых случаях это приводило к тому, что не обрабатывались запросы, содержащие аттачменты.

Анализ перехваченных объектов:

[-]Исправлена ошибка в обработке HTTP-запросов в режиме непрозрачного проксирования. В некоторых случаях это приводило к тому, что не обрабатывались запросы, содержащие аттачменты.

Консоль управления:

[*]Обновлён функционал настройки службы анализа: включение/отключение сервера агентов Microolap EtherSensor. По умолчанию сервер агентов выключен.

[-]Исправлена ошибка отображения счётчиков ICAP сервера в конфигураторе (монитор производительности).

2012-03-19 Версия 4.1.1.9899

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[-]Исправлена ошибка обработки сообщений Lotus Notes. В некоторых случаях некорректно обрабатывались строки сообщений и метаданных.

Служба EtherSensor ICAP:

[+]Добавлен режим "синхронной работы ICAP-протокола". В этом режиме сервер ICAP-сервер сначала получает от ICAP-клиента запрос целиком, и только потом отправляет ответ, даже в случае передачи больших запросов (скачивание/передача ISO-образов, или других больших файлов). Когда синхронный режим выключен - ICAP-сервер работает в потоковом режиме.

Это означает, что сервер не ждёт, пока клиент передаст ему весь запрос, а сразу же, как только может, начинает передавать ему ответ. Таким образом получается, что с точки зрения пользователя не происходит задержки в передаче файла. Это особенно актуально, когда через ICAP проходит мультимедийный трафик (например, потоковое видео).

Пользователь теперь не ждёт сначала полной загрузки видео потока на ICAP-прокси, потом на ICAP-сервер, потом получения его от ICAP-сервера обратно, и только после этого отправки его с ICAP-прокси пользователю. Необходимость включения синхронного режима связана с особенностью работы некоторых ICAP-клиентов, ориентированных в основном на работу по протоколу ICAP с антивирусами: антивирусам, как правило, необходимо сначала полное получение объекта (какого бы размера он ни был), и лишь потом они могут принять решение, какой именно ответ отдавать ICAP-клиенту.

Анализ перехваченных объектов:

[+]Встроен UDP-сервер для обработки сообщений агентов Microolap EtherSensor. Если на рабочих станциях в сети организации установлены и работают агенты Microolap EtherSensor, то они могут доставлять на сенсор информацию о соединениях, которые создают пользователи сети.

Далее при обработке перехваченных сообщений служба EtherSensor Analyser использует полученную информацию для идентификации пользователя, тем самым

точно маркируя сообщения атрибутами владельца сообщения, добавляя заголовки вида:
X-Sensor-UID: 0e515c8c-61eb-11e1-a529-000c29ff0707
X-Sensor-UID-UserName: CN=Administrator,CN=Users,DC=bigbrother,DC=foo
X-Sensor-UID-ComputerName: WS325-LOCK.bigbrother.foo

[+] Встроен механизм работы с новой лицензией. Начиная с версии 4.1 Microolap EtherSensor поддерживает лицензии с подпиской на обновления;

[-] Исправлена ошибка обработки сообщений Lotus Notes. В некоторых случаях некорректно обрабатывались строки сообщений и метаданных.

Журналирование:

[*] Повышена производительность архивирования журналов Microolap EtherSensor, сокращен размер требуемого дискового пространства;

[+] Добавлено сохранение статистики обработки сообщений Lotus Notes;

[+] Встроен механизм работы с новой лицензией. Начиная с версии 4.1 Microolap EtherSensor поддерживает лицензии с подпиской на обновление.

Консоль управления:

[*] Обновлён функционал конфигурирования службы EtherSensor ICAP;

[*] Обновлён функционал конфигурирования службы EtherSensor Analyser.

2012-01-25 Версия 4.0.14.9561

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[+] Встроен алгоритм для расчёта тайм-аута соединения с учётом текущего количества отслеживаемых соединений;

[+] Добавлен механизм переподключения сетевого адаптера, если во время работы службы EtherSensor EtherCAP адаптер был отключен, и потом заново включен (например, с помощью консоли управления Windows).

Анализ перехваченных объектов:

[*] Изменён алгоритм разбора email адресов;

[*] Ускорена загрузка детекторов;

[+] Встроена распаковка вложений, сжатых алгоритмом LZH (IBM Lotus Notes);

[+] Добавлены счётчики, показывающие количество сообщений, удалённых блоком лицензии;

[+] Обновлены детекторы: CV (careerist.ru, hh.ru, job-mo.ru, job50.ru, rabota.mail.ru, rabota.ru, rosrabota.ru, zarplata.ru), facebook.com, hotmail.com, linkedin.com, livejournal.com, mail.ru, mamba.ru, my.mail.ru, rambler.ru, pochta.ru, smsmms (beeline.ru, mts.ru, skylink.ru), vkontakte.ru.

[-] Исправлена ошибка в обработке сообщений Lotus Notes;

Консоль управления:

[+] Добавлен валидатор фильтров HTTP-объектов и фильтров сообщений. Теперь фильтр можно проверить на наличие в нём ошибок.

[+] Добавлен функционал загрузки и выгрузки отдельных журналов;

[+] Добавлен функционал отображения содержимого журнала (в режиме Plain Text);

[+] Поиск внутри журнала (в режиме Plain Text);

[+] Перемещение на заданную строку (в режиме Plain Text).

[+] Встроено отображение статистики сообщений Lotus Notes;

[+] Добавлены счётчики, показывающие количество сообщений, удалённых блоком лицензии.

[-] Исправлена ошибка диагностики при загрузке и отображении журналов;

2011-12-23 Версия 4.0.13.9421

Анализ перехваченных объектов:

[*] Изменён алгоритм обработки больших HTTP-запросов. Теперь HTTP-фильтр обрабатывает большие запросы, не загружая их в память. Ранее это могло приводить к перерасходу памяти. Данное изменение тесно связано с применением подобного фильтра:

```
<?xml version="1.0" encoding="utf-8"?>
<filter name="HTTP filter" version="1.0">
  <table name="main">

    <rule enabled="1">
      <comment>
        The rule stops processing HTTP objects whose
        request or response size is greater than 100 megabytes.
      </comment>
      <match>
        <c name="size" op="gt" value="100M"/>
      </match>
      <action name="drop" />
    </rule>

    <rule enabled="true">
      <action name="accept" />
    </rule>

  </table>
</filter>
```

[+]Обновлены детекторы: yandex.ru.

2011-12-19 Версия 4.0.12.9403

Анализ перехваченных объектов:

[+]В письмах Lotus Notes добавлена возможность распаковки больших вложений, сжатых алгоритмом LZ1.

2011-12-19 Версия 4.0.11.9393

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*]Повышена производительность обработки протокола MRA;
[*]Повышена производительность обработки протокола MSN;
[*]Повышена производительность сохранения проблемного трафика в PCAP-файлы.

Служба EtherSensor ICAP:

[-]Исправлена ошибка обработки заголовка IsTag.

Доставка результатов анализа системам-потребителям:

[*]Изменён алгоритм работы с заблокированными транспортными профилями.

Журналирование:

[*]Изменены имена директорий, в которых накапливается статистика работы Microolap EtherSensor.

Консоль управления:

[*]Добавлено явное указание кодировки в HTML файлах консоли конфигуратора:
[-]Исправлены ошибки в работе утилиты perfmon;
[-]Исправлена ошибка в утилите bugreport, приводившие к зависанию утилиты.

2011-11-29 Версия 4.0.10.9285

Анализ перехваченных объектов:

[+]Обновлены детекторы: facebook.com, mail.ru, pochta.ru, rambler.ru, smsmms (mts.ru), yandex.ru (добавлено распознавание входящих и исходящих сообщений WEB агента), CV (rabota.ru).

Консоль управления:

[-]Исправлены ошибки в работе утилиты perfmon.

2011-11-25 Версия 4.0.9.9249

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[-]Исправлена ошибка процесса остановки службы, в некоторых случаях приводившая к зависанию;

[-]Исправлена ошибка распознавания MSN-протокола.

Анализ перехваченных объектов:

[+]Обновлены детекторы: mail.ru (добавлено распознавание входящих и исходящих сообщений WEB-агента MRA), my.mail.ru, odnoklassniki.ru, vkontakte.ru, CV (job-mo.ru).

[-]Исправлена ошибка обработки MSN-протокола;

Доставка результатов анализа системам-потребителям:

[+]В журнал добавлена запись информации об использованном транспортном профиле при отправке сообщения.

Журналирование:

[-]Исправлена ошибка процесса загрузки службы EtherSensor Transfer, в некоторых случаях приводившая к зависанию.

Консоль управления:

[*]Изменён интерфейс утилиты bugreport.

[-]Исправлены ошибки в утилите bugreport.

2011-11-23 Версия 4.0.8.9215

Анализ перехваченных объектов:

[-]Исправлена ошибка декодирования заголовков X-Sensor-Ldap...

Доставка результатов анализа системам-потребителям:

[*]Расширен формат записи журнала.

Журналирование:

[*]Расширен формат записи журнала.

Консоль управления:

[*]Изменён интерфейс утилиты bugreport.

[-]Исправлены ошибки в утилите bugreport.

2011-11-18 Версия 4.0.7.9171

Анализ перехваченных объектов:

[*]Обновлены детекторы: blogger.com, facebook.com, hotmail.com, linkedin.com, mail.ru, my.mail.ru, meebo.com, myspace.com, odnoklassniki.ru, pochta.ru, rambler.ru, smsmms (megafon, mts, skylink), twitter.com, vkontakte.ru, yahoo.com, CV (careerist.ru, hh.ru, job-mo.ru, job50.ru, rabota.mail.ru, rabotavgorode.ru, rabotavia.ru, rosrabota.ru).

[-]Исправлены ошибки, приводившие к падению службы EtherSensor Analyser при обработке результатов перехвата;

Доставка результатов анализа системам-потребителям:

[*]Расширен формат записи журнала.

Журналирование:

[*]Расширен формат записи журнала.

Консоль управления:

[*]Теперь утилита bugreport собирает все текущие сообщения журнала (раньше собирала только criterror, error, warning).

2011-11-10 Версия 4.0.6.9037

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*]Обновлена библиотека Packet Sniffer SDK, отвечающая за захват трафика. Исправлены ошибки реконструкции TCP соединений.

Анализ перехваченных объектов:

[-]Исправлены ошибки, приводившие в исключительно редких ситуациях к падению службы EtherSensor Transfer при обработке результатов перехвата.

Доставка результатов анализа системам-потребителям:

[*]Изменена структура счётчиков службы EtherSensor Transfer и алгоритм их обновлений.

2011-09-29 Версия 4.0.5.8903

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*] Обновлена библиотека Packet Sniffer SDK, отвечающая за захват трафика. В дистрибутиве версии Microolap EtherSensor 4.0.4.8875 64-битные драйвера оказались не подписаны цифровой подписью, поэтому на vista/win7/win2008 (x64) захват трафика отсутствовал. Эта ошибка не проявлялась на большинстве инсталляций (win2003 x64).

Анализ перехваченных объектов:

[+] Добавлено декодирование кодировки LMBCS (Lotus Multibyte Character Set). Поддерживаются следующие кодировки: latin-1, greek, hebrew, arabic, cyrillic, latin-2, turkish, thai, unicode-16. Теперь полностью декодируются адреса, тема, тело, имена аттачментов и все другие заголовки.

2011-09-22 Версия 4.0.4.8875

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[+] Добавлен функционал для распознавания и реконструкции сессий Lotus Notes.

Анализ перехваченных объектов:

[+] Добавлен детектор сообщений Lotus Notes.

2011-09-15 Версия 4.0.3.8813

Анализ перехваченных объектов:

[+] Обновлены детекторы: CV (rabotavgorode.ru, rosrabota.ru, careerist.ru, hh.ru, job-mo.ru, rabota.mail.ru, rabotamedikam.ru, zarplata.ru), facebook.com, my.mail.ru, mail.ru, smsmms (megafon, mts, skylink), yahoo.com (входящая почта).

Журналирование:

[-] Исправлена ошибка, приводившая к утечке памяти.

2011-08-18 Версия 4.0.2.8709

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[+] Добавлена статистическая обработка протокола SSL: происходит накопление статистики SSL соединений, формируются результаты со списками SSL соединений. Данная возможность может быть отключена в конфигурации (файл ethcap.xml) следующим образом:

```
<Protocol enable="false" name="ssl" />
```

[-] Исправлена ошибка, приводившая в некоторых случаях к возникновению исключительных событий во время запуска службы;

Анализ перехваченных объектов:

[+] Обновлены детекторы: odnoklassniki.ru, pochta.ru, rambler.ru, smsmms, twitter.com, vkontakte.ru, yahoo.com, yandex.ru.

[+] Теперь все сообщения, дошедшие до стадии отправки потребителю, помечаются заголовком X-Sensor-RawSource-Type. Сделано это для того, чтобы потребитель (например, система архивирования сообщений) мог разобрать, из каких первоначальных "сырых" перехваченных данных было получено конечное сообщение. Значениями этого заголовка на сегодняшний день могут быть:

```
HttpGetRequest:      Источник сообщения - HTTP GET REQUEST;
HttpPostRequest:     Источник сообщения - HTTP POST REQUEST;
HttpPutRequest:      Источник сообщения - HTTP PUT REQUEST;
FtpFile:             Источник сообщения - FTP файл;
SmtpEml:             Источник сообщения - SMTP EML;
Pop3Eml:             Источник сообщения - POP3 EML;
IcqContactList:      Источник сообщения - ICQ Contact List;
```

IcqMessageList: Источник сообщения - ICQ Message List;
IcqFile: Источник сообщения - ICQ File;
IcqLoginInfo: Источник сообщения - ICQ Login Info;
MraUserInfo: Источник сообщения - MRA информация о пользователе;
MraContactList: Источник сообщения - MRA Contact List;
MraMessageList: Источник сообщения - MRA Message List;
MraFile: Источник сообщения - MRA File;
MsnContactList: Источник сообщения - MSN Contact List;
MsnMessageList: Источник сообщения - MSN Message List;
MsnFile: Источник сообщения - MSN File;
XmppContactList: Источник сообщения - XMPP Contact List;
XmppMessageList: Источник сообщения - XMPP Message List;
XmppFile: Источник сообщения - XMPP File;
IrcMessageList: Источник сообщения - IRC Message List;
IrcFile: Источник сообщения - IRC File;
SkypeVersionRequest: Источник данных - Get Last version запрос к ui.skype.com;
SslSessionsList: Источник данных - Список SSL сессий.

Внимание:
Необходимо иметь в виду, что некоторые почтовые системы используют механизм POST запросов для чтения входящей почты. В этом случае результат перехвата такого сообщения будет иметь заголовок X-Sensor-RawSource-Type: HttpPostRequest.

[*] Теперь все сообщения, дошедшие до стадии транспортировки, помечаются заголовком X-Sensor-LicOption. Значениями этого заголовка могут быть:
WebMail;
WebSocial;
Email;
IM;
FT;
WebMailRead.

[*] Изменено формирование From и To для сообщений WebMail, WebSocial, WebCV;

[+] Добавлена проверка и удаление пустых тел для сообщений WebMail, WebSocial, WebCV;

[+] Формируются результаты со списками SSL соединений.

Доставка результатов анализа системам-потребителям:

[*] Оптимизация расхода памяти при транспортировке сообщений.

Консоль управления:

[*] Изменён пользовательский интерфейс консоли управления;

[*] Выполнена интеграция со справочной системой Microolap EtherSensor.

[+] Добавлено отображение статистики HTTP-фильтра.

2011-07-15 Версия 4.0.1.8529

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*] Производительность обработки трафика увеличена. За счёт экономии ресурсов Microolap EtherSensor и среды выполнения стало возможным реализовать поддержку перехвата входящего HTTP трафика.

Анализ перехваченных объектов:

[*] Гарантированная обработка всех доступных как из Ethernet, так и по ICAP запросов HTTP типа GET. Это означает: если раньше был доступен анализ только тех сообщений, которые отправляются с рабочих станций через веб интерфейс, то теперь - и все получаемые сообщения могут анализироваться тоже.

[*] Контроль логинов/паролей и скачанных файлов - всё то полезное, чем сервер может ответить на запрос GET.

[+] Добавлен функционал предварительной фильтрация HTTP для отсечения заведомого мусора. Помогает снизить нагрузку на подсистему анализа. Может также использоваться и в отладочных целях.

Журналирование:

[+] Поддержка в сообщениях Microolap EtherSensor, посылаемых в файл журнала или на syslog-сервера кодировок по выбору - ликвидировано ещё одно препятствие к использованию привычных анализаторов логов.

Консоль управления:

[*] Полностью переписан конфигуратор: теперь это обычное Windows приложение (файл mconsole.exe из поставки) вместо MMC консоли, использовавшейся ранее.

[+] Накопление статистики работы Microolap EtherSensor для интеграции с внешними системами мониторинга.

2011-06-07 Версия 3.0.29.8081

Консоль управления:

[-] Исправлена ошибка в утилите bugreport, которая приводила к некорректному построению отчёта.

2011-06-06 Версия 3.0.28.8059

Анализ перехваченных объектов:

[+] Для 3.x сделан усовершенствованный метод детектирования ID из Referer для vkontakte.ru.

[-] Исправлена ошибка при формировании сообщений в WebMail (детектор !generic);

[-] Исправлена ошибка при формировании сообщений в IM (детекторы IRC и XMPP).

[-] Исправлены ошибки при фильтрации адресов сообщений;

[-] Исправлена ошибка создания заголовка сообщения. Вместо X-Sensor-Smtp-From создавался заголовок X-Sensor-Smtp-Helo.

Консоль управления:

[-] Исправлена ошибка отображения бессрочных лицензий;

[-] Исправлены ошибки чтения файла лицензии из консоли управления.

2011-04-29 Версия 3.0.27.7583

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*] Устранены наиболее вероятные места исключительных ситуаций для протоколов ftp, icq, irc, msn, mra, smtp.

Анализ перехваченных объектов:

[+] Обновлены детекторы сервисов: mail.ru, moikrug.ru.

[-] Исправлена ошибка, иногда приводившая к зависанию службы EtherSensor Analyser при запуске.

Консоль управления:

[*] Старая версия подсистемы конфигурирования/управления, основанная на MMC, заменена на приложение WinForm.

2011-03-14 Версия 3.0.25.6931

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*] Повышена надёжность обработки данных парсерами протоколов. Устранены наиболее вероятные места исключительных ситуаций для протоколов ftp, icq, irc, msn, mra, smtp;

[*] Изменена логика обработки исключительных ситуаций во время реконструкции TCP сессий.

Анализ перехваченных объектов:

[+] Обновлены детекторы служб: CV (careerist.ru, superjob.ru, zarplata.ru), livejournal.com, facebook.com, mail.ru, myspace.com, odnoklassniki.ru, vkontakte.ru, yandex.ru.

[-]Исправлена ошибка кэширования реконструированных "сырых" объектов. Ошибка приводила к остановке обработки результатов перехвата;
[-]Исправлена ошибка обработки результатов фильтра реконструированных объектов, приводившая к исключительной ситуации;
[-]Исправлена ошибка получения DNS имён по IP-адресу;
[-]Исправлена ошибка распознавания EML адресов;

Доставка результатов анализа системам-потребителям:

[-]Исправлена ошибка формирования адресов в EML конверте (from, to, cc, bcc), в протоколе SMTP во время передачи данных внешним потребителям.

Журналирование:

[*]Сокращёны ресурсы, потребляемые процессами, участвующими в ведении статистики Microolap EtherSensor.

2011-02-10 Версия 3.0.24.6617

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[-]Исправлена ошибка обработки HTTP-сессий, возникавшая в случае превышения размеров строк заголовков 4Кб.

Анализ перехваченных объектов:

[+]Добавлена совместимость с последней версией скрипта, определяющего имя и хост пользователя в трафике HTTP.
[-]Исправлена ошибка разбора имён заголовков EML-конвертов по RFC-5322;

Журналирование:

[*]Сокращено потребление ресурсов службой EtherSensor Watcher.

2011-01-28 Версия 3.0.21.6411

Анализ перехваченных объектов:

[*]Изменена конфигурация до версии 3.1., добавлен блок управления параметрами для детектирования в сообщениях WebMail полей KPPSU, KPPSH (eSafeUser, eSafeHost).
[+]Обновлены детекторы: CV (careerist.ru, jobsmarket.ru, rabota.mail.ru, rabota.ru, superjob.ru), facebook.com, mail.ru, myspace.com, odnoklassniki.ru, vkontakte.ru.

Журналирование:

[-]Исправлена ошибка нарушения XML-формата при сохранении данных статистики;
[-]Исправлена ошибка: в файлах top.hostname.XXX.xml параметр DumpTime не обновлялся по мере накопления информации.

2010-12-29 Версия 3.0.20.6277

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*]Повышена достоверность распознавания протокола XMPP/Jabber.

Анализ перехваченных объектов:

[*]Ускорена обработка сообщений (детектирование, фильтрация). Теперь одновременно могут детектироваться и фильтроваться N перехваченных объектов. N рассчитывается по формуле N = количество ядер CPU*2;
[+]Обновлены детекторы: CV (careerist.ru, hh.ru, job-mo.ru, rabota.mail.ru, rabota.by, rabotavia.ru, superjob.ru, zarplata.ru), facebook.com, livejournal.com, mail.ru, mail.ru-social, mamba.ru, moikrug.ru, myspace.com, odnoklassniki.ru, pochta.ru, vkontakte.ru, yandex.ru.

Журналирование:

[*]Теперь служба EtherSensor Watcher ведёт статистику обработки данных и накапливает информацию в директории [INSTALLDIR]\data\statistics. Накопленная информация ротируется раз в 2 месяца. Статистика на каждый день накапливается в отдельной папке внутри директории [INSTALLDIR]\data\statistics. Каждый час формируется отдельный набор файлов:

top.clients.XXX.xml:
Отображает количество соединений, созданных клиентом и общий размер данных, переданных во всех сессиях, созданных этим клиентом.

top.detectors.XXX.xml:
Отображает количество детектированных сообщений.

top.hostname.XXX.xml:
Отображает количество HTTP соединений в течение часа.

Консоль управления:

[*]Утилита bugreport теперь может открывать отчёты напрямую из ZIP архивов;

[*]Появилась возможность создавать и обнаруживать уже имеющиеся MINIDump файлы служб Microolap EtherSensor;

[*]Появилась возможность обнаруживать PCAP файлы с пакетами, перехват которых привёл к исключительной ситуации в обработке данных.

2010-12-02 Версия 3.0.19.6031

Анализ перехваченных объектов:

[-]Исправлена ошибка в фильтре сообщений - проверка состояния check-md5.

Консоль управления:

[-]Исправлена ошибка, происходившая во время создания отчёта утилитой bugreport.

2010-10-25 Версия 3.0.18.6027

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*]Повышена достоверность распознавания протокола MRA(MRIM). Вышла новая версия протокола, поддерживаемая новыми клиентами;

[+]Добавлен механизм определения "ЗАВИСШЕГО" состояния службы EtherSensor EtherCAP и выхода из этого состояния. "ЗАВИСШИМ" состоянием считается состояние, в котором служба по причине внутренних ошибок или по причине атаки прекратила перехват трафика. Пакеты, в процессе обработки которых служба перешла в "ЗАВИСШЕЕ" состояние, сохраняются в PCAP файл в директорию \log\pcaps.

[-]Исправлена ошибка в парсере протокола MRA(MRIM), приводившая к зависанию службы EtherSensor EtherCAP;

Служба EtherSensor ICAP:

[*]Буфер для сбора строк увеличен до 32К, (в соответствии со стандартом был 8К, но бывало, нам присылали строки размером 9,5К);

[*]Не проходили HTTP команды длиннее 7 символов - теперь длина увеличена до 32 символов.

[*]Также есть изменения в конфигурации службы:

```
<?xml version="1.0" encoding="utf-8"?>
<IcapConfig version="3.0">
  <SensorId>icap-01</SensorId>
  <Network max_connections="4000">
    <ListenAddress address="0.0.0.0:1344" />
  </Network>
  <Icap>
    <Preview enabled="false" size="4096" />
    <Allow204 enabled="true" />
    <RawLog enabled="false" path=".\raw-log" />
    <RequestLog enabled="false"
                http_enabled="true"
                channel="ICAP-REQUEST" />
    <AlwaysOk enabled="true" />
    <Header name="X-Client-IP" enabled="true" />
    <Header name="X-Server-IP" enabled="false" />
  </Icap>
</IcapConfig>
```

Введены новые теги:

AlwaysOk

Тег AlwaysOk является вложенным в тег Icap и включает режим "всё всегда хорошо". В этом режиме сервер ICAP при обнаружении каких либо ошибок в ICAP-протоколе со стороны клиента отвечает ему не соответствующим кодом ошибки, а кодом 204 "No modifications".

Атрибут enabled тега AlwaysOk указывает, включен режим "всё всегда хорошо" или нет:

enabled="true" - режим включен;
enabled="false" - режим отключен.

Если тег AlwaysOk отсутствует, то по умолчанию принимается, что данный режим отключен.
Если режим включен, то код ответа 204 посылается на ошибки, даже если Allow204 это запрещает.
Включать этот режим стоит только в крайних случаях, когда Вы совершенно точно знаете, что именно делаете, так как в редких случаях это может приводить к непредсказуемым сбоям в работе ICAP-клиента, поставляющего трафик.

RequestLog

Тег RequestLog является вложенным в тег Icap и определяет параметры режима журналирования ошибок протоколов ICAP и HTTP-запросов, обрабатываемых ICAP-сервером. В этот журнал сохраняются ошибки, которые могут возникать при взаимодействии ICAP-клиента и сервера, относящиеся к неправильным форматам данных, отправляемых ICAP-клиентом, некорректному использованию протокола ICAP и т.п.

Атрибут enabled тега RequestLog указывает, включен режим журналирования ошибок протоколов ICAP и HTTP или нет:
enabled="true" - режим журналирования включен;
enabled="false" - режим журналирования отключен.

Атрибут http_enabled тега RequestLog указывает, включен режим журналирования HTTP-запросов или нет:
http_enabled="true" - режим журналирования HTTP-запросов включен;
http_enabled="false" - режим журналирования HTTP-запросов отключен.
По умолчанию (если атрибут отсутствует), подразумевается что http_enabled="true".

Атрибут channel тега RequestLog указывает внутреннее системное имя для канала журналирования HTTP-запросов. Значение данного параметра всегда должно быть channel="ICAP-REQUEST" и должно меняться только при прямом указании разработчика Microolap EtherSensor.

Header
Тег Header управляет расширенными заголовками ICAP-протокола. Тег позволяет уведомлять ICAP-клиента о том, поддерживает ли сервер указанный заголовок. Тем самым становится возможным разрешать или запрещать отправку со стороны ICAP-клиента соответствующего заголовка на сервер.

Атрибут enabled тега Header указывает, включена ли поддержка указанного заголовка:
enabled="true" - поддержка заголовка включена;
enabled="false" - поддержка заголовка отключена.
Если тег отсутствует, то по умолчанию подразумевается, что данный заголовок поддерживается.

Атрибут name тега Header указывает имя расширенного заголовка.
Поддерживаемые имена расширенных ICAP-заголовков:
X-Client-IP;
X-Server-IP;
X-Client-Username;
X-Subscriber-ID;
X-Authenticated-User;
X-Authenticated-Groups.

По умолчанию (если теги Header не указаны в файле конфигурации) подразумевается, что все заголовки поддерживаются.

Анализ перехваченных объектов:

[*] Ускорена фильтрация сообщений;
[+] Обновлены детекторы: CV (careerist.ru, hh.ru, job.ru, job50.ru, jobsmarket.ru, rabota.mail.ru, rabotavgorode.ru, superjob.ru, zarplata.ru), facebook.com, livejournal.com, mail.ru, mail.ru-social, mamba.ru, moikrug.ru, meebo.com, myspace.com, odnoklassniki.ru, pochta.ru, smsmms (mts), twitter.com, vkontakte.ru, yandex.ru.
[-] Исправлена ошибка проверки на url-encoded;
[-] Исправлена ошибка при разборе MIME заголовка Content-type.

2010-10-01 Версия 3.0.17.5713

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*] В библиотеке Packet Sniffer SDK повышена производительность реконструкции TCP соединений.
[-] Исправлена ошибка при создании больших IP-фильтров;

Анализ перехваченных объектов:

[+] Обновлены детекторы: CV (careerist.ru, hh.ru, job-mo.ru, job.ru, jobsmarket.ru, rabota.ru, superjob.ru, zarplata.ru, добавлены службы job50.ru, rabotavgorode.ru, rabota.mail.ru), moikrug.ru, facebook.com, livejournal.com, loveplanet.ru, mail.ru, mail.ru-social, mamba.ru, meebo.com, myspace.com, odnoklassniki.ru, rambler.ru, smsmms, taba.ru, twitter.com, vkontakte.ru, yandex.ru.

Консоль управления:

[+] Добавлен функционал, аккумулирующий значения и расшифровку счётчиков Microolap EtherSensor в виде отчёта.

[+] Первый релиз утилиты bugreport, позволяющей собрать информацию о работе Microolap EtherSensor и службы автоматического обновления EtherSensor Updater и отправить разработчику Microolap EtherSensor для анализа.

2010-09-14 Версия 3.0.16.5573

Анализ перехваченных объектов:

[*] Изменена логика генерации имени реконструированного объекта. Теперь если Content-Type был image/* и имя файла неизвестно, то будет генерироваться имя unknown.<subtype>. То есть, для image/jpeg будет unknown.jpeg, для image/gif будет unknown.gif, и т.д.

[+] Обновлены детекторы: CV (careerist.ru, funkyjob.ru, hh.ru, job-mo.ru, job.ru, jobsmarket.ru, rabota.ru, superjob.ru, zarplata.ru), hotmail.com, moikrug.ru, facebook.com, linkedin.com, livejournal.com, mail.ru, mail.ru-social, mamba.ru, myspace.com, odnoklassniki.ru, rambler.ru, smsmms, twitter.com, vkontakte.ru, yandex.ru.

[-] Исправлена ошибка формирования конверта для MSN сообщений и контакт-листов.

Доставка результатов анализа системам-потребителям:

[-] Исправлена ошибка неправильного кодирования темы письма и других заголовков.

Консоль управления:

[-] Исправлена логическая ошибка установки и чтения значений дисковых квот.

2010-08-27 Версия 3.0.13.5377

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[-] Исправлена ошибка создания анализаторов протоколов, приводившая к падению службы EtherSensor EtherCAP.

Анализ перехваченных объектов:

[+] Добавлена раскодировка письма согласно Content-Transfer-Encoding в случае если письмо содержит только аттачмент и письмо не кодировано как MIME.

[+] Обновлены детекторы: CV (zarplata.ru), moikrug.ru, facebook.com, mail.ru, mail.ru-social, mamba.ru, odnoklassniki.ru, rambler.ru, twitter.com, vkontakte.ru, yandex.ru.

[-] Исправлена ошибка в действии DNSBL в правилах фильтрации.

[-] Исправлена ошибка, проявлявшаяся при обработке некорректных писем без тела.

[-] Исправлена ошибка в парсере EML: были проблемы с раскодированием MIME с применением транспортного кодирования, отличного от binary.

Доставка результатов анализа системам-потребителям:

[+] Реализован пул транспортных потоков. Теперь результаты анализа системе-потребителю отправляет не 1 поток, а от 1 до 10, в зависимости от объёма данных реконструированных объектов. Это существенно ускоряет работу службы EtherSensor Transfer.

2010-07-26 Версия 3.0.12.5119

Анализ перехваченных объектов:

[+] Обновлены детекторы: CV (careerist.ru, hh.ru, job-mo.ru, job.ru, rabota.ru, superjob.ru, zarplata.ru), moikrug.ru, facebook.com, loveplanet.ru, mail.ru, mail.ru-social, mamba.ru, meebo.com, odnoklassniki.ru, twitter.com, vkontakte.ru, yandex.ru.

[-] Исправлена ошибка в условии правил фильтрации для проверки дублей сообщений по MD5.

2010-07-19 Версия 3.0.11.4969

Анализ перехваченных объектов:

[+] Добавлено условие правил фильтрации для проверки дублей сообщений по MD5.

[+] Обновлены детекторы: chanboard, CV (hh.ru, job-mo.ru, job.ru, rabota.ru, superjob.ru, zarplata.ru), moikrug.ru, myspace.com, my.mail.ru, facebook.com, taba.ru, twitter.com.

[-] Исправлена ошибка определения заголовков X-Sensor-Ldap-Hostname, X-Sensor-Ldap-User.

2010-07-26 Версия 2.0.17.4175

Анализ перехваченных объектов:

[+] Обновлены детекторы: facebook.com, loveplanet.ru, mail.ru, mail.ru-social, mamba.ru, odnoklassniki.ru, vkontakte.ru, yandex.ru.

Консоль управления:

[-] В MMC-консоли управления исправлена ошибка, приводившая к исключительной ситуации при редактировании правил транспортировки результатов перехвата.

2010-07-23 Версия 2.0.16.4170

Анализ перехваченных объектов:

[+] Обновлены детекторы: accounts, facebook.com, loveplanet.ru, mail.ru, mail.ru-social, mamba.ru, meebo.com, myspace.com, odnoklassniki.ru, pochta.ru, twitter.com, vkontakte.ru, yandex.ru.

Доставка результатов анализа системам-потребителям:

[+] Реализован пул транспортных потоков. Теперь, в отличие от предыдущей версии, результаты перехвата потребителю отправляет не 1 поток, а от 1 до 10, в зависимости от объёма данных реконструированных объектов. Это существенно ускоряет работу службы EtherSensor Transfer.

2010-07-09 Версия 2.0.15.4019

Анализ перехваченных объектов:

[+] Сделано формирование заголовков в EML конверте X-Sensor-Ldap-Hostname и X-Sensor-Ldap-User, если в поле запроса User-Agent присутствуют поля eSafeHost и eSafeUser.

[+] Обновлены детекторы: accounts, blogger.com, facebook.com, fileupload, !generic, linkedin.com, livejornal.com, loveplanet.ru, mail.ru, mamba.ru, meebo.com, myspace.com, odnoklassniki.ru, plaxo.com, pochta.ru, smsmms, twitter.com, vkontakte.ru, yandex.ru.

[+] Добавлены детекторы: moimir.mail.ru.

2010-05-18 Версия 2.0.14.3656

Анализ перехваченных объектов:

[+] Реализована генерация из данных, поставляемых ICAP-сервером, следующих заголовков для EML-конвертов:
X-Sensor-Icap-Client-Username;
X-Sensor-Icap-Subscriber-Id;
X-Sensor-Icap-Authenticated-User;
X-Sensor-Icap-Authenticated-Group.

2010-05-06 Версия 2.0.13.3595

Доставка результатов анализа системам-потребителям:

[-] Исправлена ошибка обработки EML-конвертов в SMTP-клиенте транспортной службы.

2010-04-30 Версия 2.0.12.3570

Доставка результатов анализа системам-потребителям:

[-] Исправлена ошибка в обработке команды BDAT в SMTP клиенте транспортной службы.

2010-04-28 Версия 2.0.11.3551

Анализ перехваченных объектов:

[+] Добавлена обработка бинарных писем (Exchange 2010). Теперь все бинарные письма приходят как аттачменты.

[+] Обновлены детекторы: facebook.com, linkedin.com, livejournal.com, loveplanet.ru, mamba.ru, myspace.com, odnoklassniki.ru, twitter.com, vkontakte.ru, yandex.ru.

2010-03-09 Версия 2.0.11.2767

Источники данных и реконструкция объектов

Служба EtherSensor ICAP:

[*] Приведение в соответствие с обновлённым draft-stecher-icap-subid-00.txt. Теперь если ICAP-клиент посылает заголовки X-Subscriber-ID, X-Authenticated-User, X-Authenticated-Groups, то они сохраняются как свойства файла данных в паспорте: icap-x-subscriber-id, icap-x-authenticated-user, icap-x-authenticated-group соответственно.
В случае если заголовок X-Authenticated-Groups содержит несколько групп, то каждая сохраняется как отдельное свойство icap-x-authenticated-group, содержащее одну группу.

[+] Добавлены новые отладочные счётчики:
\ICAP\Request\POST
Количество POST, которые прошли через ICAP в REQMOD;

\ICAP\Request\PUT
Количество PUT, которые прошли через ICAP в REQMOD;

\ICAP\Request\Open
Количество файлов, которые открывались для сохранения POST/PUT в REQMOD;

\ICAP\Request\Open-active
Количество файлов, которые открыты сейчас для сохранения POST/PUT в REQMOD;

\ICAP\Request\Closed-and-save
Количество файлов, которые закрыли со статусом "сохранить в кэше" (обязаны присутствовать в кэше);

\ICAP\Request\Closed-and-delete
Количество файлов, которые закрыли со статусом "удалить из кэша" (были какие-то ошибки).

[+] Для raw-log сделана фильтрация в REQMOD. Запросы на Host: icap.health.check приводят к тому, что raw-log файлы для этой TCP сессии удаляются. Фильтр пока hard-coded.

[+] Теперь, если ICAP-клиент посылает заголовок X-Client-Username, то он сохраняется как свойство файла данных в паспорте icap-x-client-username. Заголовок может посылаться сервером SQUID, если на нём настроена авторизация пользователя. Настройка icap_send_client_username on|off в файле squid.conf. Возможно, другие клиенты также посылают этот заголовок, но это наверняка пока не известно.

2010-01-28 Версия 2.0.10.2766

Анализ перехваченных объектов:

[-] Исправлена ошибка в SMTP парсере, которая появилась с выходом 2.0.9.2741 в результате внесённых изменений для захвата трафика Exchange-сервера.

2010-01-26 Версия 2.0.9.2741

Анализ перехваченных объектов:

[+] Обновлены детекторы: chanboard, facebook.com, hotmail.com, linkedin.com, livejournal.com, loveplanet.ru, mail.ru, mamba.ru, meebo.com, myspace.com, nextmail.ru, odnoklassniki.ru, plaxo.com, pochta.ru, rambler.ru, smsmms, twitter.com, vkontakte.ru, yahoo.com, yandex.ru.

[+] Добавлены детекторы: Детектор accounts: детектирует события регистрации пользователей на удалённых Web сервисах. Собирает помимо логинов и паролей дополнительную информацию, которую пользователь отправляет во время регистрации (адреса, email, имена, телефоны, ники, описания...и т.д.) Детектор даёт возможность понять, какие ресурсы посещают пользователи сети на уровне перехваченных событий аутентификации для этих ресурсов.

2009-09-03 Версия 2.0.5.2500

Анализ перехваченных объектов:

[+] Обновлены детекторы: facebook.com, hotmail.com, livejournal.com, loveplanet.ru, mail.ru, mamba.ru, meebo.com, myspace.com, nextmail.ru, odnoklassniki.ru, pochta.ru, rambler.ru, smsmms, twitter.com, vbulletin, vkontakte.ru, yandex.ru, icq.

[-] Исправлены ошибки в парсере HTTP-протокола;

[-] Исправлены ошибки в парсере MRA-протокола;

2009-08-03 Версия 2.0.4.2360

Анализ перехваченных объектов:

[+] Обновлены детекторы: chanboard, facebook.com, hotmail.com, linkedin.com, livejournal.com, loveplanet.ru, mail.ru, mamba.ru, meebo.com, myspace.com, nextmail.ru, odnoklassniki.ru, rambler.ru, smsmms, twitter.com, ukr.net, vkontakte.ru, wordpress.com, yandex.ru.

[+] Добавлены детекторы: gazup.com, ifolder.ru.

2009-05-31 Версия 2.0.0.2300

Анализ перехваченных объектов:

[+] Новые детекторы:

facebook.com
события регистрации нового участника социальной сети;
события изменения профиля участника социальной сети;
сообщения передаваемые участниками социальной сети;
события отправки (загрузки) файлов участниками социальной сети;

linkedin.com
события регистрации нового участника социальной сети;
события изменения профиля участника социальной сети;
сообщения передаваемые участниками социальной сети;
события отправки (загрузки) файлов участниками социальной сети;

meebo.com
сообщения, передаваемые пользователями meebo.com

myspace.com
события регистрации нового участника социальной сети;
события изменения профиля участника социальной сети;
сообщения передаваемые участниками социальной сети;
события отправки (загрузки) файлов участниками социальной сети;

plaxo.com
события регистрации нового участника социальной сети;
события изменения профиля участника социальной сети;
сообщения передаваемые участниками социальной сети;
события отправки (загрузки) файлов участниками социальной сети;

twitter.com
события регистрации нового участника социальной сети;
события изменения профиля участника социальной сети;

сообщения передаваемые участниками социальной сети;
события отправки (загрузки) файлов участниками социальной сети;

wordpress.com
сообщения, размещаемые пользователями

mail.ru
распознавание мгновенных онлайн сообщений, передаваемых между пользователями mail.ru посредством MRA.

2009-02-26 Версия 1.0.8

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*] Повышена производительность реконструкции TCP-сессий в библиотеке Packet Sniffer SDK.

Анализ перехваченных объектов:

[*] Добавлена обработка новых сообщений в WebMail и WebSocial;

[+] Добавлены детектирование и реконструкция объектов ICQ, MRA (пока только контакт-листы и текстовые сообщения).

Доставка результатов анализа системам-потребителям:

[-] Исправлена ошибка отправки сообщений потребителю по SMTP в клиенте Microolap EtherSensor.

Журналирование:

[+] Добавлено отображение статистики отправки результатов потребителям по модулям (файл !transtat.log).

2008-10-29 Версия 1.0.7.7

Источники данных и реконструкция объектов

[+] Добавлена 32-битная версия Microolap EtherSensor.

Доставка результатов анализа системам-потребителям:

[-] Исправлена ошибка, которая приводила к дублированию писем у потребителя и к отображению некорректных счётчиков в файлах журналов.

2008-10-27 Версия 1.0.7

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*] Библиотека захвата трафика Packet Sniffer SDK версии 5.0. Эта версия обеспечивает прирост производительности захвата трафика и реконструкции соединений в 8 - 10 раз по сравнению с предыдущей версией 4.x.

Анализ перехваченных объектов:

[*] Повышена производительность модулей, обрабатывающих объекты сервисов odnoklassniki.ru, vkontakte.ru.

[+] Добавлены домены odnoklassniki.ru: odnoklassniki.ru, odnoklasniki.ru, odnoklassniki.ua, odnoklassniki.kz.

[+] Добавлены модули, обеспечивающие реконструкцию HTTP-объектов сервисов loveplanet.ru, mamba.ru, livejournal.com.

Домены loveplanet.ru:
1oveplanet.ru, alovely.ru, datelove.ru, dating.wmj.ru, flirt.me-to-you.info, flirt2008.ru, loveplanet-vip.ru, lovemir.com, love.efremov.net, love.livedate.ru, love-planet.ru, 1oveplanet.ru, loveplanet.ru, loveplanet-vip.ru, lovemoskva.ru, lov1.ru, loveopen.ru, lovedrom.ru, lovepeace.ru, mos-love.ru, planet.sbrn.ru, dating-loveplanet.ru, dating-znakomstva.ru, lovo.ru;

Домены mamba.ru:
4love.ru, date.datinglove.ru, dating.freetime.com.ua, explore.ru, flirtru.ru, flirt77.ru, fastlove.ru, facelink.ru, greatlove.ru, holiday.ru, iloveyou.ru,

jdu.ru, jzzz.info, lovemy.com.ua, love.alfa-beta.ru, love.azlyrics.ru, love.butt-head.ru, love.girlzzz.info, love.lovz.ru, love.mail.ru, love.rambler.ru, love-kiss-dating.ru, love.neolove.ru, love.pautinka.ru, love.primochka.ru, love.gay.ru, love.ignio.com, love.lesbi.ru, love.russianchat.ru, lov.ru, lovedate.ru, mamba.ru, mambo.ru, mheart.ru, romantica.ru, search.all4love.ru, svidanka.ru, vstret.ru, znakomstva.lt, znakomstva.lv, znakomstva.odnoklassniki.ru, younglover.ru, lovedosug.ru, lubovy.ru;

Домены livejournal.com:
livejournal.com, livejournal.ru.

Журналирование:

[+] Расширен набор счётчиков, отображающих показатели производительности Microolap EtherSensor. Счётчики отображаются в режиме реального времени в файлах журналов !capstat.log, !sysstat.log, !transtat.log.

[+] Расширен формат записи журнала SMTP транспорта, отправляющего результаты анализа системе-потребителю.

Консоль управления:

[+] Добавлен модуль crashreport.dll, формирующий отчёт об исключительной ситуации в случае падения любой службы Microolap EtherSensor. Формирует отчёт об исключительной ситуации в директории log\crashrpt. Отчёт об исключительной ситуации представляется в виде двух файлов: 1) минидампа приложения 2) отчёт о среде выполнения.

[+] Инсталлятор Microolap EtherSensor прописывает автозапуск службам в случае падения или исключительной ситуации.

[-] Исправлена ошибка долгого старта служб Microolap EtherSensor после перезапуска операционной системы.

2008-07-28 Версия 1.0.5

Анализ перехваченных объектов:

[+] Добавлен подсчёт MD5 Hash реконструированных объектов для идентификации дубликатов перехвата.

[+] Обновлены детекторы: mail.ru, rambler.ru, yandex.ru, pochta.ru, google.com, yahoo.com, ukr.net, odnoklassniki.ru, vkontakte.ru, squirrel-mail, file-upload, hotmail.com, nextmail.ru, newmail.ru, phpBB.

Доставка результатов анализа системам-потребителям:

[+] Добавлен заголовок X-Sensor-Object-MD5Hash в сообщения, отправляемые потребителю по SMTP.

[-] Исправлена логическая ошибка при отправке сообщений потребителю по SMTP.

2008-07-28 Версия 1.0.4

Анализ перехваченных объектов:

[+] Обновлены детекторы: mail.ru, rambler.ru, yandex.ru, pochta.ru, google.com, yahoo.com, ukr.net, odnoklassniki.ru, vkontakte.ru, squirrel-mail, file-upload, hotmail.com, nextmail.ru.

[+] Добавлены детекторы: newmail.ru, phpBB.

Консоль управления:

[+] Добавлена возможность изменять настройки журналирования.

2008-07-25 Версия 1.0.2

Анализ перехваченных объектов:

[+] Добавлены детекторы: hotmail.com, nextmail.ru.

Доставка результатов анализа системам-потребителям:

[-] Исправлена ошибка с заголовком "Sesnsor-Id".

2008-07-16 Версия 1.0.1

Источники данных и реконструкция объектов

Служба EtherSensor EtherCAP:

[*] Оптимизация расхода памяти при перехвате трафика.

Доставка результатов анализа системам-потребителям:

[+] Добавлены следующие заголовки при формировании EML для отправки потребителю по SMTP:
MailFrom/RcpTo;
Via/X-Forwarded;
Date;
Network-If-Id (теперь можно точно определить, с какого именно сетевого интерфейса был получен реконструированный объект);

[+] Заголовок, содержащий размер перехваченного объекта.

Журналирование:

[+] Добавлено архивирование журналов для экономии дискового пространства.

Консоль управления:

[+] Реализована MMC консоль конфигуратора.