User's Guide

Traffic Inspector

About this manual template:

This is a very reduced template, made for projects with up to 3 TOC levels only. Page numbering is generally defined in the MasterBackground section.

The table of contents intentionally just prints 3 levels (4 to 6 are simply ignored) and does not use chapter numbering. Page reference numbers in the table of contents are printed before the heading, for design reasons. The TOC does print page numbers at the bottom (enable Masterbackground for the TOC, if you want that).

The topics section prints the current top-level chapter at the top of the page. Sub-chapters are printed with TOC headings, but again without chapter numbering.

If you are going to use this template, please open the with the Manual Designer and save it under a new name. You can delete this text in your personal copy.

Contents

Contents

Contents

Contents

Быстрый ввод Traffic Inspector в эксплуатацию

1

Для быстрого ввода Traffic Inspector в эксплуатацию выполните следующие действия:

1. Подготовьте сервер для установки Traffic Inspector (подробнее см. в п. Подготовка сервера).
2. Установите Traffic Inspector (подробнее см. в п. Установка программы).
3. Запустите конфигуратор и в режиме **Настройка конфигурации** выберите вариант применения программы, используемую службу маршрутизации и другие основные параметры (подробнее см. в п. Настройка режима работы).
4. Запустите конфигуратор и в режиме **Настройка служб** настройте используемые службы, внешние и внутренние интерфейсы (подробнее см. в п. Настройка служб).
5. Настройте доступ к Traffic Inspector для администраторов и персонала, менеджеров и кассиров, которые будут работать с продуктом через консоль администратора (подробнее см. в п. Разграничение доступа).
6. Настройте общие параметры учетных записей пользователей. Если для них не будут заданы персональные настройки, они будут работать как параметры по умолчанию для всех групп и пользователей (подробнее см. в п. Общие настройки пользователей).
7. Сформируйте необходимое количество групп учетных записей пользователей программы (подробнее см. в п. Создание и настройка групп).
8. Создайте учетные записи пользователей программы вручную (подробнее см. в п. Создание и настройка пользователей), импортируйте их из Active Directory или из результатов сканирования локальной сети (подробнее см. в п. Импорт пользователей).
9. Установите на компьютерах пользователей клиентские агенты Traffic Inspector вручную или с помощью групповых политик Active Directory (подробнее см. в п. Клиентский агент Windows).
10. При необходимости настройте дополнительные модули Traffic Inspector (подробнее см. в п. Дополнительные модули).
11. Сформируйте правила и назначьте их соответствующим учетным записям пользователей и группам (подробнее см. в п. Виды и предназначение правил, наборы

Быстрый ввод Traffic Inspector в эксплуатацию 1

правил).

12. При необходимости настройте счетчики внешнего трафика (подробнее см. в п. Счётчики трафика).

13. Если в организации есть собственный почтовый сервер, настройте SMTP-шлюз Traffic Inspector (подробнее см. в п. SMTP-шлюз).

14. При необходимости настройте синхронизацию встроенной базы данных с внешней SQL-базой (подробнее см. в п. Синхронизация с внешней БД).

15. Настройте резервное копирование (подробнее см. в п. Резервное копирование) и обслуживание встроенной базы данных (Обслуживание БД).

Версии продукта Traffic Inspector

Обновления Traffic Inspector

Версия 3.0.1

Версия 3.0.0

Версия 2.0.1

Версия 2.0.0

Системные требования

Минимальные системные требования серверной части Traffic Inspector:

- процессор - Intel Atom D510 1,66 ГГц;
- оперативная память - 2048 Мб;
- свободного места на жестком диске (без учета места под файлы кэша и статистики) - 400 Мб;

- монитор и видеоадаптер с разрешением 1024 на 768;
- операционная система Microsoft Windows 7, 7 x64, 2008 R2, 8.1, 8.1 x64, Server 2012 R2;
- подключение к сети Интернет.

Возможные конфликты

Известны следующие возможные конфликты при работе Traffic Inspector с другим программным обеспечением:

- конфликты драйверов;
- конфликты портов;
- конфликты с антивирусным программным обеспечением.

Конфликты драйверов могут возникать со следующими драйверами:

- собственными драйверами NAT, используемыми аналогичными продуктами;
- драйверами NDIS на интерфейсах.

Для избежания потенциальных конфликтов со сторонним программным обеспечением рекомендуется не устанавливать Traffic Inspector на один компьютер с аналогичными продуктами, использующими собственные драйверы NAT, а также, по возможности, удалить все драйверы NDIS, кроме драйвера Traffic Inspector.

Конфликты портов могут возникнуть в том случае, если на сервере есть службы, использующие те же сетевые порты, что и Traffic Inspector. Для избежания этой ситуации необходимо назначить этим службам и Traffic Inspector разные порты (изменить можно как порты существующих служб, так и порты, на которых работает Traffic Inspector).

Traffic Inspector может конфликтовать с антивирусным программным обеспечением. Поэтому рекомендуется на сервер с Traffic Inspector не устанавливать антивирусное программное обеспечение, а для проверки сетевого трафика использовать встроенные модули. Если же наличие антивируса необходимо, то папку с Traffic Inspector необходимо

включить в исключения и разрешить программе любую сетевую активность.

Установка и обновление

Подготовка сервера

Для подготовки сервера к установке Traffic Inspector выполните следующие действия.

1. Установите операционную систему Windows из списка поддерживаемых (см п. Системные требования);
2. Установите необходимые для работы Traffic Inspector дополнения и компоненты;
3. Обновите операционную систему вместе с установленными компонентами.

1. Установка операционной системы

На сервере должна быть установлена одна из поддерживаемых операционных систем (см п. Системные требования).

Внимание! На бета-версиях или сокращенных нелегальных дистрибутивах операционных систем программа может работать некорректно. Поэтому настоятельно рекомендуется использовать на сервере только официальные релизы дистрибутивов операционных систем.

2. Установка дополнений и компонентов

Для корректной работы Traffic Inspector могут потребоваться следующие дополнения и компоненты.

- **Microsoft .NET Framework 4.0.** Обязательное обновление Windows, без него установка программы будет невозможна.
- **Windows Installer 3.1.** Может потребоваться для установки Microsoft. NET Framework 2.0.
- **Windows Script 5.6** (для Windows XP/2003). Может потребоваться, если не работает встроенный веб-сервер.

Замечание! *Загрузить дистрибутивы компонентов можно с сайтов*

разработчиков или с официального сайта Traffic Inspector (http://www.smart-soft.ru/ru/downloads/SystemUpdate/). Если компоненты не установлены в процессе подготовки сервера, то они могут быть инсталлированы автоматически в ходе установки Traffic Inspector.

3. Обновление

Установите все последние обновления, включая актуальные Service Pack, операционной системы и всех перечисленных выше компонентов. Не используйте бета-версии Service Pack.

Установка сервера Traffic Inspector

Для установки Traffic Inspector выполните следующие действия:

1. Запустите дистрибутив, загрузить который можно с официального сайта Traffic Inspector.
2. Если на сервере не установлено какое-либо необходимое для работы Traffic Inspector дополнительное программное обеспечение, мастер установки выдаст соответствующее предупреждение. Нажмите на кнопку **Далее**.
3. В открывшемся окне выберите необходимые компоненты и нажмите на кнопку **Далее.** При этом будут автоматически загружены и установлены необходимые программные модули.

   Замечание! *Для загрузки компонентов сервер должен быть подключен к Интернету. Также можно необходимые компоненты установить вручную до инсталляции Traffic Inspector (см. п. Подготовка сервера).*

4. После завершения установки дополнительных компонентов (или если они были установлены предварительно), на экране появится приветственное окно мастера установки. Нажмите на кнопку **Далее**.
5. Ознакомьтесь с лицензионным соглашением, примите его и нажмите на кнопку **Далее**.
6. Ознакомьтесь с представленной в окне информацией и нажмите на кнопку **Далее**.

7. Выберите роль устанавливаемого программного обеспечения - **Сервер** или **Консоль**. При выборе первого варианта на компьютер будет выполнена установка всех необходимых серверных компонентов Traffic Inspector, а также консоли управления. Второй вариант используется для установки одной только консоли на компьютеры администратора. Для гибкой настройки инсталлируемых компонентов включите флажок **Выборочная установка**. Нажмите на кнопку **Далее**.

8. Если на предыдущем шаге был включен флажок **Выборочная установка**, то вручную выберите устанавливаемые компоненты и нажмите на кнопку **Далее**.

9. Если среди устанавливаемых компонентов есть Kaspersky Gate Antivirus, прочитайте его лицензионное соглашение, примите его и нажмите на кнопку **Далее**.

10. Если установка Traffic Inspector выполняется удаленно посредством удаленного рабочего стола Windows, включите флажок **Выполняется удаленная установка**. В этом случае в сетевом экране программы будет автоматически создано правило, разрешающее соединение по порту TCP 3389. В противном случае, после инсталляции Traffic Inspector сервер будет недоступен удаленно.

11. Нажмите на кнопку **Установить,** дождитесь завершения процесса инсталляции и нажмите на кнопку **Готово**.

> ***Замечание!*** *В процессе инсталляции могут появляться всплывающие окна для подтверждения установки сетевых компонентов. В этом случае переключитесь в окно и подтвердите установку.*

Переустановка и обновление программы Traffic Inspector

Для переустановки или обновления Traffic Inspector (в рамках одной версии) выполните следующие действия:

1. Закройте все подключенные к серверу консоли администратора.

2. Остановите службу **Traffic Inspector (TrafInspSrv)**.

3. Если планируется перенос программы, например, на другую аппаратную платформу, сохраните следующие папки и файлы с информацией:

- подпапка **Config** папки установки;
- подпапка **Data** папки установки;
- файл **proxy.dat** из папки установки (в том случае, если нужно сохранить кэш прокси-сервера).

4. Деинсталлируйте Traffic Inspector.

Замечание! *Перед удалением программы настоятельно рекомендуем остановить служ бу RRAS, отключить и запретить все активные DialUp и VPN-соединения (если они используются).*

5. Перезагрузите сервер.

Замечание! *Для Windows 2003 и старше возмож на переустановка программы без перезагрузки системы.*

6. Установите Traffic Inspector (см. п. Установка программы).
7. Если осуществлялся перенос программы на новую аппаратную платформу, то скопируйте сохраненные на шаге 3 папки поверх новых.
8. Запустите службу **Traffic Inspector (TrafInspSrv)** и проверьте корректность ее работы и настроек.

Обновление Traffic Inspector с версий 2.x

Перед обновлением программы или переходом на новую версию полностью сохраните всю папку предыдущей версии, скопируйте базу, дополнительные файлы и ее дистрибутив, чтобы, в случае необходимости, иметь возможность восстановить ее.

Для обновления Traffic Inspector с версии 2.x выполните следующие действия:

1. Закройте все подключенные к серверу консоли администратора и остановите службу **Traffic Inspector**.
2. Если установка новой версии планируется на другом сервере (или на том же сервере, но с другой операционной системой), то сохраните следующие папки и файлы с информацией:

- подпапка **Config** папки установки;
- подпапка **Data** папки установки;
- файл **proxy.dat** из папки установки (в том случае, если нужно сохранить кэш прокси-сервера).

3. Деинсталлируйте старую версию Traffic Inspector и перезагрузите сервер.

> ***Замечание!*** *При возникновении проблем удаления Traffic Inspector, используйте программу Windows Installer CleanUp. После использования Windows Installer CleanUp "Панели управления" - "Установка и удаление программ" удалите драйверы Traffic Inspector, если они там есть. Затем удалите лишние файлы из папки установки старой версии Traffic Inspector.*

4. Установите Traffic Inspector версии 3.0 в ту папку, в которой была установлена старая версия. Если установка осуществляется на новом сервере (или на новой операционной системе), то установите Traffic Inspector версии 3.0 в произвольную папку, после чего скопируйте сохраненные ранее данные поверх новых.
5. После установки программы проверьте все настройки Traffic Inspector: фильтры, правила, тарифы, баланс пользователей и т.д.

Виды лицензий и дополнительных компонентов

У Traffic Inspector есть два основных вида лицензий:

- GOLD;
- FSTEC.

Также у Traffic Inspector есть так называемая триальная (пробная) версия. Она представляет собой полноценную версию GOLD с ограничением по времени работы 30 суток. Триальная версия используется для апробации функциональных возможностей программы. Лицензии приобретаются на определенное количество учетных записей (см. п. Выбор количества лицензий). Каждая лицензия включает в себя 1 год подписки на обновления и расширенную техническую поддержку (см. п. Подписка и обновления).

Лицензирование и активация 3

GOLD

Лицензия GOLD - универсальная лицензия, которая предоставляет доступ ко всем возможностям Traffic Inspector. Она может использоваться в любых организациях и в любых информационных системах за исключением тех, где требуется обязательная сертификация средств защиты.

FSTEC

Лицензия FSTEC предназначена для использования в тех организациях и информационных системах, где требуется обязательная сертификация средств защиты.

Traffic Inspector FSTEC имеет сертификат на соответствие следующим требованиям ФСТЭК России:

- «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации» - по 3 классу защищенности.
- «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» - по 4-му уровню контроля, а также может использоваться при создании автоматизированных систем до класса защищенности 1Г включительно и для защиты информации в информационных системах персональных данных до 1 класса включительно.

В комплект поставки Traffic Inspector FSTEC входят:

- Свидетельство о праве пользования программой Traffic Inspector версия ФСТЭК;
- Сертифицированный дистрибутив сертифицированного программного обеспечения (поставляется на диске в DVD-боксе и коробке);
- Формуляр на сертифицированное программное обеспечение, промаркированный специальным защитным знаком соответствия ФСТЭК России;

- Заверенная копия Сертификата ФСТЭК России на программное обеспечение;
- Инструкция.

Лицензии на дополнительные компоненты

Для Traffic Inspector существует ряд дополнительных компонентов, расширяющих функциональные возможности системы защиты, которые лицензируются отдельно. Для своей работы они требуют активированную версию Traffic Inspector. Каждая лицензия приобретается на определенное количество учетных записей (см. п. Выбор количества лицензий).

- **NetPolice для Traffic Inspector на 1 год**. Лицензия предоставляет покупателю право использовать в течение одного года модуль контекстного анализа. Он предназначен для контекстного анализа трафика, проходящего через прокси-сервер и почтовый шлюз Traffic Inspector, фильтрует сайты по категориям и их содержимому, не позволяет получить доступ к определенным сайтам или услугам сети Интернет.
- **Kaspersky Gate Antivirus для Traffic Inspector на 1 год** и **Dr.Web Gateway Security Suite для Traffic Inspector на 1 год**. Лицензии предоставляют покупателю право использовать в течение одного года Kaspersky Gate Antivirus или Dr.Web Gateway Security Suite. Данные модули предназначены для антивирусной защиты трафика, проходящего через прокси-сервер и почтовый шлюз, лечат зараженные файлы, блокируют вредоносные программы, запрещают потенциально опасное содержимое.
- **Adguard для Traffic Inspector на 1 год**. Лицензия предоставляет покупателю право использовать в течение одного года Adguard - модуль для фильтрации социальных виджетов, всплывающих окон и рекламы. В нем используется Displace-технология, позволяющая блокировать всплывающие окна и рекламные баннеры из тела страницы на любой платформе и в любом браузере.
- **AntiSpam для Traffic Inspector**. Лицензия предоставляет покупателю право использовать модуль для контроля входящих почтовых сообщений и фильтрации нежелательных писем с использованием SMTP-шлюза Traffic Inspector. Модуль

проверяет всю входящую корреспонденцию, помечает и фильтрует спам.

Выбор количества лицензий Traffic Inspector

Все лицензии, как на сам Traffic Inspector, так и на дополнительные компоненты, рассчитаны на определенное количество учетных записей. Под учетной записью в программе может быть авторизован один пользователь, один компьютер или несколько компьютеров по диапазону адресов.

> ***Замечание!*** *Объединять в одну учетную запись компьютеры по диапазону адресов имеет смысл только в том случае, если для всех этих компьютеров будут действовать одинаковые правила и тарифы. При этом надо учитывать, что вся статистика работы будет вестись не по каждому ПК отдельно, а для всей учетной записи суммарно.*

При приобретении лицензии необходимо выбирать такую лицензию, в которую включено достаточное количество учетных записей. В настоящее время предлагаются лицензии на 5, 10, 15, 25, 30, 40, 50, 75, 100, 150 и 200 учетных записей. Также есть безлимитная лицензия. При ее выборе ограничения по количеству учетных записей отсутствуют.

Пример. Допустим, в организации есть 3 отдела. Первый отдел из 5 ПК не нуждается в доступе в Интернет. Во втором отделе работает 10 сотрудников, но только 7 из них необходим доступ в Интернет и раздельный учет трафика. А третий отдел составляют 10 ПК, каждый из которых должен иметь выход в Интернет, при этом раздельное ведение статистики не нужно и правила ко всем компьютерам применяются одни и те же. В таком случае будет достаточно завести в системе 8 учетных записей - 7 для сотрудников 2 отдела, и 1 для всех компьютеров 3 отдела (предварительно необходимо назначить ПК в третьем отделе свой диапазон IP-адресов). Лицензии Traffic Inspector на дополнительные компоненты продаются на строго определенное количество учетных записей (см. выше). Поэтому для нашего примера необходима лицензия на 10 учетных записей.

При необходимости приобретенную лицензию можно расширить, увеличив количество доступных учетных записей. Для этого достаточно оплатить разницу между лицензиями, получить активационные данные и активировать с их помощью Traffic Inspector. При этом переустановка или перенастройка программы не нужна.

Лицензирование и активация 3

Подписка и обновления Traffic Inspector

При приобретении подписки покупателям предоставляется:

- полный доступ ко всем вышедшим в период действия подписки обновлениям Traffic Inspector;
- расширенная техническая поддержка (помощь в настройке программы, диагностика и решение проблем посредством удаленного подключения, детальное изучение вопроса клиента с возможностью консультации разработчиков);
- доступ к новым дистрибутивам сертифицированной ФСТЭК версии (для владельцев лицензии FSTEC).

Подписка предоставляется автоматически при:

- покупке лицензии Traffic Inspector – на 12 месяцев;
- при переходе с ранних версий (PRO, Lite+, HomeNet и Standard) на версию GOLD – на 6 месяцев;
- при переходе с версии GOLD на версию FSTEC – на 6 месяцев.

После завершения подписки ее можно продлить.

После завершения подписки в том случае, если она не будет продлена:

- лицензия на Traffic Inspector – бессрочная; можно продолжать пользоваться продуктом без ограничений, при этом всегда будут доступны сборки, вышедшие до истечения срока действия подписки, но нельзя будет активировать новые версии, выпущенные после этой даты;
- вам будет предоставляться бесплатная базовая техническая поддержка (решение проблем с активацией программы, консультации по e-mail и телефону без детальной диагностики проблемы и исследований).

Лицензирование и активация 3

Активация Traffic Inspector

Активация Traffic Inspector необходима для полнофункциональной работы сервера и всех дополнительных компонентов. Данные об активации отображаются на вкладке **Активация** консоли администратора (подробнее о консоли см. в п. Консоль администратора).

Сервер устанавливается с лицензией **DEMO**. Данная лицензия является демонстрационной и не предназначена для коммерческого использования. Она может применяться неограниченное количество времени, однако имеет существенное ограничение по количеству учетных записей (не более 3). Для снятия ограничений и начала нормальной работы с сервером программу необходимо активировать.

> ***Замечание!*** *Активация Traffic Inspector осуществляется путем подключения к серверу разработчиков. Поэтому компьютер, на котором установлена программа, долж ен быть подключен к Интернету.*

Активация триальной версии

Триальная версия - полная версия Traffic Inspector, предназначенная для оценки работоспособности программы. Она имеет ограничение по сроку работы - 30 суток с момента активации. Впоследствии триальную версию можно перевести в рабочую, не переустанавливая и не перенастраивая, просто активировав ее с использованием приобретенной лицензии (см. выше).

Для активации триальной версии выполните следующие действия:

1. Запустите консоль администратора и подключитесь к серверу Traffic Inspector (см. п. Консоль администратора).
2. Перейдите в раздел **Активировать** и запустите мастера активации. В мастере выберите тип **Временная активация**.
3. Введите все данные, необходимые для активации. Разрешите или запретите новостную рассылку о Traffic Inspector.

4. Просмотрите информацию о предстоящем процессе, запустите его и дождитесь завершения.

> ***Замечание!*** *Активация может длиться в течение нескольких минут в зависимости от скорости подключения к Интернету, степени загруженности линий связи и других факторов.*

5. После завершения процесса программа будет активирована на 30 суток. Информация об активации будет отображаться в разделе **Активация** консоли администратора.

Активация приобретенной лицензии

При приобретении лицензии вы получите два значения – ID продукта (или просто ID) и PIN-код (PIN). После этого для активации установленного сервера Traffic Inspector выполните следующие действия:

1. Запустите консоль администратора и подключитесь к серверу Traffic Inspector (см. п. Консоль администратора).
2. Перейдите в раздел **Активировать** и запустите мастера активации. В мастере выберите тип **Постоянная активация**.
3. Введите полученные от продавца ID и PIN**.**
4. Просмотрите информацию о предстоящем процессе, запустите его и дождитесь завершения.

> ***Замечание!*** *Активация может длиться в течение нескольких минут в зависимости от скорости подключения к Интернету, степени загруженности линий связи и других факторов.*

5. После завершения активации будет показан результат процесса, а также перечень доступных согласно приобретенной лицензии дополнительных компонентов.

Активация дополнительных компонентов

Лицензирование и активация 3

Лицензии на использование дополнительных компонентов могут быть приобретены уже после установки, активации и настройки сервера Traffic Inspector. В этом случае для активации используется специальный ключ, полученный от продавца.

> ***Замечание!*** *Данная процедура используется для активации всех компонентов, кроме Dr. Web Gateway Space Security.*

Для активации дополнительных компонентов выполните следующие действия:

1. Запустите консоль администратора и подключитесь к серверу Traffic Inspector (см. п. Консоль администратора).
2. Перейдите в раздел **Активировать,** запустите мастера активации и перейдите к активации дополнительных опций.
3. Введите полученные от продавца ID и PIN основной лицензии на Traffic Inspector, а также полученный ключ активации.
4. Запустите процесс активации и дождитесь его завершения.

Восстановление утерянного ключа

Если данные для активации приобретенной лицензии были утеряны, вы можете восстановить их. Для этого выполните следующие действия:

1. Запустите консоль администратора и подключитесь к серверу Traffic Inspector (см. п. Консоль администратора).
2. Откройте раздел **Активировать,** запустите мастера активации и перейдите к процедуре восстановления утерянного ключа.
3. Заполните необходимые поля. При этом будет сформирован запрос, который автоматически будет отправлен в службу поддержки. После его обработки специалисты компании свяжутся с вами.

Компоненты Traffic Inspector 4

Консоль администратора Traffic Inspector

Консоль администратора является основным способом управления Traffic Inspector. Она представляет собой оснастку консоли управления Windows (MMC – Microsoft Management Console). С помощью консоли администратора можно управлять сервером Traffic Inspector как локально, так и удаленно. Во втором случае необходимо предварительно установить консоль на компьютер администратора (см. п. Установка программы).

Запуск консоли администратора и подключение к серверу Traffic Inspector

Для запуска консоли администратора и подключения к серверу Traffic Inspector выполните следующие действия:

1. Запустите **Консоль администратора**.
2. Если вы хотите подключиться к удаленному серверу, укажите его IP-адрес или имя хоста. Если вы хотите подключиться к локальному серверу, сервер не указывайте.
3. Авторизуйтесь на сервере. Сделать это можно от имени текущего пользователя Windows. В этом случае никаких дополнительных данных указывать не нужно. Можно авторизоваться от имени произвольного пользователя Windows. В этом случае необходимо вручную указать имя пользователя, его пароль и домен (при необходимости можно включить сохранение этих данных, чтобы при последующих подключениях не вводить данные авторизации повторно). Два указанных способа возможны для администраторов с типом учетной записи **Учетная запись Windows** (подробнее о типах учетных записей см. в п. Управление администраторами).

   Для авторизации администраторов с типом учетной записи **Встроенная учетная запись** введите заданные в настройках администратора логин и пароль.

Основы интерфейса консоли администратора

Поскольку консоль администратора Traffic Inspector является оснасткой к консоли управления Windows, то она имеет стандартный интерфейс. Окно консоли разделено на две части. В левой отображается список доступных разделов. Он иерархический с

произвольной степенью вложенности. То есть в каждом разделе могут быть подразделы, эти подразделы в свою очередь поделены еще на части и т.д. В правой части окна отображается содержимое активного в данный момент раздела или подраздела.

В верхней части главной страницы консоли администратора отображается имя сервера Traffic Inspector, к которому она подключена, имя пользователя, кнопки для управления доступом, вызова справки и отключения от сервера.

Также на главной странице отображается общая информация о работе программы, новости с сайта разработчика, статистика по сетевым интерфейсам, сведения по работающим сервисам и пр.

> ***Замечание!*** *Более подробно о работе в консоли управления, настройке ее внешнего вида, таблиц и пр. можно прочитать в руководстве пользователя вашей версии Windows.*

Отключение от сервера

Для отключения от сервера откройте главную страницу консоли администратора и нажмите на "крестик".

Веб-сервер Traffic Inspector

Общие сведения

В состав Traffic Inspector входит собственный веб-сервер. Он предназначен для обеспечения работы веб-интерфейса (см. п. Веб-интерфейс). По умолчанию веб-сервер включен и настроен на работу на порту TCP 8081 и закрыт для доступа из внешних сетей. При необходимости эти параметры можно изменить (см. п. Настройка веб-сервера).

Управление веб-сервером осуществляется в разделе **Сервисы -> Web-сервер** консоли администратора. На главной странице раздела размещен блок, состоящий из двух вкладок. На вкладке **Информация** отображаются основные сведения о работе веб-сервера. На вкладке **Действия** располагаются ссылки на различные операции, связанные с веб-сервером.

Администратор может просмотреть информацию о текущих подключениях к веб-серверу.

Для этого в разделе **Сервисы -> Web-сервер** консоли администратора откройте подраздел **Сессии**.

Настройка веб-сервера Traffic Inspector

Настройка веб-сервера осуществляется в специальном окне, которое открывается из блока **Действия**, расположенного в разделе **Сервисы -> Web-сервер** консоли администратора.

Окно настроек состоит из следующих вкладок:

- **Сервер**;
- **Сертификаты** (отображается в том случае, если включен SSL-сервер);
- **Страницы по умолчанию**;
- **Клиентский агент**;
- **Настройки портала**.

Вкладка Сервер

На вкладке **Сервер** настраиваются основные параметры работы веб-сервера. В частности, на ней можно изменить TCP-порт, на котором он будет работать (по умолчанию 8081). TCP-порт может быть статическим. В этом случае указывается точное его значение. Также он может быть динамическим. В этом случае порт будет выбираться Traffic Inspector автоматически из числа свободных в данный момент.

> ***Замечание!*** *При выборе динамического порта к серверу лучше всего обращаться по порту HTTP прокси-сервера, а уже он сделает перенаправление на порт веб-сервера.*

На этой же вкладке можно включить SSL-сервер, который обеспечивает шифрованную передачу трафика между веб-интерфейсом и веб-сервером. При этом можно изменить его сетевой порт (по умолчанию 8443), который обязательно является статическим (то есть указывается конкретный TCP-порт).

> ***Замечание!*** *Для работы SSL-сервера необходимо зарегистрировать как*

минимум один сертификат (подробнее о работе с сертификатами см. в п. Издательство сертификатов).

Здесь же можно включить автоматическое создание разрешающего правила для веб-сервера во внешнем сетевом экране. Эту функцию удобно использовать в тех случаях, когда необходим удаленный доступ к веб-интерфейсу через Интернет. При ее включении в межсетевом экране будут автоматически создаваться необходимые правила.

Вкладка Сертификаты

Данная вкладка используется для настройки сертификатов, необходимых для создания защищенных SSL-каналов для безопасной передачи трафика между веб-интерфейсом и веб-сервером. На ней отображается перечень доступных сертификатов, уже установленных в хранилище сервера (поле **Список доступных сертификатов**).

Если в системе планируется использование SSL-каналов с зашифрованным трафиком для удаленного доступа к веб-серверу, то установите необходимый сертификат для внутренних сетей, выбрав его из списка доступных. Если веб-сервер будет доступен из Интернета, то также установите сертификат для внешних сетей. Обратите внимание, что сертификаты для внутренних и внешних сетей могут быть как одинаковыми, так и различными, потому что имя хоста сервера при запросе из разных сетей может быть разным.

Если на сервере не установлены подходящие сертификаты, то их можно выписать самостоятельно в окне **Издательство сертификатов** (см. п. Издательство сертификатов), которое можно запустить с вкладки **Сертификаты** окна настройки веб-севера

Вкладка Страницы по умолчанию

На вкладке **Страницы по умолчанию** задаются названия файлов, которые будут открываться веб-сервером, если при запросе указан только раздел. По умолчанию в Traffic Inspector задан перечень наиболее распространенных файлов. Список можно изменять по своему усмотрению, а также быстро вернуть в первоначальное состояние.

Вкладка Клиентский агент

Вкладка **Клиентский агент** используется для настройки работы сервера с клиентскими веб-агентами по протоколу HTTP (подробнее об агентах см. п. Клиентский агент Windows). В частности, можно запретить передачу трафика в открытом виде. В этом случае весь обмен информацией между веб-агентом и веб-сервером будет осуществляться только по защищенному SSL-каналу (для этого необходимо настроить на веб-сервере сертификаты безопасности).

Здесь же необходимо указать файл с шаблоном в формате XSL, который определяет внешний вид агентов.

> ***Замечание!*** *Путь к файлу указывается относительно папки установки (пример: /agent.xsl). Данная настройка является общей, для отдельных пользователей и их групп может быть задан другой шаблон.*

Вкладка Настройки портала

Вкладка **Настройки портала** используется для установки основных параметров работы веб-интерфейса. На ней можно указать имя сервера, которое будет отображаться на страницах веб-интерфейса, а также включить или выключить показ в отчетах сервера статистики данных по всем сессиям пользователей. При включении этой функции в отчетах сервера статистики будет отображаться подробная информация по всем сессиям веб-сервера. В противном случае будут отображаться данные только по текущей сессии.

Издательство сертификатов в Traffic Inspector

Сертификаты безопасности необходимы для работы веб-сервера с защищенным SSL-каналом, по которому все данные между точкой доступа через веб-интерфейс и веб-сервер передаются в зашифрованном виде. Если на сервере нет подходящих установленных сертификатов, то их необходимо создать. Для этого выполните следующие действия:

1. Откройте окно **Издательство сертификата**. Сделать это можно из блока **Web-сервер** раздела **Сервисы -> Web-сервер** консоли администратора.

2. На вкладке **Операции** выберите тип операции - создание нового сертификата издательства (CA) или создание сертификата для веб-сервера с использованием существующего издательства.

   Замечание! *Если сертификат издательства создавался ранее, необходимо учитывать, что после создания нового сертификата издательства необходимо будет установить его на все пользовательские компьютеры.*

3. На вкладке **Формирование запроса** укажите имя хоста сервера или его IP-адрес во внутренних сетях организации. Если будет настраиваться доступ к веб-интерфейсу из внешних сетей, при этом имя сервера или его IP-адрес со стороны этих внешних сетей отличаются от внутренних, то введите имя хоста сервера или его IP-адрес со стороны внешних сетей.

   Здесь же укажите число лет, на которое будет выписан сертификат.

4. Дождитесь завершения процесса. При этом на экран будет выдана информация о его результатах.

Управление разделами веб-сервера Traffic Inspector

Разделы веб-сервера представляют собой отдельные директории или сайты, доступ к которым пользователей возможен с помощью браузера. Список существующих разделов отображается в подразделе **Разделы** раздела **Сервисы -> Web-сервер** консоли администратора.

Все разделы в списке отсортированы по именам виртуального пути – тем самым они соответствуют внутренней иерархии сервера. Каждый раздел может содержать произвольное количество подразделов с любой степенью вложенности. Наличие ошибок приводит к неработоспособности только конкретного раздела и всех его подразделов.

В случае возникновения проблем с доступностью разделов и/или отображением внесенных в их настройки изменений, сайты можно перегрузить. Перегружать можно как произвольный раздел, так и все сайты. Запуск операции выполняется с помощью контекстного меню.

Замечание! *Перезагрузить можно только те разделы, для которых настроена обработка ASP.NET.*

Разделы по умолчанию

Для корректной работы служб программы, веб-интерфейса (описание веб-интерфейса приведено в п. Веб-интерфейс) и веб-агента при установке Traffic Inspector автоматически создается ряд разделов, удалять которые не рекомендуется:

- **/** - корневой раздел веб-интерфейса (главная страница портала), открыт для всех пользователей;
- **/download** - раздел для размещения файлов для загрузки, по умолчанию в нем размещен дистрибутив клиента, открыт для всех пользователей;
- **/portal** - корневой раздел портала веб-интерфейса, **Личная статистика** веб-интерфейса, открыт для всех, пользователей и настроен как ASP.NET-приложение;
- **/portal/admin** - раздел **Администрирование** веб-интерфейса, открыт только для пользователей группы **Администраторы**;
- **/portal/user** - раздел **Личная статистика** веб-интерфейса, открыт только для пользователей Traffic Inspector.

Если по какой-либо причине настройки разделов сбились или пропали сами разделы, для восстановления их по умолчанию выполните следующие действия:

1. Остановите службу Traffic Inspector.
2. Удалите файлы WWWServConfig.xml и WWWServConfig.bak.xml, расположенные в подпапке **Config** папки установки Traffic Inspector.
3. Запустите службу Traffic Inspector.

Создание и настройка разделов

Для создания и настройки разделов выполните следующие действия:

1. Откройте окно свойств нового или существующего раздела. Сделать это можно из раздела **Сервисы -> Web-сервер -> Разделы** консоли администратора.

2. На вкладке **Раздел сервера** укажите путь к разделу относительно корневого (корневой раздел – "**/**"). Для ввода подраздела к уже существующему разделу введите имя раздела, а после него имя подраздела, например, так: "*/portal/user*".

   Замечание! *Использовать в виртуальных путях русские буквы нельзя, поскольку это может привести к некорректной работе ASP.NET-приложений.*

   По умолчанию для введенного виртуального пути автоматически создается одноименная подпапка в корневом разделе. При необходимости ее можно переопределить, вручную указав произвольную папку на сервере.

3. На вкладке **Опции раздела** включите или выключите функцию просмотра содержимого раздела пользователями программы. От нее зависит, что увидят пользователи, которые будут обращаться не к конкретному файлу, а непосредственно к разделу (при этом в разделе не будет файла по умолчанию). Если функция будет включена, то пользователям будет показано содержимое раздела в виде файлов и папок, а если выключена – страница с ошибкой. При включении функции просмотра можно сделать так, чтобы при обращении пользователя к разделу всегда будет отображаться его содержимое вне зависимости от наличия в нем файла по умолчанию.

   Замечания! *Данные настройки удобно использовать для создания разделов с файловым архивом.*

4. На вкладке **Настройки доступа** определите параметры доступа в веб-серверу с внешних сетей. Доступ может быть полностью закрыт, открыт только для защищенных с помощью SSL-соединений (протокол HTTPS) или полностью открыт (доступ возможен по протоколам HTTP и HTTPS). Здесь же можно разрешить или запретить анонимный доступ (доступ без авторизации), всех активных и отключенных (находящихся в статусах **Стоп**, **Пауза** и **Запрещен**) пользователей Traffic Inspector.

5. На вкладке **Пользователи и группы** настройте доступ к данному разделу. Доступ

можно предоставлять как целым группам, так и отдельным администраторам. Права выдаются с помощью отдельных, независимых друг от друга списков. То есть можно разрешить доступ к разделу всем членам одной или нескольких групп и дополнительно – произвольным администраторам из других групп.

> ***Замечание!*** *Члены групп с ролью* ***Администратор*** *всегда имеют доступ ко всем разделам.*

6. На вкладке **ASP.NET** настройте порядок обработки страниц ASP.NET. Здесь возможны три варианта. Первый из них – наследование. При его выборе способ обработки страниц раздела будет наследоваться от вышестоящего раздела структуры.

   Второй вариант – конфигурирование ASP.NET как отдельного приложения. В этом случае раздел становится корневым для ASP.NET-приложения. Для этого сайта будет запущен отдельный хост-процесс .NET Framework для заданного физического и виртуального пути. Если внутри этого раздела будут добавляться другие разделы, например, для особых настроек по доступу, то для них нужно будет использовать первый вариант обработки страниц. Повторно включать конфигурирование ASP.NET, как отдельного приложения, в подразделах не нужно.

   Третий вариант – обращения пользователей к данному разделу вообще не будут обрабатываться через ASP.NET-хостинг.

Управление перенаправлениями в Traffic Inspector

Перенаправления позволяют переводить запросы пользователей с адресов веб-сервера на другие ресурсы, как внутренние, так и внешние. Список существующих перенаправлений отображается в подразделе **Перенаправления** раздела **Сервисы -> Web-сервер** консоли администратора.

Перенаправления по умолчанию

Для корректной работы веб-интерфейса при установке Traffic Inspector автоматически создается ряд перенаправлений, удалять которые не рекомендуется:

- **/** - перенаправление с корневой страницы веб-интерфейса на раздел **/portal**;
- **/admin/** - перенаправление с адреса **/admin** веб-интерфейса на раздел **/portal/admin/**;
- **/user/** - перенаправление с адреса **/admin** веб-интерфейса на раздел **/portal/user/**.

Создание и настройка перенаправлений

Для создания и настройки перенаправлений выполните следующие действия:

1. Откройте окно свойств нового или существующего перенаправления веб-сервера. Сделать это можно из раздела **Сервисы -> Web-сервер -> Перенаправления** консоли администратора.
2. На вкладке **Запрос** настройте запросы, которые будут перенаправляться веб-сервером на другой адрес. Для этого укажите адрес обращения пользователей относительно корневой страницы веб-интерфейса (например, "*/admin/*"). Также можно выбрать протокол, для которого веб-сервер будет осуществлять перенаправление. Это может быть HTTP, HTTPS или оба сразу.

   Здесь же можно временно заблокировать (запретить) правило, не удаляя его.
3. На вкладке **Перенаправление** настройте адрес, на который будет осуществляться перенаправление запросов, указанных на предыдущем шаге. Он может быть относительным (на раздел веб-сервера, например, "*/portal/admin/*") или абсолютным (адрес любого ресурса в Интернете или локальной сети). Дополнительно можно указать тип перенаправления – временное или постоянное. Первый вариант обычно выбирается при временном перенаправлении, например, ввиду недоступности ресурса. При этом при обращении для метода GET возвращается HTTP-отклик с кодом 302, для POST – 303. Второй вариант используется при постоянном перенаправлении. При этом при обращении возвращается HTTP-отклик с кодом 301.

Веб-интерфейс

Веб-интерфейс представляет собой небольшой сайт, который работает на входящем в состав Traffic Inspector веб-сервере (подробнее см. в п. Общие сведения). Он может

использоваться для решения широкого спектра задач, как пользователями, так и администраторами программы.

Веб-интерфейс состоит из следующих разделов, предназначенных для выполнения различных операций:

- **Администрирование**;
- **Личная статистика**;
- **Клиентский агент**.

Администрирование Traffic Inspector

Данный раздел предназначен для администраторов Traffic Inspector. Пользователь, который не зарегистрирован в программе как администратор, доступа к нему не имеет. В разделе можно выполнять следующие операции:

- Просматривать основную информацию о пользователях программы – параметры тарификации, используемые тарифы, параметры идентификации, действующие ограничения.
- Просматривать список текущих сессий пользователей программы, а также подробную информацию о каждой из них.
- Зачислять на счета пользователей программы оплату.
- Отправлять сообщения всем или выбранным пользователям программы.
- Просматривать отчеты (работа аналогична работе в разделе **Отчеты** консоли администратора, подробнее см. в п. Виды и назначение отчётов).
- Просматривать журналы событий (подробнее см. в п. Журналы событий).
- Просматривать лог изменения администраторов программы.
- Использовать сервис Whois.

Личная статистика пользователя Traffic Inspector

Данный раздел предназначен для пользователей программы и доступен только после авторизации на сервере Traffic Inspector. В нем можно выполнять следующие операции:

- Просматривать основную информацию о себе– параметры тарификации, используемые тарифы, параметры идентификации, действующие ограничения.
- Просматривать различные отчеты о своей работе.

Клиентский агент Traffic Inspector

Доступ в данный раздел возможен без авторизации на сервере Traffic Inspector. В нем можно загрузить дистрибутив клиентского агента Windows (подробнее см. в п. Клиентский агент Windows), а также запустить веб-агент (подробнее см. в п. Веб-агент).

Раздел Администрирование

Раздел **Администрирование** консоли администратора используется для управления правами доступа и настройки пользователей, имеющих право использования консоли. К ним относятся не только непосредственно системные администраторы и администраторы безопасности, но и ряд других сотрудников, которые могут выполнять ограниченный набор действий, например, управлять лимитами пользователей Traffic Inspector, вести учет платежей и пр.

На главной странице раздела **Администрирование** отображен блок **Группы управления**, а также блоки всех созданных ранее групп управления, то есть групп пользователей консоли администратора.

Блок **Группы управления** состоит из двух вкладок. На вкладке **Информация** отображается общее количество созданных групп управления, а также число активных в текущий момент сессий управления (консолей администратора, подключенных к данному серверу Traffic Inspector). Вкладка **Действия** содержит ссылки на операцию создания новой группы (подробнее см. в п. Разграничение доступа) и просмотр сессий управления (см. ниже).

Блок каждой группы управления состоит из двух вкладок. На вкладке **Информация** отображается общее количество пользователей в данной группе. На вкладке **Действия** размещаются ссылки на свойства группы, а также на операцию добавления в нее нового пользователя.

Раздел **Администрирование** состоит из раздела **Сессии** и разделов всех созданных групп управления. В разделе **Администрирование -> Сессии** отображается список всех открытых в данный момент сессий управления. Для каждой сессии показывается имя пользователя, способ его авторизации, уровень доступа, группа управления и прочая информация.

В разделах групп управления отображается список входящих в них пользователей. Также в них доступны различные операции с пользователями консоли администратора (подробно см. в п. Разграничение доступа).

Разграничение доступа

Traffic Inspector предусматривает следующие способы доступа к системе для администрирования, просмотра личной статистики и выполнения прочих действий:

- использование консоли администратора;
- использование веб-интерфейса (см. п. Веб-интерфейс);
- доступ с помощью других приложений через API (см. SDK).

Все учетные записи подразделяются на две большие категории:

- **пользователи Traffic Inspector** (далее пользователи программы) – сотрудники организации, выходящие в Интернет через сервер Traffic Inspector;
- **администраторы** – не только системные администраторы, а все пользователи консоли администратора, которые могут обладать доступом только к определенным ее функциям.

В Traffic Inspector реализованы следующие виды учетных записей администраторов:

- **учетная запись Windows** – задается в системе как учетная запись Windows с указанием компьютера или домена;
- **встроенная учетная запись** – задается в системе как логин и пароль, которые хранятся непосредственно в базе Traffic Inspector;
- **учетная запись пользователя программы** – задается в системе как ассоциация с существующим пользователем программы, используется для доступа только через веб-интерфейс.

Все администраторы Traffic Inspector объединены в группы, в которых задаются их роли и ограничения в правах. В системе реализованы три предопределенные роли:

- **Администратор**. Администраторы имеют полный доступ ко всем возможностям консоли администратора без каких-либо ограничений.
- **Менеджер**. Менеджеры имеют следующие права:
  - ограниченный доступ к функциям биллинга;
  - добавление и удаление пользователей программы в рамках заданных групп;
  - изменение настроек заданных групп (добавление и удаление групп не допускается);
  - просмотр отчетов по пользователям заданных групп.
- **Кассир**. Кассиры имеют следующие права:
  - ограниченный доступ к функциям биллинга;
  - ввод оплаты, изменение персональных настроек тарифов, управление сессиями и выполнение прочих операций, доступных в мониторе работы (подробнее см. в п. Монитор работы: возможности и управление);
  - просмотр отчетов по пользователям заданных групп.

В рамках разграничения доступа администраторов выполняются следующие операции:

- управление группами (см. п. Управление группами);
- управление администраторами (см. п. Управление администраторами).

Доступ через консоль администратора

Доступ через консоль администратора возможен только под заданными учетными записями администраторов. В зависимости от типа пользователя аутентификация возможна по протоколу NTLM (для учетных записей Windows) или логину и паролю (встроенные учетные записи). Пользователи программы доступа к консоли администратора не имеют.

Доступ через веб-интерфейс

В веб-интерфейсе программы можно назначить различные типы доступа для каждого виртуального директория. Возможен и анонимный доступ.

Аутентификация выполняется стандартными средствами веб-сервера через протокол HTTP/SSL, может использоваться Basic и NTLM. Если для виртуального директория разрешен анонимный доступ, то аутентификация и авторизация не выполняются.

В процессе авторизации проверяются все возможные учетные записи. А также проверяется наличие уже имеющейся авторизации пользователя программы с данного IP-адреса. При этом возможна авторизация сразу в двух вариантах одновременно – как администратора и как пользователя программы. Применяется в веб-приложениях, например, в веб-интерфейсе есть два основных раздела – личный для пользователя программы и раздел администратора.

Профили

В Traffic Inspector предусмотрена функция сохранения произвольных данных пользователей программы в профиле. В веб-интерфейсе это используется для сохранения персональных настроек.

Администрирование 5

Профиль – это набор произвольных данных для каждой учетной записи, зарегистрированной в программе. На веб-сервере можно авторизоваться сразу под двумя учетными записями – как администратор и как пользователь программы, отсюда возможен одновременный доступ к двум профилям. Профиль пользователей используется для сохранения настроек в разделе личной статистики, профиль администратора – в разделе администрирования портала.

Для того, чтобы иметь возможность применять определенные настройки сразу для групп профилей (настройки "по умолчанию"), реализованы следующие профили:

- для групп администраторов;
- для всех групп администраторов, в качестве этого профиля выступает предопределенная группа **Администраторы**;
- для всех пользователей программы.

Другими словами, для администраторов есть три уровня иерархии профилей, для пользователей программы – два.

Для управления данными профилей предусмотрены операции очистки и копирования.

Все функции работы с профилями доступны через API, т.е. этот функционал может использовать любое внешнее приложение для хранения своих произвольных данных.

Данные профилей размещаются в базе данных profile.db3. Удаление этого файла приведет к полной очистке данных всех профилей.

Управление группами

Все администраторы Traffic Inspector объединены в группы, в которых задаются их роли и ограничения в правах. Сразу после установки в Traffic Inspector присутствует одна предопределенная группа **Администраторы**. Ее члены обладают полными полномочиями, им доступны все функции консоли администратора. По умолчанию группа настроена таким образом, что в нее автоматически попадают все локальные пользователи.

> ***Замечание!*** *Настоятельно рекомендуется изменить настройки группы* ***Администраторы****, указав конкретные группы Windows или отдельных пользователей. В противном случае возможен несанкционированный доступ к настройкам Traffic Inspector.*

Список существующих групп отображается в разделе **Администрирование** консоли администрирования (подробнее см. в п. Раздел Администрирование). Кроме того, для каждой группы создается свой собственный подраздел в разделе **Администрирование**, в котором отображаются входящие в нее пользователи.

В рамках управления группами администраторов в Traffic Inspector реализованы следующие операции:

- создание/изменение группы администраторов;
- удаление группы администраторов.

Создание/изменение группы администраторов

Для создания новой группы или настройки уже существующей выполните следующие действия:

> ***Замечание!*** *Создавать новые группы могут только администраторы с ролью* ***Администратор****. Настраивать существующие группы могут администраторы с ролями* ***Администратор*** *и* ***Менеджер*** *(только указанные в настройках группы менеджера группы).*

1. Для создания новой группы откройте окно свойств новой или существующей группы администраторов. Сделать это можно в блоке **Группы доступа** и в блоках групп, расположенных в разделе **Администрирование** консоли администратора.
2. На вкладке **Группа** введите название группы и, при необходимости, введите свой комментарий.
3. В Traffic Inspector реализована функция автоматического добавления пользователей. При ее настройке учетные записи из одной или нескольких групп Windows будут

автоматически переноситься в группу администраторов Traffic Inspector. Для настройки этой функции на вкладке **Автодобавление** создайте список групп Windows для импорта учетных записей. Вводить группы можно вручную (вместе с доменом в формате "*domain\group*") или выбирать из списка существующих в системе.

> ***Замечание!*** *При вводе названий групп возможно использование двух макросов:*
>
> - ***** - *любой пользователь Windows;*
> - ***domain** - *любой пользователь из домена domain.*

4. На вкладке **Права группы** укажите роль создаваемой группы: **Администратор**, **Менеджер** или **Кассир** (подробнее о ролях см. в п. Разграничение доступа). Если была выбрана роль **Менеджер** или **Кассир**, то можно указать группы пользователей Traffic Inspector, к которым у создаваемой группы администраторов будет доступ.
5. На вкладке **Профиль** членам данной группы можно разрешить или запретить изменять собственные профили (подробнее про профили см. в п. Разграничение доступа).
6. Сохраните внесенные изменения.

Удаление группы администраторов

Удаления существующей группы администраторов осуществляется с помощью контекстного меню при нажатии правой кнопкой мыши на соответствующем подразделе раздела **Администрирование**.

Управление администраторами

Администраторы в Traffic Inspector могут существовать только в составе групп управления, определяющих их роль и права доступа. Список администраторов каждой группы отображается в соответствующем подразделе раздела **Администрирования** консоли администратора.

В рамках управления администраторами в Traffic Inspector реализованы следующие

операции:

- создание/изменение администратора;
- перенос администратора в другую группу;
- удаление администратора.

Создание/изменение администратора

Для создания или изменения администратора выполните следующие действия:

> ***Замечание!*** *Управлять администраторами могут только администраторы с ролью* ***Администратор****.*

1. Откройте окно свойств нового или существующего администратора. Сделать это можно из подраздела нужной группы раздела **Администрирование** консоли администратора или из блоков, расположенных на главной странице раздела **Администрирование**.
2. Если создается новый администратор, то на вкладке **Тип пользователя** выберите с помощью переключателя нужный вид учетной записи администратора (подробнее об учетных записях администраторов см. в п. Разграничение доступа).

   > ***Замечание!*** *Вид учетной записи определяется при ее создании и в будущем не может быть изменен. Поэтому при редактировании существующего администратора в окне его свойств вкладка* ***Тип пользователя*** *отсутствует.*

3. На вкладке **Учетная запись** укажите параметры учетной записи. Если на предыдущем этапе был выбран тип **Учетная запись Windows**, то введите имя пользователя вместе с именем домена или компьютера (в формате "*Domain\UserName*" или "*CompName \UserName*"). Для встроенной учетной записи укажите имя пользователя и пароль. А для учетных записей пользователей программы – существующую учетную запись пользователя Traffic Inspector, ее можно выбрать из общего списка или найти в окне поиска пользователей (подробнее о поиске пользователей см. в п. Поиск

пользователей).

На этой же вкладке можно временно отключить доступ администратора к консоли администратора, не удаляя при этом его учетную запись.

4. На вкладке **Профиль** настройте параметры сохранения профиля (подробнее о профилях см. в п. Разграничение доступа). Они могут наследоваться от группы или быть персональными. В процессе настройки персональных параметров можно разрешить или запретить администратору сохранять свой профиль.
5. При необходимости на вкладке **Дополнительно** введите свои комментарии к данному администратору.

> ***Замечание!*** *При автоматическом создании учетных записей администраторов (подробнее см. в п. Управление группами) Traffic Inspector записывает в поле* ***Примечание*** *соответствующий комментарий.*

6. Сохраните внесенные изменения.

Перенос администратора в другую группу

Перенос существующего администратора из одной группы в другую осуществляется в подразделе исходной группы раздела **Администрирование** консоли администратора с помощью контекстного меню. В процессе переноса необходимо выбрать группу. При этом у администратора автоматически будут изменены права доступа и настройки, которые берутся из настроек группы. При переносе можно временно заблокировать администратора, не удаляя его учетной записи.

Удаление администратора

Удаление администратора осуществляется в подразделе группы раздела **Администрирование** консоли администратора с помощью контекстного меню.

6 Конфигурирование интернет-соединения и локальной сети

Конфигуратор

Конфигуратор является средством основной настройки Traffic Inspector. Он представляет собой специальный мастер, который позволяет поэтапно установить основные параметры работы сервера, настроить режим работы, службы, сетевые интерфейсы и пр.

Конфигуратор может работать в одном из двух режимов:

- **Настройка конфигурации**;
- **Настройка служб**.

В режиме **Настройка конфигурации** осуществляется установка основных параметров – выбор режима работы сервера, настройка службы маршрутизации и пр. Обычно она выполняется однократно в процессе первоначальной настройки Traffic Inspector (подробнее см. в п. Настройка режима работы).

В режиме **Настройка служб** осуществляется управление службами и сетевыми интерфейсами, настройка NAT и пр. действия (подробнее см. в п. Настройка служб).

Запуск конфигуратора осуществляется с вкладки **Действия** блока **Настройки Traffic Inspector**, размещенного на главной странице раздела **Настройки** консоли администратор. Режим работы конфигуратора выбирается на вкладке **Выбор действия** окна конфигуратора.

> ***Замечание!*** *До настройки конфигурации службы не могут быть настроены. Поэтому при первом запуске конфигуратора вкладка* ***Выбор действия*** *не отображается, а конфигуратор автоматически работает в режиме* ***Настройка конфигурации****.*

Настройка режима работы

Настройка режима работы Traffic Inspector выполняется в конфигураторе следующим образом:

1. Запустите конфигуратор (см. п. Конфигуратор) и на вкладке **Выбор действия** выберите режим работы **Настройка конфигурации**.

> ***Замечание!*** *При первом запуске конфигуратора вкладка* ***Выбор действия***

не отображается, а сам конфигуратор автоматически будет работать в режиме настройки конфигурации.

2. На вкладке **Вариант применения** выберите один из двух возможных режимов работы Traffic Inspector:

   - **Сервер - сетевой шлюз** – режим работы, при котором весь сетевой трафик идет через сервер с Traffic Inspector. Программа в этом режиме играет роль сетевого шлюза. При этом поддерживаются все ее функциональные возможности.

   - **Режим прослушки - внешний шлюз** – режим работы, при котором сетевой трафик идет через внешний (относительно Traffic Inspector) шлюз. При этом сетевая карта сервера с Traffic Inspector работает в режиме прослушивания, а трафик для учета снимается с драйвера программы (предварительно необходимо любым способом направить трафик на эту сетевую карту, например, с помощью порта зеркалирования управляемого коммутатора). Блокировка трафика пользователей возможна при использовании управляемых коммутаторов с поддержкой SNMP. Также возможна работа через прокси Traffic Inspector.

3. Если в качестве варианта применения Traffic Inspector был выбран **Сервер - сетевой шлюз**, то на вкладке **Настройка служб Windows** просмотрите основную информацию о предварительной настройке служб Windows и локальной сети.

4. Если в качестве варианта применения Traffic Inspector был выбран **Сервер - сетевой шлюз**, то на вкладке **Текущая конфигурация** ознакомьтесь с информацией о текущей конфигурации. Обратите внимание, что программа проверит соответствие сервера и запущенных на нем служб требуемым и, при необходимости, выдаст предупреждение о необходимости выполнения тех или иных настроек.

5. Если в качестве варианта применения Traffic Inspector был выбран **Сервер - сетевой шлюз**, то на вкладке **Службы маршрутизации** выберите один из следующих вариантов настройки служб маршрутизации:

   - **Настраивается самостоятельно** – при выборе этого варианта необходимо самостоятельно настроить службы маршрутизации с помощью встроенных средств

Windows.

- **Используется NAT от службы Internet Connection Sharing** – при выборе этого варианта Traffic Inspector будет использовать NAT от службы ICS, причем сама служба будет автоматически настроена программой.

  Замечание! *При использовании данного варианта в процессе конфигурирования внутреннего сетевого интерфейса система может сменить его IP-адрес на свой, что может привести к необходимости перенастройки локальной сети.*

- **Используется NAT от службы Routing and Remote Access Server** - при выборе этого варианта Traffic Inspector будет использовать NAT от серверной службы RRAS, причем основные настройки службы будут выполнены программой автоматически. Данный способ обеспечивает максимальные функциональные возможности.

6. Если в качестве варианта применения Traffic Inspector был выбран **Сервер - сетевой шлюз**, то на вкладке **Windows Firewall** выберите один из следующих вариантов действий с файрволом, входящим в состав Windows:

   - **Не конфигурировать** – Traffic Inspector не будет выполнять никаких действий с Windows Firewall. Выберите этот вариант, если отключаете файрвол самостоятельно или, вопреки рекомендациям, не будете отключать его вообще.

   - **Отключить** – Traffic Inspector автоматически отключит Windows Firewall.

     Замечание! *Во избежание конфликтов настоятельно рекомендуется отключить Windows Firewall, поскольку в составе Traffic Inspector есть собственный файрвол.*

7. Сохраните внесенные изменения.

Настройка служб

Настройка служб выполняется в конфигураторе следующим образом:

1. Запустите конфигуратор (см. п. Конфигуратор) и на вкладке **Выбор действия** выберите

режим работы **Настройка служб Traffic Inspector**.

> ***Замечание!*** *При первом запуске конфигуратора вкладка* ***Выбор действия*** *не отображается, а сам конфигуратор автоматически будет работать в режиме настройки конфигурации. Настройка служб будет доступна только после настройки режима работы (см. п. Настройка режима работы).*

2. На вкладке **Опции конфигурации** с помощью флажков включите или отключите следующие возможности и сервисы Traffic Inspector:

   - **Внешний сетевой экран Traffic Inspector** – это отдельная служба, использующая фильтрацию входящего трафика на внешнем интерфейсе для защиты сервера и локальной сети (подробнее см. в п. Внешний сетевой экран).
   - **Маршрутизация по условию – Advanced Routing** – функция одновременного использования нескольких подключений к Интернету. Обеспечивает направление разного трафика на разные внешние интерфейсы (подробнее см. в п. Advanced Routing - работа с несколькими внешними интерфейсами).

     > ***Замечание!*** *Данная функция имеет смысл, если на сервере с Traffic Inspector есть несколько подключений к Интернету, то есть несколько внешних сетевых интерфейсов.*

   - **RAS сервер** – использование встроенного в службу маршрутизации Windows RAS-сервера, который позволяет подключать клиентов через VPN и различные модемы.
   - **"Публичные" внутренние сети** – включается в том случае, если среди подключенных к серверу с Traffic Inspector локальных сетей есть "не доверенные". При включении этого флажка появляется возможность задавать отдельные правила и внутренние сетевые экраны для публичных и локальных ("доверенных") сетей.
   - **Поддержка VLAN (IEEE 802.1Q)** – поддержка виртуальных Ethernet-сетей на уровне драйвера Traffic Inspector.
   - **DVB карта** – при включении этого флажка становится возможным настроить прием

и передачу данных с разных внешних сетевых интерфейсов (обычно используется в тех случаях, когда получение трафика идет через спутник, а его отправка – по наземному или мобильному каналу передачи).

3. На вкладке **Службы** укажите TCP-порт, на котором будет работать служба HTTP-прокси Traffic Inspector (по умолчанию используется порт 8080), которая включает в себя поддержку протоколов HTTP, HTTPS, FTP (через HTTP/GET).

   Замечание! *Служ бу* HTTP-прокси выключить полностью нельзя. При необходимости можно ограничить доступ к ней пользователей с помощью правил.

   На этой же вкладке включите или отключите службу SOCKS и SMTP-шлюз, указав при этом порты, на которых они будут работать. Служба SOCKS обеспечивает проксирование протокола SOCKS (по умолчанию работает на порту 1080). SMTP-шлюз имеет смысл включать только в том случае, если в локальной сети есть внутренний почтовый сервер и есть необходимость учитывать входящий почтовый трафик этого сервера по пользователям.

4. На вкладке **Внутренние интерфейсы** укажите те сетевые интерфейсы сервера, которые подключены к локальным сетям. Сделать это можно вручную или же автоматически. Во втором случае Traffic Inspector самостоятельно отметит как внутренние те интерфейсы, которые имеют "внутренние" IP-адреса.

5. Если на вкладке **Опции конфигурации** было включено использование "публичных" внутренних сетей, то на вкладке **Тип внутренней сети** отметьте те интерфейсы, которые подключены к "публичным" сетям. При необходимости можно отнести к "публичным" и интерфейс RAS-сервера Windows.

6. На вкладке **Внешние интерфейсы** укажите внешние сетевые интерфейсы (в списке доступных отображаются все сетевые интерфейсы сервера за исключением тех, которые ранее были отмечены как внутренние). Сделать это можно вручную или автоматически. Во втором случае Traffic Inspector самостоятельно отметит как внешние те интерфейсы, которые имеют "внешние" IP-адреса.

Также на этой вкладке включите или выключите автоматическое отнесение интерфейсов к категории внешних. Сделать это можно для интерфейсов, имеющих маршрут по умолчанию, а также для RAS и DialDemand соединений, который не были отмечены в списке администратором.

7. Если на вкладке **Опции конфигурации** был включен внешний сетевой экран, на вкладке **Внешний сетевой экран** укажите те внешние сетевые интерфейсы, для которых экран будет включен (по умолчанию сетевой экран включен для всех внешних интерфейсов).

8. На вкладке **Настройка NAT** укажите те внешние и внутренние сетевые интерфейсы, для которых будет настроена поддержка NAT. Также при необходимости включите конфигурирование интерфейса RAS-сервера Windows. В этом случае интерфейс RAS сервера будет автоматически сконфигурирован даже в том случае, если он не отмечен в списке.

9. Если на вкладке **Опции конфигурации** был включен флажок **Используется DVB карта (Интернет через спутник)**, на вкладке **Интернет через спутник** в выпадающем списке **Выберите интерфейс на прием** укажите сетевой интерфейс DVB-карты, а в выпадающем списке **Выберите интерфейс на передачу** – сетевой интерфейс, по которому осуществляется передача данных спутниковому провайдеру (наземный канал связи, мобильный канал и пр.).

10. На вкладке **Использование DNS** выберите один из возможных режимов использования прокси-сервером DNS.

    - **Нормальный** – стандартный режим, при котором Traffic Inspector максимально используется DNS и доступны все функциональные возможности.

    - **Экономный** – режим, при котором в прокси-сервере имя хоста преобразуется в IP-адрес только после аутентификации и авторизации. При этом исключаются "лишние" DNS-запросы от пользователей, которым не разрешена работа, однако при этом некоторые функциональные возможности могут оказаться недоступными. Например, не будут работать правила "для всех", где имеются в качестве условий IP-адреса и

сети. Также, при выборе данного режима, отключаются все настройки, связанные с DNS.

- **DNS не использовать** – в этом режиме Traffic Inspector, независимо от настроек, не будет работать с DNS.

11. Если сервер удовлетворяет требованиям резервирования каналов (подробнее см. в п. Резервирование каналов), то на вкладке **Резервирование каналов** включите или выключите эту функцию. При включении включите или выключите запуск мастера настройки резервирования (подробнее о данном мастере см. в п. Резервирование каналов).

12. Сохраните внесенные изменения.

Общие настройки пользователей

С помощью общих настроек устанавливаются основные параметры системы по работе с учетными записями пользователей, а также задаются настройки по умолчанию. Настройки по умолчанию автоматически назначаются новым группам и пользователям вне групп (пользователи в группах получают их из настроек групп). Однако, при необходимости, администратор может вручную изменить их как для отдельных пользователей, так и для целых их групп.

Общие настройки пользователей задаются в специальном окне. Для его открытия на главной странице раздела **Пользователи и группы** консоли администратора перейдите в блоке **Пользователи и группы** на вкладку **Действия** и нажмите на ссылку **Общие настройки пользователей**.

Окно общих настроек состоит из следующих вкладок:

- На вкладке **Авторизация** задаются основные параметры авторизации пользователей.
  - В Traffic Inspector реализована возможность автоматического конфигурирования агентов. При ее включении сервер будет принимать и отвечать на широковещательные сообщения от агентов. Процедура позволяет агенту найти сервер, если адрес сервера не указан, и включена опция автоматического поиска сервера (по умолчанию она включена). При установке в одном сегменте сети нескольких серверов

с Traffic Inspector функцию конфигурирования широковещательными сообщениями следует включать только на одном сервере.

- В Traffic Inspector реализована функция самостоятельной смены пароля пользователями через клиентский агент. В общих настройках ее можно разрешить или запретить. Функция смены пароля работает только при авторизации пользователя программы через встроенный логин и пароль. Для Windows-аутентификации она недоступна.
- Если пользователь авторизован через прокси-сервер, то его авторизация удерживается, пока не закрыто TCP-соединение. Если пользователь авторизован агентом, то авторизация подтверждается по каждому запросу данных. В случае если подтверждений нет в течение определенного времени, авторизация отключается. Время таймаута авторизации можно изменять (по умолчанию оно равно 1 минуте).
- В Traffic Inspector реализована интеграция с DHCP, которую можно включить или выключить. При включении интеграции в настройках пользователей становится возможным использовать резервирование в DHCP программой (подробнее см. в п. Создание и настройка пользователей).

- На вкладке **Настройки агентов** настраиваются следующие параметры работы сервера с агентами:
  - Количество секунд, через которые обновляются данные в клиентских агентах.
  - Протокол, по которому работают агенты с явно не заданным протоколом (используется по умолчанию) – UDP, HTTP или SSL. Эту настройку агенты получают в процессе процедуры автоконфигурирования.
  - Запрет или разрешение работы старых агентов, которые не поддерживают протокол обмена данными v.2.
  - Обычно в агентах отображается информация о текущем балансе их лицевых счетов. В общих настройках можно выключить отображение баланса для тех пользователей, для которых активирован безлимитный доступ.

- По умолчанию, в процессе аутентификации агентом выполняется проверка системного времени (сравнивается системное время на компьютере пользователя и сервере). При необходимости ее можно отключить. Рекомендуется сделать, если возможно подключение пользователей с системным временем, отличающимся от системного времени сервера.

  Замечание! *Выключение данного флажка снижает безопасность механизма аутентификации.*

- На вкладке **Автодобавление** настраиваются параметры автоматического добавления пользователей в базу Traffic Inspector. Данная функция работает для пользователей, которые успешно прошли Windows-аутентификацию, но не найдены среди пользователей Traffic Inspector. Она доступна только при использовании интегрированной Windows-аутентификации (NTLM).

  - Функцию автодобавления можно включить или выключить в зависимости от конкретных условий использования Traffic Inspector.

  - Можно указать группу Windows, члены которой будут автоматически добавляться в базу Traffic Inspector. Это может быть как группа домена, так и локальная группа.

    Замечание! *По умолчанию пользователи добавляются в список вне групп. Для того чтобы можно было отдельных пользователей добавлять в разные группы, в настройках групп пользователей имеются соответствующие настройки (подробнее см. в п. Создание и настройка групп).*

    При добавлении пользователей будут прописываться настройки по умолчанию, соответствующие группе, куда они добавляются. В настройках тарифа можно задать настройки по умолчанию. В этом случае пользователю на счет может добавляться сумма и задаваться доступ с автоотключением, в противном случае включается безлимитный доступ.

- На вкладке **Расписание** можно указать дни недели и часы, когда пользователям будет

разрешена работа в Интернете. В строках отображаются дни недели, а в столбцах - время суток (для просмотра времени суток, за которое отвечает данный столбец, наведите мышку на верхнюю строку кнопок). Синим цветом отмечены разрешенные часы, серым – запрещенные. Для изменения статуса целого дня нажмите на соответствующую кнопку в первом столбце, определенного часа во все дни недели – на кнопку в первой строке, а для изменения статуса конкретного часа в определенный день недели – на соответствующую ячейку таблицы.

- Вкладка **Сетевая статистика** предназначена для настройки параметров сохранения сетевой статистики (подробнее о сетевой статистике см. в п. Управление сетевой статистикой).
  - Запись сетевой статистики можно разрешить или запретить в зависимости от необходимости.
  - При разрешении сбора сетевой статистики можно установить частоту ее записи в базу данных журнала (в минутах).
  - При разрешении сбора сетевой статистики можно установить количество записываемых активных направлений из коллектора.
  - При разрешении сбора сетевой статистики можно указать минимальное количество исходящих и входящих пакетов, которое необходимо для записи данных коллектора (если количество зафиксированных пакетов данных менее заданного, то запись не выполняется).
  - При необходимости можно включить блокировку пользователей при превышении в сетевой статистики определенного количества записей. При включении этой функции необходимо указать время, на которое пользователь будет заблокирован (в минутах).
  - По умолчанию в сетевую статистику попадает только неотфильтрованный и тарифицированный трафик. Однако, при необходимости можно включить запись всего трафика без исключений. Это может быть полезным для фиксации дополнительных событий нарушения правил авторизации.

Замечание! *Включение данной возможности существенно увеличивает объем анализируемых данных и может привести к повышению нагрузки на процессор. При ограниченных ресурсах рекомендуется только для отладки.*

- Вкладка **Контроль нарушений** позволяет настроить функцию контроля нарушений политики авторизации.
  - При включении функции контроля нарушений политики авторизации сетевая статистика записывается в отдельный коллектор. При этом можно указать промежутки времени (в минутах), через которые будет осуществлять запись, и количество активных направлений.
  - При необходимости можно включить блокировку пользователей, нарушивших политики авторизации. При включении этой функции необходимо указать время, на которое пользователь будет заблокирован (в минутах).
- На вкладке **Фильтрация** задаются настройки фильтрации трафика.
  - Трафик наружу по умолчанию может быть разрешен или запрещен. В первом случае будет разрешена передача любого трафика, за исключением того, для которого были созданы запрещающие правила (данный вариант используется по умолчанию). Во втором случае, наоборот, передача любого трафика наружу будет запрещена. Однако можно создавать разрешающие правила для отдельных видов трафика (подробнее см. в п. Виды и предназначение правил, наборы правил).
  - Такую же настройку можно сделать для пользователей, которые работают в кредит. Она не будет распространяться на лиц с положительным балансом лицевого счета.
- Вкладка **HTTP мимо прокси** используется для настройки обработки трафика по протоколу HTTP мимо прокси-сервера Traffic Inspector. Настройка для авторизованных и неавторизованных (в том числе для трафика, разрешенного разрешающими фильтрами **Для всех**) пользователей осуществляется отдельно друг от друга аналогичным образом.
  - Можно включить безусловное перенаправление всех запросов, получаемых сервером на порт TCP 80, на прокси-сервер Traffic Inspector.

- Можно включить безусловную блокировку всех HTTP-запросов, получаемых мимо прокси-сервера.

- На вкладке **Перенаправление TCP** включаются и отключаются правила перенаправления TCP-соединений со стороны пользователей (подробнее см. в п. Перенаправление запросов).

- Вкладка **Ограничения** предназначена для настройки следующих ограничений:

  - Можно установить максимально допустимое количество одновременных TCP-сессий для одного пользователя (значение 0 – без ограничений).

  - В прокси-сервере есть функция проверки наличия атрибута RANGE в запросе (запросы на многопоточную загрузку). Это позволяет при необходимости запретить многопоточную загрузку через HTTP-прокси.

  - При необходимости можно ограничить скорости подключения к Интернету пользователей. Ограничения задаются в специальном окне. В нем можно настраивать лимиты на входящую и исходящую скорости для обычной работы и работы в кредит (в Кбит/с), а также ограничения на количество передаваемых пакетов в секунду.

- На вкладке **Уровни фильтрации** можно задать наименования четырех стандартных уровней фильтрации, которые отображаются в агентах пользователей и на страницах браузера при срабатывании блокировки (подробнее об уровнях фильтрации см. в п. Виды правил и операции с ними). Ввести наименование можно вручную или быстро вернуться к значениям по умолчанию.

- На вкладке **Запись в журнал** задается частота записи состояния пользователя в базу данных журналов. Периодичность в отчетах влияет на степень детализации динамики работы пользователя. Чем чаще производятся записи, тем подробнее будут отчеты, но и больше данных будет записываться в базу данных. Если периодическую запись отключить, то она будет осуществляться только раз в сутки и при изменении состояния пользователя.

Управление пользователями 7

Создание и настройка групп

Объединение пользователей в группы позволяет создавать единые настройки, которые актуальны для всех членов группы. Настройки могут быть установлены по умолчанию, в этом случае они берутся из общих настроек (подробнее см. в п. Общие настройки пользователей). Также их можно настраивать для каждой группы индивидуально.

В Traffic Inspector существует предопределенная группа **Пользователи вне группы**. В нее автоматически помещаются пользователи, не входящие ни в одну из созданных администратором групп. Свойства предопределенной группы можно настраивать обычным образом, однако удалить ее невозможно.

Для каждой группы в разделе **Пользователи и группы** консоли администратора создается свой подраздел. В нем отображается список входящих в нее пользователей с краткой информацией по каждому из них. Также для каждой группы на главной странице раздела **Пользователи и группы** создается свой блок, состоящий из двух вкладок. На вкладке **Информация** отображается количество членов группы, а на вкладке **Действие** – ссылки на доступные операции.

В рамках управления группами пользователей в Traffic Inspector реализованы следующие операции:

- создание/изменение группы;
- настройка атрибутов группы;
- добавление в группу пользователей;
- удаление группы.

Создание/изменение группы

Для создания новой или редактирования уже существующей группы выполните следующие действия:

1. Откройте окно свойств новой или существующей группы. Сделать это можно в блоке **Пользователи и группы** или в блоке самой группы, которые расположены на главной

странице раздела **Пользователи и группы** консоли администратора.

2. На вкладке **Наименование** в поле введите название группы (оно должно быть уникальным) и, при необходимости, произвольный комментарий. Если создается новая группа, то на вкладке **Наименование** можно включить установку всех параметров по умолчанию. В этом случае больше никаких настроек для создания группы выполнять не нужно, все они будут автоматически загружены из общих настроек (подробнее см. в п. Общие настройки пользователей). В противном случае на следующих вкладках будет необходимо установить собственные параметры группы.

   При редактировании группы возможность загрузки параметров по умолчанию отсутствует. Редактирование осуществляется путем ручного изменения параметров на следующих вкладках.

3. На вкладке **Авторизация** настройте опции авторизации членов данной группы. Они могут загружаться из общих настроек пользователей или же быть у группы собственными. При использовании второго варианта разрешите или запретите самостоятельную смену паролей пользователем и установите таймаут авторизации (подробнее об этих параметрах см. в п. Общие настройки пользователей). При необходимости, членам группы можно запретить авторизацию через прокси или с использованием SOCKS.

4. На вкладке **Настройки агентов** настройте XSL-шаблон, который определяет внешний вид агентов у членов группы. Его можно указать вручную или использовать заданный по умолчанию (подробнее см. в п. Настройка веб-сервера).

   Агенты Traffic Inspector могут автоматически конфигурировать браузеры клиентов для доступа к Интернету. Если эта функция необходима членам группы, то включите ее, а если она не нужна, то выключите. Также можно настроить загрузку данного параметра из настроек по умолчанию (общая настройка, которая разрешает или запрещает операцию, задается в настройках прокси-сервера, подробнее см. в п. Основные настройки прокси-сервера).

   На этой же вкладке включите или отключите проверку системного времени при аутентификации членов группы (подробнее о данной функции см в п. Общие

настройки пользователей). Или включите использование значения, заданного в общих настройках.

5. При необходимости на вкладке **VLAN** задайте единый идентификатор виртуальной сети для всех членов группы. В противном случае укажите значение "0".

6. Если в данную группу возможно автодобавление пользователей, то на вкладке **Автодобавление** укажите доменную или локальную Windows-группу, соответствующую редактируемой.

   Замечание! *Windows-группу предварительно необходимо добавить на вкладке Автодобавление окна общих настроек пользователей. При автодобавлении, прежде всего, проверяется членство в Windows-группе Windows, заданной в общих настройках. Именно этим определяется, разрешена ли данная функция для клиента. А затем проверяется членство в группе, заданной в настройках группы. Таким образом, происходит управление добавлением нового клиента в группу.*

7. На вкладке **Тарификация** настройте тариф, который должен использоваться для членов группы. В его качестве можно выбрать тариф по умолчанию (подробнее см. в п. Тарифы) или же указать произвольный тариф из списка ранее созданных.

   По умолчанию для пользователей в Traffic Inspector используются персональные лицевые счета. При этом все правила и блокировки срабатывают персонально. Если есть необходимость, включите ведение группового учета и укажите предварительно созданный коллективный счет (подробнее см. в п. Коллективные счета). В этом случае в процессе тарификации расходы будут списываться не с персональных счетов членов группы, а с общего коллективного счета.

8. На вкладке **Расписание** настройте расписание доступа членов группы к Интернету. Оно может загружаться из общих настроек пользователя или задаваться для данной группы индивидуально (подробнее о работе на вкладке см. в п. Общие настройки пользователей).

9. На вкладке **Сетевая статистика** настройте параметры сохранения сетевой статистики членов группы. Они могут загружаться из общих настроек пользователя или задаваться для данной группы индивидуально (подробнее о параметрах см. в п. Общие настройки пользователей).

10. На вкладке **Контроль нарушений** настройте параметры блокировки членов группы при выявлении нарушений политики авторизации. Они могут загружаться из общих настроек пользователя или задаваться для данной группы индивидуально (подробнее о параметрах см. в п. Общие настройки пользователей).

11. На вкладке **Фильтрация** настройте параметры фильтрации трафика членов группы. Они могут загружаться из общих настроек пользователя или задаваться для данной группы индивидуально (подробнее о параметрах см. в п. Общие настройки пользователей).

12. На вкладке **Правила группы "до"** укажите правила, которые будут действовать для всех членов группы до индивидуальных правил, назначенных конкретным пользователям. При необходимости включите автоматическую трансляцию для группы правил, заданных в общих настройках правил (подробнее см. в п. Внутренний сетевой экран). Дополнительно к этим правилам можно назначить свои. Добавлять можно как отдельные правила, так и целые их группы.

13. На вкладке **Правила группы "после"** укажите правила, которые будут действовать для всех членов группы после индивидуальных правил, назначенных конкретным пользователям. Настройка осуществляется так же, как и настройка правил "до" (см. выше).

14. На вкладке **HTTP мимо прокси** настройте параметры обработки трафика по протоколу HTTP мимо прокси-сервера для членов группы. Они могут загружаться из общих настроек пользователя или задаваться для данной группы индивидуально (подробнее о параметрах см. в п. Общие настройки пользователей).

15. На вкладке **TCP перенаправления** настройте параметры перенаправления TCP-

соединений для членов группы. Они могут загружаться из общих настроек пользователя или задаваться для данной группы индивидуально (подробнее о параметрах см. в п. Общие настройки пользователей).

16. На вкладке **Ограничения** настройте ограничения, действующие для членов группы. Они могут загружаться из общих настроек пользователя или задаваться для данной группы индивидуально (подробнее об ограничениях см. в п. Общие настройки пользователей).

    Дополнительно к этим ограничениям включите или отключите доступ членов группы к различным службам Traffic Inspector.

17. На вкладке **Шейпер** настройте ограничения по скорости доступа членов группы к Интернету. Индивидуальные ограничения для членов группы могут загружаться из общих настроек пользователей или задаваться для данной группы индивидуально (подробнее о параметрах см. в п. Общие настройки пользователей). Суммарные ограничения на группу позволяют установить доступную всей группе полосу пропускания. Суммарные ограничения задают отдельно на прием и передачу трафика.

    Замечание! *Доступная группе полоса пропускания делится между всем активными в данный момент членами пропорционально, однако, с учетом индивидуальных ограничений конкретных пользователей.*

18. Если трафик всех членов группы нужно направлять наружу через определенный внешний интерфейс, то выберите его на вкладке **Роутинг**.

19. На вкладке **SMTP** настройте параметры фильтрации сообщений членов группы на SMTP-шлюзе. Они могут загружаться из общих настроек пользователя (подробнее см. в п. Общие настройки пользователей) или задаваться для данной группы индивидуально (подробнее см. в п. Создание и настройка групп).

20. При необходимости настройте на вкладке **Автоматизация** выполнение скриптов автоматизации и других операций для членов группы. Если нужно чтобы при изменении состояния пользователя система автоматически выполняла определенное

действие, то включите запуск соответствующего скрипта (подробнее о скриптах см. в SDK). С помощью этой функции можно, например, настроить рассылку уведомлений о блокировке/разблокировании пользователей и пр. Также, при необходимости, включите реагирование системы на превышение заданных в тарифе пользователя лимитов (подробное описании тарифов см. в п. Тарифы). При включении укажите одно из двух возможных действий – блокирование счета пользователя или выполнение указанного скрипта.

21. На вкладке **Запись в журнал** настройте параметры записи данных о состоянии членов группы в базу данных журналов. Они могут загружаться из общих настроек (подробнее см. в п. Общие настройки пользователей) и настроек прокси-сервера (подробнее см. в п. Основные настройки прокси-сервера) или задаваться для данной группы индивидуально.

22. Сохраните внесенные изменения.

Настройка атрибутов группы

Атрибуты используются для хранения любой дополнительной информации объекта конфигурации (подробнее см. в п. Атрибуты). Изменение атрибутов группы осуществляется в специальном окне, запустить которое можно в блоке группы на главной странице раздела **Пользователи и группы**. В этом окне отображается список всех атрибутов, которые могут устанавливаться для групп пользователей. Значения атрибутов можно вводить вручную или выбирать в выпадающем списке (для некоторых типов атрибутов) их значение.

Добавление пользователей в группу

Добавление пользователей в созданные группы описано в п. Создание и настройка пользователей.

Удаление группы

Удаление группы выполняется с помощью контекстного меню, вызываемого при нажатии правой кнопкой мыши на соответствующем подразделе раздела **Пользователи и группы**. Если при удалении в группе были пользователи, то они будут перенесены в специальную группу **Пользователи вне группы**.

Создание и настройка пользователей

Списки пользователей отображаются в подразделах групп в разделе **Пользователи и группы** консоли администратора. Для каждого пользователя показывается его имя, логин, IP- и MAC-адреса, а также адрес электронной почты. Помимо этого в подразделах групп отображается панель со списком всех правил, которые действуют для выбранного в данный момент пользователя– правила группы (подробнее см. в п. Создание и настройка групп) и персональные правила.

В рамках управления пользователями в Traffic Inspector реализованы следующие операции:

- создание/изменение учетной записи пользователя;
- изменение типа учетной записи пользователя;
- изменение группы учетной записи пользователя;
- настройка атрибутов учетной записи пользователя;
- удаление учетной записи пользователя.

Создание/изменение учетной записи пользователя

Для создания новой или редактирования уже существующей учетной записи пользователя выполните следующие действия:

1. Откройте окно свойств новой или существующей учетной записи пользователя. Если нужно создать новую учетную запись пользователя в группе, то вызывать окно свойств следует из подраздела нужной группы в разделе **Пользователи и группы** консоли

администратора или из блока этой группы, который размещен на главной странице раздела **Пользователи и группы**.

2. Если создается новый пользователь, то на вкладке **Способ подключения** укажите один из возможных типов пользователя:

   - **Прямое подключение** – выберите, если пользователь подключен непосредственно к локальной сети, в которой работает сервер Traffic Inspector;
   - **Подключение через RAS сервер Windows** – выберите, если пользователь подключается к локальной сети через RAS-сервер посредством VPN или какого-либо модема;
   - **Только почтовый трафик** – выберите, если создаваемый пользователь будет использоваться только для учета почтового трафика SMTP-шлюза (авторизация на сервере для таких пользователей недоступна).

3. Если создается новый пользователь, то на вкладке **Способ авторизации** выберите и настройте способ авторизации пользователя на сервере Traffic Inspector.

   - **Учетная запись (логин) Windows** – выберите этот вариант, если авторизация пользователя будет осуществляться на основе его Windows-логина. Для его настройки в поле **Логин** введите Windows-логин в формате "Domain\UserName". Можно указывать домен Windows или имя компьютера. Если домен не указан, то используется домен по умолчанию. Если сервер является членом домена, то пишется имя этого домена. Если нет, то по умолчанию подразумевается локальный логин, и используется имя компьютера. Пароль для Windows-авторизации вводить не надо. Также при выборе данного варианта можно включить флажок **Загрузить данные из Active Directory**. При этом в свойства пользователя из Active Directory будут автоматически загружены его имя и адрес электронной почты.
   - **Учетная запись (логин) Traffic Inspector** – выберите этот вариант, если авторизация пользователя будет осуществляться по данным, заданным в полях **Имя** и **Пароль**.

- **IP-адрес пользователя или диапазон адресов** – при выборе этого варианта будет осуществляться автоматическая авторизация пользователя по его IP-адресу.
- **MAC адрес** – при выборе этого варианта будет осуществляться автоматическая авторизация пользователя по его MAC-адресу.

4. На вкладке **Наименование** введите отображаемое имя пользователя (оно будет использоваться в консоли администратора, агенте, отчетах и т.д.) и, при необходимости, произвольное примечание. Здесь же можно временно запретить работу пользователя, не удаляя его учетную запись.

   Если создается новый пользователь, то определите, как будет настраиваться большая часть параметров – загружаться из настроек группы и/или общих настроек или определяться вручную администратором. При выборе первого варианта в окне свойств остаются только несколько вкладок с параметрами, которые необходимо настроить. При выборе второго – в окне будут отображены все вкладки со всеми параметрами пользователя. При изменении существующего пользователя все вкладки отображаются всегда.

5. На вкладке **Авторизация** настройте параметры авторизации пользователя. Можно настроить как один, так и несколько способов авторизации. Во втором случае авторизация будет осуществляться по комбинации признаков. Возможными признаками являются заданные логин и пароль, IP-адрес (конкретный адрес или диапазон адресов), MAC-адрес.

   При необходимости с помощью флажка **Вносить MAC и IP в таблицу стека TCP/IP** включите регистрацию статических ARP-записей. Она позволяет обеспечить лучшую защиту авторизации, т.к. стек TCP-/IP-системы на пакеты с другой комбинацией MAC +IP реагировать не будет. Это также ускоряет работу сети, т.к. стеку TCP/IP не требуется определение сетевых адресов путем рассылки ARP-запросов. Информация о внесении статической ARP-записи для пользователя отображается в мониторе работы.

   При необходимости разрешите Traffic Inspector добавлять резервирование в DHCP (при использовании авторизации IP+MAC).

Замечание! *Функция резервирования в DHCP доступна только в том случае, если на вкладке Авторизация общих настроек включена интеграция с DHCP (подробнее см. в п. Общие настройки пользователей).*

6. Если требуется тарификация через SMTP-шлюз, то на вкладке **E-Mail** укажите адреса для SMTP-шлюза. Если клиент прописан с логином Windows и использует Active Directory, то все его адреса электронной почты можно загрузить из Active Directory. Если другие параметры авторизации, кроме как по адресу электронной почты, не указаны, то клиент получает особый тип авторизации по e-mail. Такого клиента можно использовать только для учета почтового трафика.

7. Определите на вкладке **Доступ** тип доступа пользователя, выбрав один из двух вариантов:

   - **Безлимитный** – пользователь сможет работать вне зависимости от текущего баланса;
   - **Автоотключение** – при окончании денег на счету работа пользователя будет заблокирована (однако возможна настройка работы в кредит).

   При необходимости здесь же определите период времени, в течение которого пользователю будет разрешена работа.

8. При необходимости на вкладке **VLAN** задайте единый идентификатор виртуальной сети для всех членов группы. В противном случае укажите на той вкладке значение "0". Или включите загрузку данного параметра по умолчанию из настроек группы или общих настроек.

9. При необходимости на вкладке **Опции авторизации** разрешите или запретите самостоятельную смену пароля пользователем и установите таймаут авторизации. Или включите загрузку данного параметра по умолчанию из настроек группы или общих настроек.

10. При необходимости на вкладке **Настройка агента** настройте параметры работы агента. Вкладка аналогична соответствующей вкладке окна свойств группы (см. п. Создание и настройка групп).

11. При необходимости на вкладке **Тарификация** настройте параметры работы агента. Вкладка аналогична соответствующей вкладке окна свойств группы (см. п. Создание и настройка групп). Если необходимо, чтобы в мониторе работы нельзя было остановить работу пользователя, то включите флажок **Блокировать остановку работы**.

12. При необходимости на вкладке **Расписание** настройте расписание работы пользователя. Вкладка аналогична соответствующей вкладке окна свойств группы (см. п. Создание и настройка групп).

13. При необходимости на вкладке **Сетевая статистика** настройте параметры записи сетевой статистики пользователя. Вкладка аналогична соответствующей вкладке окна свойств группы (см. п. Создание и настройка групп).

14. При необходимости на вкладке **Контроль нарушений** настройте параметры контроля нарушений политик авторизации пользователем. Вкладка аналогична соответствующей вкладке окна свойств группы (см. п. Создание и настройка групп).

15. При необходимости на вкладке **Фильтрация** настройте параметры фильтрации трафика пользователя. Для этого установите индивидуальный минимальный уровень фильтрации из четырех возможных. Также можно для данного пользователя отключить запрещающие IP-правила и внутренний сетевой экран.

16. На вкладке **Правила** настройте действующие для пользователя правила. Добавлять в список можно как отдельные правила, так и целые их группы. Также укажите, будут или нет на данного пользователя распространяться правила "до" и "после" его группы (подробнее см. в п. Создание и настройка групп).

17. При необходимости на вкладке **HTTP мимо прокси** настройте обработку трафика по протоколу HTTP мимо прокси-сервера для пользователя. Вкладка аналогична соответствующей вкладке окна свойств группы (см. п. Создание и настройка групп).

18. При необходимости на вкладке **TCP перенаправления** выберите перенаправления TCP-соединений для пользователя. Вкладка аналогична соответствующей вкладке окна свойств группы (см. п. Создание и настройка групп).

19. При необходимости на вкладке **Ограничения** настройте ограничения для

пользователя. Вкладка аналогична соответствующей вкладке окна свойств группы (см. п. Создание и настройка групп).

20. При необходимости на вкладке **Шейпер** настройте индивидуальные ограничения по скорости передачи данных для пользователя. Для этого введите нужные лимиты на входящую и исходящую скорости для обычной работы и работы в кредит (в Кбит/с), а также ограничения на количество передаваемых пакетов в секунду. Или включите загрузку ограничений из настроек группы.

21. При необходимости на вкладке **Роутинг** выберите внешний интерфейс, через который нужно направить трафик пользователя. Вкладка аналогична соответствующей вкладке окна свойств группы (см. п. Создание и настройка групп).

22. При необходимости на вкладке **SMTP** настройте параметры фильтрации сообщений пользователя SMTP-шлюзом. Вкладка аналогична соответствующей вкладке окна свойств группы (см. п. Создание и настройка групп).

23. При необходимости на вкладке **Автоматизация** настройте параметры автоматизации управления доступом пользователя к Интернету. Вкладка аналогична соответствующей вкладке окна свойств группы (см. п. Создание и настройка групп).

24. При необходимости на вкладке **Запись журнал** настройте параметры записи в журнал данных о состоянии пользователя. Вкладка аналогична соответствующей вкладке окна свойств группы (см. п. Создание и настройка групп).

25. Сохраните внесенные изменения.

Изменение типа учетной записи пользователя

Данная операция позволяет не только отредактировать параметры пользователя, но и изменить его способы подключения и авторизации (при обычном редактировании это сделать нельзя). Запускается она из контекстного меню в подразделе группы пользователя раздела **Пользователи и групп** консоли администратора. Изменение типа пользователя выполняется в окне свойств пользователя, которое аналогично окну свойств нового пользователя (см. выше).

Изменение группы учетной записи пользователя

Учетную запись существующего пользователя можно переместить в другую группу. При этом все его настройки, оставленные по умолчанию, будут сменены на настройки из новой группы. Индивидуальные настройки останутся неизменными. Смена группы выполняется в специальном окне, открывающемся с помощью контекстного меню, вызываемого при клике правой кнопкой мыши на нужном пользователе (в подразделе исходной группы раздела **Пользователи и группы**). В этом окне указывается новая группа. Также одновременно в нем можно на время заблокировать пользователя, не удаляя его учетную запись, изменить тип доступа (безлимитный или автоотключение), а также задать ограничение на доступ по датам.

Настройка атрибутов учетной записи пользователя

Атрибуты используются для хранения любой дополнительной информации объекта конфигурации (подробнее см. в п. Атрибуты). Изменение атрибутов пользователя осуществляется в специальном окне, запустить которое можно с помощью контекстного меню, вызываемого при клике правой кнопкой мыши на нужном пользователе (в подразделе его группы раздела **Пользователи и группы**). В этом окне отображается список всех атрибутов, которые могут устанавливаться для пользователей. Значения атрибутов можно вводить вручную или выбирать в выпадающем списке (для некоторых типов атрибутов) их значение.

Удаление учетной записи пользователя

Удаление учетной записи пользователя выполняется с помощью контекстного меню, вызываемого при клике правой кнопкой мыши на нужном пользователе (в подразделе его группы раздела **Пользователи и группы**).

Управление пользователями 7

Импорт пользователей

В Traffic Inspector реализована возможность импорта пользователей программы из Active Directory или результатов сканирования локальной сети. С ее помощью можно быстро зарегистрировать в системе больше количество пользователей.

Импорт пользователей из Active Directory

Данная операция позволяет загрузить список учетных записей пользователей из Active Directory. В процессе ее выполнения создаются пользователи с авторизацией по учетной записи Windows (подробнее см. в п. Способы авторизации пользователей). Для импорта пользователей выполните следующие действия (необходимо, чтобы контроллер домена был доступен серверу Traffic Inspector).

1. Запустите мастер импорта пользователей. Сделать это можно из блока **Пользователи и группы** одноименного раздела консоли администратора.
2. На вкладке **Выбор режима** выберите вариант **Импорт пользователей Windows**.
3. На вкладке **Подключение к AD** настройте параметры доступа к контроллеру домена. Для подключения к текущему домену (домену, к которому относится сервер Traffic Inspector) никаких дополнительных параметров можно не указывать – подключение будет осуществлено автоматически от имени пользователя, от которого запущена служба Traffic Inspector. Также можно использовать произвольные параметры подключения – полное имя домена, полное имя контроллера домена, логин и пароль пользователя.
4. На вкладке **Параметры пользователей** выберите группу, в которую будут записаны отобранные пользователи (или не выбирайте, чтобы они попали в группу **Пользователи вне группы**, см. подробнее в п. Создание и настройка групп), тип доступа (безлимитный или автоотключение, подробнее см. в п. Создание и настройка пользователей) и разрешите или запретите их работу после создания.
5. Запустите процесс создания пользователей и дождитесь его завершения.

Импорт пользователей из результатов сканирования сети

Данная операция может использоваться для локальных сетей, в которых нет развернутого домена Windows. С ее помощью можно быстро создать пользователей с авторизацией по IP-адресу, MAC-адресу или комбинации этих параметров. Для импорта пользователей выполните следующие действия:

1. Запустите мастер импорта пользователей. Сделать это можно из блока **Пользователи и группы** одноименного раздела консоли администратора.
2. На вкладке **Выбор режима** выберите вариант **Сканирование сети**.
3. На вкладке **Сканирование сети** выберите подсеть, которая будет сканироваться. Доступны подсети всех сетевых интерфейсов Traffic Inspector, которые были указаны как внутренние. После завершения сканирования в списке будут отображены все найденные клиенты. Для каждого из них показывается имя хоста (если он есть), IP-адрес, MAC-адрес и пользователь программы (если для данного IP-адреса в Traffic Inspector уже существует пользователь). Отметьте нужные клиенты, которые нужно зарегистрировать в Traffic Inspector.
4. На вкладке **Параметры пользователя** выберите группу, в которую будут записаны отобранные пользователи (или не выбирайте, чтобы они попали в группу **Пользователи вне группы**, см. подробнее в п. Создание и настройка групп). Здесь же выберите способ их авторизации (IP-адрес, MAC-адрес или IP-адрес+MAC-адрес, подробнее см. в п. Способы авторизации пользователей), тип доступа (безлимитный или автоотключение, подробнее см. в п. Создание и настройка пользователей) и разрешите или запретите их работу после создания.
5. Запустите процесс создания пользователей и дождитесь его завершения.

Поиск пользователей

Поиск пользователей осуществляется с помощью специального окна **Выбор пользователей**, вызвать которое можно из контекстного меню, из некоторых других окон и с помощью иконки, расположенной на панели инструментов консоли администратора.

Для поиска пользователей выполните следующие действия.

1. Запустите одним из вышеперечисленных пользователей окно **Выбор пользователей**.
2. На вкладке **Тип поиска пользователей** выберите один из трех вариантов поиска:
   - **По имени** – поиск осуществляется по текстовым параметрам пользователей;
   - **По IP адресу** – в процессе поиска проверяется, соответствует ли IP-адрес пользователя заданному;
   - **По MAC адресу** – в процессе поиска проверяет соответствие MAC-адреса сетевой карты пользователя заданному.
3. В зависимости от выбранного на предыдущем шаге типа поиска на вкладке **Поиск по имени**, **Поиск по IP адресу** или **Поиск по MAC адресу** настройте его параметры.
   - Для поиска по имени введите искомую строку (или символ "*" для поиска любой строки) и укажите способ сравнения – полное совпадение, поиск по началу строки (срабатывает, если введенная строка является началом значения параметра) или по ключевому слову (срабатывает, если введенная строка входит в состав значения параметра). При необходимости настройте область поиска, указав параметры пользователей, в которых будет осуществляться поиск.
   - Для поиска по IP-адресу введите искомый адрес и определите область поиска. Поиск может осуществляться среди IP-адресов, заданных в параметрах авторизации пользователей, и среди IP-адресов, с которых были авторизованы пользователи по имени или MAC-адресу.

     Замечание! *Для поиска долж на быть выбрана как минимум одна из двух перечисленных областей поиска.*

   - Для поиска по MAC-адресу введите искомый адрес.
4. На вкладке **Выбор групп** отметьте флажками те группы, в которых будет осуществляться поиск.
5. Запустите поиск и дождитесь его завершения. Список найденных пользователей будет

отображен на вкладке **Выбор пользователя**.

Атрибуты

Атрибуты используются для хранения любой дополнительной информации объекта конфигурации. Они могут быть определены для пользователей, групп пользователей, коллективных счетов и внешних счетчиков. Например, это могут быть любые дополнительные настройки, внутренние промежуточные данных скриптов автоматизации, модулей расширения или сторонних приложений.

Данные атрибутов могут отображаться в виде дополнительных колонок в списках пользователей, групп, коллективных счетов, внешних счетчиках, а также в мониторе работы пользователей и внешних счетчиков. В этих разделах консоли также имеется возможность редактирования и просмотра данных атрибутов в отдельном окне.

Все операции с атрибутами также доступны через API (см. SDK).

Список существующих в системе атрибутов расположен в разделе **Объекты -> Атрибуты** консоли администратора. С помощью иконок, расположенных на панели инструментов, список можно фильтровать по области применения атрибутов (например, атрибуты для пользователей, групп пользователей и пр.).

В рамках управления атрибутами в Traffic Inspector реализованы следующие операции:

- создание/изменение атрибута;
- очистка данных атрибута;
- удаление атрибута.

Создание/изменение атрибута

Для создания нового или изменения существующего атрибута выполните следующие действия:

1. Откройте окно свойств существующего или нового атрибута. Сделать это можно из блока **Атрибуты**, расположенного на главной странице раздела **Объекты** консоли администратора или с помощью контекстного меню в разделе **Объекты -> Атрибуты**.

Замечание! *Если для атрибута уже вводились данные, то ряд параметров этого атрибута будет недоступен для редактирования (в частности, нельзя изменить его тип). Если атрибут все-таки нужно отредактировать, то предварительно необходимо очистить все его данные.*

2. На вкладке **Наименование** введите в поле уникальное имя атрибута и, при необходимости, его описание. На этой же вкладке выберите тип атрибута из списка возможных. В Traffic Inspector доступны следующие типы:
   - **String** – строка или текст произвольной длины (длина не ограничена);
   - **Integer** – целое число со знаком, для хранения используется 64-разрядная переменная;
   - **Boolean** – логическое значение (да или нет);
   - **Float** – дробное число в десятичном формате (хранится и отображается с точностью до 4 знаков после запятой);
   - **DateTime** – дата со временем или без.
3. На вкладке **Применение** с помощью флажков определите списки объектов, в которых может применяться данный атрибут.
4. На вкладке **Опции** настройте доступ к данным атрибута администраторам с ограниченными правами (подробнее о типах администраторов см. в п. Разграничение доступа). Для этого выберите один из следующих вариантов:
   - **Все** – атрибут доступен всем администраторам без исключения;
   - **Менеджеры и администраторы** – атрибут недоступен администраторам из групп с ролью **Кассир**;
   - **Администраторы** – атрибут доступен только администраторам из групп с ролью **Администратор**.
5. На вкладке **Опции** настройте следующие дополнительные параметры атрибута:

- Включите или отключите отображение данных атрибута в отдельных колонках в правой части списка (разделы пользователей, группы, коллективные счета, контролируемые и информационные счетчики). По умолчанию функция включена. Данные атрибута имеет смысл показывать в списках, если это дополнительные настройки и т.д. Если это внутренние данные (переменные) скриптов или внешних приложений, то функцию лучше выключить.

- Включите или отключите отображение данных атрибута в отдельных колонках в правой части списка монитора работы пользователей (атрибуты пользователей и коллективных счетов) или внешних счетчиков.

> ***Замечание!*** *Запрос данных атрибутов в мониторе работы – операция, требующая дополнительных ресурсов сервера. Если в мониторе работы включено автообновление, то отображать данные атрибутов там без особой необходимости не следует.*

- Разрешите или запретите редактирование данных атрибута в консоли (если запретить их редактирование, то изменить данные можно будет только через API).

6. Сохраните внесенные изменения.

Очистка данных атрибута

В процессе очистки удаляются все данные для данного атрибута. При этом становится возможным изменение всех его параметров, включая тип. Удаление данных атрибута выполняется с помощью контекстного меню, вызываемого при нажатии правой кнопкой мыши на атрибуте в разделе **Объекты -> Атрибуты** консоли администратора.

Удаление атрибута

Удаление атрибута возможно только в том случае, если отсутствуют связанные с ним данные. Поэтому перед удалением необходимо предварительно очистить данные (см. выше).

Удаление атрибута выполняется с помощью контекстного меню, вызываемого при нажатии правой кнопкой мыши на атрибуте в разделе **Объекты -> Атрибуты** консоли администратора.

Работа Traffic Inspector с одним сетевым интерфейсом

Основным режимом работы Traffic Inspector является работа с двумя или более сетевыми интерфейсами. В этом случае некоторые из них (как минимум один) являются внутренними, то есть "смотрят" в локальную сеть, а остальные (как минимум один) – внешними, к ним подключаются каналы от вышестоящих провайдеров. В этом режиме Traffic Inspector обладает полной функциональностью.

Однако у Traffic Inspector есть режим работы с одним сетевым интерфейсом. В этом случае этот интерфейс подключается к локальной сети и на него любым возможным способом направляется зеркалируемый трафик. Обычно для этого используется порт зеркалирования управляемого коммутатора, установленного непосредственно перед прокси-сервером организации. В этом случае на сервер Traffic Inspector поступает весь трафик, которым отправляют наружу и принимают извне. Однако это будет не основной трафик, а только его копия. В связи с чем, часть функций, связанная с фильтрацией и преобразованием информации (например, удаление из трафика вредоносного ПО) может оказаться недоступна. Блокирование данных возможно только при использовании управляемых коммутаторов с поддержкой SNMP.

Использование режима работы с одним сетевым интерфейсом оправдано тогда, когда доступ к Интернету является критичным для работы пользователей локальной сети. В этих случаях Traffic Inspector не пропускает через себя основной трафик, а значит никакие сбои в системе не могут помешать пользователям выполнять свои обязанности. При этом Traffic Inspector может использоваться для тарификации, ведения подробной статистики, а также для оперативного оповещения администраторов о возникновении тех или иных ситуаций, требующих внимания с их стороны.

Выбор режима работы осуществляется на вкладке **Вариант применения** конфигуратора (подробнее см. в п. Настройка режима работы). При этом во всех остальных настройках станут неактивны функции, работа которых невозможна в данном режиме, установка

внешних сетевых интерфейсов (все сетевые интерфейсы будут считаться внутренними) и пр.

Удаление/добавление сетевых интерфейсов

Управление сетевыми интерфейсами осуществляется с помощью конфигуратора (подробнее о конфигураторе см. в п. Конфигуратор).

Для удаления или добавления сетевого интерфейса выполните следующие действия:

1. Запустите конфигуратор.
2. На вкладке **Выбор действия** выберите режим **Настройка служб Traffic Inspector**.
3. Для удаления/добавления внутренних сетевых интерфейсов перейдите на вкладку **Внутренние интерфейсы,** включите флажки у тех интерфейсов, которые нужно добавить, и выключите у тех, которые нужно удалить.
4. Для удаления/добавления внешних сетевых интерфейсов перейдите на вкладку **Внешние интерфейсы,** включите флажки у тех интерфейсов, которые нужно добавить, и выключите у тех, которые нужно удалить.
5. Сохраните внесенные изменения.

Управление трафиком на локальных интерфейсах

В рамках управления трафиком на локальных интерфейсах решаются следующие задачи:

- создание и настройка отдельных правил и целых их групп, с помощью которых решаются задачи разграничения доступа из внутренней сети, фильтрации нежелательного контента и т.п.;
- создание и настройка тарифов, с помощью которых ведется суммовой учет потребляемого пользователями трафика;
- создание и настройка правил для отдельных IP-сетей;
- создание и настройка перенаправлений TCP-соединений.

Работа Traffic Inspector с сетевыми интерфейсами

8

Виды и предназначение правил, наборы правил

Имеются в виду правила, с помощью которых решаются задачи разграничения доступа из внутренней сети, фильтрации нежелательного контента и т.д. Правила отображаются в разделе **Правила -> Правила пользователей** консоли администратора. На главной его странице отображается перечень всех существующих правил, которые не входят в наборы (правила, входящие в состав наборов, отображаются в подразделе соответствующих наборов, подробнее см. в п. Наборы правил). Помимо этого на странице присутствует специальная панель, в которой перечисляются все объекты, в которых задействовано активное в данный момент правило с возможностью быстрого перехода к их настройке.

Правила могут назначаться как отдельным пользователям, так и целым их группам (подробнее см. в п. Создание и настройка групп и п. Создание и настройка пользователей).

Объекты, используемые в правилах

При создании правил, а также в некоторых других настройках программы могут использоваться так называемые объекты. Их применение позволяет облегчить настройку Traffic Inspector. В правилах доступны следующие объекты:

- **IP-сети** – наборы заданных сетей;
- **URL-списки** – правила обработки URL-запросов;
- **Категории контента** – категории, к которым может относиться загружаемый из Интернета пользователями контент.

IP-сети

IP-сети представляют собой списки IP-адресов и сетей, которые могут использоваться в различных настройках программы, в том числе, в правилах. Каждый список может состоять как из одного, так и из нескольких выражений, описывающих один адрес или целую сеть.

Перечень IP-сетей, созданных в системе, находится в разделе **Объекты -> IP-сети** консоли администратора. Раздел состоит из двух частей. В верхней отображается список IP-сетей. Нижняя часть состоит из двух вкладок. На вкладке **IP сети** отображаются

основные параметры выбранной сети, а на вкладке **Список** – список ее выражений.

Также в разделе **Объекты** есть блок **IP-сети**, состоящий из двух вкладок. На вкладке **Информация** отображается общее количество созданных в системе сетей, а на вкладке **Действия** – ссылки на некоторые операции.

В рамках управления IP-сетями в Traffic Inspector реализованы следующие операции:

- настройка параметров DNS по умолчанию;
- создание/изменение IP-сети;
- проверка выражения;
- загрузка обновлений;
- удаление IP-сети.

Настройка параметров DNS по умолчанию

В списках выражений IP-сетей можно использовать имена хостов. Однако в этом случае программе должно быть разрешено использование DNS (подробнее см. в п. Настройка служб). При необходимости можно настроить параметры по умолчанию, которые потом можно будет использовать в настройках IP-сетей. Для этого выполните следующие действия:

1. Запустите окно параметров распознавания имен через DNS. Сделать это можно в блоке **IP-сети**, размещенном на главной странице раздела **Объекты**.
2. В открывшемся окне укажите периодичность повторной проверки IP-адреса хоста, если последняя проверка была успешной (в часах) и неуспешной (в минутах). А также промежуток времени (в часах), через который хост будет удален из списка, если по каким-то причинам не удалось определить его IP-адрес.
3. Сохраните внесенные изменения.

Создание/изменение IP-сети

Для создания новой или изменения существующей IP-сети выполните следующие действия.

1. Откройте окно новой или существующей IP-сети. Сделать это можно с помощью контекстного меню в разделе **Объекты -> IP-сети** консоли администратора или в блоке **IP-сети**, размещенном на главной странице раздела **Объекты**.

2. На вкладке **IP сети** в поле введите наименование создаваемого списка и, при необходимости, произвольные примечания.

3. На вкладке **DNS** определите параметры использования DNS для преобразования заданных в списке выражений имен хостов в IP-адреса. Их можно установить вручную (параметры аналогичны параметрам по умолчанию, см. выше) или включить использование настроек по умолчанию.

4. При необходимости включите автоматическое обновление списка с внешнего источника по протоколу HTTP. При включении задайте адрес списка, из которого будут загружаться обновления, а также в специальном окне настройте расписание загрузки. При необходимости измените формат загружаемого списка, сменив его значение на **BGP export list**, и укажите имя сети (согласно формату BGP export list в одном списке может описываться несколько сетей). Для определения имени сети можно открыть список в браузере, имя будет после ключевого слова **aggregation**.

5. На вкладке **Список** настройте список выражений, определяющих IP-сеть. Каждое выражение пишется в отдельной строке. В Traffic Inspector могут использоваться выражения следующих типов:

   - **IP-адрес** – одиночный IP-адрес.
   - **IP-сеть** – задается в формате IP/MASK. Маска может задаваться в формате IP-адреса, а также длины в битах. Например, 192.168.0.1/24 или 192.168.0.1/255.255.255.0.
   - **Диапазон адресов** – задается в виде двух адресов через "-". Например, 192.168.0.4-192.168.0.11.
   - **Имя хоста** – задается имя хоста. Это имя путем DNS-запроса будет

преобразовываться в IP-адрес. В DNS-зоне под именем может быть прописано и несколько IP-адресов – программа будет работать со всеми. Это удобно, если требуется описать ресурс, IP-адрес которого может меняться.

Настраивать список можно вручную. Также он может быть импортирован из предварительно подготовленного файла.

> ***Замечание!*** *Функция загрузки с внешнего источника доступна только в том случае, если были настроены параметры на вкладке* ***Автозагрузка****.*

Также подготовленный список может быть выгружен в виде текстового файла.

6. Сохраните внесенные изменения.

Проверка выражения

В Traffic Inspector реализована функция проверки выражения, которая позволяет проверить, принадлежит введенное выражение указанной IP-сети или нет. Проверка осуществляется в специальном окне, вызов которого осуществляется с вкладки **Список** окна свойства IP-сети или с помощью контекстного меню раздела **Объекты -> IP-сети** консоли администратора.

В окне проверки введите IP-адрес тестируемого ресурса и запустите проверку. Если адрес попал в список, то отображается номер первой строки (нумерация с "1"), где это условие выполнилось.

Загрузка обновлений

Данная функция позволяет сразу загрузить обновления списка выражений IP-сети, не дожидаясь срабатывания расписания. Ее запуск осуществляется с вкладки **Список** окна свойства IP-сети или с помощью контекстного меню раздела **Объекты -> IP-сети** консоли администратора.

> ***Замечание!*** *Функция обновления доступна только в том случае, если были настроены параметры на вкладке* ***Автозагрузка*** *окна свойств IP-сети.*

Удаление IP-сети

Удаление IP-сети осуществляется с помощью контекстного меню раздела **Объекты -> IP-сети** консоли администратора.

URL-списки

URL-списки содержат правила обработки URL-запросов. Их основой является набор выражений, по которым проверяются URL-адреса, запрашиваемые пользователями. С их помощью можно, например, определить рекламу, сайты определенной тематики, конкретные веб-проекты и т.п. URL-списки используются в различных настройках программы, в частности, в правилах пользователей и правилах HTTP-прокси.

Перечень URL-списков, созданных в системе, находится в разделе **Объекты -> URL-списки** консоли администратора. Раздел состоит из двух частей. В верхней отображается список URL-списков. Нижняя часть состоит из двух вкладок. На вкладке **URL списки** отображаются основные параметры выбранного URL-списка, а на вкладке **Список** – список его выражений.

Также в разделе **Объекты** есть блок **URL-списки**, состоящий из двух вкладок. На вкладке **Информация** отображается общее количество созданных в системе URL-списков, а на вкладке **Действия** – ссылки на некоторые операции.

В рамках управления URL-списками в Traffic Inspector реализованы следующие операции:

- создание/изменение URL-списка;
- проверка выражения;
- загрузка обновлений;
- удаление URL-списка.

Создание/изменение URL-списка

Для создания нового или изменения существующего URL-спсика выполните следующие

действия:

1. Откройте окно свойств нового или существующего URL-списка. Сделать это можно с помощью контекстного меню раздела **Объекты -> URL-списки** консоли администратора или в блоке **URL-списки**, который размещен на главной странице раздела **Объекты**.

2. На вкладке **Описание** введите наименование создаваемого списка и, при необходимости, произвольные примечания. Здесь же выберите тип списка.

   - **Вхождение подстроки** – при использовании данного варианта Traffic Inspector будет проверять, входят ли в URL-адреса указанные на вкладке **Список** строки. Его удобно использовать для поиска четко определенных подстрок. Например, если в список добавить значение "*foto*", то URL-адрес при вхождении этой подстроки в любую его часть будет соответствовать списку (например, http://foto.ru, http://company.com/foto, http://company.com/pics/foto.jpg и т.д.).

   - **Регулярные выражения** – при использовании данного варианта строки в списке представляют собой регулярные выражения. Это позволяет задавать значительно более сложные условия с использованием специального синтаксиса (подробнее о синтаксисе регулярных выражений см. в п. !!!). Они позволяют определять искомые подстроки более точно, с учетом дополнительных факторов, что обеспечивает меньшее количество ложных срабатываний.

   При необходимости на вкладке можно выключить чувствительность к регистру. В этом случае анализ URL-адресов будет осуществляться без учета регистра символов.

3. При необходимости включите автоматическое обновление списка с внешнего источника по протоколу HTTP. При включении задайте адрес списка, из которого будут загружаться обновления, а также в специальном окне настройте расписание загрузки.

4. На вкладке **Список** настройте список выражений. Создавать его можно вручную, при этом каждое выражение пишется в отдельной строке. Также список может быть загружен из предварительно подготовленного файла.

Замечание! *Функция загрузки с внешнего источника доступна только в*

*том случае, если были настроены параметры на вкладке **Автозагрузка**.*

Список может быть выгружен в виде текстового файла.

> ***Замечание!** HTTP-прокси при обработке запроса передает URL вида <Host>/<Path>?<Parameters>. Другие части полного URL не передаются – префикс протокола (http//), IP-порт, логин и т.д. Это необходимо учитывать при формировании списка, а также его тестовой проверке.*

5. Сохраните внесенные изменения. При закрытии окна свойств производится проверка синтаксиса регулярных выражений. Если при этом будут найдены ошибки, то отобразится сообщение, на какой строке списка это произошло. В верхней части окна редактирования списка есть поле, где отображается номер редактируемой строки.

Проверка выражения

В Traffic Inspector реализована функция проверки выражения, которая позволяет проверить, соответствует URL-адрес указанному URL-списку или нет. Проверка осуществляется в специальном окне, вызвать которое можно с вкладки **Список** окна свойства URL-списка или с помощью контекстного меню раздела **Объекты -> URL-списки** консоли администратора.

В окне введите тестируемый URL-адрес и запустите проверку. Если адрес попал в список, то отображается номер первой строки (нумерация с "1"), где это условие выполнилось.

Загрузка обновлений

Данная функция позволяет сразу загрузить обновления списка выражений URL-списка, не дожидаясь срабатывания расписания. Ее запуск осуществляется с вкладки **Список** окна свойства URL-списка или с помощью контекстного меню раздела **Объекты -> URL-списки** консоли администратора.

> ***Замечание!** Функция обновления доступна только в том случае, если были настроены параметры на вкладке **Автозагрузка** окна свойств* URL-списка.

Удаление URL-списка

Удаление URL-списка осуществляется с помощью контекстного меню раздела **Объекты -> URL-списки** консоли администратора.

> ***Замечание!*** *URL-список не может быть удален, если он используется в других настройках программы. При удалении такого URL-списка будет выведено сообщение об ошибке с указанием использующей его настройки.*

Категории контента

Категории контента используются в правилах анализа по IP- и HTTP-контенту. Модули Traffic Inspector, в частности **AdGuard** и **NetPolice для Traffic Inspector**, присваивают ресурсам категорию контента. Затем правила анализа IP- и HTTP-контента могу проводить различные действия с трафиком указанной категории контента.

Перечень категорий контента, созданных в системе, находится в разделе **Объекты -> Категории контента** консоли администратора. Также в разделе **Объекты** есть блок **Категории контента**, состоящий из двух вкладок. На вкладке **Информация** отображается общее количество созданных в системе категорий контента, а на вкладке **Действия** – ссылки на некоторые операции.

В рамках управления категориями контента в Traffic Inspector реализованы следующие операции:

- создание/изменение категории контента;
- удаление категории контента.

Создание/изменение категории контента

Для создания новой или изменения существующей категории контента выполните следующие действия:

1. Откройте окно свойств новой или существующей категории контента. Сделать это можно с помощью контекстного меню раздела **Объекты -> Категории контента**

консоли администратора или в блоке **Категории контента** главной страницы раздела **Объекты**.

2. На вкладке **Тип контента** введите наименование создаваемого списка и, при необходимости, произвольные примечания.
3. Сохраните внесенные изменения.
4. После сохранения категории настройте необходимые правила модуля расширения **NetPolice для Traffic Inspector**, с помощью которых к этой категории будет относиться нужный HTTP-контент (подробнее см. в п. Правила NetPolice для Traffic Inspector).

Удаление категории контента

Удаление категории контента осуществляется с помощью контекстного меню раздела **Объекты -> Категории контента** консоли администратора.

Виды правил и операции с ними

В Traffic Inspector реализованы следующие типы правил.

- **Разрешение + действие** – комбинированное правило, которое разрешает соответствующий заданным условиям трафик и одновременно позволяет задавать дополнительные действия.
- **Запрет** - правило, блокирующее трафик, который удовлетворяет заданным условиям. Для трафика, проходящего через HTTP-прокси, можно задать дополнительные действия.
- **Управляемое пользователем** – предустановленные правила F1-F4, переключаемые пользователем в клиентском агенте. По умолчанию правило F1 содержит список ключевых баннеров и баннерных сетей и настроен на блокировку анимаций и изображений; правило F2 блокирует мультимедиа-контент; F3 блокирует еще и все изображения; F4 пропускает только текст. Эти настройки по умолчанию можно изменять.
- **Только "действия"** – к трафику, соответствующему заданным условиям, применяются указанные в настройках действия.

Работа Traffic Inspector с сетевыми интерфейсами 8

В рамках управления правилами в Traffic Inspector реализованы следующие операции:

- создание/изменение правил;
- изменение типа правила;
- включение правила в набор правил;
- удаление правил.

Создание/изменение правил типа "Разрешение + действие"

Правило типа "**Разрешение + действие**", по сути, является разрешающим правилом. То есть в нем задаются условия, при соблюдении которых трафик будет разрешен. После срабатывания правила на разрешение дальнейшая обработка этого трафика другими правилами ниже по списку прекращается.

Если правило используется для пользователей, то правило может быть дополнено действиями. В этом случае одновременно с разрешением трафика Traffic Inspector выполняет заданные действия, например, делает трафик бесплатным, ограничивает его скорость и т.п.

Для создания нового или редактирования уже существующего правила **Разрешение + действие** выполните следующие действия.

1. Откройте окно свойств нового или существующего правила. Если нужно создать новое правило в составе набора правил, то следует использовать контекстное меню в соответствующем нужному набору подразделе в разделе **Правила -> Группы правил** консоли администратора. Если нужно создать правило без набора, то необходимо использовать контекстное меню в разделе **Правила -> Правила пользователей** или блок **Правила действия**, расположенный на главной странице раздела **Правила**.
2. На вкладке **Наименование** введите в поле уникальное наименование правила и, при необходимости, его произвольное описание.

Замечание! *Рекомендуется не пренебрегать описанием правил. Это*

значительно облегчает управление правилами, особенно при большом их количестве.

3. Если правило нужно временно отключить, не удаляя совсем, то включите флажок **Запретить правило**.

4. На вкладке **Тип трафика** укажите, какой трафик будет обрабатываться данным правилом:

   - **Любой трафик** – при выборе данного варианта обрабатывается весь трафик для отмеченных флажками служб Traffic Inspector (то есть правило может распространяться как на какую-то одну, так сразу и на несколько служб), однако условия могут задаваться только по IP-адресам, протоколам и портам.

   - **Трафик через прокси-сервер** – данный вариант позволяет обрабатывать трафик только HTTP-прокси, но при этом поддерживаются условия по URL-адресам, типам и категориям контента.

5. На вкладке **Тип трафика** выберите тип правила, в данном случае – **Разрешение + действие**.

6. На вкладке **IP адрес** укажите IP-адреса назначения (IP-адреса, на которые направляет трафик), для которых будет срабатывать данное правило. Возможны следующие варианты:

   - **Любой** – правило будет срабатывать для всего трафика.

   - **Сам сервер** – правило будет срабатывать при обращении на любой сетевой интерфейс самого сервера.

   - **IP адрес или сеть** – правило будет срабатывать при обращении внешний IP-адрес, соответствующий указанному или входящий в указанный диапазон.

   - **Использовать список** – правило будет срабатывать при обращении к указанной в выпадающем списке IP-сети (подробнее про IP-сети см. в п. IP-сети). При выборе этого варианта можно непосредственно с данной вкладки перейти к

редактированию активной или созданию новой IP-сети.

7. Если на вкладке **Тип трафика** был выбран вариант **Любой трафик**, то на вкладке **IP протокол** настройте протокол и, при необходимости, порт трафика, который будет учитываться данным правилом. Сделать это можно с помощью подсказки или вручную. В первом случае выберите шаблон одного из наиболее распространенных типов трафика (например, ICMP, DNS client, HTTP client, FTP client и т.п.). При этом все параметры будут настроены автоматически.

   Для ручной настройки самостоятельно выберите нужный протокол. Если был выбран вариант UDP или TCP, то дополнительно укажите сетевой порт. Это может быть один конкретный порт, диапазон номеров сетевых портов или динамический порт.

8. Если на вкладке **Тип трафика** был выбран вариант **Трафик через прокси-сервер**, то на вкладке **Протокол** выберите протокол для работы через HTTP-прокси. Возможны следующие варианты:

   - **Любой** – любой протокол, поддерживаемый HTTP-прокси.
   - **HTTP** – прямое проксирование HTTP-протокола. При выборе данного варианта можно заблокировать отправку данных методом POST.
   - **HTTP/TUNN** – проксирование исходящих TCP-соединений методом CONNECT. Может использоваться как для проксирования произвольного трафика, так и только для защищенных SSL-соединений. Во втором случае необходимо ввести в поле **Порт назначения** порт 443 (стандартный порт для SSL-соединений) или нажать на кнопку **Ограничить только для SSL**.
   - **FTP** – протокол FTP поверх протокола HTTP с использованием метода GET.

   При необходимости на данной вкладке можно указать интервал сетевых портов или конкретный порт, на который будет распространяться действие данного правила.

9. Если на вкладке **Тип трафика** был выбран вариант **Трафик через прокси-сервер**, то на вкладке **Проверка URL** задайте параметры проверки URL-адресов. Возможны следующие варианты.

- **Не проверять** – проверка URL-адресов не осуществляется.
- **URL запрос или строка в формате регулярных выражений** – осуществляется поиск в URL-адресе указанной строки, которая может представлять собой конкретный URL-запрос или строку, содержащую регулярные выражения (подробнее о синтаксисе регулярных выражений см. в п. !!!).
- **Список** – осуществляется проверка соответствия URL-адреса выбранному URL-списку (подробнее про URL-списки см. в п. URL-списки). При выборе этого варианта можно прямо с данной вкладки перейти к редактированию активного или созданию нового URL-списка.

При выборе вариантов **URL запрос или строка в формате регулярных выражений** или **Список** существует возможность проверить корректность работы условий. Тестирование осуществляется в отдельном окне, вызов которого осуществляется непосредственно с данной вкладки. Для проверки по строке введите адрес и строку и запустите процесс тестирования. Для проверки адреса по списку введите только адрес. Результат проверки будет отображен в том же окне в виде надписи **YES** (результат положительный) или **NO** (результат отрицательный).

10. Если на вкладке **Тип трафика** был выбран вариант **Трафик через прокси-сервер**, то на вкладке **Анализ контента** настройте условия отбора трафика на основе анализа передаваемого контента. Отбор может осуществляться по типу данных. В этом случае флажками отметьте нужные типы из списка возможных. Если нужна фильтрация по категориям контента с помощью модуля расширения **NetPolice для Traffic Inspector** (подробнее о модуле см. в п. NetPolice для Traffic Inspector), то выберите нужную категорию из числа предварительно созданных (подробнее о категориях контента см. в п. Категории контента). Обе проверки могут использоваться как отдельно друг от друга, так и вместе.

11. В Traffic Inspector реализована возможность фильтрации трафика с помощью фильтра U32. Если в этом фильтре есть необходимость, то включите его на вкладке **Расширенная фильтрация** и задайте свое собственное правило или выберите из списка одно из предустановленных.

12. На вкладке **Дополнительно** выберите состояние счета, при котором данное правило будет срабатывать (при любом состоянии счета, при работе в кредит или не в кредит). Это позволяет, например, блокировать доступ пользователей к определенным ресурсам при работе в кредит. Также укажите, для каких типов локальных сетей должно срабатывать данное правило (для любых, только для локальных или только для публичных).

13. Если есть необходимость создания правила, которое обрабатывает трафик, направленный другим правилом (функцией маршрутизации) на определенный интерфейс, то на вкладке **Дополнительно** включите эту функцию и выберите нужный сетевой интерфейс.

14. При необходимости на вкладке **Расписание** настройте расписание действия правила (работа на вкладке аналогична работе на одноименной вкладке окна свойств группы, подробнее см. в п. Создание и настройка групп). Здесь же можно указать период действия правила по датам.

15. При необходимости настройте изменение тарификации трафика, соответствующего данному правилу. Для этого на вкладке **Тарификация** выберите один из следующих вариантов действия:

- **Сделать бесплатным** – трафик, соответствующий правилу, не будет тарифицироваться (то есть при его получении баланс пользователя меняться не будет).
- **Посчитать по другому тарифу** – трафик, соответствующий правилу, будет тарифицироваться не по обычному для пользователя, а согласно выбранному в выпадающем списке тарифу.

> ***Замечание!*** *При применении правила для неавторизованных пользователей данное действие смысла не имеет, а поэтому выполняться не будет.*

> ***Замечание!*** *При изменении этой настройки для работающих пользователей может произойти пересчет тарификации.*

16. На вкладке **Шейпер** выберите действие шейпера для данного правила. Доступны следующие варианты работы шейпера:

- **Ничего не делать** – выберите этот вариант для выключения шейпера для данного правила.
- **Не использовать этот трафик для определения скорости и передавать эти данные без задержек** – включите для трафика, который необходимо передавать без ограничения скорости.
- **Применить правило для шейпера** – выберите этот вариант для ограничения скорости передачи трафика, соответствующего данному правилу. При этом можно настроить следующие дополнительные параметры:
  - **Ограничивать скорость** – включите, если нужно ограничить скорость на прием и/или передачу данных до указанных величин.
  - **Увеличить приоритет трафика при обработке пакетов в очереди** – включите, если нужно задать для трафика определенный приоритет. Приоритет задается цифрой от 1 до 9 (9 – самый высокий). Traffic Inspector учитывает приоритет при передаче пакетов из очереди.
  - **Также делать приоритет и при ограничении скорости в группе** – включите, если для трафика будет использоваться отдельная очередь (отдельная на каждую группу). Такой трафик получает еще более высокий приоритет.

17. При необходимости на вкладке **Роутинг** настройте перенаправление трафика, соответствующего правилу, на другой интерфейс. Сам факт выполнения этого действия может использоваться и как условие для правила (см. шаг 13). Так как правила обрабатываются строго по списку, то, размещая такие правила после правила, которое сделало перенаправление, можно собрать логику применения условий в зависимости от используемого внешнего интерфейса. Например, применить скидки (наценки). Следует также учесть, что настройки пользователей (групп) применяются после просмотра списка (подробнее см. в п. Advanced Routing - работа с несколькими внешними интерфейсами).

Для настройки роутинга включите его и укажите нужный внешний интерфейс.

18. Сохраните внесенные изменения.

Создание/изменение правила типа "Запрет"

Правила типа **Запрет** блокируют передачу трафика, соответствующего заданным в них условиям. После этого обработка трафика другими правилами, следующим за запрещающим, прекращается.

Создание нового или редактирование уже существующего правила типа **Запрет** в основном аналогично созданию или редактированию правила типа **Разрешение + действие** (см. выше). Однако между ними есть следующие различия:

1. В правиле типа **Запрет** отсутствуют вкладки **Тарификация**, **Шейпер** и **Роутинг**. Соответственно, недоступны все связанные с ним настройки (шаги 15-17 процедуры настройки правила типа **Разрешение + действие**).

2. В правиле типа **Запрет** можно настроить размер объекта, при котором трафик будет запрещен. Сделать это можно на вкладке **Размер объекта**, где нужно включить эту функцию и указать размер объекта (в КБайт). Это позволяет запретить пользователям загружать файлы большого объема.

3. В правиле типа **Запрет** можно указать страницу, на которую будет автоматически направлен пользователь при срабатывании правила, то есть при блокировке HTTP-трафика (она будет показана вместо запрашиваемой). Сделать это можно на вкладке **Перенаправление**, где нужно включить данную функцию и указать адрес нужной страницы. Адрес можно ввести абсолютный (например, "*http://company.ru*") или относительный (относительно подпапки \root папки установки Traffic Inspector, например, "*/images/blank.jpg*"). Также при включении перенаправления необходимо выбрать метод перенаправления:

   - **Временное перенаправление** – используется при перенаправлении одного ресурса страницы (например, позволяет вместо баннера вывести пустой рисунок);

- **Постоянное перенаправление**-- используется при перенаправлении запроса всей страницы на другой сайт.

4. В правиле типа **Запрет** на вкладке **Блокировка** можно настроить действия Traffic Inspector при блокировке ресурсов HTTP-прокси.

   - Определите, будет или нет система при блокировке ресурсов загружаемой страницы пытаться извлечь их из кэша. Запрет этого действия имеет смысл для ресурсов с явно нежелательным контентом, которые, однако, могли попасть в кэш (например, загружались другими пользователями).
   - Включите или выключите замену заблокированных и не найденных в кэше изображений и flash-роликов пустыми файлами. Рекомендуется использовать эту функцию, чтобы по возможности сохранять целостность веб-страниц.
   - Определите, что будет отображаться в барузере при блокировке всей веб-страницы – пустая страница или страница с описанием причины блокировки.
   - При необходимости дополните стандартную страницу с причиной блокировки собственным комментарием – произвольным текстом.

Создание/изменение правил типа "Управляемое пользователем"

Правила типа **Управляемое пользователем** являются запрещающими правилами, переключаемыми пользователем в клиентском агенте. В отличие от других, правила данного типа делятся на 4 уровня фильтрации (в программе обозначаются F1-F4). По умолчанию правило F1 содержит список ключевых баннеров и баннерных сетей и настроен на блокировку анимаций и изображений, правило F2 блокирует мультимедиа-контент, F3 блокирует вообще все изображения, а F4 пропускает только текст. Для этого при установке Traffic Inspector автоматически создаются соответствующие правила. При необходимости их можно изменять обычным порядком или дополнять своими с указанием уровня фильтрации.

Управление правилами данного типа полностью аналогично управление правилами типа

Запрет (см. выше). Единственным отличием является необходимость выбора уровня фильтрации на вкладке **Тип правила**.

Создание/изменение правил типа "Только действие"

Правила типа **Только действие** используются для выполнения над описанным в них трафиком тех или иных действий. После срабатывания правила обработка трафика другими правилами ниже по списку продолжается.

Управление правилами данного типа полностью аналогично управление правилами типа **Разрешение + действие** (см. выше). Однако необходимо учитывать разницу между правилами этих типов.

Изменение типа правила

Данная операция позволяет не только отредактировать параметры правила, но и изменить его тип и тип трафика (при обычном редактировании это сделать нельзя). Запускается она с помощью контекстного меню подраздела набора, в котором находится правило, или непосредственно в разделе **Правила -> Правила пользователей**. Выполняется изменение типа правила в окне свойств правила аналогичном окну свойств нового правила (см. выше).

Включение правила в набор правил

Правила можно включать в состав наборов или переносить из одного набора в другой (подробнее о наборах правил см. в п. Наборы правил). Запускается эта операция с помощью контекстного меню подраздела исходного набора или непосредственно в разделе **Правила -> Правила пользователей**. Смена набора осуществляется в специальном окне, в котором нужно выбрать новый набор. Тут же, при необходимости, можно временно заблокировать правило, не удаляя его.

Удаление правила

Удаление правила осуществляется с помощью контекстного меню подраздела исходного набора или непосредственно в разделе **Правила -> Правила пользователей**.

Наборы правил

Наборы правил позволяют объединить в группу несколько правил и использовать этот набор как одно целое. Наборами правил удобно оперировать, когда создано несколько правил, и эту группу правил нужно назначить нескольким пользователям и/или группам. Предусмотрено создание нового правила в наборе или добавление уже существующих правил в набор.

Наборы правил отображаются в разделе **Правила -> Группы правил**. На главной его странице отображается перечень всех существующих наборов. Помимо этого на странице присутствует специальная панель, в которой перечисляются все объекты, в которых задействована активная в данный момент группа с возможностью быстрого перехода к их настройке.

Для каждого набора правил в разделе **Правила -> Группы правил** создается собственный подраздел, в котором размещен список входящих в него правил. Также на главной странице раздела **Правила** есть блок **Группа правил**. На его вкладке **Информация** отображаются данные о количестве созданных наборов правил и об общем количестве правил, входящих в них, а на вкладке **Действия** – ссылки на доступные операции.

В рамках управления наборами правил в Traffic Inspector реализованы следующие операции:

- создание/изменение набора правил;
- удаление набора правил.

Создание/изменение набора правил

Для создания или изменения набора правил выполните следующие действия:

1. Откройте окно свойств нового или существующего набора правил. Сделать это можно с помощью контекстного меню раздела **Правила -> Группы правил** или в блоке

Группы правил, размещенном на главной странице раздела **Правила**.

2. На вкладке **Наименование** введите уникальное наименование набора правил и, при необходимости, его описание.

> ***Замечание!*** *Рекомендуется не пренебрегать описанием наборов правил. Это значительно облегчает управление правилами, особенно при большом их количестве.*

3. При необходимости на вкладке **Наименование** временно отключите набор правил, не удаляя его совсем.

4. Сохраните внесенные изменения.

Удаление набора правил

Удаления набора правил осуществляется с помощью контекстного меню в разделе **Правила -> Группы правил**.

Тарифы

Тарифы используются для суммового учета потребляемого пользователями трафика или времени подключения. Ведя статистику, Traffic Inspector автоматически изменяет баланс пользователя с учетом текущего тарифа. Тарифы могут назначаться как отдельным пользователям, так и целым их группам (см. п. Создание и настройка пользователей и п. Создание и настройка групп). Кроме того, посещение определенных ресурсов может тарифицироваться по тарифам, отличным от основного. Настраивается это с помощью правил (подробнее см. в п. Виды и предназначение правил, наборы правил).

В Traffic Inspector имеется предустановленный тариф **<Default>**. Он используется как тариф по умолчанию. Удалить его нельзя, но все его настройки можно менять. Также можно назначить тарифом по умолчанию свой собственный тариф.

В Traffic Inspector реализовано два вида тарифов – с учетом трафика и времени подключения. В первом учитывается трафик пользователя. В зависимости от настроек это может быть входящий или исходящий трафик или оба вместе. Во втором учитывается

время подключения пользователя к серверу Traffic Inspector.

Список тарифов расположен в разделе **Учет трафика -> Тарифы** консоли администратора. Также в разделе **Учет трафика** есть блок **Тарифы**, состоящий из двух вкладок. На вкладке **Информация** отображается общее количество созданных в системе тарифов, а также название тарифа по умолчанию, а на вкладке **Действия** – ссылки на некоторые операции.

В рамках управления тарифами в Traffic Inspector реализованы следующие операции:

- создание/изменение тарифа;
- назначение тарифа по умолчанию;
- смена тарифа;
- удаление тарифа.

Настройка тарифа с учетом трафика и тарифа с учетом времени подключения значительно отличаются друг от друга, поэтому рассматривать эти операции мы будет отдельно друг от друга.

Создание/изменение тарифа с учетом трафика

Для создания нового или изменения существующего тарифа с учетом трафика выполните следующие действия:

1. Откройте окно свойств нового или существующего тарифа. Сделать это можно с помощью контекстного меню в разделе **Учет трафика -> Тарифы** консоли администратора или в блоке **Тарифы**, размещенном на главной странице раздела **Учет трафика**.
2. Введите на вкладке **Тариф** наименование тарифа и, при необходимости, произвольные примечания. Здесь же выберите тип тарифа – **По трафику**.
3. На вкладке **Настройки** установите основные параметры тарифа.
   - Выберите единицу измерения, в которой будет вестись списание средств со счетов

пользователей. Это может быть одна из денежных единиц или же мегабайты. При выборе последнего варианта учет будет вестись в трафике.

- Укажите стоимость одного мегабайта трафика. Если же в качестве единицы измерения были выбраны мегабайты, то в данном поле введите значение "1".
- Если нужно, чтобы при запуске сессии пользователю на счет сразу начислялась какая-то сумма, то укажите ее в поле **Оплата по умолчанию**. Обратите внимание, что указанная сумма будет автоматически присваиваться пользователю при его автодобавлении.
- Если нужно, чтобы в тарифе была предусмотрена возможность работы в кредит, то укажите сумму кредита. В этом случае будет возможна работа пользователя при отрицательном балансе, не превышающем размер кредита (при превышении работа пользователя будет заблокирована). В противном случае введите значение "0".

> ***Замечание!*** *Traffic Inspector позволяет задать особые условия при работе пользователя в кредит. Например, можно ограничить его скорость, запретить доступ к определенному контенту и пр. Реализуется это с помощью правил (подробнее см. в п. Виды и предназначение правил, наборы правил).*

4. На вкладке **За трафик** настройте способ тарификации. Для этого выберите один из следующих вариантов:
   - **Только входящий** – в тарифе будет учитываться только входящий трафик, то есть весь исходящий трафик будет бесплатным;
   - **Только исходящий** – в тарифе будет учитываться только исходящий трафик, то есть весь входящий трафик будет бесплатным;
   - **Сумма входящего и исходящего** – тарифицироваться будет сумма входящего и исходящего трафика;
   - **Максимальное значение** – тарифицироваться будет тот трафик (входящий или исходящий), который пользователь потратил больше за весь учетный период.

На этой же вкладке настройте параметры тарификации.

- Укажите количество бесплатных мегабайт, входящих в данный тариф, или введите значение "0", если тарифне подразумевает наличие предоплаченного трафика.
- Если исходящий трафик платный, то при необходимости задайте его стоимость (в процентах относительно стоимости, указанной на вкладке **Настройки**). Имеет смысл в тех случаях, когда у провайдера стоимость исходящего трафика отличается от стоимости входящего. По умолчанию используется значение "100%", при котором стоимость исходящего равна входящему. Настройка корректирует объем всех исходящих данных, поступающих для учета, т.е. все данные отображаются уже с учетом этой поправки.
- При необходимости укажите стоимость трафика, извлекаемого из кэша HTTP-прокси (в процентах относительно стоимости, заданной на вкладке **Настройки**). По умолчанию используется значение "0%", при котором трафик из кэша не тарифицируется.
- При необходимости укажите в данном поле стоимость почтового трафика (в процентах относительно стоимости, заданной на вкладке **Настройки**). По умолчанию используется значение "100%", то есть почтовый трафик тарифицируется наравне с обычным.

5. На вкладке **Абонентская плата** выберите тип абонентской платы:

- **Почасовая за реальное время работы** – выберите это значение в том случае, если абонентская плата должна начисляться за реальное время работы. При этом Traffic Inspector будет учитывать поминутно только то время, когда пользователь активен. При выборе этого варианта задается стоимость за час работы.
- **Посуточная за время сессии** – выберите этот вариант, если абонентская плата должна начисляться посуточно за все время сессии с начала ее старта независимо от состояния пользователя. При этом задается стоимость за сутки работы.

Замечание! *Для временного приостановления начисления абонентской*

*платы можно перевести пользователя в состояние **Пауза**.*

6. На вкладке **Лимиты** с помощью переключателя выберите способ расчета лимита.

   - **Лимит на трафик** – выберите этот вариант, если нужно, чтобы лимит вычислялся как трафик в мегабайтах на основании заданного на вкладке **За трафик** способа тарификации. При этом можно задать отдельные лимиты потребляемого трафика в мегабайтах (если задано значение "0", то лимит отсутствует) на сутки, неделю и месяц.

   - **Лимит на деньги** – выберите этот вариант, если нужно, чтобы лимит вычислялся не в мегабайтах, а в выбранных на вкладке **Настройки** единицах измерения. При этом Traffic Inspector сначала вычисляет трафик в мегабайтах на основании заданного способа тарификации, после чего переводит его, в соответствии с ценой, в стоимость. При этом можно задать отдельные лимиты потребляемого трафика в мегабайтах (если задано значение "0", то лимит отсутствует) на сутки, неделю и месяц.

7. Сохраните внесенные изменения. Если изменялся уже существующий тариф, то будет автоматически запущен мастер смены тарифа (см. ниже).

Создание/изменение тарифа с учетом времени подключения

Для создания нового или изменения существующего тарифа с учетом времени подключения выполните следующие действия:

1. Откройте окно свойств нового или существующего тарифа. Сделать это можно с помощью контекстного меню в разделе **Учет трафика -> Тарифы** консоли администратора или в блоке **Тарифы**, размещенном на главной странице раздела **Учет трафика**.

2. Введите на вкладке **Тариф** наименование тарифа и, при необходимости, произвольные примечания. Здесь же выберите тип тарифа – **По времени**.

3. На вкладке **Настройки** установите основные параметры тарифа.

   - Если нужно, чтобы при запуске сессии пользователю на счет сразу начислялась какая-то сумма, то укажите ее в поле **Оплата по умолчанию**. Обратите внимание, что

указанная сумма будет автоматически присваиваться пользователю при его автодобавлении.

- Если нужно, чтобы в тарифе была предусмотрена возможность работы в кредит, то укажите сумму кредита. В этом случае будет возможна работа пользователя при отрицательном балансе, не превышающем размер кредита (при превышении работа пользователя будет заблокирована). В противном случае введите значение "0".

> ***Замечание!*** *Traffic Inspector позволяет задать особые условия при работе пользователя в кредит. Например, можно ограничить его скорость, запретить доступ к определенному контенту и пр. Реализуется это с помощью правил (подробнее см. в п. Виды и предназначение правил, наборы правил).*

4. При необходимости на вкладке **Лимиты** задайте лимиты на время подключения пользователя в часах (если задано значение "0", то лимит отсутствует). Лимиты можно задавать на сутки, неделю и месяц.
5. Сохраните внесенные изменения. Если изменялся уже существующий тариф, то будет автоматически запущен мастер смены тарифа (см. ниже).

Назначение тарифа по умолчанию

В Traffic Inspector существует тариф **<Default>**, являющийся тарифом по умолчанию. Однако при необходимости можно назначить тарифом по умолчанию любой другой тариф. Сделать это можно с помощью контекстного меню в разделе **Учет трафика -> Тарифы** консоли администратора. При назначении тарифа по умолчанию будет запущен мастер смены тарифа (см. ниже). После завершения этого мастера выбранный тариф станет тарифом по умолчанию. При этом его наименование сменится на **Default**.

Смена тарифа

Процедура смены тарифа осуществляется с помощью специального мастера, который

автоматически запускается всегда после изменения тарифов, а также при всех действиях с пользователями, группами и коллективными счетами, связанными со сменой основного тарифа. Она необходима, чтобы корректно сменить тариф для использующих его пользователей.

Для смены тарифа выполните следующие действия:

1. На вкладке **Выберите действие** окна мастера выберите действие, которое должно быть выполнено с лицевыми счетами пользователей данного тарифа.
   - **Перерасчет** – при выборе данного действия баланс пользователя будет пересчитан с учетом нового тарифа, учетный период при этом не изменяется.
   - **Новая сессия биллинга** – при выборе данного действия будет запущена новая сессия биллинга (новый учетный период). При этом баланс лицевого счета пользователя обнуляется (на него может быть зачислена определенная сумма, см. описание настроек тарифа).
   - **Новая сессия биллинга с переносом остатков** – данный вариант аналогичен предыдущему, однако в новую сессию биллинга будут перенесены текущий баланс лицевого счета пользователя.
2. На вкладке **Комментарий администратора** введите комментарий, поясняющий причину смены тарифа. При необходимости включите его показ пользователям. В этом случае данный комментарий будет виден пользователям в отчетах.
3. Запустите процесс и дождитесь его завершения.

Удаление тарифа

Удаление тарифа осуществляется с помощью контекстного меню в разделе **Учет трафика -> Тарифы** консоли администратора.

> ***Замечание!*** *Тариф не может быть удален, если он используется в других настройках программы. При попытке удаления такого тарифа будет выведено сообщение об ошибке с указанием настройки, использующей этот*

тариф.

Коллективные счета

Коллективные счета позволяют вести учет затрат на Интернет не индивидуально по каждому пользователю, а суммарно по группам или определенным пользователям. При этом возможна комбинированная система учета. То есть некоторые пользователи могут работать по своим собственным индивидуальным счетам, а другие – по одному или нескольким коллективным.

Коллективный счет можно назначить целой группе. При этом он автоматически назначается всем ее членам. Выполняется эта операция на вкладке **Тарификация** окна свойств группы (подробнее см. в п. Создание и настройка групп). Также коллективный счет можно назначить отдельному пользователю. Сделать это можно на вкладке **Тарификация** окна свойств пользователя (подробнее см. в п. Создание и настройка пользователей). Кроме того, назначать коллективный счет группам и пользователям можно с помощью специальной операции добавления члена коллективного счета (см. ниже).

Список коллективных счетов расположен в разделе **Учет трафика -> Коллективные счета** консоли администратора. Также для каждого коллективного счета в данном разделе создается собственный подраздел. В нем отображается список участников коллективного счета. Кроме того, в разделе **Учет трафика** есть блок **Коллективные счета**, состоящий из двух вкладок. На вкладке **Информация** отображается общее количество созданных в системе коллективных счетов, а на вкладке **Действия** – ссылки на некоторые операции.

В рамках управления коллективными счетами в Traffic Inspector реализованы следующие операции:

- создание/изменение коллективного счета;
- настройка атрибутов коллективного счета;
- добавление членов коллективного счета;
- удаление коллективного счета.

Работа Traffic Inspector с сетевыми интерфейсами

8

Создание/изменение коллективного счета

Для создания нового или изменения существующего коллективного счета выполните следующие действия:

1. Откройте окно свойств нового или существующего коллективного счета. Сделать это можно с помощью контекстного меню в разделе **Учет трафика -> Коллективные счета** консоли администратора или в блоке **Коллективные счета**, размещенном на главной странице раздела **Учет трафика**.

2. Введите на вкладке **Наименование** наименование коллективного счета, при необходимости, произвольные примечания.

3. На вкладке **Тарификация** определите способ тарификации членов группы. Здесь возможны два варианта:

   - **Использовать основной тариф** – для всех членов группы будет использоваться единый, указанный здесь же тариф, вне зависимости от их персональных настроек.
   - **Использовать дополнительные тарифы** – тарификация для каждого члена коллективного тарифа будет осуществляться по его персональным правилам (заданным в свойствах пользователя программы или свойствах его группы).

4. На вкладке **Блокировки** выберите способ учета баланса. Здесь возможны два варианта:

   - **Автоотключение** – заблокировать всех членов коллективного счета, если его баланс станет отрицательным (работа в кредит для коллективных счетов не поддерживается).
   - **Безлимитный** – работа всех членов коллективного счета будет доступна вне зависимости от значения его баланса.

   На этой же вкладке разрешите или запретите автоматическую блокировку работы пользователей, если коллективный счет находится в состояниях **Стоп** или **Пауза**.

5. При необходимости настройте на вкладке **Автоматизация** выполнение скриптов

автоматизации и других операций для членов коллективного счета. Если нужно, чтобы при изменении состояния счета система автоматически выполняла определенное действие, то включите запуск соответствующего скрипта (подробнее о скриптах см. в SDK). Также при необходимости включите реагирование системы на превышение заданных в тарифе лимитов (подробное описании тарифов см. в п. Тарифы). При включении укажите одно из двух возможных действий – блокирование коллективного счета или выполнение указанного скрипта.

6. На вкладке **Запись в журнал** настройте параметры записи данных о состоянии членов коллективного счета в базу данных журналов. Они могут загружаться из общих настроек или задаваться для членов коллективного счета индивидуально.

7. Сохраните внесенные изменения.

Настройка атрибутов коллективного счета

Атрибуты используются для хранения любой дополнительной информации объекта конфигурации (подробнее см. в п. Атрибуты). Изменение атрибутов коллективного счета осуществляется в специальном окне, запустить которое можно с помощью контекстного меню в разделе **Учет трафика -> Коллективные счета** консоли администратора. В этом окне отображается список всех атрибутов, которые могут устанавливаться для коллективных счетов. Значения атрибутов можно вводить вручную или выбирать в выпадающем списке (для некоторых типов атрибутов) их значение.

Добавление членов коллективного счета

Операция добавления членов коллективного счета позволяет задавать целым группам или отдельным пользователям данный коллективный счет, отключая для них персональное ведение баланса.

> ***Замечание!*** *Также назначить группам и отдельным пользователям коллективный счет можно в их свойствах (подробнее см. п. Создание и*

настройка групп и п. Создание и настройка пользователей).

Для добавления членов коллективного счета выполните следующие действия.

1. Откройте окно добавления членов коллективного счета. Сделать это можно с помощью контекстного меню в подразделе коллективного счета раздела **Учет трафика -> Коллективные счета** консоли администратора.

2. На вкладке **Выбор** определите, кого вы будете добавлять – целые группы или отдельных пользователей.

3. Если было выбрано добавление групп, то на вкладке **Выбор группы** укажите одну или несколько групп, которые будут добавлены в члены коллективного счета.

4. Если было выбрано добавление пользователей, то в окне **Выбор пользователей** с помощью поиска (подробнее о работе в окне см. в п. Поиск пользователей) выведите список пользователей и отметьте среди них одного или нескольких нужных.

5. Сохраните внесенные изменения.

Удаление коллективного счета

Удаление коллективных счетов осуществляется с помощью контекстного меню в разделе **Учет трафика -> Коллективные счета** консоли администратора.

Правила сетей

Правила сетей позволяют задавать правила для IP-сетей. В них могут быть описаны как отдельные компьютеры по IP-адресам, так целые и сети в виде диапазонов IP-адресов. При применении правил список просматривается сверху вниз. Выбирается и применяется только одно самое первое правило, которое попало под условие. Поэтому, если задан диапазон адресов, порядок правил имеет значение.

В Traffic Inspector есть одно предустановленное правило **All IP addresses**, которое описывает все адреса в диапазоне 0.0.0.0 – 255.255.255.255. Оно используется для задания настроек правил по умолчанию и всегда размещается внизу списка. То есть описанные в

нем настройки применяются ко всем сетям, которые не попали под действие других правил сетей. Удалить это правило через консоль администратора нельзя. Если по какой-то причине оно все же было удалено, то его следует ввести заново.

Список правил сетей находится в разделе **Правила -> Правила сетей** консоли администратора. Также в разделе **Правила** есть блок **Правила сетей**, состоящий из двух вкладок. На вкладке **Информация** отображается общее количество созданных в системе правил сетей, а на вкладке **Действия** – ссылки на некоторые операции.

В рамках управления правилами сетей в Traffic Inspector реализованы следующие операции:

- создание/изменение правила сетей;
- удаление правила сетей.

Создание/изменение правила сетей

Для создания нового или изменения существующего правила сетей выполните следующие действия:

1. Откройте окно свойств нового или существующего правила сетей. Сделать это можно с помощью контекстного меню в разделе **Правила -> Правила сетей** или в блоке **Правила сетей**, расположенном на главной странице раздела **Правила**.
2. На вкладке **Наименование** введите уникальное наименование правила сетей и, при необходимости, произвольное примечание.
3. На вкладке **IP адреса и сети** определите сети, которые будут обрабатываться данным правилом. Сделать это можно вручную или с помощью определенных ранее IP-сетей (подробнее про IP-сети см. в п. IP-сети). В первом случае укажите один конкретный IP-адрес или IP-адреса границ диапазона. Во втором - выберите предварительно созданную IP-сеть. При выборе этого варианта можно непосредственно с данной вкладки перейти к редактированию активной или созданию новой IP-сети.
4. Если возможна ситуация, когда работа нескольких пользователей будет осуществляться

с одного IP-адреса (обычно это происходит при использовании сервера терминалов), то на вкладке **Сервер терминалов** включите одноименный флажок. При этом будет отключена сквозная авторизация с указанного IP-адреса, а для каждой сессии HTTP-прокси или SOCKS будет запрашиваться отдельная аутентификация. Это обеспечит корректный подсчет трафика для каждого пользователя сервера терминалов.

> ***Замечание!*** *Рекомендуется создать соответствующее правило для каждого сервера терминалов. В каждом таком правиле на вкладке* ***IP адреса и сети*** *необходимо указать IP-адрес одного сервера терминалов.*

5. На вкладке **Аутентификация** настройте следующие параметры аутентификации:

- Разрешите или запретите BASIC аутентификацию через HTTP. Если есть риск перехвата трафика сети злоумышленниками, то данный способ аутентификации лучше запретить, поскольку при нем данные передаются в открытом виде.
- Разрешите или запретите использование NTLM для авторизации, интегрированной с Windows. Имеет смысл запретить данный способ аутентификации, если NTLM не используется.

> ***Замечание!*** *Для протокола SSL, при котором трафик передается в зашифрованном виде, оба вида аутентификации разрешены всегда, вне зависимости от состояния флажков.*

- При необходимости укажите минимальный промежуток времени (в секундах) между запросами на авторизацию. Если ввести значение "0", то ограничение не устанавливается.

6. Сохраните внесенные изменения.

Удаление правила сетей

Удаление правил сетей осуществляется с помощью контекстного меню в разделе **Правила -> Правила сетей** консоли администратора.

Работа Traffic Inspector с сетевыми интерфейсами

8

Перенаправление запросов

В Traffic Inspector реализована возможность перенаправления исходящих TCP-соединений пользователей, которые задаются с помощью правил перенаправления. Для перенаправленного трафика правила пользователей работают в контексте перенаправленных IP-адресов и портов. В сетевой статистике будут отображаться перенаправленные IP-адреса и порты. Для перенаправленного трафика не будет работать правило блокировки **HTTP мимо прокси**, что позволяет сделать перенаправление HTTP-трафика на любой сервер аналогично встроенному Transparent Proxy. Перенаправление работает на уровне драйвера программы и позволяет перенаправить любой TCP-трафик.

Список правил перенаправления находится в разделе **Правила -> Перенаправление запросов** консоли администратора. Также в разделе **Правила** есть блок **Перенаправление запросов**, состоящий из двух вкладок. На вкладке **Информация** отображается общее количество созданных в системе правил перенаправления, а на вкладке **Действия** – ссылки на некоторые операции.

В рамках управления правилами перенаправления запросов в Traffic Inspector реализованы следующие операции:

- создание/изменение правила перенаправления;
- удаление правила перенаправления.

Создание/изменение правила перенаправления

Для создания нового или изменения существующего правила перенаправления выполните следующие действия.

1. Откройте окно свойств нового или существующего правила перенаправления. Сделать это можно с помощью контекстного меню в разделе **Правила -> Перенаправление запросов** консоли администратора или в блоке **Перенаправление запросов**, размещенном на главной странице раздела **Правила**.
2. На вкладке **Наименование** введите в поле уникальное наименование правила и, при необходимости, произвольное примечание.

3. При необходимости на этой же вкладке временно отключите правило перенаправления, не удаляя его совсем.

4. На вкладке **Условия** задайте условие, при выполнении которого будет выполняться перенаправление TCP-соединения. Сделать это можно вручную или с помощью определенных ранее IP-сетей (подробнее про IP-сети см. в п. IP-сети). В первом случае введите один конкретный IP-адрес или IP-адреса границ диапазона. Во втором - укажите предварительно созданную IP-сеть. При выборе этого варианта можно перейти к редактированию активной или созданию новой IP-сети непосредственно с данной вкладки. Здесь же укажите TCP-порт или TCP-порты, при попытке соединения по которым будет выполняться перенаправление.

5. На вкладке **Перенаправление** укажите, куда должны перенаправляться удовлетворяющие заданным условиям TCP-соединения. Это может быть IP-адрес сетевого интерфейса сервера, со стороны которого идет запрос, или произвольный IP-адрес. При необходимости укажите номер TCP-порта, на который будет меняться TCP-порт соединения.

6. Если перенаправляемый с помощью данного порта трафик нужно сделать нетарифицируемым (то есть бесплатным), то включите эту возможность на вкладке **Перенаправление**.

7. Сохраните внесенные изменения.

Удаление правила перенаправления

Удаление правила перенаправления осуществляется с помощью контекстного меню в разделе **Правила -> Перенаправление запросов** консоли администратора.

Работа с внешними интерфейсами

В рамках настройки служб Traffic Inspector, привязанных к сетевым интерфейсам внешних сетей решаются следующие задачи:

- создание и настройка счетчиков трафика;

- публикация служб;
- настройка резервирования каналов связи.

Счётчики трафика

Важной особенностью Traffic Inspector является двойной учет трафика. Биллинг учитывает трафик пользователей, снимая его с внутренних интерфейсов. Однако данные биллинга не позволяют точно оценить трафик, потребляемый у провайдера, т.к. трафик может потреблять сам сервер, какой-то трафик может быть неавторизованным и т.д.

В Traffic Inspector дополнительно к биллингу представлен учет внешнего трафика. Внешний трафик снимается с внешних интерфейсов. Его учет решают следующие задачи:

- контроль суммарного трафика, потребляемого у провайдера, с целью проверить выставленные им счета, планирования потребления трафика, предстоящих затрат и недопущения его перерасхода;
- детальный анализ потребления в контексте ресурсов, внешних сетей, протоколов, портов и прочих критериев;
- учет и анализ трафика, отфильтрованного на сетевом экране.

Теоретически сумма трафика всех пользователей должна соответствовать суммарному трафику, потребляемому у провайдера, но в реальных условиях появляются расхождения:

- трафик пользователей снимается с внутренних интерфейсов, и невозможно учесть трафик, потребляемый самим сервером. Это относится как к различным служебным запросам, связанным с функционированием сети (ICMP, DNS), так и к трафику других служб, установленных на нем;
- бывают ситуации, когда пользователи работают на самом сервере, также потребляя трафик;
- некоторый трафик из внутренней сети может получиться неавторизованным, если есть разрешающие правила для всех на внешние сети;
- данные по трафику для пользователей заносятся в его счетчики уже с учетом скидок,

Работа Traffic Inspector с сетевыми интерфейсами 8

заданных в правилах. Некоторый трафик может быть описан как бесплатный.

Для решения задач учета внешнего трафика используются внешние счетчики. Счетчики могут быть контролируемыми и информационными. Общий список внешних счетчиков размещен в разделе **Учет трафика -> Счетчики** консоли администратора. Главная страница этого разделе поделена на две части. В верхней отображается перечень зарегистрированных в системе счетчиков, а в нижней – состояние выделенного в данный момент счетчика и сетевая статистика по нему.

Также на главной странице раздела **Учет трафика** есть блок **Внешние счетчики**, который состоит из двух вкладок. На вкладке **Информация** отображается общее количество контролируемых и информационных счетчиков, а на вкладке **Действие** – ссылки на некоторые операции с ними.

Настройка отображения

В Traffic Inspector реализована возможность настройки отображения информации со счетчиков трафика. Для этого выполните следующие действия.

1. Откройте окно настройки отображения. Сделать это можно из блока **Внешние счетчики**, расположенного на главной странице раздела **Учет трафика** консоли администратора.
2. Перейдите на вкладку **Автообновление страниц** и задайте параметры автоматического обновления информации с внешних счетчиков. Если необходимо, чтобы данные автоматически обновлялись на страницах консоли администратора, то включите флажок **Автообновление страниц с данными** и укажите интервал (в секундах) обновления. Автообновление данных в мониторах работы включено всегда. При необходимости измените в соответствующем разделе заданный интервал обновления (по умолчанию он равен 5 секундам).
3. При необходимости измените внешний редактор, который используется для редактирования текстов, например, списков (по умолчанию качестве внешнего редактора используется Notepad, входящий в комплект поставки операционных систем

семейства Windows). Для этого перейдите на вкладку **Внешний редактор** и укажите его.

4. Перейдите на вкладку **Сетевая статистика** и настройте следующие параметры отображения сетевой статистики в мониторах работы:

   - Максимальное количество строк, которое может отображаться в мониторах работы.
   - Включите или выключите отображение данных в мониторах пользователей в мегабайтах. Во втором случае данные будут показываться в байтах.
   - Включите или выключите отображение сведений по количеству переданных/принятых сетевых пакетов в мониторах работы.
   - Включите или выключите отображение данных в мониторах внешних счетчиков в мегабайтах. Во втором случае данные будут показываться в байтах.

5. Сохраните внесенные изменения.

Контролируемые счетчики

Контролируемые счетчики предназначены для контроля потребления трафика от вышестоящего провайдера как платного ресурса. Провайдеров может быть несколько. Кроме того, у провайдера возможна разная тарификация для разных сетей. Контролируемые счетчики описываются как внешние IP-адреса или сети, в них в качестве условия можно задать внешний интерфейс.

Каждый пакет, снимаемый драйвером на внешних интерфейсах, проверяется в списке контролируемых счетчиков на предмет соответствия и учитывается только на самом первом счетчике, условиям которого он соответствует. Порядок счетчиков в этом списке имеет принципиальное значение. Самым последним в этом списке обязательно должен быть счетчик на весь трафик – он по умолчанию создается после установки программы (счетчик **Весь Интернет**), и его удалять ни в коем случае нельзя. Таким образом, каждый пакет должен быть учтен только на одном счетчике, а сумма по всем счетчикам – соответствовать суммарному трафику, потребленному у провайдеров.

Общее правило настройки контролируемых счетчиков – необходимо создать отдельные счетчики для каждого вышестоящего провайдера. Причем для каждого типа трафика с

отдельным тарифом у вышестоящего провайдера создается отдельный счетчик. Допустим, у провайдера есть льготный трафик, например, бесплатный внутрисетевой или льготный местный – описание этого производится в отдельных контролируемых счетчиках. В результате количество контролируемых счетчиков может быть больше, чем количество вышестоящих провайдеров.

Общий список всех внешних счетчиков (контролируемых и информационных) находится в разделе **Учет трафика -> Счетчики** консоли администратора. Помимо этого в этом разделе отдельно для контролируемых счетчиков есть специальный подраздел.

В рамках управления контролируемыми счетчиками в Traffic Inspector реализованы следующие операции:

- общие настройки контролируемых счетчиков;
- создание/изменение контролируемого счетчика;
- настройка атрибутов контролируемого счетчика;
- сброс контролируемого счетчика;
- удаление контролируемого счетчика.

Общие настройки контролируемых счетчиков

Общие настройки позволяют задавать настройки, которые будут применяться для контролируемых счетчиков по умолчанию. Однако, при необходимости, можно отключить использование этих настроек непосредственно в свойствах счетчика и задать индивидуальные параметры (см. ниже).

Для установки общих параметров контролируемых счетчиков выполните следующие действия:

1. Откройте окно настройки общих параметров контролируемых счетчиков. Сделать это можно с помощью контекстного меню в разделе **Учет трафика -> Счетчики -> Контролируемые счетчики** консоли администратора.

2. При необходимости на вкладке **Контролируемые счетчики** включите ведение сетевой статистики и укажите интервал ее записи, количество записываемых направлений (записываются самые активные направления) и минимальное количество сетевых пакетов, необходимых для записи (берется максимальное значение от исходящих и входящих пакетов).
3. Настройте параметры записи трафика в журнал. Для этого укажите периодичность (в минутах), с которой трафик будет сохраняться.
4. Сохраните внесенные изменения.

Создание/изменение контролируемого счетчика

Для создания нового или изменения существующего контролируемого счетчика выполните следующие действия:

1. Откройте окно свойств нового или существующего контролируемого счетчика. Сделать это можно с помощью контекстного меню в разделе **Учет трафика -> Счетчики -> Контролируемые счетчики** консоли администратора или в блоке **Внешние счетчики**, расположенном на главной странице раздела **Учет трафика**.
2. На вкладке **Наименование** введите уникальное наименование контролируемого счетчика и, при необходимости, произвольное примечание. Здесь же можно при необходимости временно заблокировать счетчик, не удаляя его. При этом счетчик не будет считать трафик, а также система не будет предпринимать никаких действий, связанных с его состоянием (например, блокировать сети).

   Замечание! *Счетчик* ***Весь Интернет*** *(счетчик по умолчанию для всего трафика) запретить нельзя.*

4. На вкладке **Условия** выберите внешний сетевой интерфейс, с которого будет снимать трафик данный счетчик. Если нужно снимать трафик со всех внешних интерфейсов, то укажите значение "-".
5. Если данный счетчик должен учитывать трафик, поступающий только с определенного

IP-адреса или сети, то укажите их в разделе **Внешняя сторона** на вкладке **IP адрес**. Сделать это можно вручную или с помощью определенных ранее IP-сетей (подробнее про IP-сети см. в п. IP-сети). В первом случае укажите один конкретный IP-адрес или IP-адреса границ диапазона, а во втором – предварительно созданную IP-сеть. При выборе второго варианта с помощью кнопок можно перейти к редактированию активной или созданию новой IP-сети непосредственно с данной вкладки.

6. Если данный счетчик должен учитывать только трафик, поступающий на определенный внутренний IP-адрес или сеть, укажите их в разделе **Сторона сервера** на вкладке **IP адрес**.

7. При необходимости на вкладке **Лимиты** настройте лимиты данного счетчика. Всего может быть три вида ограничений, каждый из которых может быть настроен как на прием, так и на передачу.

   - **Предупреждение** – при превышении данных лимитов администратору или администраторам с помощью службы SMTP отправляется уведомление (для этого должно быть настроено соответствующее действие, см. ниже).

   - **Лимит блокировки** – при превышении данных лимитов, помимо отправки сообщения администратору, система заблокирует внешнее соединение. Если в счетчике заданы конкретные сети, то блокируется доступ только на эти сети. Если же счетчик задан на весь трафик, то доступ во внешнюю сеть отключается полностью кроме сетей, описанных другими счетчиками. Эти меры могут быть весьма полезны, когда администратору приходится на какое-то время оставлять сеть без присмотра, и блокирование доступа в Интернет становится предпочтительнее, чем перерасход трафика. Появление различных новых вирусов, распространяющихся через Интернет и приводящих к генерации огромного трафика за небольшое время, делает наличие такой возможности весьма важным.

   - **Ежедневный лимит блокировки** – аналогичен предыдущему лимиту, однако трафик считается посуточно отдельным счетчиком, который будет обнуляться в полночь.

8. На вкладке **Действия** включите или отключите основные действия, выполняемые Traffic Inspector при превышении лимитов:

   - Блокирование внешних сетей при превышении лимитов **Лимит блокировки** и **Ежедневный лимит блокировки**.
   - Оповещение администраторов по электронной почте при изменении состояния счетчика (для этого должна быть настроена рассылка в службе отправки Traffic Inspector, подробнее см. в п. Служба отправки).

9. При блокировке или отмене блокировки система может автоматически запускать произвольную внешнюю программу или сценарий. Это применяется для выполнения различных действий, например, можно автоматически поднять резервный канал Интернета или произвести некоторую информационную рассылку. Для настройки этой возможности перейдите на вкладку **Запуск внешний программ** и укажите исполняемый файл нужной программы или файл сценария, строку параметров их запуска и рабочую папку.

10. В Traffic Inspector реализована возможность автоматического запуска внутренних скриптов при изменении статуса счетчика. При необходимости включите ее на вкладке **Автоматизация** и укажите предварительно созданный скрипт (подробнее о скриптах см. в документации по SDK).

11. Если для данного счетчика нужно установить собственные параметры записи сетевой статистики, отличные от обычных (см. выше), то на вкладке **Сетевая статистика** отключите их загрузку из параметров по умолчанию и настройте их самостоятельно (описание параметров см. выше в разделе **Общие настройки контролируемых счетчиков**).

12. Если для данного счетчика нужно установить собственные параметры записи трафика в журнал, то на вкладке **Журнал** отключите их загрузку из параметров по умолчанию и настройте их самостоятельно (описание параметров см. выше в разделе **Общие настройки контролируемых счетчиков**).

13. Сохраните внесенные изменения.

Работа Traffic Inspector с сетевыми интерфейсами

8

Настройка атрибутов контролируемого счетчика

Атрибуты используются для хранения любой дополнительной информации объекта конфигурации (подробнее см. в п. Атрибуты). Изменение атрибутов контролируемого счетчика осуществляется в специальном окне, запустить которое можно с помощью контекстного меню в разделе **Учет трафика -> Счетчики -> Контролируемые счетчики** консоли администратора. В этом окне отображается список всех атрибутов, которые могут устанавливаться для контролируемых счетчиков. Значения атрибутов можно вводить вручную или выбирать в выпадающем списке (для некоторых типов атрибутов) их значение.

Сброс контролируемого счетчика

Под сбросом контролируемого счетчика понимается обнуление всех его данных. Выполнение этой операции осуществляется с помощью контекстного меню в разделе **Учет трафика -> Счетчики** консоли администратора.

Удаление контролируемого счетчика

Удаление контролируемого счетчика осуществляется с помощью контекстного меню в разделе **Учет трафика -> Счетчики -> Контролируемые** консоли администратора.

> ***Замечание!*** *Счетчик, описывающий по умолчанию весь трафик (**Весь Интернет**) удалить нельзя.*

Информационные счетчики

Информационные счетчики служат для отдельного учета потребления различного трафика с целью последующего анализа. При их конфигурировании, кроме внешних сетей и интерфейсов, можно задать тип IP-протокола, а также порты для TCP и UDP. В информационных счетчиках пакеты учитываются для каждого счетчика независимо от других, т.е. возможны ситуации, когда пакет не учитывается ни в одном счетчике или учитывается сразу в нескольких счетчиках.

Работа Traffic Inspector с сетевыми интерфейсами

8

При установке программы по умолчанию имеется несколько информационных счетчиков для наиболее используемых протоколов – HTTP, FTP, SMTP, POP3 и других.

Для информационного счетчика может быть задан особый тип – **Счетчик безопасности**. Это счетчик, учитывающий только отфильтрованный трафик на внешнем сетевом экране. Он устанавливается на входящий или исходящий трафик. Это полезно для анализа различных сетевых атак и сетевого "мусора": флуда, сканирования портов, ICMP. Один такой счетчик на весь отфильтрованный трафик присутствует по умолчанию. При необходимости вместо одного такого счетчика можно добавить несколько, введя разграничения по различным критериям.

Общий список всех внешних счетчиков (контролируемых и информационных) находится в разделе **Учет трафика -> Счетчики** консоли администратора. Помимо этого в этом разделе отдельно для информационных счетчиков есть специальный подраздел.

В рамках управления информационными счетчиками в Traffic Inspector реализованы следующие операции:

- общие настройки информационных счетчиков;
- создание/изменение информационного счетчика;
- настройка атрибутов информационного счетчика;
- сброс информационного счетчика;
- удаление информационного счетчика.

Общие настройки информационных счетчиков

Общие настройки позволяют задавать настройки, которые будут применяться для информационных счетчиков по умолчанию. Однако при необходимости можно отключить использование этих настроек непосредственно в свойствах счетчика и задать индивидуальные параметры (см. ниже).

Для установки общих параметров информационных счетчиков выполните следующие действия:

1. Откройте окно настройки общих параметров информационных счетчиков. Сделать это можно с помощью контекстного меню в разделе **Учет трафика -> Счетчики -> Информационные счетчики**.

2. При необходимости на вкладке **Информационные счетчики** включите ведение сетевой статистики и укажите интервал ее записи, количество записываемых направлений (записываются самые активные направления) и минимальное количество сетевых пакетов, необходимых для записи (берется максимальное значение от исходящих и входящих пакетов).

3. Настройте параметры записи трафика в журнал. Для этого укажите периодичность (в минутах), с которой трафик будет сохраняться.

4. Сохраните внесенные изменения.

Создание/изменение информационного счетчика

Для создания нового или изменения существующего информационного счетчика выполните следующие действия.

1. Откройте окно свойств нового или существующего информационного счетчика. Сделать это можно с помощью контекстного меню в разделе **Учет трафика -> Счетчики -> Информационные счетчики** консоли администратора или в блоке **Внешние счетчики**, расположенном на главной странице раздела **Учет трафика**.

2. На вкладке **Наименование** введите уникальное наименование информационного счетчика и, при необходимости, произвольное примечание. Здесь же можно при необходимости временно заблокировать счетчик, не удаляя его. При этом счетчик не будет считать трафик, а также система не будет предпринимать никаких действий, связанных с его состоянием (например, блокировать сети).

4. На вкладке **Тип счетчика** выберите тип информационного счетчика:

   - **Обычный** – ведет учет трафика, который пропущен драйвером Traffic Inspector на внешних интерфейсах;

- **Счетчик безопасность (Вх.)** – ведет учет входящего трафика, который был отфильтрован, то есть заблокирован сетевым экраном, используется для анализа сетевой активности.

- **Счетчик безопасность (Исх.)** – аналогичен предыдущему, но ведет учет исходящего трафика.

5. На вкладке **Условия** выберите внешний сетевой интерфейс, с которого будет снимать трафик данный счетчик. Если нужно снимать трафик со всех внешних интерфейсов, то выберите значение "-".

6. Если данный счетчик должен учитывать трафик, поступающий только с определенного IP-адреса или сети, то укажите их в разделе **Внешняя сторона** на вкладке **IP адрес**. Сделать это можно вручную или с помощью определенных ранее IP-сетей (подробнее про IP-сети см. в п. IP-сети). В первом случае укажите один конкретный IP-адрес или IP-адреса границ диапазона, а во втором – предварительно созданную IP-сеть. При выборе второго варианта можно перейти к редактированию активной или созданию новой IP-сети непосредственно из данной вкладки.

7. Если данный счетчик должен учитывать только поступающий определенный внутренний IP-адрес или сеть, укажите их в разделе **Сторона сервера** на вкладке **IP адрес**.

8. Если данный счетчик должен учитывать только трафик, передаваемый по определенному протоколу, то укажите его и, при необходимости, сетевой порт. Сделать это можно с помощью подсказки или вручную. В первом случае выберите в шаблон одного из наиболее распространенных типов трафика (например, ICMP, DNS client, HTTP client, FTP client и т.п.). При этом все параметры будут настроены автоматически.

   Для ручной настройки выберите нужный протокол. Если был выбран вариант UDP или TCP, то также укажите сетевой порт. Это может быть конкретный номер, диапазон номеров сетевых портов или динамический порт.

9. В Traffic Inspector реализована возможность автоматического запуска внутренних скриптов при изменении статуса счетчика. При необходимости включите ее на вкладке

Автоматизация и укажите предварительно созданный скрипт (подробнее о скриптах см. в документации по SDK).

10. Если для данного счетчика нужно установить собственные параметры записи сетевой статистики, отличные от обычных (см. выше), то на вкладке **Сетевая статистика** выключите загрузку параметров по умолчанию и самостоятельно настройте их (описание параметров см. выше в разделе **Общие настройки информационных счетчиков**).

11. Если для данного счетчика нужно установить собственные параметры записи трафика в журнал, то на вкладке **Журнал** выключите загрузку параметров по умолчанию и самостоятельно настройте их (описание параметров см. выше в разделе **Общие настройки информационных счетчиков**).

12. Сохраните внесенные изменения.

Настройка атрибутов информационного счетчика

Атрибуты используются для хранения любой дополнительной информации объекта конфигурации (подробнее см. в п. Атрибуты). Изменение атрибутов информационного счетчика осуществляется в специальном окне, запустить которое можно с помощью контекстного меню в разделе **Учет трафика -> Счетчики -> Информационные счетчики** консоли администратора. В этом окне отображается список всех атрибутов, которые могут устанавливаться для информационных счетчиков. Значения атрибутов можно вводить вручную или выбирать в выпадающем списке (для некоторых типов атрибутов) их значение.

Сброс информационного счетчика

Под сбросом информационного счетчика понимается обнуление всех его данных. Выполнение этой операции осуществляется с помощью контекстного меню в разделе **Учет трафика -> Счетчики** консоли администратора.

Работа Traffic Inspector с сетевыми интерфейсами

8

Удаление информационного счетчика

Удаление информационного счетчика осуществляется с помощью контекстного меню в разделе **Учет трафика -> Счетчики -> Информационные** консоли администратора.

Публикация служб

В Traffic Inspector реализована функция публикации служб. Она используется для обеспечения доступа к внутренним ресурсам локальной сети из Интернета. С ее помощью можно опубликовать корпоративный почтовый сервер, веб-сервер, FTP-сервер и т.п. В Traffic Inspector сразу после инсталляции есть предустановки для публикации наиболее популярных служб (HTTP, FTP, RDP и пр.).

В рамках публикации служб реализованы следующие функции:

- создание и редактирование правил публикации для одного порта или диапазона портов;
- синхронизация правил с RRAS и ICS;
- автоматическое создание разрешающего правила в сетевом экране и пользователя в программе.

Управление публикацией служб осуществляется с помощью правил публикации. Список правил публикации размещен в разделе **Сервисы -> Публикация служб** консоли администратора. Также в разделе **Сервисы** есть блок **Публикация служб**, состоящий из двух вкладок. На вкладке **Информация** отображается общее количество созданных в системе правил публикации, а также название тарифа по умолчанию, а на вкладке **Действия** – ссылки на некоторые операции.

В рамках управления правилами публикации в Traffic Inspector реализованы следующие операции:

- создание/изменение правила публикации;
- удаление правила публикации.

Работа Traffic Inspector с сетевыми интерфейсами

8

Создание/изменение правила публикации

Для создания нового или изменения существующего правила публикации выполните следующие действия:

1. Откройте окно свойств нового или существующего правила публикации. Сделать это можно с помощью контекстного меню в разделе **Сервисы -> Публикация служб** консоли администратора или в блоке **Публикация служб**, размещенном на главной странице раздела **Сервисы**. Также ссылки на публикацию с использование предустановленных шаблонов разных сетевых сервисов расположены в правой панели в разделе **Сервисы -> Публикация служб**.

2. На вкладке **Параметры публикации** выберите публикуемую службу. Если это один из наиболее распространенных сервисов, то Traffic Inspector автоматически проставит нужные параметры, при этом часть вкладок окна свойств правила публикации будет скрыта. Если выбрать вариант **Другая служба**, все параметры публикации необходимо будет задать самостоятельно. Здесь же введите имя публикуемого сервера в локальной сети или его IP-адрес.

   Замечание! *IP-адрес обязательно должен входить в одну из подсетей, заданных для внутренних интерфейсов.*

3. На вкладке **Проверка параметров** просмотрите данные о найденных подходящих правилах сетевого экрана (разрешающее правило для подходящего протокола и порта) и пользователя (пользователь с авторизацией по IP-адресу сервера и безлимитным доступом), от имени которого будет осуществляться публикация. Если подходящих правил и пользователя нет, то можно включить их автоматическое создание. Если этого не сделать, данные операции придется выполнять вручную.

   Замечание! *Для публикации служб создается пользователь для сервера, на котором она запущена. Таким образом, если на одном сервере размещено сразу несколько служб (например, веб-сервер, почтовые сервер и FTP-сервер), публикация их всех возможна от имени одного пользователя. В*

создании своего пользователя для каждой службы нет необходимости.

4. На вкладке **Наименование** введите наименование правила публикации и, при необходимости, произвольные примечания. Здесь же можно включить использование параметров публикации по умолчанию (доступно только при выборе на вкладке **Параметры публикации** службы, для которых в Traffic Inspector есть предустановки), а также временно отключить правило публикации, не удаляя его совсем.

5. На вкладке **Настройки публикации** выберите внешний сетевой интерфейс, через который будет осуществляться публикация, и укажите адрес сервера, на котором располагается публикуемая служба. Также задайте протокол (TCP или UDP) и внешний и внутренний порт или диапазон портов. Обратите внимание, что порты могут быть как одинаковыми, так и различными. Это позволяет осуществлять автоматическую смену порта в процессе перенаправления запроса.

6. На вкладке **Правила сетевого экрана** выберите один из следующих вариантов действий по настройке правил сетевого экрана:

   - **Создать новое правило сетевого экрана** – при выборе этого варианта Traffic Inspector автоматически создаст в сетевом экране разрешающее правило для указанного ранее протокола и порта.

   - **Использовать существующее правило** – при выборе этого варианта укажите одно из созданных ранее правил сетевого экрана. При необходимости его можно отредактировать прямо с данной вкладки.

   - **Настроить позже** – при выборе этого варианта после завершения настройки правила публикации необходимо будет вручную создать нужное правило сетевого экрана (подробнее о создании правил сетевого экрана см. в п. Правила внешнего сетевого экрана).

> ***Замечание!*** *Вкладка* ***Правила сетевого экрана*** *доступна в том случае, если автоматическое создание правила не было включено на вкладке* ***Проверка параметров****.*

7. На вкладке **Настройка пользователя** выберите один из следующих вариантов действий по настройке правил сетевого экрана:

- **Создать нового пользователя** – при выборе этого варианта Traffic Inspector автоматически создаст нового пользователя для сервера, на котором размещена публикуемая служба.
- **Выбрать пользователя** – при выборе этого варианта укажите одного из созданных ранее пользователей. При необходимости его можно отредактировать прямо с данной вкладки.
- **Настроить позже** – при выборе этого варианта после завершения настройки правила публикации необходимо будет вручную создать нужного пользователя программы (подробнее о создании пользователей см. в п. Создание и настройка пользователей).

> ***Замечание!*** *Вкладка* ***Настройка пользователя*** *доступна в том случае, если автоматическое создание пользователя не было включено на вкладке* ***Проверка параметров***.

8. Сохраните внесенные изменения.

Удаление правила публикации

Удаление правила публикации осуществляется с помощью контекстного меню в разделе **Сервисы -> Публикация служб** консоли администратора.

Резервирование каналов

Под резервированием каналов понимается автоматическое переключение на резервный канал подключения к Интернету в том случае, если основной по каким-то причинам (например, авария на линии) оказывается недоступным. Она может использоваться только при выполнении следующих условий:

- к серверу Traffic Inspector подключено два или больше внешних сетевых интерфейсов;
- в Windows настроена служба RRAS, при этом интерфейсов, на которых включена NAT, должно быть не менее двух;

- функция Advanced Routing должна быть отключена.

Для включения и настройки резервирования каналов выполните следующие действия:

1. Запустите конфигуратор в режиме настройки служб (подробнее см. в п. Настройка служб).
2. На вкладке **Резервирование каналов** включите запуск мастера настройки резервирования каналов, после чего сохраните настройки и завершите работу конфигуратора. При этом будет запущен мастер настройки резервирования каналов.
3. На вкладке **Настройки** укажите интервал проверки доступности основного канала связи (по умолчанию 30 минут) и время ожидания отклика. При необходимости введите IP-адрес, по доступности которого будет проверяться работоспособность канала связи (если это не сделать, то будет проверяться значение по умолчанию). Также здесь можно включить запись результатов проверки в файл.
4. На вкладке **Список интерфейсов** выберите не менее двух интерфейсов, участвующих в резервировании. Порядок интерфейсов в списке определяет приоритет каналов связи (верхний интерфейс считается основным, нижележащие– резервными).
5. На вкладке **Ограничения** определите, кто может использовать резервный канал связи. По умолчанию он доступен всем пользователям. При необходимости выключите эту настройку и отметьте флажками те группы пользователей, кому разрешена работа на резервном канале связи. Доступ к Интернету всех остальных пользователей при недоступности основного интерфейса будет блокироваться. Эта настройка имеет смысл в том случае, если резервный канал имеет значительно меньшую пропускную способность, чем основной. В этом случае можно разрешить работу на нем только тем, кому доступ в Интернет необходим для выполнения своих обязанностей.
6. На вкладке **Применение настроек** запустите процесс настройки. Если Traffic Inspector выявит какие-то проблемы с настройкой интерфейсов и маршрутов, то на этой вкладке будет выдано соответствующее предупреждение. В этом случае самостоятельно устраните проблему путем внесения необходимых изменений в настройки службы RRAS Windows или включите процедуру автонастройки.

7. Сохраните внесенные изменения.

Внутренний сетевой экран

Внутренний сетевой экран предназначен для ограничения доступа к серверу Traffic Inspector из локальных сетей, для ограничения передачи трафика между разными локальными сетями, для назначения общих для всех пользователей и групп правил и т.д. Для настройки внутреннего сетевого экрана выполните следующие действия.

1. Откройте окно настройки внутреннего сетевого экрана. Сделать это можно с помощью контекстного меню в разделе **Правила -> Правила пользователей** или из блока **Правила пользователей**, размещенного на главной странице раздела **Правила**.

2. На вкладке **Внутренний сетевой экран** включите или отключите работу экрана для локальных и публичных сетей (подробнее о типах сетей см. в п. Настройка служб). При включении, по умолчанию, будет запрещен весь трафик, кроме служебного. Если нужно будет разрешить передачу данных по определенным протоколам и портам, то после включения внутреннего сетевого экрана создайте необходимые разрешающие правила (подробнее о создании правил см. в п. Виды и предназначение правил, наборы правил).

3. На вкладке **Внутренний сетевой экран** разрешите или запретите прохождение трафика между локальными сетями, публичными сетями и между локальными и публичными сетями.

4. На вкладке **Публичные сети** разрешите или запретите для публичных сетей следующие виды трафика:

   - широковещательные запросы (Broadcast);
   - исходящий трафик по протоколу ICMP;
   - исходящий трафик по протоколу UDP;
   - исходящие TCP-соединения;
   - трафик DHCP-сервера;

- трафик DNS-сервера;
- трафик PPTP-сервера;
- трафик IPSec.

5. При необходимости на вкладке **Запрет для неавторизованных** сформируйте список запрещающих правил, которые будут действовать для всех неавторизованных пользователей.
6. При необходимости на вкладке **Общие разрешения** сформируйте список разрешающих правила, которые будут действовать для всех пользователей.
7. При необходимости на вкладке **Правила "До группы"** сформируйте список произвольных правил, которые будут применяться для всех авторизованных пользователей до персональных правил и правил групп, в которые они входят.
8. При необходимости на вкладке **Правила "После группы"** сформируйте список произвольных правил, которые будут применяться для всех авторизованных пользователей после персональных правил и правил групп, в которые они входят.
9. Сохраните внесенные изменения.

Внешний сетевой экран

Внешний сетевой экран (firewall) – это отдельная служба, использующая фильтрацию входящего трафика на внешнем интерфейсе.

Концепция сетевого экрана – по умолчанию разрешить все исходящие запросы и запретить все входящие. Для этого на входящий трафик на внешнем интерфейсе разрешены TCP-пакеты без SYN-флага (для установленных соединений) и отклики по ICMP.

Для того чтобы изнутри прозрачно работали приложения по протоколу UDP, реализована динамическая фильтрация. При появлении исходящих UDP-пакетов на какой-то внешний IP-адрес, на него временно открывается входящие правило, что позволяет принять отклик от удаленного сервера и пропустить его внутрь. Через минуту после прекращения передачи трафика это правило удаляется.

Все вышеперечисленное относится к настройкам по умолчанию. С целью полностью закрыть сервер и все подключенные к нему сети извне сетевой экран достаточно просто включить. Снаружи будет закрыто все, в том числе ICMP. Отфильтрованный трафик учитывается на информационных счетчиках (подробнее см. в п. Информационные счетчики), где его можно оценить количественно и качественно, используя сетевую статистику. Если надо дополнительно разрешить входящие запросы по TCP, UDP, ICMP или другой IP-трафик, то следует добавить правила на разрешение (подробнее о правилах внешнего сетевого экрана см. в п. Правила внешнего сетевого экрана).

В программе имеется механизм классификации типа трафика – контролируемый и неконтролируемый. Это относится только к исходящим TCP- и UDP-пакетам, для другого трафика такое разграничение недоступно. К контролируемому относятся:

- исходящие пакеты от прокси- и SOCKS-сервера;
- TCP- и UDP-пакеты от авторизованных пользователей, прошедшие через внутренние интерфейсы и далее через роутер операционной системы или NAT.

В сетевом экране предусмотрены условия фильтрации по этому типу трафика, что позволяет эффективно отсечь нежелательный трафик, например, от служб самого сервера или пользовательских программ, работающих на самом сервере.

Включается внешний сетевой экран в конфигураторе (подробнее см. в п. Настройка служб). Он может быть включен как для всех, так и только для некоторых внешних сетевых интерфейсов.

Настройка внешнего сетевого экрана осуществляется в специальном окне, вызвать которое можно с помощью контекстного меню в разделе **Правила -> Правила внешнего сетевого экрана** консоли администратора или из блока **Правила сетевого экрана**, расположенного на главной странице раздела **Правила**.

Для настройки внешнего сетевого экрана включите или выключите следующие разрешения.

- **Исходящий ICMP** – разрешает отправку ICMP-запроса от сервера и прием всех типов отклика. Тип трафика - любой, контролируемый и неконтролируемый.

- **Исходящий UDP**– разрешает запрос от сервера и включает динамическую фильтрацию на прием.

- **Исходящее TCP-соединение** – разрешает отправку любых TCP-пакетов и прием TCP-пакетов без SYN-флага. Входящие TCP-соединения запрещены.

  Замечания! *Для исходящих UDP и TCP-соединений можно включить разрешение отправки только контролируемого трафика (по умолчанию отключено). Если предполагается ввести ограничения на неконтролируемый трафик, то настройку следует обязательно включить. В этом случае может потребоваться добавить в списки разрешения на необходимый неконтролируемый трафик.*

  Замечание! *Трафик обновлений Panda Gate Antivirus неконтролируемый, но в правила сетевого экрана вставляется временное правило на разрешение обновлений, поэтому обновление будет работать даже при запрете неконтролируемого трафика.*

- **DNS клиент** – разрешает трафик DNS. Тип трафика – любой. По умолчанию включено. Если динамический UDP запрещен или разрешен только для контролируемого трафика, то это правило как раз разрешит нормальную работу DNS-служб сервера. При включении во внешнем сетевом экране задаются следующие разрешения:

  - разрешение, исходящий, UDP порт назначения 53;
  - разрешение, входящий,UDP порт источника 53;
  - разрешение, исходящий, TCP порт назначения 53;
  - разрешение, входящий,TCP порт источника 53.

- **SNTP клиент** – разрешает SNTP-трафик. Тип трафика – любой. По умолчанию включено. Если динамический UDP запрещен или разрешен только для контролируемого трафика, то данное правило разрешит нормальную работу служб синхронизации времени сервера. При включении во внешнем сетевом экране задаются следующие разрешения:

- разрешение, исходящий, UDP порт назначения 123;
- разрешение, входящий, UDP порт источника 123.

- **DHCP сервер**– разрешает трафик DHCP-сервера. Тип трафика – любой. По умолчанию включено. При включении во внешнем сетевом экране задаются следующие разрешения:
  - разрешение, исходящий, UDP порт назначения 67;
  - разрешение, входящий, UDP порт источника 67.
- **VPN/PPTP/L2TP клиент** – разрешает трафик для VPN-, PPTP- и L2TP-клиентов. Тип трафика – любой. При включении во внешнем сетевом экране задаются следующие разрешения:
  - разрешение, исходящий, TCP порт назначения 1723;
  - разрешение, входящий, TCP порт источника 1723;
  - разрешение, исходящий, протокол №47, порт любой;
  - разрешение, входящий, протокол №47, порт любой.
- **IPSec/L2TP клиент** – разрешает трафик для клиентов IPSec и L2TP. Тип трафика – любой. Для клиентских VPN-соединений по протоколу L2TP следует включить данное и предыдущее разрешение. При включении во внешнем сетевом экране задаются следующие разрешения:
  - разрешение, исходящий, UDP порт назначения 500;
  - разрешение, входящий, UDP порт источника 500;
  - разрешение, входящий, UDP порт назначения 500;
  - разрешение, исходящий, UDP порт источника 500;
  - разрешение, исходящий, протокол №50, порт любой;
  - разрешение, входящий, протокол №50, порт любой;
  - разрешение, исходящий, протокол №51, порт любой;

- разрешение, входящий, протокол № 51, порт любой.

- **Remote Desktop Server** – разрешает трафик для удаленных рабочих столов. Тип трафика – любой. При включении во внешнем сетевом экране задаются следующие разрешения:

  - разрешение, любое направление, порт назначения 3389.

    Замечание! *Данное разрешение устанавливается автоматически при включении в процессе инсталляции флажка* ***Выполняется удалённая установка*** *(подробнее см. в п. Установка программы).*

- **FTP server** – разрешает трафик по протоколу FTP. FTP-DATA (для пассивного режима) отдельно разрешать не надо – они будут открываться автоматически. Тип трафика – любой. При включении во внешнем сетевом экране задаются следующие разрешения:

  - разрешение, исходящий, TCP порт назначения 21;

  - разрешение, входящий, TCP порт источника 21.

Правила внешнего сетевого экрана

Правила внешнего сетевого экрана позволяют задавать явные разрешения или запреты на прохождение через него того или иного вида трафика. Они необходимы в тех случаях, когда внешний сетевой экран включен/выключен. Например, при включенном экране правила разрешения необходимы для публикации внутренних сетевых служб в Интернете (подробнее см. в п. Публикация служб). Если подходящие правила не создать, то трафик к этим службам будет заблокирован внешним сетевым экраном.

Список правил внешнего сетевого экрана находится в разделе **Правила -> Правила внешнего сетевого экрана** консоли администратора. Также на главной странице раздела **Правила** есть блок **Правила сетевого экрана,** состоящий из двух вкладок. На вкладке **Информация** отображается состояние внешнего сетевого экрана и общее количество созданных для него правил, а на вкладке **Действия** – ссылки на некоторые операции.

В рамках управления правилами внешнего сетевого экрана в Traffic Inspector реализованы

следующие операции:

- создание/изменение правила внешнего сетевого экрана;
- удаление правила внешнего сетевого экрана.

Создание/изменение правила внешнего сетевого экрана

Для создания нового или изменения существующего правила внешнего сетевого экрана выполните следующие действия:

1. Откройте окно свойств нового или существующего правила внешнего сетевого экрана. Сделать это можно из контекстного меню в разделе **Правила -> Правила внешнего сетевого экрана** консоли администратора или в блоке **Правила сетевого экрана**, расположенного на главной странице раздела **Правила**.
2. На вкладке **Наименование** введите уникальное наименование правила и, при необходимости, произвольный комментарий. Здесь же можно временно отключить правило, не удаляя его совсем.
3. На вкладке **Тип правила** выберите один из возможных типов.
   - **Разрешить трафик** – соответствующий заданным в правилах условиям трафик будет пропущен внешним сетевым экраном.
   - **Запретить трафик** – соответствующий заданным в правилах условиям трафик будет блокирован внешним сетевым экраном. Данные правила срабатывают до правил общих настроек сетевого экрана, поэтому имеют перед ними приоритет.
4. На вкладке **Условия** задайте основные признаки трафика, для которого будет работать данное правило. Для этого выберите направление передачи сетевых пакетов (прием, передача или любое). Здесь же можно указать, для каких внешних интерфейсов будет работать правило – только для какого-то одного или для всех сразу.
5. При необходимости на вкладке **IP адрес** задайте внешние и внутренние адреса, участвующие в передаче трафика, на который будет действовать данное правило. Задать параметры внешней стороны можно вручную или с помощью определенных

ранее IP-сетей (подробнее про IP-сети см. в п. IP-сети). В первом случае укажите один конкретный IP-адрес или IP-адреса границ диапазона. Во втором – выберите предварительно созданную IP-сеть. При выборе этого варианта можно непосредственно с данной вкладки перейти к редактированию активной или созданию новой IP-сети. Задать параметры внутренней стороны можно только вручную, введя один конкретный IP-адрес или IP-адреса границ диапазона.

6. При необходимсти на вкладке **IP протокол** настройте протокол и порт трафика, который будет учитываться данным правилом. Сделать это можно с помощью подсказки или вручную. В первом случае выберите шаблон одного из наиболее распространенных типов трафика (например, ICMP, DNS client, HTTP client, FTP client и т.п.). При этом все параметры будут настроены автоматически.

   Для ручной настройки самостоятельно выберите нужный протокол. Если был выбран вариант UDP или TCP, то дополнительно укажите сетевой порт. Это может быть один конкретный порт, диапазон номеров сетевых портов или динамический порт.

7. При необходимости на вкладке **Расписание** настройте расписание действия правила (работа на вкладке аналогична работе на одноименной вкладке окна свойств группы, подробнее см. в п. Создание и настройка групп).

8. Если правило должно быть временным, то на вкладке **Автоудаление** укажите дату и время его окончания и выберите, что должна сделать система при его наступлении – удалить правило или заблокировать его, не удаляя.

9. Сохраните внесенные изменения.

Удаление правила внешнего сетевого экрана

Удаление правила внешнего сетевого экрана осуществляется с помощью контекстного меню в разделе **Правила -> Правила внешнего сетевого экрана** консоли администратора.

Работа с сетевыми службами 10

Advanced Routing - работа с несколькими внешними интерфейсами

Advanced routing – это функция, позволяющая полноценно задействовать несколько подключений к Интернету одновременно. Для нее обычно используется терминология Source Routing или Policy Routing, но, учитывая ее отличия реализации в Traffic Inspector, было решено ввести отдельный термин.

Роутер Windows позволяет иметь несколько маршрутов по умолчанию, но всегда использует только один из них. При этом выбирается маршрут с наивысшим приоритетом. Единственным способом задействовать в Windows несколько подключений является назначение отдельных маршрутов по адресам назначения. Для решения задачи полноценного использования нескольких подключений к сети Интернет требуется наличие маршрутизации по другим критериям, но в Windows эта возможность не поддерживается. Динамическая маршрутизация, которая реализована в этой операционной системе, не позволяет решить поставленную задачу.

На рынке имеются решения для Windows, частично обладающие необходимым функционалом. В них задача решается с помощью реализации параллельного маршрутизатора. Решение в Traffic Inspector уникально тем, что в нем используется маршрутизатор Windows. А это в свою очередь позволяет полностью задействовать все сетевые службы Windows и обеспечить корректную работу через свой прокси-сервер и SOCKS.

Для настройки функции Advanced routing выполните следующие действия:

1. На все внешние интерфейсы, с которыми будет работать данная функция, назначьте маршруты (шлюзы) по умолчанию. Сделать это можно с помощью статических маршрутов в RRAS, IP-настройки интерфейсов или в утилите route.exe.
2. Подключите все интерфейсы, с которыми будет работать Advanced routing, поскольку программа при конфигурировании позволяет делать привязки только к активным интерфейсам.
3. Запустите конфигуратор в режиме **Настройка служб** (подробнее см. в п. Настройка служб) и на вкладке **Опции конфигурации** включите функцию Advanced routing. В

списке интерфейсов консоли внешний интерфейс, для которого функция Advanced routing разрешена, будет отмечен иконкой со стрелкой. Если стрелки нет, то у интерфейса нет маршрута по умолчанию.

4. Примените опцию к пользователям, группам, а также настройте правила пользователей. Настройки, связанные с функцией Advanced routing, находятся на вкладках **Роутинг**.

Advanced routing решает задачу выбора внешнего интерфейса, отличного от интерфейса по умолчанию, в зависимости различных критериев: пользователь, группа, тип трафика и т.д. Это позволяет автоматически направлять разные виды трафика через разные каналы связи, что, собственно говоря, и требуется.

В правилах пользователей есть одна особенность в использовании Advanced routing. В окне свойств правила можно использовать факт перенаправления пакета на другой интерфейс как условие для правила (подробнее см. в п. Виды и предназначение правил, наборы правил). Так как правила обрабатываются строго по списку, то, размещая такие правила после правила, которое сделало перенаправление, можно собрать логику применения условий в зависимости от используемого внешнего интерфейса (например, применить другие тарифы). Но следует учесть, что настройки пользователей (групп) применяются позже просмотра списка.

В случае использования спутникового подключения, когда трафик принимается с одного интерфейса (DVB-карта), а передается через другой, оба эти интерфейса стоит обязательно указать в процессе конфигурирования интерфейсов (подробнее см. в п. Настройка служб).

Для анализа работы этой функции в сетевой статистике пользователя имеется соответствующий атрибут – имя внешнего интерфейса, куда был перенаправлен трафик.

У функции Advanced routing есть определенные ограничения.

1. Функция не применяется для трафика, идущего с самого сервера, за исключением служб прокси-сервера программы и SOCKS.
2. Для трафика, идущего с самого сервера через дополнительные внешние сетевые интерфейсы (кроме интерфейса по умолчанию), могут возникать коллизии, если на эти

же IP-адреса идет трафик, перенаправленный Advanced routing. Для исключения этих коллизий программа производит анализ таблицы маршрутов и не применяет Advanced routing, если трафик маршрутизируется в правильном направлении штатным роутером. Поэтому, в первую очередь, стоит тщательно настроить роутер Windows.

3. Имеется ограничение на количество внешних интерфейсов с задействованной функцией Advanced routing– не более 7 LAN и не более 7 WAN-интерфейсов.
4. Функция не работает через прокси-сервер, если используется форвардинг (каскад).
5. Ввиду ограничений пп.1 и 2 не следует использовать Advanced routing, если задача маршрутизации может быть решена средствами роутера Windows.

Резервирование в DHCP для пользователей

В Traffic Inspector реализована интеграция с DHCP-сервером. Суть ее заключается в создании аренды во внешнем DHCP-сервере для IP-адреса, с которого авторизовался пользователь, для данного пользователя. Эта функция работает при выполнении следующих условий:

- внешним DHCP-сервером сервер Windows;
- роль DHCP-сервера установлена на том же сервере, что и Traffic Inspector.

Общее включение функции резервирования в DHCP осуществляется в общих настройках пользователей (подробнее см. в п. Общие настройки пользователей). После этого необходимо активировать резервирование для пользователей или целых их групп (подробнее см. в п. Создание и настройка пользователей и в п. Создание и настройка групп).

С целью детального анализа характера трафика пользователей и внешнего трафика для пользователей и внешних счетчиков может быть включен сбор и запись сетевой статистики.

Статистика собирается в контексте IP-адресов, типов протоколов и портов. Для трафика, снятого с HTTP-прокси, записывается еще и имя хоста.

Для сбора сетевой статистики для каждого объекта учета, пользователя или счетчика

заводится коллектор – временная таблица счетчиков, где записи группируются по IP-адресам, протоколам, портам и именам хостов. Данные в коллекторе группируются по IP-адресам, хостам и протоколам. По портам данные также группируются, но здесь прослеживается отдельная логика, которой решаются задачи, с одной стороны, минимизации количества записей, а с другой – запись подробной информация о характере трафика.

Для TCP-трафика данные группируются по порту TCP-сервера. Если имеется несколько соединений на один порт сервера одного адреса, то данные пишутся в одну запись и порт со стороны пользователя не учитывается.

Определить, где сервер, для UDP в общем невозможно, т.к. протокол не является сеансовым. Поэтому для минимизации количества записей порты более 1023 трактуются как динамические, и данные пишутся в одну запись. Есть возможность описать список портов, для которых трафик всегда будет писаться отдельными записями, т.е. без группировки.

В сетевую статистику также пишутся следующие атрибуты трафика:

- Стоимость трафика и дополнительный тариф (только для сетевой статистики пользователя).
- Ограничение скорости отдельно для входящего и исходящего трафика. Ограничение не следует путать с реальной скоростью (только для сетевой статистики пользователя).
- Маршрут – имя внешнего интерфейса, на который трафик должен быть перенаправлен при работе Advanced Routing (только для сетевой статистики пользователя).
- Признак контролируемого трафика (только для внешних счетчиков).

Трафик с разными атрибутами не группируется, т.е. пишется в отдельные записи сетевой статистики.

По умолчанию для пользователей пишется только платный трафик. Но имеется настройка, где можно включить запись всего трафика, снимаемого с внутренних интерфейсов (подробнее см. в п. Общие настройки программы). Для учета неавторизованного трафика,

в этом случае, существует отдельный коллектор. Запись всего трафика может потребоваться для отладки работы программы.

Каждый внешний IP-адрес в коллекторе с использованием DNS может быть преобразован в имя. Это делается отдельной службой, процесс преобразования автономный и на производительности программы никак не сказывается. Но, при наличии большого количества коллекторов, могут появиться проблемы с ресурсами в системе. Поэтому для пользователей это преобразование по умолчанию отключено. Также оно может быть отключено с целью экономии DNS-трафика.

Записи в таблице коллектора сортируются по одному из критериев: входящему, исходящему, сумме или максимуму. Для пользователей этот критерий сортировки берется из тарифа, для внешних счетчиков задается отдельно. Данные коллектора доступны для просмотра в реальном времени и позволяют оценить, что в данный момент происходит в сети, как в контексте пользователя, так и внешнего трафика.

Сетевая статистика с заданным периодом времени пишется в базу данных журнала, и коллектор при этом очищается. С целью минимизации количества записей в журнал из коллектора пишутся все или только наиболее активные записи – в соответствии с их сортировкой. Количество сохраняемых записей и интервал их сохранения определяет степень детализации данных, используемых в дальнейшем для генерации отчетов. Также есть возможность ограничить запись данных по количеству пакетов в коллекторе.

Запись сетевой статистики для счетчика с отфильтрованным трафиком позволяет вести детальный анализ сетевых атак.

Настройка глубины сбора сетевой статистики

В Traffic Inspector реализована возможность управления глубиной сбора сетевой статистики. Ее настройка позволяет соблюдать баланс между полнотой собранной информацией и задействованными при ее обработке и хранении системными ресурсами сервера.

Глубина сбора сетевой статистики может быть задана в общих настройках пользователей. В этом случае она будет работать для всех групп и пользователей, в которых заданы параметры использования сетевой статистики по умолчанию. Также глубину сбора можно

настроить для групп (в этом случае она будет распространяться на всех членов группы, для которых заданы параметры использования сетевой статистики по умолчанию) и отдельных пользователей.

Настройка глубины сбора сетевой статистики выполняется в окне общих настроек пользователей (подробнее см. в п. Общие настройки пользователей), свойств группы (подробнее см. в п. Создание и настройка групп) или свойств пользователя (подробнее см. в п. Создание и настройка пользователей) на вкладке **Сетевая статистика**. В ходе нее необходимо задать интервал записи собранной сетевой статистики из коллекторов в базу данных, количество записываемых активных направлений из каждого коллектора, а также минимальное количество сетевых пакетов (берется максимальное значение от исходящих и входящих пакетов), необходимых для записи.

Отчёты по сетевой статистике

На основе сетевой статистики могут строиться наглядные отчеты по пользователям, контролируемым и информационным счетчикам, нарушениям политик. Подробно работа с отчетами по сетевой статистике описана в п. Отчёты по сетевой статистике.

Блокировка по сетевой статистике

В Traffic Inspector реализована возможность автоматической блокировки пользователя на определенное время на основе его сетевой статистики. Эта функция позволяет решить целый ряд определенных задач, в том числе, бороться с сетевыми вирусами, которые при заражении компьютера начинают генерировать большое количество запросов на разные IP-адреса. Это приводит к быстрому заполнению коллекторов записями с разными направлениями.

Блокировка может быть задана в общих настройках пользователей. В этом случае она будет работать для всех групп и пользователей, в которых заданы параметры использования сетевой статистики по умолчанию. Также блокировку можно включать и настраивать для групп (в этом случае она будет распространяться на всех членов группы, для которых заданы параметры использования сетевой статистики по умолчанию) и отдельных пользователей.

Настройка блокировки по сетевой статистике выполняется в окне общих настроек

пользователей (подробнее см. в п. Общие настройки пользователей), свойств группы (подробнее см. в п. Создание и настройка групп) или свойств пользователя (подробнее см. в п. Создание и настройка пользователей) на вкладке **Сетевая статистика**. При включении блокировки укажите количество активных направлений, при котором она будет срабатывать, а также время (в минутах), на которое будет заблокирован пользователь.

Запись сетевой статистики во встроенную базу

По умолчанию сетевая статистика сохраняется во встроенную базу данных, которая устанавливается на сервер автоматически вместе с Traffic Inspector. Использование встроенной базы удобно тем, что не требует от администратора никакой дополнительной настройки и работает сразу после инсталляции Traffic Inspector. Однако у этого варианта есть следующие ограничения:

- ограничение на объем файлов встроенной базы данных;
- снижение производительности (в частности, при построении отчетов) при хранении большого объема информации.

Для избежания этих недостатков при хранении больших объемов информации рекомендуется использовать для хранения сетевой статистики внешнюю базу данных. В этом случае данные из встроенной базы будут периодически выгружаться во внешнюю. А при формировании отчетов будет производиться автоматический выбор источника данных – встроенная база данных или внешний SQL-сервер (подробнее см. в п. Возможные типы БД) в зависимости от актуальности информации.

Запись сетевой статистики во внешнюю базу

В Traffic Inspector вся сетевая статистика всегда записывается во встроенную базу данных. Однако при большом объеме информации это может стать причиной значительного падения производительности системы (подробнее см. в п. Запись сетевой статистики во встроенную базу). Поэтому Traffic Inspectorможет быть настроена для работы с внешним SQL-сервером. В этом случае сетевая статистика будет автоматически по заданному администратором расписанию копироваться из встроенной базы данных во внешнюю.

Управление сетевой статистикой 11

Настройка работы с внешним SQL-сервером дает следующие преимущества.

- Можно значительно уменьшить размер файла встроенной базы данных для журналов. Даже для небольшой сети этот файл очень быстро разрастается, скорость работы программы падает (прежде всего, в плане формирования отчетов) и затрудняется выбор между временем хранения данных и производительностью. Внешний SQL-сервер позволяет эффективно работать с очень большими базами данных.
- С учетом того, что вся оперативная работа программы производится с локальной базой данных, временная неработоспособность внешнего SQL-сервера не критична. SQL-сервер может быть развернут на любом другом компьютере сети.
- Несколько серверов Traffic Inspector могут копировать свои данные на один внешний SQL-сервер в единую базу данных со своим уникальным идентификатором, что позволяет формировать сводные отчеты.

Возможные типы БД

В Traffic Inspector в качестве внешней базы данных могут использоваться следующие СУБД.

- **Microsoft SQL Server** – высокопроизводительный сервер с платной лицензией. Поддерживаются версии Microsoft SQL Server 2005 и выше. Бесплатные версии с приставкой Express в названии имеют существенные ограничения (в частности, по размеру баз данных), а поэтому для использования совместно с Traffic Inspector не подходят. Microsoft SQL Server – высокопроизводительный сервер с платной лицензией.
- **MySQL** – популярный бесплатный сервер, имеющий, однако, относительно низкую производительность при работе с большими отчетами. Не рекомендуется к использованию. Поддерживаются версии 5.0 и выше. Для работы с MySQL на сервере с Traffic Inspector потребуется установка MySQL ODBC 5.1 Driver.
- **Postgree SQL** – высокопроизводительный бесплатный сервер. Поддерживаются версии 8.0 и выше. Для работы с Postgree SQL на сервере с Traffic Inspector потребуется установка OLE DB provider for PostgreSQL.

Управление сетевой статистикой 11

Синхронизация с внешней БД

Настройка синхронизации с внешней базой данных выполняется в два этапа.

1. Подготовка внешней базы данных.
2. Настройка синхронизации в Traffic Inspector.

Подготовка внешней базы данных

В первую очередь подготовьте сервер, на котором будет работать СУБД. Это может быть как сам компьютер с Traffic Inspector, так и любой другой компьютер в локальной сети. Второй вариант предпочтительней, поскольку позволяет уменьшить нагрузку на компьютере с Traffic Inspector при формировании ресурсоемких отчетов. При его использовании сеть должна быть достаточно быстрой, т.к. объем передаваемых данных может быть большим. Для варианта отдельного размещения внешнего SQL-сервера может потребоваться настройка его сетевых протоколов, как на SQL-сервере, так и у клиента, то есть со стороны Traffic Inspector (см. документацию на соответствующий SQL-сервер). После подготовки сервера установите на нем нужную СУБД и настройте ее работу в соответствии с руководством по ее развертыванию и настройке.

Настройка синхронизации в Traffic Inspector

Для настройки синхронизации встроенной базы данных с внешней выполните следующие действия:

1. Запустите мастер настройки синхронизации. Сделать это можно из блока **Обслуживание БД**, расположенного на главной странице раздела **Настройки**.
2. На вкладке **Выбор внешнего SQL сервера** выберите один из трех доступных типов внешнего SQL-сервера: Microsoft SQL Server, MySQL или PostgreeSQL (подробнее о возможных типах внешней базы данных см. в п. Возможные типы БД).
3. На вкладке **Настройки для SQL сервера** установите параметры доступа к внешнему серверу, которые зависят от его типа.

- Для Microsoft SQL Server укажите сетевое имя сервера или его IP-адрес, выберите и настройте способ аутентификации (интегрированный или с использованием встроенных учетных записей СУБД).
- Для MySQL введите сетевое имя сервера или его IP-адрес, порт, на котором работает СУБД, а также логин и пароль встроенного пользователя MySQL.
- Для PostgreeSQL укажите сетевое имя сервера или его IP-адрес, а также логин и пароль встроенного пользователя СУБД.

Здесь же проверьте соединение с сервером по указанным настройкам, чтобы убедиться в их корректности и работоспособности СУБД.

4. На вкладке **Идентификация сервера** задайте уникальный номер данной сервера Traffic Inspector. Сделать это необходимо, если в указанной внешней базе данных будет собираться сетевая статистика с нескольких серверов Traffic Inspector. В этом случае каждому из них необходимо задать свой уникальный номер. Если же во внешнюю базу данных будет копироваться информация только с одного сервера, то укажите значение "0".

   На этой же вкладке задайте отображаемое имя сервера Traffic Inspector, которое будет использоваться в сводных отчетах по нескольким серверам.

   > ***Замечание!*** *Уникальный номер сервера и его отображаемое имя задают один раз. В дальнейшем эти параметры изменять нельзя.*

5. На вкладке **Настройки синхронизации** задайте расписания загрузки информации из встроенной базы данных во внешнюю. По умолчанию эта операция выполняется каждые 15 минут. В зависимости от конкретных условий использования это время можно уменьшить (это позволит улучшить актуальность данных на внешнем SQL-сервере, но увеличит затраты системных ресурсов) или увеличить.

6. На вкладке **Настройки очистки данных** задайте параметры удаления информации из встроенной базы данных. Для этого укажите количество дней, в течение которых они будут храниться. Очистка выполняется один раз в сутки. Минимальное время хранения – 1 сутки. Большее значение увеличит размер встроенной базы данных, однако может

быть полезно, если внешний SQL-сервер по какой-то причине часто бывает недоступен. По умолчанию очистка выполняется в 2 часа ночи, однако впоследствии это время можно изменить, отредактировав соответствующую задачу.

7. Сохраните внесенные изменения.

После выполнения мастера синхронизации с внешней базой данных в разделе **Настройки -> Обслуживание БД** будет отображаться информация о задачах синхронизации и очистки. При необходимости можно изменить расписание синхронизации в описанном выше мастере и время запуска процедуры очистки встроенной базы данных в специальном окне, которое можно вызвать из блока **Обслуживание БД** в разделе **Настройки -> Обслуживание БД** (подробнее о данном разделе см. в п. Обслуживание БД).

Особенности работы с внешними БД

Типы аутентификации

В Traffic Inspector реализованы следующие типы аутентификации пользователей программы, которые могут использоваться в разных ситуациях:

- учетная запись Windows;
- встроенная учетная запись;
- IP-адрес;
- MAC-адрес.

При создании пользователя программы сразу же указывается использующийся для него тип аутентификации.

Учетная запись Windows

Данный тип аутентификации подразумевает использование для авторизации пользователей их учетных записей в операционных системах семейства Windows. Это

могут быть как учетные записи с отдельных компьютеров, так и учетные записи доменов. Использование данного типа аутентификации удобно тогда, когда за одними и теми же компьютерами могут работать разные пользователи. В этих случаях можно привязать весь потребляемый трафик не к устройству, а именно к человеку, который за ним работает. Кроме того, использование учетной записи Windows обеспечивает автоматическую авторизацию пользователей, избавляя их от необходимости многократного ввода пароля. Стоит однако отметить, что, в первую очередь, данный тип аутентификации рекомендуется применять в сетях с развернутыми доменами.

Пользователи программы с данным типом аутентификации могут быть созданы вручную или в процессе импорта из Active Directory (подробнее см. в п. Импорт пользователей). В качестве параметра авторизации используется только логин учетной записи Windows в формате *domain\username* (в качестве domain может выступать как домен Windows, так и имя локального компьютера).

Встроенная учетная запись

При использовании данного типа аутентификации авторизационные данные пользователей хранятся непосредственно в базе Traffic Inspector. Этот вариант, как и предыдущий, позволяет не привязываться к конкретным компьютерам. Кроме того, он позволяет отказаться и от привязки к учетным записям Windows. Однако при его применении пользователям придется каждый раз для авторизации вводить свой логин и пароль.

Пользователи программы со встроенными учетными записями могут быть созданы только вручную. При этом необходимо задавать их логины и пароли.

IP-адрес

При использовании данного типа аутентификации в качестве авторизационного параметра используются не данные пользователя, а IP-адрес компьютера или другого устройства, который подключается к серверу Traffic Inspector. Аутентификация

выполняется автоматически в момент подключения, причем никак не зависит от пользователя, который осуществляет работу. Поэтому данный вариант удобен в тех случаях, когда трафик должен засчитывать именно для компьютера. Например, в компаниях, в которых за каждым ПК может работать только один пользователь, для серверов и т.д.

Кроме того, в некоторых случаях использование аутентификации по IP-адресу позволяет уменьшить количество требуемых для приобретения лицензий. Например, если для какого-то отдела не нужен персональный учет потребления трафика по каждому сотруднику в отдельности, то для них можно зарегистрировать в Traffic Inspector одного пользователя с аутентификацией по IP-адресу, указав сразу диапазон IP-адресов. В этом случае трафик всех работников этого отдела будет учитывать в одном пользователе, что позволит уменьшить количество пользователей в лицензии (подробнее см. в п. Выбор количества лицензий).

Пользователи программы с аутентификацией по IP-адресам могут быть созданы вручную или путем импорта из результатов сканирования сети локальной сети (подробнее см. в п. Импорт пользователей). В качестве параметра авторизации может выступать конкретный IP-адрес или целый диапазон IP-адресов.

MAC-адрес

Аутентификация по MAC-адресу, в целом, похожа на аутентификацию по IP-адресу. Только в качестве параметра авторизации выступает не IP-адрес, а MAC-адрес сетевого интерфейса клиента. Данный тип удобно использовать в тех случаях, когда IP-адреса компьютеров могут с течением времени меняться. Например, в сетях, в которых работает DHCP-сервер. Пользователи программы с аутентификацией по MAC-адресам могут быть созданы вручную или путем импорта из результатов сканирования сети локальной сети (подробнее см. в п. Импорт пользователей).

Интеграция с Microsoft Active Directory

В рамках интеграции Traffic Inspector с Microsoft Active Directory реализованы следующие операции:

- загрузка данных о пользователях с типом аутентификации **Учетная запись Windows**;
- импорт пользователей из Microsoft Active Directory;
- аутентификация пользователей на основе их учетной записи Windows.

В Traffic Inspector нет каких-либо общих параметров, которые позволяют настроиться на работу с каким-то определенным контроллером домена. Это позволяет программе одновременно работать с пользователями, относящимися к разным доменам.

Загрузка данных о пользователях с типом аутентификации **Учетная запись Windows** включает в себя получение из Active Directory полного имени указанного пользователя и адресов его электронной почты. Обращение к контроллеру осуществляется по имени домена, который извлекается из логина пользователя (подробнее см. в п. Создание и настройка пользователей).

В рамках импорта пользователей из Microsoft Active Directory осуществляется подключение к контроллеру текущего или произвольного домена, чтение каталога существующих учетных записей и загрузка информации о них при создании пользователей программы (подробнее см. в п. Импорт пользователей).

Аутентификация пользователей на основе их учетной записи осуществляется автоматически. При этом выполняется подключение к контроллеру домена, указанного в логине пользователя, по протоколу NTLM.

Способы авторизации пользователей

Если типы аутентификации определяют то, по каким параметрам выполняется аутентификация (учетная запись Windows, встроенная учетная запись, IP-адрес или MAC-адрес, подробнее см. в п. Типы аутентификации), то под способами авторизации пользователей понимаются средства, с помощью которых пользователи могут проходить авторизацию на сервере.

На данный момент в Traffic Inspector реализованы следующие способы авторизации пользователей:

- авторизация с помощью клиентского агента, установленного на компьютере (подробнее

см. в п. Клиентский агент Windows);

- авторизация с помощью веб-агента (подробнее см. в п. Веб-агент);
- прозрачная авторизация по протоколу NTLM (подробнее см. в п. Прозрачная авторизация NTLM).

Клиентский агент Windows

Клиентский агент Windows – небольшое приложение, которое устанавливается на компьютере пользователя. Он предназначен для выполнения следующих операций:

- авторизации пользователя;
- переключения режимов фильтрации и кэширования;
- отображения баланса – остатка на счете;
- смены пароля;
- автоматического конфигурирования браузеров.

Установка клиентского агента Traffic Inspector

По умолчанию дистрибутив клиентского агента Windows размещен в разделе **Клиентский агент** веб-интерфейса (подробнее про веб-интерфейс см. в п. Веб-интерфейс). Оттуда его можно загрузить и установить на компьютер пользователя. Установка агента осуществляется точно так же, как и установка любого программного обеспечения с помощью обычного мастера, при выполнении которого можно изменить папку инсталляции.

Также на официальном сайте Traffic Inspector доступен MSI-пакет установщика (http://www.smart-soft.ru/files/3.0/TrafInspAg.zip), который можно использовать для инсталляции агента на серверах и рабочих станциях с помощью групповых политик Active Directory.

По умолчанию после установки клиентский агент будет запускаться автоматически при старте компьютера. Также его можно запустить принудительно в обычном порядке.

Настройка клиентского агента Traffic Inspector

Для настройки клиентского агента после установки выполните следующие действия:

1. Запустите агент, при этом в системном трее появится его значок. Нажмите на него правой кнопкой мыши и в открывшемся меню выберите пункт **Настройка**.

2. На вкладке **Логин** выберите используемый тип аутентификации.

   - **По IP или MAC** – при выборе данного способа авторизация будет осуществляется по IP-адресу или MAC-адресу автоматически при подключении к серверу Traffic Inspector.

   - **По имени** – при выборе данного способа авторизация будет осуществляться по учетной записи пользователя. Если речь идет об учетной записи Windows, то либо задайте нужные логин, домен и пароль, либо включите использование текущего пользователя (учетной записи, под которой пользователь авторизован на компьютере в данный момент). Если используется встроенная учетная запись, то укажите свой логин и пароль, заданные администратором Traffic Inspector в свойствах пользователя. При необходимости можно включить сохранение авторизационных данных. В этом случае авторизация будет осуществляться автоматически. В противном случае нужно будет вводить пароль при каждом подключении к серверу Traffic Inspector.

3. На вкладке **Соединение** настройте параметры подключения к серверу Traffic Inspector. Для этого включите его автоматический поиск или задайте имя хоста или IP-адрес, по которому он размещен. Здесь же задайте протокол, по которому будет осуществляться обмен данными с сервером или включите его автоматическое определение (по рекомендациям сервера).

   > ***Замечание!*** *Автоматический поиск сервера должен быть включен в общих настройках пользователей (подробнее см. в п. Общие настройки пользователей), в противном случае обязательно нужно указать имя хоста или IP-адрес сервера Traffic Inspector.*

4. На вкладке **Горячие клавиши** включите или отключите использование "горячих" клавиш для быстрого управления теми или иными функциями агента, а также, при необходимости, задайте нужные сочетания клавиш.

5. На вкладке **Дополнительно** настройте следующие параметры работы агента:

   - Включите или выключите автоматическое отключение от сервера Traffic Inspector при блокировке компьютера или смене учетной записи Windows с последующим автоматическим подключением при разблокировании или возврате к текущей учетной записи.
   - Включите или выключите использование индивидуальных настроек агента для каждого пользователя.
   - Включите или выключите звуковое оповещение (сами звуки настраиваются в панели управления Windows). Возможно оповещение о следующих событиях: подключение к серверу Traffic Inspector, отключение от него, возникновение ошибки подключения, запрет доступа, получение сообщения от администратора.
   - Включите или выключите напоминание о том, что баланс лицевого счета стал меньше указанной суммы.

6. Сохраните внесенные изменения.

Работа с клиентским агентом

В процессе работы с клиентским агентом пользователям доступны следующие операции:

- подключение к серверу Traffic Inspector (авторизация на сервере Traffic Inspector);
- просмотр состояния подключения и текущего баланса;
- выбор уровня фильтрации и кэширования;
- смена пароля пользователя.
- автоконфигурирование браузера.

Аутентификация пользователей 12

Подключение к серверу Traffic Inspector может осуществляться автоматически при запуске агента. Включить или выключить эту функцию можно с помощью контекстного меню агента. Также устанавливать подключение можно вручную с помощью того же контекстного меню или из окна самого агента. Если в клиенте настроена автоматическая авторизация (см. выше), то при установке подключения никаких запросов пользователю выдаваться не будет. В противном случае может потребоваться ввод логина и/или пароля.

Просмотр состояния подключения и текущего баланса осуществляется в окне агента. Также здесь можно просмотреть трафик, потребленный пользователем в рамках текущего сеанса соединения с сервером Traffic Inspector.

В главном окне агента можно устанавливать текущий уровень фильтрации:

- F0 – фильтрация отключена;
- F1 – фильтрация баннеров;
- F2 – фильтрация мультимедиа-контента;
- F3 – фильтрация графики;
- F4 – фильтрация всего, кроме текста.

Сами правила для разных уровней фильтрации задаются в группе правил Agent, которая создается автоматически при установке Traffic Inspector. При необходимости их можно изменять (подробнее см. в п. Виды правил и операции с ними).

Аналогичным образом можно настраивать и уровень кэширования (подробнее о кэшировании см. в п. Прокси-сервер, настройки и возможности).

Смена пароля с помощью агента возможна только для встроенных учетных записей и только в том случае, если эта операция разрешена в общих настройках пользователей (подробнее см. в п. Общие настройки пользователей). Выполняется она с помощью контекстного меню агента.

Автоматическое конфигурирование браузера возможно в том случае, если оно разрешено в настройках прокси-сервера (подробнее см. в п. Основные настройки прокси-сервера). При его выполнении браузер на компьютере пользователя настраивается для работы через

прокси-сервер. Запускается операция с помощью контекстного меню агента.

Веб-агент

Веб-агент представляет собой веб-приложение, которое выполняет аналогичные клиентскому агенту действия (подробнее см. в п. Клиентский агент Windows), хотя и обладает меньшими функциональными возможностями. Основным достоинством веб-агента является возможность его использования на компьютерах, работающих под управлением любых операционных систем (Linux, Unix, Mac OS и пр.), а также на планшетах и смартфонах. А это позволяет подключаться к серверу Traffic Inspector и использовать его возможности практически с любого компьютера или мобильного устройства. Запускается веб-агент из раздела **Клиентский агент** веб-интерфейса, доступного всем пользователям даже без авторизации на сервере Traffic Inspector (подробнее см. в п. Веб-интерфейс).

В веб-агенте реализованы следующие операции:

- авторизации пользователя;
- переключения режимов фильтрации и кэширования;
- отображения баланса – остатка на счете.

Авторизация пользователя на сервере Traffic Inspector может выполняться как автоматически, так и с вводом логина и пароля. Это зависит от используемого типа аутентификации и настроенных параметров авторизации данного пользователя (подробнее про авторизацию см. в п. Клиентский агент Windows).

Переключение режимов фильтрации и кэширования, а также просмотр текущего баланса лицевого счета и потребленного за текущий сеанс подключения к серверу Traffic Inspector трафика осуществляется непосредственно на странице веб-агента.

Прозрачная авторизация NTLM

Прозрачная авторизация по протоколу NTLM работает только в том случае, если для пользователя выбран тип учетной записи **Учетная запись Windows** (подробнее см. в п. Типы аутентификации). В этом случае возможна авторизация пользователей по их логину и паролю в домене Windows. Также можно использовать текущего пользователя, в этом

случае авторизация осуществляется от имени учетной записи, под которой человек работает на компьютере.

Подробнее об использовании прозрачной авторизации NTLM см. в п. Интеграция с Microsoft Active Directory.

Возможности Traffic Inspector можно расширять за счет подключения дополнительных модулей. С их помощью, в частности, реализовано сканирование трафика и удаление из него вредоносного программного обеспечение, антиспам, тематическая категоризация сайтов и целый ряд других возможностей. Сервер программы (служба) находит и подключает дополнительные модули при старте службы.

Для каждого загруженного модуля в разделе **Модули расширения** консоли администратора создается свой подраздел. Его содержимое и структура определяется непосредственно модулем. Кроме того, на главной странице **Модули расширения** для каждого дополнительного модуля есть собственный блок, который отображает краткую информацию о нем, а также содержит ссылки на те или иные операции.

Для упрощения процедуры установки дополнительных модулей в консоли администратора имеется механизм их автоматической установки. Он обеспечивает загрузку модулей с сайта разработчика, его автоматическую установку и последующее обновление при необходимости. Управление загрузкой дополнительных модулей осуществляется в окне **Опции загрузки модулей**, запустить которое можно из блока **Модули расширения** одноименного раздела консоли администратора. В нем можно включить и отключить загрузку тех или иных модулей.

Данные обрабатываются модулями по очереди, согласно заданному порядку. Это значит, что сначала их обрабатывает один дополнительный модуль, потом следующий по списку и т.д. Это может быть важным, например, при проверке трафика несколькими антивирусами. Порядок обработки задается в окне **Опции загрузки модулей**.

При установке модулей возможно появление ошибки связанной с тем, что файл модуля уже занят на чтение и на запись недоступен. Это может быть связано с тем, что его уже загрузил этот экземпляр консоли. В этом случае будет предложено принудительно перезапустить приложение, модули расширения будут установлены сразу после его

повторного запуска. Если ошибка опять повторяется, то скорее всего файл модуля расширения занят другим приложением, например, открыт еще один экземпляр консоли – закройте ее.

Антивирусные модули

Kaspersky Gate Antivirus

Антивирусный сканер разработан компанией Kaspersky Lab. и выполнен в виде модуля расширения к программе Traffic Inspector.

Если на сервере установлено другое антивирусное ПО, проверяющее файлы на диске, то его работа может вызвать конфликты. Следует **ОБЯЗАТЕЛЬНО** исключить из проверки другим антивирусом все файлы сканера, все директории целиком.

Для оценки работы модуля предусмотрен демонстрационный (триальный) режим на один месяц. Модуль при этом никаких ограничений по функциональным возможностям не имеет. Продлить оценочный период нельзя. Если сама программа активирована в триальном режиме, то оценочный период модуля начинается с момента активации. При постоянном активировании программы для включения триального режима этого модуля необходимо связаться с продавцом, разрешить режим и повторно активировать программу.

Постоянный режим активации модуля предусмотрен на конечный срок и на конкретное количество пользователей, при этом модуль активируется в процессе активации самой программы.

Предусмотрено два типа лицензирования модуля по количеству пользователей.

1. Как у программы Traffic Inspector. В этом случае трафик всех пользователей программы проверяется антивирусом.
2. Отдельное лицензирование. В этом случае для Kaspersky Gate Antivirus может быть приобретено меньшее количество лицензий, чем у Traffic Inspector.

При отдельном лицензировании появляются дополнительные настройки – предусматривается возможность включить антивирусную проверку, как для отдельных клиентов, так и для групп. Для запоминания этих настроек используется дополнительный

атрибут клиента и группы – Kaspersky Gate Antivirus. Описания атрибутов добавляются автоматически при запуске программы. Удалить атрибут из описания нельзя.

Для разрешения антивирусной проверки значение атрибута должно быть **Да**. Любое другое или пустое значение атрибута означает, что проверка отключена. Изменить значение атрибута можно в окне редактирования дополнительных атрибутов групп (подробнее см. в п. Создание и настройка групп) и пользователей (подробнее см. в п. Создание и настройка пользователей). Если дано разрешение на всю группу, то эта настройка у отдельного пользователя игнорируется.

Для удобного контроля лицензий в консоли модуля имеются списки пользователей и групп, для которых включена антивирусная проверка. В списках групп отображается количество лицензий, используемых в рамках каждой группы. В перечне пользователей отображаются только одиночные лицензии. Кроме этого, в списках предусмотрена операция удаления лицензии у пользователя или группы. В отдельном перечне отображаются пользователи, у которых лицензии отсутствуют. Их трафик проверяться не будет.

Модуль поставляется без антивирусной базы, поэтому после установки ее следует загрузить.

Настройка Kaspersky Gate Antivirus

Общие сведения о состоянии модуля Kaspersky Gate Antivirus отображаются в разделе **Модули расширения -> Kaspersky Gate Antivirus** консоли администратора.

На главной странице этого раздела присутствуют два блока. Блок **Kaspersky Gate Antivirus** состоит из двух вкладок. На вкладке **Информация** отображается основная информация о состоянии модуля и его антивирусной базы данных, а на вкладке **Действия** приведены ссылки на основные операции. В блоке **Статистика** показывается краткая статистика работы модуля.

В рамках управления модулем Kaspersky Gate Antivirus в Traffic Inspector реализованы следующие операции:

- настройка модуля Kaspersky Gate Antivirus;

- обновление антивирусных баз модуля Kaspersky Gate Antivirus;
- просмотр подробного отчета о работе модуля Kaspersky Gate Antivirus.

Настройка модуля Kaspersky Gate Antivirus

Для настройки модуля Kaspersky Gate Antivirus выполните следующие действия.

1. Откройте окно настройки модуля Kaspersky Gate Antivirus. Сделать это можно из блока **Kaspersky Gate Antivirus** в разделе **Модули расширения -> Kaspersky Gate Antivirus** консоли администратора.
2. На вкладке **Функции антивируса** включите или выключите проверку разных видов трафика - HTTP и почтового. При включении проверки почтового трафика появляется возможность задать исключения путем указания тегов писем, которые не будут обрабатываться антивирусом (теги сообщениям присваиваются SMTP-шлюзом на основе заданных администратором правил, подробнее см. в п. Контроль почтового трафика дополнительными модулями).
3. На вкладке **Настройки сканера** установите параметры работы антивирусного сканера. В первую очередь укажите количество процессов сканирования. По умолчанию используется только один процесс. При большом объеме обрабатываемого трафика их число можно увеличить, однако это потребует большего количество системных ресурсов сервера.

   На этой же вкладке задайте параметры сканирования трафика. Для этого включите или отключите автоматическое лечение зараженных объектов (обратите внимание, что вылечить зараженные объекты удается не всегда), проверку сжатых исполняемых файлов и обработку архивов. При включении последней функции укажите предельно допустимую вложенность обрабатываемых архивных файлов. В противном случае будет возможно проведение DoS-атаки путем отправки небольших по объему архивов, многократно вложенных друг в друга. Обработка таких файлов может занять большое количество системных ресурсов и привести к некорректной работе сервисов сервера.

   Здесь же включите или выключите эвристический анализ трафика, который

обеспечивает поиск вредоносного программного обеспечения, не описанного в антивирусной базе модуля. Включение функции увеличивает затраты системных ресурсов, но улучшает надежность защиты. При включении эвристического анализа выберите желаемый уровень сканирования – низкий, средний или детальный. Чем выше уровень, тем больше чувствительность сканера. Но при этом увеличиваются затраты системных ресурсов, а также повышается риск ложного срабатывания антивируса.

4. На вкладке **Обновление** включите или выключите автоматическое обновление антивирусных баз модуля. При включении настройте расписание автоматического обновления.

   Замечание! *Настройка автоматического обновления антивирусных баз модуля разрешены, если разрешено обновление сканера вообще, то есть не используется демонстрационный реж им.*

5. При необходимости на вкладке **Настройки соединения** изменить таймаут соединения с сервером обновления (по умолчанию 60 секунд).

6. Сохраните внесенные изменения.

Обновление антивирусных баз модуля Kaspersky Gate Antivirus

Обновление антивирусных баз модуля Kaspersky Gate Antivirus может осуществляться как автоматически по заданному расписанию (см. выше) или запускаться вручную. Ручной запуск осуществляется из блока из блока **Kaspersky Gate Antivirus** в разделе **Модули расширения -> Kaspersky Gate Antivirus** консоли администратора.

Обновление возможно только в том случае, если не используется демонстрационный режим (подробнее см. в п. Kaspersky Gate Antivirus).

Просмотр подробного отчета о работе модуля Kaspersky Gate Antivirus

Просмотр отчета о работе модуля осуществляется в разделе **Отчеты -> Антивирус**

консоли администратора. Подробно работа с ним описана в п. Отчёты по работе дополнительных модулей.

Dr.Web Gateway Security Suite

Антивирусный сканер разработан компанией ООО «Доктор Веб» (http://www.drweb.com/) и выполнен в виде модуля расширения к программе Traffic Inspector.

Если на сервере установлено другое антивирусное ПО, проверяющее файлы на диске, то его работа может вызвать конфликты. Следует **ОБЯЗАТЕЛЬНО** исключить из проверки другим антивирусом все файлы модуля Dr.Web.

Для оценки работы модуля предусмотрен демонстрационный (триальный) режим на один месяц. Модуль при этом никаких ограничений по функциональным возможностям не имеет. Продлить оценочный период нельзя. Если сама программа активирована в триальном режиме, то оценочный период модуля начинается с момента активации. При постоянном активировании программы для включения триального режима этого модуля необходимо связаться с продавцом, разрешить режим и повторно активировать программу.

Постоянный режим активации модуля предусмотрен на конечный срок и на конкретное количество пользователей, при этом модуль активируется в процессе активации самой программы.

Предусмотрено два типа лицензирования модуля по количеству пользователей.

1. Как у программы Traffic Inspector. В этом случае трафик всех пользователей программы проверяется антивирусом.
2. Отдельное лицензирование. В этом случае для Dr.Web Gateway Security Suite может быть приобретено меньшее количество лицензий, чем у Traffic Inspector.

При отдельном лицензировании появляются дополнительные настройки – предусматривается возможность включить антивирусную проверку как для отдельных пользователей, так и для групп. Для запоминания этих настроек используется дополнительный атрибут пользователя и группы – Dr.Web Gateway Security Suite. Описания атрибутов добавляются автоматически при запуске программы. Удалить

атрибут из описания нельзя.

Для разрешения антивирусной проверки значение атрибута должно быть **Да**. Любое другое или пустое значение атрибута означает, что проверка отключена. Изменить значение атрибута можно в окне редактирования дополнительных атрибутов групп (подробнее см. в п. Создание и настройка групп) и пользователей (подробнее см. в п. Создание и настройка пользователей). Если дано разрешение на всю группу, то эта настройка у отдельного пользователя игнорируется.

Для удобного контроля лицензий в консоли модуля имеются списки пользователей и групп, для которых включена антивирусная проверка. В списках групп отображается количество лицензий, используемых в рамках каждой группы. В перечне пользователей отображаются только одиночные лицензии. Кроме этого, в списках предусмотрена операция удаления лицензии у пользователя или группы. В отдельном перечне отображаются пользователи, у которых лицензии отсутствуют. Их трафик проверяться не будет.

Модуль поставляется без антивирусной базы, поэтому после установки ее следует загрузить.

Настройка Dr.Web Gateway Security Suite

Общие сведения о состоянии модуля Dr.Web Gateway Security Suite отображаются в разделе **Модули расширения ->Dr.Web Gateway Security Suite** консоли администратора.

На главной странице этого раздела присутствуют два блока. Блок **Dr.Web Gateway Security Suite** состоит из двух вкладок. На вкладке **Информация** отображается основная информация о состоянии модуля и его антивирусной базы данных, а на вкладке **Действия** приведены ссылки на основные операции. В блоке **Статистика** показывается краткая статистика работы модуля.

В рамках управления модулем Dr.Web Gateway Security Suite в Traffic Inspector реализованы

следующие операции:

- настройка модуля Dr.Web Gateway Security Suite;
- обновление антивирусных баз модуля Dr.Web Gateway Security Suite;
- просмотр подробного отчета о работе модуля Dr.Web Gateway Security Suite.

Настройка модуля Dr.Web Gateway Security Suite

Для настройки модуля Dr.Web Gateway Security Suite выполните следующие действия.

1. Откройте окно настройки модуля Dr.Web Gateway Security Suite. Сделать это можно из блока **Dr.Web Gateway Security Suite** в разделе **Модули расширения -> Dr.Web Gateway Security Suite** консоли администратора.
2. На вкладке **Функции антивируса** включите или выключите проверку разных видов трафика – HTTP и почтового. При включении проверки почтового трафика появляется возможность задать исключения путем указания тегов писем, которые не будут обрабатываться антивирусом (теги сообщениям присваиваются SMTP-шлюзом на основе заданных администратором правил, подробнее см. в п. Контроль почтового трафика дополнительными модулями).
3. На вкладке **Настройки сканера** установите параметры работы антивирусного сканера. Для этого включите или отключите автоматическое лечение зараженных объектов (обратите внимание, что вылечить зараженные объекты удается не всегда), проверку сжатых исполняемых файлов и обработку архивов. При включении последней функции укажите предельно допустимую вложенность обрабатываемых архивных файлов. В противном случае будет возможно проведение DoS-атаки путем отправки небольших по объему архивов, многократно вложенных друг в друга. Обработка таких файлов может занять большое количество системных ресурсов и привести к некорректной работе сервисов сервера. Также можно указать максимальный размер самого архива и распаковываемого объекта из архива объекта для проверки.

   Здесь же включите или выключите эвристический анализ трафика, который

обеспечивает поиск вредоносного программного обеспечения, не описанного в антивирусной базе модуля (включение функции увеличивает затраты системных ресурсов, но улучшает надежность защиты) и, при необходимости, задайте максимальное время сканирования.

4. На вкладке **Обновление** включите или выключите автоматическое обновление антивирусных баз модуля. При включении настройте расписание автоматического обновления.
5. При необходимости на вкладке **Настройки соединения** изменить таймаут соединения с сервером обновления (по умолчанию 60 секунд).
6. Сохраните внесенные изменения.

Обновление антивирусных баз модуля Dr.Web Gateway Security Suite

Обновление антивирусных баз модуля Dr.Web Gateway Security Suite может осуществляться как автоматически по заданному расписанию (см. выше) или запускаться вручную. Ручной запуск осуществляется из блока из блока **Dr.Web Gateway Security Suite** в разделе **Модули расширения -> Kaspersky Gate AntivirusDr.Web Gateway Security Suite** консоли администратора.

Просмотр подробного отчета о работе модуля Dr.Web Gateway Security Suite

Просмотр отчета о работе модуля осуществляется в разделе **Отчеты -> Антивирус** консоли администратора. Подробно работа с ним описана в п. Отчёты по работе дополнительных модулей.

Adguard

Дополнительный модуль Adguard для Traffic Inspector – серверное средство фильтрации рекламы, социальных виджетов и всплывающих окон. Модуль интегрируется в программу Traffic Inspector и анализирует входящий трафик, автоматически удаляя рекламу и всплывающие окна с загружаемых пользователями веб-страниц. Преимуществом модуль перед традиционными программами для блокировки рекламы является то, что он

работает на сервере и прозрачен для пользователей. То есть не требует установки дополнительного программного обеспечения на компьютерах конечных пользователей локальной сети.

В данном модуле используется новая Displace-технология, позволяющая убирать рекламу и всплывающие окна прямо из тела страницы в любом браузере и на любой платформе. Установив Adguard для Traffic Inspector на шлюзе, пользователи могут пользоваться "чистым" Интернетом на компьютерах, ноутбуках, планшетах, смартфонах, мобильных телефонах.

Модуль основан на технологической базе популярного антибаннера Adguard и полностью исключает рекламу с веб-страниц при отсутствии ложных срабатываний. Помимо блокировки по URL-маскам, плагин фильтрует рекламу по html-коду, характерным для баннеров размерам и ряду других признаков, используемых в современных программах подобного рода.

Основные задачи модуля Adguard – снижение расхода трафика, увеличение скорости загрузки страниц за счет исключения рекламных элементов, защита от вирусов, распространяемых через недобросовестные рекламные сети, а также повышение эффективности использования сети Интернет за счет исключения отвлекающих факторов. Экономия трафика при использовании модуля составляет до 40%, уменьшение времени загрузки страниц – до 70%.

Система отчетности Adguard содержит информацию о количестве заблокированных рекламных элементов и трафика, сэкономленного за счет блокировки рекламы.

Плагин поддерживает 4 листа фильтрации, имеющих различное назначение.

1. Стандартный лист. Фильтрует рекламу и рекламные сети.
2. Лист счетчиков. Блокирует загрузку и показ счетчиков, например, LiveInternet.
3. Лист социальных виджетов. Блокирует виджеты Facebook Connect, Like, Tweet и других социальных сервисов.
4. Фильтр для иностранных сайтов. Данный лист фильтрации рекламы оптимизирован

для использования на сайтах на разных языках (английском, немецком, испанском, японском и пр.).

Такое разделение позволяет гибко настраивать режим фильтрации. Например, если пользователи имеют отношение к SEO, предпочтительно оставить показ счетчиков на страницах, а все остальные элементы можно убрать.

Все листы фильтрации автоматически обновляются несколько раз в неделю, поддерживаются в актуальном состоянии и соответствуют реалиям рекламного рынка.

Для полноценной работы модуля достаточно установить его вместе с программой Traffic Inspector, плагин не требует обучения.

Пользователям можно установить программу-агента для легкого управления фильтрацией: F0 – без фильтрации, F1 – блокировать рекламу, F2 – блокировать счетчики и т.д. (подробнее об агентах см. в п. Клиентский агент Windows).

Модуль активируется на необходимое количество учетных записей.

Настройка Adguard

Общие сведения о состоянии модуля Adguard отображаются в разделе **Модули расширения -> Adguard** консоли администратора.

На главной странице этого раздела присутствует основной блок **Adguard**, который состоит из двух вкладок. На вкладке **Информация** отображается основная информация о состоянии модуля и краткая статистика его работы, а на вкладке **Действия** приведены ссылки на основные операции. Помимо него на этой странице находится еще целый ряд блоков, в которых показывается краткая информация о состоянии фильтров, использующихся данным модулем.

В рамках управления модулем Adguard в Traffic Inspector реализованы следующие операции:

- настройка модуля Adguard.

Настройка модуля Adguard

Для настройки модуля Adguard выполните следующие действия:

1. Откройте окно настройки модуля Adguard. Сделать это можно из блока **Adguard** в разделе **Модули расширения ->Adguard** консоли администратора.

2. На вкладке **Ражим работы** разрешите или запретите работу модуля (данная функция позволяет временно отключить модуль, не выгружая или не удаляя его).

   Здесь же с помощью двух шкал определите интервал уровней фильтрации, при которой пользователям будет разрешена работа. Например, для того, чтобы запретить работу с выключенным фильтром рекламы, сдвиньте индикатор верхней шкалы в положение F1.

3. На вкладке **Фильтрация по размерам** настройте функцию блокирования рекламы на веб-страницах по их размерам по размерам изображений и флеш-роликов. Для этого отметьте флажками нужные стандартные размеры баннеров. При необходимости можно включить блокировку всех изображений и флеш роликов, размеры которых лежат в пределах от 400 до 650 пикселей по горизонтали и от 60 до 95 пикселей по вертикали.

   > ***Замечание!*** *При включении блокировки по интервалу размеров также могут оказаться заблокированными изображения и флеш-ролики, не относящиеся к рекламе.*

4. На вкладке **Настройки фильтрации** включите или выключите функцию замены рекламных изображений на ссылки на них. Если ее включить, вместо баннеров будет выводиться ссылка **Заблокирована**, ведущая на заблокированный контент. В противном случае вместо баннеров будет отображаться пустое место.

   Здесь же включите или выключите использование javascript-библиотеки Adguard. Она используется для блокировки всплывающих окон, а также баннеров, которые динамические рисуются на веб-странице (блокировка в данном случае осуществляется по размерам этих баннеров).

5. На вкладке **Список фильтров** включите или отключите нужные фильтры.

6. Если подключение к Интернету осуществляется через вышестоящий прокси-сервер, то

на вкладке **Настройки подключения** включите его использование модулем Adguard (сам прокси-сервер задается в окне общих настроек программы, подробнее см. в п. Общие настройки программы).

7. Сохраните внесенные изменения.

Phishing Blocker

Модуль защиты от фишинга Phishing Blocker использует условно бесплатный проект Google Safe Browsing. Суть его работы сводится к проверке имени хоста или IP-адреса по собственной базе данных мошеннических проектов. Если ответ положительный, то данный хост или IP-адрес приписывается к одной из предварительно созданных категории контента (подробнее о категориях контента см. в п. Категории контента).

Отнесение ресурса к этой категории позволяет произвести фильтрацию нежелательного контента. Для этого необходимо настроить правило, запрещающее доступ к сайтам данной категории (подробнее о правилах см. в п. Виды и предназначение правил, наборы правил). Это позволит предотвратить посещение пользователями заведомо мошеннических веб-проектов. По умолчанию используется автоматически создаваемое правило Phishing Blocker, которое можно назначить отдельным пользователям или целым их группам. При необходимости можно создать и другие правила и с разными действиями, связанными с данной категорий контента.

> ***ВНИМАНИЕ!*** *Если во внешнем сетевом экране исходящие TCP соединения по умолчанию запрещены, то долж но быть разрешено соединение на хост sb-ssl.google.com. Сам модуль это разрешение не создает. Разрешение надо создавать не на IP-адрес (он мож ет меняться), а на имя хоста. Для этого создайте описание IP-сети с этим именем в списке и привяж ите его к разрешающему правилу сетевого экрана.*

Общие сведения о состоянии модуля Phishing Blocker отображаются в разделе **Модули расширения ->Phishing Blocker** консоли администратора.

На главной странице этого раздела размещен блок **Phishing Blocker**, который состоит из двух вкладок. На вкладке **Информация** отображается основная информация о состоянии

модуля и краткая статистика его работы, а на вкладке **Действия** приведены ссылки на основные операции.

В рамках управления модулем Phishing Blocker в Traffic Inspector реализованы следующие операции:

- настройка модуля Phishing Blocker;
- проверка произвольного ресурса.

Настройка модуля Phishing Blocker

Для настройки модуля Phishing Blocker выполните следующие действия.

1. Откройте окно настройки модуля Phishing Blocker. Сделать это можно из блока **Phishing Blocker** в разделе **Модули расширения -> Phishing Blocker** консоли администратора.
2. На вкладке **Настройки плагина** разрешите или запретите работу модуля (данная функция позволяет временно отключить модуль, не выгружая или не удаляя его). Здесь же введите свой ключ к сервису Google Safe Browsing (Google Safe Browsing API Key), укажите категорию контента, к которой будут относиться ресурсы из базы мошеннических сайтов (по умолчанию используется автоматически создаваемая категория **Вредоносное ПО**) и включите или отключите отправку сообщения об опасном ресурсе пользователю.

   Если у вас нет ключа к сервису Google Safe Browsing, то получите его, выполнив следующие действия

   1. Нажмите на кнопку **Получить** на вкладке **Настройки плагина** или откройте в браузере страницу https://developers.google.com/safe-browsing/key_signup?hl=ru-RU&csw=1.
   2. Авторизуйтесь на сервере Google.
   3. Примите лицензионное соглашение сервиса, сгенерируйте ключ и сохраните его.
3. На вкладке **Режимы работы** выберите один из двух возможных режимов работы

модуля.

- **Асинхронный режим** – рекомендуемый режим работы. При получении запроса со стороны клиента в прокси-сервере отравляется запрос к сервису Google Safe Browsing через Интернет. При этом прокси-сервер продолжает работу, не дожидаясь отклика от сервиса. Проверка отклика от сервиса производится при получении заголовков отклика прокси-сервером. В этом режиме совсем не снижается скорость работы, если отклик от сервиса приходит быстрее, чем от сервера, на который отправил запрос прокси.
- **Синхронный режим** – в данном режиме все операции выполняются последовательно. Сначала ресурс проверяется сервисом, а после получения результата работа прокси-сервера продолжается. Этот режим работает медленнее, но позволяет немного экономить трафик – если ресурс был заблокирован, то прокси-сервер запрос отправлять не будет.

4. На вкладке **Настройки соединения** установите таймаут ответа сервиса Google Safe Browsing (по умолчанию 7 секунд). Если подключение к Интернету осуществляется через вышестоящий прокси-сервер, то здесь включите его использование модулем Phishing Blocker (сам прокси-сервер задается в окне общих настроек программы, подробнее см. в п. Общие настройки программы).

5. На вкладке **Кэширование** включите или отключите кэширование результатов запросов к сервису Google Safe Browsing. При включении укажите срок хранения записей к кэше (по умолчанию 48 часов). По истечению этого времени данные будут удаляться. Кэш размещается в памяти программы.

> ***Замечание!*** *В случае появления флуда размер кэша может аномально увеличиваться (см. статистику на главной странице модуля).*
>
> ***Замечание!*** *Модуль имеет ограничение на размер кэшы (10000 объектов), при превышении этого лимита наиболее старые данные будут удаляться принудительно .*

6. Сохраните внесенные изменения.

Дополнительные модули Traffic Inspector 13

Проверка произвольного ресурса

В Traffic Inspector реализована возможность проверки произвольного ресурса на его наличие в базе Google Safe Browsing. Она может использоваться для проверки запроса (URL) и позволяет увидеть присвоение запросу типа рейтинга в соответствии с заданными правилами

Для выполнения проверки откройте раздел **Модули расширения ->Phishing Blocker -> Проверка** консоли администратора и введите запрос – URL-адрес. Результат проверки будет отображен на этой же странице. В него входят данные, полученные от сервиса, а также примененные правила и назначенные типы категорий контента.

RASdialer

Модуль RASdialer предназначен для управления сетевыми RAS-соединениями (модемы, VPN клиенты и т.д) в режиме сервиса Windows, т.е. без сеанса пользователя. Это актуально для десктопных версий Windows, в которых нет службы RRAS.

Соединение для дозвона может быть назначено только одно. Для соединения могут быть назначены дополнительные условия – активный внешний интерфейс и расписание. Если эти условия назначены и выполнены, то соединение устанавливается, если они не выполнены, то имеющиеся соединение разрывается. Следует отметить, что если состояние соединения изменилось извне программы (например, вручную пользователем), то служба отработает эту ситуацию и произведет соединение (или отключит его), если его состояние не будет соответствовать ее настройкам.

Для настройки службы соединение должно быть создано и настроено средствами Windows.

> ***Замечание!*** *Соединение долж но быть создано в профиле* ***Для всех****, а не для конкретного пользователя. Параметры логина (имя пользователя и пароль) могут быть сохранены в настройках соединения. В этом случае в*

настройках модуля их можно не указывать.

> ***Замечание!*** *После запуска службы программы модуль начинает дозвон только после успешного старта сетевых интерфейсов программы. Т.е., если в процессе запуска произошла ошибка конфигурирования сетевых интерфейсов, работа модуля (дозвон) запущен не будет. Но он будет запущен позже, как только сетевые интерфейсы будут успешно настроены.*

Общие сведения о состоянии модуля RASdialer отображаются в разделе **Модули расширения -> RASdialer** консоли администратора.

На главной странице этого раздела размещен блок **RASdialer**, который состоит из двух вкладок. На вкладке **Информация** отображается основная информация о состоянии модуля, а на вкладке **Действия** приведены ссылки на основные операции.

В рамках управления модулем RASdialer в Traffic Inspector реализованы следующие операции:

- настройка модуля RASdialer.

Для настройки модуля RASdialer выполните следующие действия.

1. Откройте окно настройки модуля RASdialer. Сделать это можно из блока **RASdialer** в разделе **Модули расширения -> RASdialer** консоли администратора.
2. Настройте следующие параметры работы модуля.
   - Разрешите или запретите разрешить дозвон по выбранному RAS-соединению. Соединение будет устанавливаться, если выполнены заданные ниже условия.
   - Выберите имя RAS-соединения. Это соединение должно быть создано средствами Windows, полностью настроено и сохранено в профиле "для всех".

     > ***Замечание!*** *Не следует путать RAS-соединения с соединениями службы RRAS.*

   - При необходимости введите имя пользователя и пароль. Если их не указывать, то

будут использованы сохраненные данные соединения.

- Включите или выключит автоматическое соединение при условии активности внешнего интерфейса. При включении этой функции соединение будет устанавливаться только, если данный сетевой интерфейс активен.
- При необходимости RAS-соединение к другому RAS соединению (в Windows данная возможность для постоянных соединений недоступна).
- При необходимости задайте расписание, согласно которому разрешается использование данного RAS соединения.
- Включите или включите автоматическое отключение соединения при остановке службы программы.

3. Сохраните внесенные изменения.

NetPolice для Traffic Inspector

NetPolice для Traffic Inspector – дополнительный модуль для контентной фильтрации нежелательных интернет-ресурсов, разработанный совместно с ЦАИР. В нем реализовано два способа фильтрации:

- правила по блокировке категорий (в том числе по спискам категорий, рекомендованным Минобрнауки РФ);
- анализ по URL и словам на странице.

Принцип работы модуля заключается в отнесении анализируемых страниц к тем или иным категориям контента (подробнее о категориях контента см. в п. Категории контента) на основе их содержимого с использованием сервиса NetPolice. После этого можно настроить правила, регулирующие доступ к сайтам этих категорий категории (подробнее о правилах см. в п. Виды и предназначение правил, наборы правил). Соответствие между результатом работы сервиса NetPolice и категориям контента устанавливаются с помощью правил модуля. Правил в модуле может быть произвольное количество. Они могут использовать разные категории контента. Это позволяет гибко реализовать различные виды фильтрации по типу контента, а также другие действия.

Дополнительные модули Traffic Inspector

13

Для оценки работы модуля предусмотрен демонстрационный (триальный) режим на один месяц. Модуль при этом никаких ограничений по функциональным возможностям не имеет. Продлить оценочный период нельзя. Если сама программа активирована в триальном режиме, то оценочный период модуля начинается с момента активации. При постоянном активировании программы для включения триального режима этого модуля необходимо связаться с продавцом, разрешить режим и повторно активировать программу.

Постоянный режим активации модуля предусмотрен на конечный срок и на конкретное количество пользователей, при этом модуль активируется в процессе активации самой программы.

Предусмотрено два типа лицензирования модуля по количеству пользователей:

1. Как у программы Traffic Inspector. В этом случае для всех пользователей программы будут работать правила модуля NetPolice для Traffic Inspector.
2. Отдельное лицензирование. В этом случае для модуля NetPolice для Traffic Inspector может быть приобретено меньшее количество лицензий, чем у Traffic Inspector.

При отдельном лицензировании появляются дополнительные настройки – предусматривается возможность включить использование возможностей модуля как для отдельных пользователей, так и для целых их групп. Для запоминания этих настроек используется дополнительный атрибут пользователя и группы – NetPolice. Описания атрибутов добавляются автоматически при запуске программы. Удалить атрибут из описания нельзя.

Для разрешения возможностей модуля значение атрибута должно быть **Да**. Любое другое или пустое значение атрибута означает, что проверка отключена. Изменить значение атрибута можно в окне редактирования дополнительных атрибутов групп (подробнее см. в п. Создание и настройка групп) и пользователей (подробнее см. в п. Создание и настройка пользователей). Если дано разрешение на всю группу, то эта настройка у отдельного пользователя игнорируется.

Для удобного контроля лицензий в консоли модуля имеются списки пользователей и

групп, для которых включены возможности модуля. В списках групп отображается количество лицензий, используемых в рамках каждой группы. В перечне пользователей отображаются только одиночные лицензии. Кроме этого, в списках предусмотрена операция удаления лицензии у пользователя или группы. В отдельном перечне отображаются пользователи, у которых лицензии отсутствуют. Для них возможности модуля использоваться не будут.

Настройка NetPolice для Traffic Inspector

Общие сведения о состоянии модуля NetPolice для Traffic Inspector отображаются в разделе **Модули расширения -> NetPolice для Traffic Inspector** консоли администратора.

На главной странице этого раздела присутствуют два блока. Блок **NetPolice для Traffic Inspector** состоит из двух вкладок. На вкладке **Информация** отображается основная информация о состоянии модуля и краткая статистика его работы, а на вкладке **Действия** приведены ссылки на основные операции. В блоке **Статистика** показывается краткая статистика работы модуля.

В рамках управления модулем NetPolice для Traffic Inspector в Traffic Inspector реализованы следующие операции:

- настройка модуля NetPolice для Traffic Inspector;
- проверка произвольного ресурса;
- создание и настройка правил модуля (работа с правилами модуля описано в п. Правила NetPolice для Traffic Inspector).

Настройка модуля NetPolice для Traffic Inspector

Для настройки модуля NetPolice для Traffic Inspector выполните следующие действия:

1. Откройте окно настройки модуля NetPolice для Traffic Inspector. Сделать это можно из блока **NetPolice для Traffic Inspector** в разделе **Модули расширения -> NetPolice для Traffic Inspector** консоли администратора.

2. На вкладке **Режим работы** разрешите или запретите работу модуля (данная функция позволяет временно отключить модуль, не выгружая или не удаляя его). Здесь же выберите один из двух возможных режимов работы модуля.

   - **Асинхронный режим** – рекомендуемый режим работы. При получении запроса со стороны клиента в прокси-сервере отравляется запрос к сервису NetPolice через Интернет. При этом прокси-сервер продолжает работу, не дожидаясь отклика от сервиса. Проверка отклика от сервиса производится при получении заголовков отклика прокси-сервером. В этом режиме совсем не снижается скорость работы, если отклик от сервиса приходит быстрее, чем от сервера, на который отправил запрос прокси.

   - **Синхронный режим** – в данном режиме все операции выполняются последовательно. Сначала ресурс проверяется сервисом, а после получения результата работа прокси-сервера продолжается. Этот режим работает медленнее, но позволяет немного экономить трафик – если ресурс был заблокирован, то прокси-сервер запрос отправлять не будет.

3. На вкладке **Статистика** включите или отключите запись статистики работы модуля в базу данных. При включении настройте параметры записи. Для этого укажите промежуток времени (в минутах), через который будет выполняться запись, а также, при необходимости, включите дополнительные условия записи – количество первых по трафику записей, количество запросов к хосту, общий объем трафика хоста.

4. На вкладке **Настройки соединения** установите таймаут ответа сервиса NetPolice (по умолчанию 7 секунд). Если подключение к Интернету осуществляется через вышестоящий прокси-сервер, то здесь включите его использование модулем Phishing Blocker (сам прокси-сервер задается в окне общих настроек программы, подробнее см. в п. Общие настройки программы).

5. На вкладке **Кэширование** включите или отключите кэширование результатов запросов к сервису NetPolice. При включении укажите срок хранения записей к кэше (по умолчанию 24 часа). По истечении этого времени данные будут удаляться. Кэш размещается в памяти программы.

6. При необходимости на вкладке **Термины** включите или выключите анализ текста и URL-адресов проверяемых веб-страниц. Данная функция позволяет автоматически блокировать веб-страницы, в тексте которых встречаются термины из заданного списка. При ее включении сформируйте такой список, предварительно выбрав его тип из двух возможных.

- **Вхождение подстроки** – при использовании данного варианта Traffic Inspector будет проверять, входят ли в текст и URL-адреса указанные строки. Его удобно использовать для поиска четко определенных подстрок.
- **Регулярные выражения** – при использовании данного варианта строки в списке представляют собой регулярные выражения. Это позволяет задавать значительно более сложные условия с использованием специального синтаксиса (подробнее см. в п. !!!). Они позволяют определять искомые подстроки более точно, с учетом дополнительных факторов, что обеспечивает меньшее количество ложных срабатываний.

Здесь же укажите количество терминов на странице, необходимых для срабатывания блокировки (по умолчанию 2 термина).

> ***Замечание!*** *При однократном вхож дении любого термина списка в URL-адрес веб-страница будет заблокирована.*

7. Сохраните внесенные изменения.

Проверка произвольного ресурса

В Traffic Inspector реализована возможность проверки произвольного ресурса на его наличие в базе NetPolice. Она может использоваться для проверки запроса (URL) и позволяет увидеть присвоение запросу типа рейтинга в соответствии с заданными правилами

Для выполнения проверки откройте раздел **Модули расширения -> NetPolice для Traffic Inspector -> Проверка** консоли администратора и введите запрос – URL-адрес. Результат проверки будет отображен на этой же странице. В него входят данные, полученные от

сервиса, а также примененные правила.

Правила NetPolice для Traffic Inspector

Правила модуля NetPolice для Traffic Inspector используются для того, чтобы преобразовать полученный от сервиса NetPolice результат запроса в категорию контента, что позволит использовать их в правилах пользователей и групп пользователей (подробнее о принципе работы модуля NetPolice для Traffic Inspector см. в п. NetPolice для Traffic Inspector).

Список правил модуля NetPolice для Traffic Inspector размещен в разделе **Модули расширения -> NetPolice для Traffic Inspector -> Правила**. В рамках управления этими правилами в Traffic Inspector реализованы следующие операции:

- создание/изменение правила модуля NetPolice для Traffic Inspector;
- удаление правила модуля NetPolice для Traffic Inspector.

Создание/изменение правила модуля NetPolice для Traffic Inspector

Для создания нового или изменения существующего правила модуля NetPolice для Traffic Inspector выполните следующие действия.

1. Откройте окно свойств нового или существующего правила модуля. Сделать это можно с помощью контекстного меню в разделе **Модули расширения -> NetPolice для Traffic Inspector -> Правила** консоли администратора.
2. На вкладке **Наименование** укажите уникального наименование правила и, при необходимости, произвольны примечания. Здесь же можно временно запретить работу правила, не удаляя его из системы.
3. На вкладке **Условия** выберите одну или несколько категорий сервиса NetPolice, которые будут обрабатываться данным правилом.
4. На вкладке **Выбор типа контента** выберите одну из предварительно созданных или введите наименование новой категории контента. Именно к ней будут относиться веб-страницы, соответствующие выбранным на предыдущей вкладке категориям сервиса NetPolice.

5. При необходимости на вкладке **Правило пользователей** укажите действие, которое должно быть выполнено для выбранной на предыдущей вкладке категории контента – разрешить или запретить доступ. Это позволит автоматически создать соответствующее правило пользователей. Также правила можно с выбранной категорией контента создавать и позднее вручную, используя разные действия и делая их более гибким (например, можно ограничить скорость доступа к ресурсам определенной тематики, сделать трафик нетарифицируемым и пр., подробнее см. в п. Виды и предназначение правил, наборы правил).

   Замечание! *Вкладка Правило пользователей доступна в окне свойств нового правила модуля. При редактировании уж е существующего ее нет.*

6. Если на вкладке **Правило пользователей** было выбрано создание нового правила пользователей, то на вкладке **Настройки правила** задайте его имя, а также выберите область его применения – в правилах "До группы", "После группы" или для определенных групп.

7. Сохраните внесенные изменения.

Удаление правила модуля NetPolice для Traffic Inspector

Удаление правила модуля осуществляется с помощью контекстного меню в разделе **Модули расширения -> NetPolice для Traffic Inspector -> Правила** консоли администратора.

AntiSpam

Модуль AntiSpam – самообучающееся серверное средство антиспама. Он интегрируется в почтовый шлюз программы Traffic Inspector и анализирует все сообщения, приходящие на внутренний почтовый сервер. Он распознает спам согласно заданным правилам и алгоритмам, которые выводятся собственной самообучающейся системой данного решения.

Программный продукт имеет модульную структуру, в основу которой легли классический байесовский классификатор, а также уникальные исследования и доработки в области

методик маскирования нежелательной корреспонденции и определения специфических признаков спама. Помимо этого в модуле предусмотрена возможность ручного создания правил для распознавания рекламных и обычных писем на основе поиска в их текстах определенных выражений (подробнее о правилах модуля AntiSpam см. в п. Правила AntiSpam).

Для оценки работы модуля предусмотрен демонстрационный (триальный) режим на один месяц. Модуль при этом никаких ограничений по функциональным возможностям не имеет. Продлить оценочный период нельзя. Если сама программа активирована в триальном режиме, то оценочный период модуля начинается с момента активации. При постоянном активировании программы для включения триального режима этого модуля необходимо связаться с продавцом, разрешить режим и повторно активировать программу.

Постоянный режим активации модуля предусмотрен на конечный срок и на конкретное количество пользователей, при этом модуль активируется в процессе активации самой программы.

Предусмотрено два типа лицензирования модуля по количеству пользователей:

1. Как у программы Traffic Inspector. В этом случае для всех пользователей программы будет работать модуль AntiSpam.
2. Отдельное лицензирование. В этом случае для модуля AntiSpam может быть приобретено меньшее количество лицензий, чем у Traffic Inspector.

При отдельном лицензировании появляются дополнительные настройки – предусматривается возможность включить использование возможностей модуля как для отдельных пользователей, так и для целых их групп. Для запоминания этих настроек используется дополнительный атрибут пользователя и группы – AntiSpam. Описания атрибутов добавляются автоматически при запуске программы. Удалить атрибут из описания нельзя.

Для разрешения возможностей модуля значение атрибута должно быть **Да**. Любое другое или пустое значение атрибута означает, что проверка отключена. Изменить значение

атрибута можно в окне редактирования дополнительных атрибутов групп (подробнее см. в п. Создание и настройка групп) и пользователей (подробнее см. в п. Создание и настройка пользователей). Если дано разрешение на всю группу, то эта настройка у отдельного пользователя игнорируется.

Для удобного контроля лицензий в консоли модуля имеются списки пользователей и групп, для которых включены возможности модуля. В списках групп отображается количество лицензий, используемых в рамках каждой группы. В перечне пользователей отображаются только одиночные лицензии. Кроме этого, в списках предусмотрена операция удаления лицензии у пользователя или группы. В отдельном перечне отображаются пользователи, у которых лицензии отсутствуют. Для них возможности модуля использоваться не будут.

Настройка AntiSpam

Общие сведения о состоянии модуля AntiSpam отображаются в разделе **Модули расширения -> AntiSpam** консоли администратора.

На главной странице раздела находится блок **AntiSpam**, который состоит из двух вкладок. На вкладке **Информация** отображается основная информация о состоянии модуля и краткая статистика его работы, а на вкладке **Действия** приведены ссылки на основные операции.

В рамках управления модулем AntiSpam в Traffic Inspector реализованы следующие операции:

- настройка модуля AntiSpam;
- настройка правил модуля (подробнее про правила модуля AntiSpam см. в п. Правила AntiSpam);
- просмотр подробного отчета о работе модуля.

Настройка модуля AntiSpam

Для настройки модуля AntiSpam выполните следующие действия:

1. Откройте окно настройки модуля AntiSpam. Сделать это можно из блока **AntiSpam** в разделе **Модули расширения -> AntiSpam** консоли администратора.

2. На вкладке **Действия** определите уровень агрессивности антиспама. Чем он выше, тем большее количество спама он будет блокировать. Но при этом увеличивает риск его ложного срабатывания. Здесь же при необходимости укажите теги, с которыми письма будут в любом случае классифицироваться как не спам или вообще не будут обрабатываться (теги сообщениям присваиваются SMTP-шлюзом на основе заданных администратором правил, подробнее см. в п. Контроль почтового трафика дополнительными модулями). Также на этой вкладке можно ограничить максимальный размер обрабатываемых модулем сообщений и включить или выключить автоматическое включение в спам всех писем, содержащих символы, не относящиеся к русскому и английскому алфавитам.

3. На вкладках **Спам**, **Обычные письма** и **Сомнительные письма** определите изменения, которые должен внести модуль AntiSpam в рекламные, нерекламные и письма с подозрением на рекламу соответственно. Среди возможных изменений – добавление в тему указанной подстроки (например, "*[SPAM]*"), добавление соответствующего заголовка (например, "*X-AntiSpam: SPAM*"), а также изменение весового коэффициента письма.

4. На вкладке **Настройки** включите или отключите удаление данных обработанных писем (удаление старых писем ускоряет работу со списком писем и предотвращает чрезмерный рост базы данных). При включении укажите срока хранения этой информации укажите срок хранения писем (по умолчанию 30 дней). Здесь же включите или выключите хранение подробной статистики, указав при включении срок ее жизни (чем больше хранится статистики, тем точнее, но при этом и дольше работает антиспам).

5. Сохраните внесенные изменения.

Просмотр подробного отчета о работе модуля Antispam

Просмотр отчета о работе модуля осуществляется в разделе **Отчеты -> Антиспам** консоли администратора. Подробно работа с ним описана в п. Отчёты по работе дополнительных модулей.

Правила AntiSpam

Правила модуля AntiSpam используются для распознавания рекламных и обычных писем на основе поиска в их текстах, а также данных отправителя и/или получателя заданных администратором выражений.

Список правил модуля размещен в разделе **Модули расширения -> AntiSpam -> Правила**. В рамках управления этими правилами в Traffic Inspector реализованы следующие операции:

- создание/изменение правила модуля AntiSpam;
- удаление правила модуля AntiSpam.

Создание/изменение правила модуля AntiSpam

Для создания нового или изменения существующего правила модуля AntiSpam выполните следующие действия:

1. Откройте окно свойств нового или существующего правила модуля. Сделать это можно с помощью контекстного меню в разделе **Модули расширения -> AntiSpam -> Правила** консоли администратора.
2. На вкладке **Наименование** задайте строку, наличие которой в сообщении необходимо для срабатывания данного правила. Здесь же с помощью флажков определите область поиска – текст письма, тема письма, данные получателя и отправителя. Также укажите, какой статус будет присваиваться письму при срабатывании данного правила – спам или не спам.
3. Сохраните внесенные изменения.

Удаление правила модуля AntiSpam

Удаление правила модуля осуществляется с помощью контекстного меню в разделе **Модули расширения -> AntiSpam -> Правила** консоли администратора.

RBL SMTP filter

Модуль RBL SMTP filter расширяет функциональные возможности SMTP-шлюза программы Traffic Inspector и предназначен для фильтрации нежелательной почты – спама. Принцип его работы основан на проверке IP-адресов сервера отправителя в RBL-службах путем отправки на них DNS-запросов. Если проверяемый IP-адрес в этих службах зарегистрирован, то с сообщением можно произвести различные действия, например, отфильтровать.

RBL-службы – это, как правило, бесплатные публичные службы, которые представляют собой каталоги IP-адресов (или целых сетей), публикуемых в сети Интернет своим DNS-сервером. Эти каталоги могут содержать следующие данные.

1. IP-адреса SMTP-серверов с Open Relay. Их могут использовать спамеры для рассылки своей почты.
2. IP-адреса анонимных HTTP-прокси серверов и SOCKS. Они также могут использоваться спамерами.
3. Списки адресов, с которых идет массовая рассылка спама.
4. IP-сети, администраторы которых не пресекают рассылку из них спама.
5. DUL (Dial-Up User List) – списки IP-сетей провайдеров, откуда динамически выдаются IP-адреса конечным пользователям Интернет.

Модуль RBL SMTP фильтр может анализировать как IP-адрес отправителя (того, кто непосредственно отправляет почту на SMTP-шлюз), так и IP-адреса всей цепочки отправителей, которые берутся из заголовков сообщения. Это позволяет с большей эффективностью выявлять нежелательную почту.

По смыслу эти службы можно разделить на следующие группы, в зависимости от этого подход к их использованию должен быть разный.

- Черные списки. Это одиночные адреса, с которых была зарегистрирована массовая

рассылка спама, или которые потенциально могут быть использованы для этого. Это вышеперечисленные типы п.1-3. Сообщения с этими IP-адресами могут фильтроваться.

- Серые списки. Это вышеперечисленный тип п.3. Сообщения с этими IP-адресами фильтровать нельзя, их можно пометить, или добавить весовой коэффициент сообщения, увеличив вероятность фильтрации по весу.
- DUL. Фильтрация сообщений этими службами – очень эффективный метод, позволяющий пресечь прямую рассылку сообщений непосредственно с рабочих компьютеров, напрямую подключенных к Интернету, или из небольших сетей. Такие пользователи, имея динамический IP-адрес, как правило, своего почтового сервера не имеют и легальную почту отправляют через SMTP-сервер провайдера. Прямая же отправка с такого IP-адреса говорит о том, что используется какая-то программа массовой рассылки писем, или этот компьютер заражен троянской спамерской программой. Особенностью использования таких RBL DUL служб является то, что ими надо проверять только IP-адрес отправителя, и ни в коем случае не IP-адреса из заголовков.

Следует отметить, что реально у некоторых служб четкой границы между "черными" и "серыми" списками нет. Поэтому надо очень аккуратно подходить к использованию каждой конкретной службы – изучить материалы в Интернете, отзывы и т.л., иначе это может привести к потере большого количества писем. В программе имеется достаточно функциональных возможностей для гибкой настройки правил фильтрации и обработки почты.

После установки модуля появляется соответствующий раздел в консоли администратора. Также в списке статистики блокировок SMTP-шлюза появляется 2 дополнительных счетчика:

- RBL – счетчик отфильтрованных сообщений по IP-адресу отправителя
- RBL/Header – счетчик отфильтрованных сообщений по IP-адресам в заголовках.

DNS-запросы на все RBL-службы для всех IP-адресов отправляются одновременно, т.е. увеличение количества RBL-служб не приводит к дополнительным задержкам. Время

ожидания (таймаут) едино для всех запросов.

Для экономии DNS-трафика в модуле имеется собственный кэш. В нем запоминаются результаты последних запросов для каждой службы, которые могут повторно использоваться в течение некоторого времени.

Настройка RBL SMTP Filter

Общие сведения о состоянии модуля RBL SMTP Filter отображаются в разделе **Модули расширения -> RBL SMTP Filter** консоли администратора.

На главной странице раздела находится блок **RBL SMTP Filter**, который состоит из двух вкладок. На вкладке **Информация** отображается основная информация о состоянии модуля и краткая статистика его работы, а на вкладке **Действия** приведены ссылки на основные операции.

В рамках управления модулем RBL SMTP Filter в Traffic Inspector реализованы следующие операции:

- настройка модуля;
- настройка используемых RBL-служб (подробнее RBL-службы см. в п. Службы RBL SMTP Filter);
- проверка произвольного IP-адреса.

Настройка модуля

Для настройки модуля RBL SMTP Filter выполните следующие действия.

1. Откройте окно настройки модуля RBL SMTP Filter. Сделать это можно из блока **RBL SMTP Filter** в разделе **Модули расширения -> RBL SMTP Filter** консоли администратора.
2. На вкладке **RBL служба** разрешите или запретите работу модуля (данная функция позволяет временно отключить модуль, не выгружая или не удаляя его). Здесь же установите таймаут запросов к RBL-службам. При этом следует учесть, что также дополнительно может запрашиваться DNS INFO. Поэтому таймаут необходимо

задавать с учетом времени отклика по 2-м DNS-запросам (по умолчанию 20 секунд, рекомендуется указывать не менее 10 секунд). Так как все запросы на все службы обрабатываются параллельно, то к количеству служб таймаут привязывать не надо.

На этой же вкладке выберите способ проверки IP-адреса отправителя – по соединению или приему заголовков. Дело в том, что анализ IP-адреса отправителя может производиться по событиям CONNECT или HEADERS в зависимости от настройки. Анализ по соединению позволяет экономить трафик, анализ по приему заголовков позволяет получить более детальные отчеты по отфильтрованным сообщениям – с темой, адресами отправителя и получателя. Анализ IP-адресов из заголовков производится по событию HEADERS. Т.е. если сообщение фильтруется, то шлюзом принимаются только его заголовки.

При необходимости здесь же задайте исключения путем указания тегов писем, которые не будут обрабатываться данным модулем (теги сообщениям присваиваются SMTP-шлюзом на основе заданных администратором правил, подробнее см. в п. Контроль почтового трафика дополнительными модулями). Также на вкладке **RBL служба** можно включить отправку DNS-запросов RBL-службам напрямую (по умолчанию запросы отправляются через службу DNS Client Windows).

3. На вкладке **Кэширование** настройте собственный кэш модуля, в котором хранятся результаты запросов к RBL-службам. Для этого укажите срок жизни записей для обнаруженных и необнаруженных в базах RBL-служб IP-адресов.

4. На вкладке **Действия** задайте параметры пометки сообщений для всех RBL-служб по умолчанию. Это может быть добавление к сообщению заголовков или изменение его темы. Эти настройки работают аналогично соответствующим настройкам SMTP-шлюза (подробнее см. в п. Контроль почтового трафика на SMTP шлюзе). Для темы и заголовков доступны параметры подстановки.

   - %WEIGH% – весовой коэффициент сообщения на момент его пометки.
   - %RULE% – имя правила, при действии которого произведена пометка.
   - %MARK% – ранее сформированная пометка темы другим правилом.

- %IP% – проверяемый IP адрес. По этому параметру в помеченном сообщении можно определить, по какому IP-адресу сработала служба.
- %ZONE% – DNS зона службы.

5. Сохраните внесенные изменения.

Проверка произвольного IP-адреса

В Traffic Inspector реализована возможность проверки произвольного IP-адреса на его наличие в базах RBL-служб. Для выполнения проверки откройте раздел **Модули расширения -> RBL SMTP Filter -> Проверка** консоли администратора и введите запрос – IP-адрес. Результат проверки будет отображен на этой же странице. В него входят данные, полученные от всех активных RBL-служб.

Службы RBL SMTP Filter

Traffic Inspector может работать с произвольным количеством RBL-служб. Их список размещен в разделе **Модули расширения -> RBL SMTP Filter -> Службы**. Сразу после установки в программе есть ряд готовых записей для наиболее популярных RBL-служб. При необходимости их можно изменять, а также добавлять свои собственные.

В рамках управления RBL-службами в Traffic Inspector реализованы следующие операции:

- создание/изменение RBL-службы;
- мониторинг состояния RBL-служб;
- удаление RBL-службы.

Создание/изменение RBL-службы

Для создания новой или изменения существующей RBL-службы выполните следующие действия.

1. Откройте окно свойств новой или существующей RBL-службы. Сделать это можно с помощью контекстного меню в разделе **Модули расширения -> RBL SMTP Filter ->**

Службы консоли администратора.

2. На вкладке **Наименование** введите уникальное наименование RBL-службы и, при необходимости, произвольные примечания. Здесь же можно временно отключить RBL-службу, не удаляя ее из системы.

3. На вкладке **RBL Служба** задайте DNS-зона RBL-службы. На основании этого параметра будет формироваться DNS-запрос на проверку IP-адресов (DNS-зона конкретной RBL-службы можно узнать на ее официальном сайте). На этой же вкладке включите или выключите поддержку службы DUL (подробнее об использовании DUL см. в п. RBL SMTP filter), введите, при необходимости, адрес официального сайта RBL-службы и включите или отключите разные способы проверки IP-адреса (по отправителю и по соединению).

   > ***Замечание!*** *При включении поддерж ки служ бы DUL необходимо оставить проверку только IP-адресов отправителей.*

   При необходимости задайте исключения путем указания тегов, которые не будут обрабатываться данным модулем (теги сообщениям присваиваются SMTP-шлюзом на основе заданных администратором правил, подробнее см. в п. Контроль почтового трафика на SMTP шлюзе)

4. При необходимости на вкладе **Отклик** настройте список IP-адресов, при получении которых в DNS-отклике сработает это правило. Если список пуст, то правило сработает на любой отклик. Некоторые RBL-службы представляют интегрированные DNS-зоны, включающие сразу несколько разных по сути служб. Разные службы возвращают разные IP-адреса откликов. Эта настройка позволяет настроить правило так, чтобы оно срабатывало только на отклики конкретных служб такой интегрированной зоны.

5. На вкладке **Действия** выберите действие, которое будет выполнять модуль при получении от RBL-службы положительного ответа (IP-адрес признан потенциально опасным с точки зрения рассылки спама).

   - **Блокировать** – сообщение будет признано спамом и немедленно заблокировано.
   - **Обработать** – обработка сообщения будет продолжена. При выборе данного

варианта можно задайте действия, которые будут с ним выполнены. К ним относится добавление или уменьшение весового коэффициента сообщения на указанное значение, а также пометка сообщения путем добавления в тему стандартной или произвольной подстроки или добавления к сообщению стандартного или произвольного заголовка.

6. Сохраните внесенные изменения.

Мониторинг состояния RBL-служб

Мониторинг состояния RBL-служб осуществляется в разделе **Модули расширения -> RBL SMTP Filter -> Монитор** консоли администратора. В нем отображается список работающих RBL-служб с краткой информацией по их состоянию. В частности, показывается задержка ответа, общая статистика работы, даты и время последнего срабатывания и последней ошибки и т.д. Эти данные позволяют получить наглядное представление о работоспособности и текущем состоянии RBL-служб.

Удаление RBL-службы

Удаление RBL-служб осуществляется с помощью контекстного меню в разделе **Модули расширения -> RBL SMTP Filter -> Службы** консоли администратора.

Почтовые службы программы Traffic Inspector – это SMTP-шлюз и служба отправки сообщений. Обе SMTP-службы выполняют достаточно узкие задачи. Они не являются полноценным SMTP-сервером и не могут использоваться для отправки сообщений из локальной сети наружу – почтовый сервер организации должен это делать напрямую сам.

SMTP-шлюз

SMTP-шлюз используется в том случае, если в сети имеется свой почтовый сервер. Совместно со службой отправки сообщений он применяется для приема входящей почты снаружи с целью ее фильтрации и тарификации. Если почтовый сервер находится внутри сети, то использование SMTP-шлюза заменяет задачу наружной публикации SMTP-

сервера.

Использование SMTP-шлюза для приема почты вместо прямой публикации SMTP-службы почтового сервера имеет следующие преимущества:

- гибкая тарификация принимаемого почтового трафика;
- мощные возможности фильтрации нежелательных и опасных сообщений, как самим шлюзом, так и модулями расширения (RBL-списки, антивирусы и т.д.);
- фильтрация сообщений может производиться в самом начале процесса приема сообщения, что ведет к большой экономии трафика.

Эту службу можно задействовать и в случае, если почтовый сервер организации находится снаружи, что, правда, приведет к довольно большому расходованию внешнего трафика.

SMTP-шлюз представляет собой обычный SMTP-сервер, реализация SMTP-протокола в нем самая минимальная. Служба включается в конфигураторе (подробнее см. в п. Настройка служб) и привязывается ко всем IP-адресам всех внешних интерфейсов. Иначе, если внешних сетей в программе не назначено, эта служба будет недоступна. Доступ на TCP-порт SMTP-сервера шлюза во внешнем сетевом экране откроется автоматически.

Для фильтрации сообщений имеется набор правил самого SMTP-шлюза, а также могут подключаться различные модули расширения (плагины). Обработка сообщения правилами производится не только после приема сообщения целиком, но также по каждому событию, связанному с определенными стадиями приема сообщения в рамках SMTP-протокола. Это позволяет настроить процедуру фильтрации таким образом, чтобы сообщения можно было отфильтровать как можно раньше, экономя при этом трафик.

Для анализа работы SMTP-шлюза, отладки правил и поиска потерянных сообщений ведутся логи в нескольких журналах.

- Журнал трассировки – может быть отдельно включена трассировка SMTP-протокола и применений правил. Используется для отладки (трассировка включается в настройках SMTP-шлюза – подробнее см. в п. Настройка SMTP-шлюза).

- Журнал блокировок сообщений – в этот журнал заносятся все факты блокировок и их причины. Используется для поиска потерянной почты.
- Журнал антивирусной проверки – общий для всех служб программы, применяющих антивирусную проверку трафика – HTTP-прокси и SMTP-шлюз.

Служба отправки сообщений

Служба отправки сообщений – это SMTP-клиент со встроенной очередью отправки. В настройках этой службы можно указать только один конкретный IP-адрес внутреннего почтового сервера, производить доставку сообщений на произвольные почтовые сервера путем анализа DNS MX-записей, как это делает полноценный SMTP-сервер, она не умеет.

Наличие внутренней очереди сообщений обеспечивает их хранение в случае временной недоступности почтового сервера организации.

Настройка SMTP-шлюза

Основная информация о работе SMTP-шлюза приводится в разделе **Сервисы -> SMTP-шлюз** консоли администратора. В нем отображается одноименный блок, состоящий из двух вкладок. На вкладке **Информация** показываются внешний порт, на котором запущена служба, основная статистика работы, количество заблокированных писем и т.п. На вкладке **Действия** размещены ссылки на некоторые операции с SMTP-шлюзом. Аналогичный блок, только с меньшим количеством отображаемых данных, размещен также в разделе **Сервисы** консоли администратора.

Для настройки SMTP-шлюза выполните следующие действия.

1. Откройте окно свойств SMTP-шлюза. Сделать это можно из блока **SMTP-шлюз** в одноименном разделе консоли администратора.
2. На вкладке **SMTP сервер** включите или выключите доступ на порт сервера (порт задается в конфигураторе при включении SMTP-шлюза, подробнее см. в п. Настройка служб) со всех внешних адресов. В первом случае будет автоматически создано правило, разрешающее трафик на данный порт с любых внешних сетей. Во втором

случае необходимо будет вручную создать одно или несколько разрешающих правил сетевого экрана, которые разрешат трафик только с определенных IP-адресов или IP-сетей (подробнее о правила сетевого экрана см. в п. Правила внешнего сетевого экрана). Доступ с других адресов будет заблокирован.

Здесь же задайте таймаут соединения, то есть время простоя, при котором входящее TCP-соединение будет закрыто (по умолчанию 120 секунд). Также можно настроить задержку выдачи приглашения. Это мера, обеспечивающая дополнительную фильтрацию спама. Приглашение SMTP-сервера отправляет не сразу, а через указанное количество секунд (по умолчанию 10 секунд) после установления TCP-соединения с отправителем. Если же отправитель начал отправку сообщения, не дожидаясь получения приглашения, то такое соединение будет прервано. Для отключения этой функции задайте задержку, равную 0.

На этой же вкладке пропишите имя домена (или доменное имя хоста), которое будет использоваться в ответе на команды HELO и EHLO. По умолчанию Traffic Inspector подставляет имя сервера

3. На вкладке **Общие ограничения** задайте максимально возможный размер сообщений в килобайтах (по умолчанию 2048) и максимально возможное число получателей в одном письме (по умолчанию 50). При необходимости создайте список исключений – адресов электронной почты получателей, для которых перечисленные выше ограничения не будут действовать. Также можно отдельно указать максимальное количество получателей в одном письме, которое будет действовать на все письма без исключений (по умолчанию 500). Данные ограничения позволяют предотвратить получение различных нежелательных сообщений – спама, рассылок вредоносного программного обеспечения и пр.

4. По умолчанию SMTP-шлюз принимает сообщения только для тех адресов, которые прописаны в настройках авторизации пользователей программы, а все остальные сообщения блокируются. При этом весь почтовый трафик будет соотнесен конкретным пользователем и учтен в биллинге. Если в сообщении несколько получателей, то каждый получатель будет обрабатываться отдельно. Если прием на адрес какого-либо

отдельного получателя запрещен, то он будет исключен из списка получателей сообщения. Если исключаются все получатели, то сообщение фильтруется.

При необходимости можно указать домены, на который будет возможен прием почты независимо от того, прописан адрес получателя в программе или нет. В этом случае почтовый трафик будет учитываться только для тех сообщений, адрес получателей которых имеется у пользователей программы. Для настройки этой функции сформируйте список почтовых доменов (в формате *domain.com*) на вкладке **Получатель**.

5. При необходимости на вкладке **Отправитель** включите проверку сообщений по отправителю (обработка осуществляется автоматически при наступлении события MailFrom, описание событий см. в п. Контроль почтового трафика на SMTP шлюзе). Под проверкой подразумевается проверка реальности почтового домена отправителя на предмет наличия у него DNS MX-записи. При включении настройте действия, которые будет выполнять Traffic Inspector по результатам обработки письмами, которые прошли и не прошли проверку. Для успешных сообщений включите или выключите дальнейшую обработку сообщения правилами и, при необходимости, укажите число, на которое будет уменьшен их рейтинг. Для не прошедших проверку писем включите их блокировку или укажите число, на которое будет увеличен их рейтинг.

6. На вкладке **Действия** укажите рейтинг, при котором сообщение будет признано нежелательным и заблокировано (рейтинг сообщения вычисляется в ходе его обработки SMTP-шлюзом и дополнительными модулями, в ходе которых он может как увеличиваться, так и уменьшаться), а также задайте код и текст отклика отправителю (по умолчанию используется код 554 и текст *Access denided*). Изменение кода на другой может изменить характер поведения отправителя почты при срабатывании блокировки (подробнее см. RFC на протокол SMTP). Текстовое сообщение является чисто информационным и на поведение отправителя, как правило, влияния не оказывает.

   Здесь же, при необходимости, задайте действия, которые будет выполнять SMTP-шлюз с сообщениями, рейтинг которых больше указанного значения. Это могут быть следующие действия:

- Добавление к письмам произвольных заголовков. При создании заголовков можно использовать параметр подстановки *%WEIGH%* (весовой коэффициент на момент пометки сообщения).
- Перенаправление на указанный адрес. Следует учесть, что это сообщение будет отправляться обычным порядком через ту же службу отправки сообщений, поэтому адрес должен нормально восприниматься SMTP-сервером организации. Авторизация для этого адреса в программе не требуется, тарифицироваться данная почта будет для тех получателей, на чей адрес она пришла. При редиректе тема сообщения заменяется на список адресов получателей.
- Изменение темы сообщения согласно указанному шаблону. В шаблоне можно использоваться следующие параметры подстановки:
  - %WEIGHT% – весовой коэффициент на момент пометки сообщения.
  - %MARK% – ранее сформированная пометка темы другим правилом.
  - %SUBJ% – исходная тема сообщения.

> ***Замечание!*** *Пометка сообщения может в дальнейшем использоваться для его последующей обработки в почтовом сервере организации или клиентской почтовой программе. Редирект же можно использовать для пересылки всех потенциально неже лательных сообщений в почтовый ящик – "отстойник".*

7. На вкладке **Правила обработки сообщений** задайте настройки по умолчанию для правил обработки сообщений. Для этого введите шаблон, согласно которому будет изменяться тема сообщения. В шаблоне можно использоваться следующие параметры подстановки:
   - %WEIGH% – весовой коэффициент на момент пометки сообщения.
   - %RULE% – имя правила, при действии которого произведена пометка.
   - %SUBJ% – исходная тема сообщения.

Здесь же можно указать заголовки, которые будут добавляться к сообщениям. В заголовках могут использоваться параметры подстановки %WEIGH% и %RULE% (описание см. выше).

8. На вкладке **Антивирус** настройте действия, которые будет выполнять SMTP-шлюз для инфицированных сообщений, лечение которых невозможно. Для этого включите или выключите "тихий" прием. При включении такое письмо принимается и отправляющей стороне возвращается код успешного приема сообщения. В противном случае отправляющей стороне возвращается код ошибки. Также включите или выключите оповещение получателей. При включении инфицированное сообщение будет заблокировано, а всем его получателем будет отправлено автоматически сформированное письмо с отчетом о найденных вирусах.

   На этой же вкладке, при необходимости, настройте действие, выполняющееся с письмами, которые по тем или иным причинам не могут быть проверены антивирусом. Это может быть блокировка сообщения или выполнение одного или нескольких обработок:

   - Добавление к рейтингу сообщения указанного числа.
   - Добавление к теме сообщения указанной метки (в метке можно использовать параметр подстановки %MARK% – ранее сформированная пометка темы другим правилом).
   - Добавление к сообщению одного или нескольких произвольных заголовков.

   > ***Замечание!*** *Антивирусная проверка выполняется с помощью дополнительных модулей Traffic Inspector (подробнее см.в разделе Дополнительные модули).*

9. На вкладке **Тарификация** включите или выключите следующие параметры тарификации.

   - Пропорциональное разделение трафика, потраченного на прием сообщения, между всеми получателями пропорционально. При выключении этого параметра каждому получателю будет засчитан весь трафика в полном объеме.

- Прием сообщений для пользователей, работа которых приостановлена.
- Прием сообщений для пользователей, отключенных по датам.
- Прием сообщений для пользователей, отключенных из-за отрицательного баланса.
- Запрет приема сообщений для пользователей, работающих в кредит.
- Запись трафика, потраченных на загрузку отфильтрованных впоследствии сообщений, на баланс их получателей.

10. На вкладке **Оповещение администраторов** включите или выключите отправку оповещений администратору о блокировке сообщений и об обнаружении в них вирусов.

> ***Замечание!*** *Отправка осуществляется с помощью служ бы отправки, которая предварительно долж на быть настроена (подробнее см. в п. Служ ба отправки).*

11. Если есть необходимость ведения подробной записи действий SMTP-шлюза в отдельном журнале, то на вкладке **Трассировка** включите запись трассировки SMTP-протокола. Это может быть полезно для отладки взаимодействия с различными SMTP-серверами. Здесь же можно включить запись трассировки обработки правил. Это может пригодиться для отладки работы логики правил.

> ***Замечание!*** *Трассировку рекомендуется включать только временно с целью выполнения отладки приема сообщений, поскольку она значительно увеличивает размер базы данных.*

12. Сохраните внесенные изменения.

Контроль почтового трафика на SMTP шлюзе

Для контроля почтового трафика используются так называемые правила SMTP-шлюза. Также для контроля могут использоваться дополнительные модули (подробнее см. в п. Контроль почтового трафика дополнительными модулями). Обработка сообщения правилами SMTP-шлюза производится не только после приема сообщения целиком, но также по каждому событию, связанному с определенными стадиями приема сообщения в

рамках SMTP-протокола. Это позволяет настроить процедуру фильтрации таким образом, чтобы сообщения можно было отфильтровать как можно раньше, экономя при этом трафик.

При каждом событии для анализа доступны только те атрибуты сообщений, которые уже имеются (приняты):

- IP-адрес и DNS-имя хоста отправителя;
- e-mail адрес отправителя;
- e-mail адрес получателя;
- тема сообщения;
- внутренние заголовки сообщения;
- IP-адреса в заголовках (их можно использовать для анализа трассировки пути доставки сообщений).

В правилах могут проверяться только эти атрибуты, используется синтаксис регулярных выражений. Анализ всего сообщения целиком доступен только в дополнительных модулях.

Предусмотрены следующие события, по которым производятся действия обработки сообщений.

- **Connect**. Событие происходит в момент попытки установления соединения с SMTP-сервером. Доступны только атрибуты IP-адреса и имени хоста. По этому событию можно сразу отсечь попытку соединения с определенных хостов ("черные списки") или, наоборот, разрешить прием любой почты ("белые списки").
- **HELO**. Событие происходит по приему соответствующей SMTP-команды (HELO или EHLO).
- **MailFrom**. Событие происходит по приему адреса отправителя. По данному событию можно произвести анализ этого адреса в правилах. Также имеется функция анализа валидности почтового домена адреса отправителя на предмет наличия DNS MX-записи.

- **RcptTo**. Событие происходит по приему адреса получателя. По событию можно произвести анализ этого адреса в правилах. Если получателей несколько, то это событие вызывается по каждому адресу получателя отдельно. На данной стадии SMTP-шлюз также производит поиск пользователя программы по его e-mail адресу в параметрах авторизации, и, если прием почты для этого получателя запрещен, SMTP-клиенту возвращается ответ с ошибкой. SMTP-сессия может и не закрываться, SMTP-клиент в силе продолжить отправку сообщения для другого получателя.

- **Headers**. Событие происходит по приему заголовков сообщения, при этом доступны атрибуты заголовков. Тема сообщения находится в заголовках, поэтому она также доступна для анализа. Доступен и список IP-адресов заголовков.

- **Complete**. Событие происходит по принятию всего сообщения. Доступны все атрибуты. По этому событию также производится антивирусная проверка сообщения.

Операцию фильтрации сообщения по данным заголовков можно производить по событию их приема. Но следует иметь в виду, что SMTP-клиент на этой стадии отправки сообщения, скорее всего, анализировать код возврата не будет, и прекращение приема данных тела сообщения воспримет как ошибку связи, а через некоторое время предпримет попытку повторной отправки. Поэтому такую фильтрацию лучше всего делать по приему сообщения целиком (событие Complete).

В SMTP-шлюзе имеется механизм добавления (отнимания) так называемого весового коэффициента сообщения, что позволяет реализовать его обработку по совокупности разных признаков. Если в самом конце приема и анализа сообщения этот вес превысит определенный заданный порог, то сообщение может быть отфильтровано (подробнее о настройки блокировки по рейтингу см. в п. Настройка SMTP-шлюза).

Кроме такого радикального действия, как блокировка, может быть сделана пометка сообщения в теме или его заголовках. Эти признаки в дальнейшем могут использоваться для фильтрации сообщений в почтовом сервере организации или непосредственно в пользовательской почтовой программе. Последняя может использовать пометки в теме для распределения принятых сообщений в разных папках. Помечаться сообщение может при превышении его веса заданным порогом, а также отдельными правилами.

Список правил SMTP-шлюза размещен в разделе **Сервисы -> SMTP-шлюз -> Правила** консоли администратора. Он может отображаться в двух видах – упрощенном или экспертном. Переключение между ними осуществляется с помощью вкладок в нижней части страницы. В упрощенном виде правила SMTP-шлюза отображаются в виде белых и черных списков IP-адресов, отправителей, получателей и тем. При этом ссылка правила ведет на вкладку **Выражение** окна его свойств (подробнее об этом см. ниже). Такой подход позволяет максимально просто и быстро настраивать стандартные правила SMTP-шлюза. В экспертном режиме управление правилами осуществляется в ручном режиме. При этом доступны все возможные операции.

В рамках управления правилами SMTP-шлюза в Traffic Inspector реализованы следующие операции:

- создание/изменение правила SMTP-шлюза;
- проверка произвольного выражения;
- удаление правила SMTP-шлюза.

Создание/изменение правила SMTP-шлюза

Для создания нового или изменения существующего правила SMTP-шлюза выполните следующие действия:

1. Откройте окно свойств нового или существующего правила SMTP-шлюза. Сделать это можно с помощью контекстного меню в разделе **Сервисы -> SMTP-шлюз -> Правила** консоли администратора.
2. На вкладке **Наименование** введите уникальное наименование правила SMTP-шлюза и, при необходимости, произвольные примечания. Здесь же можно временно отключить правила, не удаляя его из системы.
3. На вкладке **Правило** выберите событие, при наступлении которого данное правило SMTP-шлюза должно срабатывать (описание событий см. выше) и с помощью флажков отметьте те атрибуты, в которых будет осуществлять поиск заданных выражений.

Замечание! *Перечень доступных атрибутов зависит от выбранного события (см. описание событий выше).*

Если среди атрибутов для анализа был выбран IP-адрес отправителя, то можно указать, откуда будут браться выражения для сравнения – из списка в свойствах самого правила SMTP-шлюза (по умолчанию) или же из описания указанной IP-сети (подробнее про IP-сети см. в п. IP-сети). Второй вариант очень удобно использовать в тех случаях, когда нужно, к примеру, всегда разрешить почту из удаленных филиалов (описание IP-адресов филиалов содержатся в описании соответствующей IP-сети и могут использоваться при составлении правил пользователей, правил SMTP-шлюза, при настройке сетевого экрана и пр.).

4. На вкладке **Способ обработки выражений** выберите тип обработки – вхождение подстроки или регулярные выражения. В первом случае список выражений будет представлять собой обычные текстовые строки, которые и будут искаться в значениях указанных атрибутов. Во втором случае в списке будут содержаться регулярные выражения, которые позволяют значительно более точно настроить поиск и уменьшить риск ложных срабатываний (подробнее о синтаксисе регулярных выражений см. в п. !!!). Здесь же включите или выключите чувствительность поиска к регистру символов.

5. На вкладке **Действия** настройте действие, которое будет выполнять SMTP-шлюз с сообщениями, которые удовлетворяют заданным условиям. Здесь возможны следующие варианты.

   - **Продолжать проверку** – к сообщению применяются заданные на этой же вкладке действия (см. ниже), его загрузка (если оно еще не было полностью загружено) и обработка продолжается в обычном порядке.

   - **Блокировать** – сообщение блокируется, его дальнейший прием прекращается.

   - **Разрешить** – к сообщению применяются заданные на этой же вкладке действия (см. ниже), его загрузка продолжается (если оно еще не было полностью загружено), но больше никаких проверок оно не проходит (за исключением проверки

антивирусами). То есть данное действие аналогично "белому" списку.

- **На следующее событие** – к сообщению применяются заданные на этой же вкладке действия (см. ниже), его загрузка продолжается (если оно еще не было полностью загружено), проверка этого сообщения по данному событию по другим правилам этого списка прекращается. Но для последующих событий все проверки сообщения производятся в обычном порядке.

При необходимости на этой же вкладке настройте следующие действия, которые могут применяться к сообщению.

- Изменение весового коэффициента – рейтингу сообщения добавляется или из него вычитается указанное значение.
- К сообщению добавляется или из него удаляется указанная отметка. Эти отметки могут использоваться, в том числе, в дополнительных модулях (антивирус, антиспам и т.п.) как условия для выборочной обработки.

6. На вкладке **Пометка сообщений** настройте правила автоматического изменения темы сообщения и добавление к нему одного или нескольких произвольных заголовков. По умолчанию эти настройки загружаются из свойств SMTP-шлюза (подробнее см. описание вкладки **Правила обработки сообщений** в п. Настройка SMTP-шлюза). Однако при необходимости их можно установить для правила индивидуальные параметры.
7. При необходимости на вкладке **Автозагрузка** настройте параметры автоматической загрузки списка выражений по протоколу HTTP. Для этого укажите URL-адрес списка и укажите расписание выполнения операции загрузки.
8. На вкладке **Выражения** настройте список выражений. Создавать его можно вручную, при этом каждое выражение пишется в отдельной строке. Также список может быть загружен из предварительно подготовленного файла.

> ***Замечание!*** *Функция загрузки с внешнего источника доступна только в том случае, если были настроены параметры на вкладке* ***Автозагрузка****.*

Список может быть выгружен в виде текстового файла.

9. Сохраните внесенные изменения.

Проверка произвольного выражения

В Traffic Inspector реализована функция проверки выражения, которая позволяет проверить, соответствует указанное выражение данному правилу или нет. Проверка осуществляется в специальном окне, вызвать которое можно с вкладки **Список** окна свойства правила SMTP-шлюза или с помощью контекстного меню раздела **Сервисы -> SMTP-шлюз -> Правила** консоли администратора.

В окне введите тестируемый запрос и запустите проверку. Если адрес соответствует правилу, то отображается номер первой строки (нумерация с "1") списка выражений, где это условие выполнилось.

Удаление правила SMTP-шлюза

Удаление правила SMTP-шлюза осуществляется с помощью контекстного меню в разделе **Сервисы -> SMTP-шлюз -> Правила** консоли администратора.

Контроль почтового трафика дополнительными модулями

В Traffic Inspector реализована возможность почтового трафика дополнительными модулями – антивирусом, антиспамом и пр. (перечень возможных дополнительных модулей, условия их использования и настройка подробно описаны в разделе Дополнительные модули). Проверка писем дополнительными модулями осуществляется после проверки их средствами непосредственно SMTP-шлюза (подробнее см. в п. Контроль почтового трафика на SMTP шлюзе). Таким образом, до дополнительных модулей доходят только полностью загруженные и пропущенные правилами SMTP-шлюза сообщения.

В Traffic Inspector реализована возможность условной проверки сообщений дополнительными модулями. Это значит, что не все письма в обязательном порядке проходят проверку антивирусом, антиспамом и пр. В качестве условий используются

теги, которые могут добавляться в сообщения правилами SMTP-шлюза (подробнее см. в п. Контроль почтового трафика на SMTP шлюзе). В свойствах дополнительных модулей (подробнее см. в Дополнительные модули) можно указывать, с какими тегами письма будут проверяться или, наоборот не будут проверяться.

В ходе выполнения проверки почтового трафика дополнительные модули могут выполнять с сообщениями различные действия, в частности, пытаться вылечить от вирусов, блокировать их, изменять рейтинг, по которому SMTP-шлюз может блокировать сообщения (подробнее см. в п. Настройка SMTP-шлюза). Разные дополнительные модули могут выполнять разные действия (подробнее см. в разделе Дополнительные модули).

Служба отправки

Служба отправки состоит из SMTP-клиента и очереди сообщений. SMTP-клиент ни к каким сетевым интерфейсам не привязан. Эта служба, кроме пересылки сообщений, принятых почтовым шлюзом, используется и для рассылки оповещений администраторам. Поэтому она всегда включена, и ее настройки доступны независимо от того, используется SMTP-шлюз или нет.

Основная информация о работе службы отправки приводится в разделе **Сервисы -> SMTP-службы** консоли администратора. В нем отображается одноименный блок, состоящий из двух вкладок. На вкладке **Информация** показываются статистика работы службы, а на вкладке **Действия** размещены ссылки на некоторые операции со службой отправки. Аналогичный блок размещен также в разделе **Сервисы** консоли администратора.

Очередь сообщений **Сервисы -> SMTP-службы -> Очередь отправки** консоли администратора. Если SMTP-сервер, куда отправляются сообщения, находится во внутренней сети и процесс передачи сообщения быстрый, то в этом случае очередь отправки почти всегда должна быть пустой. Статистику отправки можно наблюдать на главной странице службы.

Для сообщения в очереди отображается его статус и сообщение об ошибке. Служба отправки сообщений при невозможности отправки будет пытаться отправить его повторно в течение определенного времени, после чего удалит.

Если сообщения скапливаются и очередь растет, то выполните следующие действия.

- Проверьте настройки службы отправки. Пошлите проверочное сообщение.
- Проверьте работу SMTP-сервера, не перегружен ли он.
- Сообщение может нести в себе ошибку – сервер его отвергает. Проверьте системный журнал: там фиксируются все ошибки отправки.

Эти сообщения очереди находятся на сервере в папке *\MailRoot\Queue*. Предусмотрена возможность их просмотра через консоль – используйте кнопку или контекстное меню. Сообщение будет считано в виде стандартного EML-файла, и будет запущено приложение, которое в системе используется для просмотра таких файлов. Как правило, это Outlook Express.

Также, в консоли администратора есть возможность дать команду на немедленную отправку сообщений из очереди. Это может быть полезно, когда проблемы отправки устранены и ждать времени, когда служба сделает это сама, нет необходимости.

Если сообщение в очереди ошибочно или не нужно, его можно удалить.

Настройка службы отправки

Для настройки службы отправки выполните следующие действия.

1. Откройте окно свойств службы отправки. Сделать это можно в блоке **SMTP-службы** в разделе **Сервисы -> SMTP-службы** консоли администратора.
2. На вкладке **Отправка сообщений** укажите SMTP-сервер, на который будут отправляться сообщения. Для этого можно использовать как имя хоста, так и IP-адрес. Данный сервер может находиться как во внутренней сети, так и локально на самом сервере с Traffic Inspector. В последнем случае для исключения конфликтов, возможно, придется разнести TCP-порты у разных SMTP-сервера и SMTP-служб Traffic Inspector. Поменять порт SMTP-сервера, на который будут отправляться письма, можно на этой же вкладке.

   Здесь же задайте параметры аутентификации на SMTP-сервера.

3. На вкладке **Параметры отправки** настройте таймаут соединения с сервером (по умолчанию 120 секунд), а также укажите, через сколько минут служба отправки будет повторять отправку сообщений при неудаче (по умолчанию 15 минут) и через сколько часов так и не отправленные сообщения будут удаляться из очереди (по умолчанию 48 часов).

4. На вкладке **Оповещение** включите или выключите функцию автоматической отправки администратору различных оповещений по электронной почте. При включении разрешите или запретите отправку оповещений о предупреждениях и введите адрес электронной почты, от имени которого будут отправляться письма.

5. Для уменьшения количества генерируемых почтовых сообщений от оповещений в Traffic Inspector реализовано объединение нескольких оповещений в одно. Оповещения копятся некоторое время в отдельной очереди и затем отправляются в виде одного сообщения. При выгрузке службы программы, если в этих очередях имеются неотправленные сообщения, они запоминаются на диске, и будут отправлены при последующем запуске службы программы. Для настройки времени нахождения оповещения в очереди на вкладке **Оповещение** укажите максимальное количество оповещений в одном сообщении (по умолчанию 20 оповещений), а также максимальное время в минутах, через которое оповещение будет отправлено в любом случае, независимо от количества оповещений в очереди (по умолчанию 60 минут).

6. На вкладке **Список рассылки** сформируйте список адресов электронной почты, по которым будут рассылаться оповещения. На этой же вкладке можно применить заданные настройки и отправить тестовое сообщение.

   Замечание! *Вкладка* ***Список рассылки*** *доступна только в том случае, если функция оповещения включена.*

7. Сохраните внесенные изменения.

Виды и назначение отчётов

Отчеты позволяют администратору сети получать наглядную информацию о работе Traffic Inspector, дополнительных модулей и пользователей. Они размещаются в разделе **Отчеты**

консоли администратора. Для каждого отчета в нем создан собственный подраздел, в котором и осуществляется его просмотр.

В целом алгоритм работы со всеми отчетами одинаков. Для просмотра отчета откройте его подраздел, с помощью доступных фильтров настройте параметры отбора информации и запустите генерацию отчета. Сформированный отчет можно сортировать по любым столбцам, распечатывать целиком или постранично и экспортировать в Microsoft Excel. Некоторые данные в отчетах кликабельны, например, имя хоста (открывает это имя в браузере, установленном по умолчанию), IP-адрес (запускает сервис Whois для данного IP-адреса).

Для настройки общих параметров отображения отчетов откройте раздел **Отчеты -> Параметры отчетов** консоли администратора и укажите количество строк, которые должны отображаться на одной странице табличного отчета и таймаут соединения с сервером, а также включите или выключите отображение интервальных (более подробных) отчетов по трафику.

В Traffic Inspector реализованы следующие отчеты.

- **Отчеты по трафику** – могут применяться для индивидуального и сравнительного анализа трафика за заданный период времени. При его формировании используются записи журнала пользователей и счетчиков.
- **Отчеты по сетевой статистике** – могут применяться для индивидуального и сравнительного анализа трафика за заданный период времени. При его формировании используются записи журнала пользователей и счетчиков.
- **Отчеты по прокси-серверу** – используются для детального анализа сетевого контента, проходящего через прокси-сервер.
- **Отчет по активности пользователей** – отражает активность пользователей за указанный период времени.
- **Отчеты по работе SMTP-шлюза** – журналы по работе с письмами, полученными SMTP-шлюзом.

- **Отчеты по работе дополнительных модулей** – используются для просмотра статистики работы дополнительных модулей: антиспама, антивируса, контекстной фильтрации.

Отчёты по трафику

В Traffic Inspector реализовано три отчета по трафику:

- **По пользователям** – позволяет вывести информацию о трафике в разрезе пользователей и счетчиков;
- **По времени** – отображает информацию о трафике пользователей и счетчиков по дням или часам;
- **По скорости** – отражает изменения трафика в единицу времени для счетчиков.

Отчет по пользователям

Табличный отчет для просмотра трафика по пользователям, группам пользователей и счетчикам. Отчет по пользователям размещен в разделе **Отчеты -> Трафик -> По пользователям** консоли администратора. Для настройки отображения отчета используются следующие параметры.

- Интервал дат, за который строится отчет.
- Отдельные пользователи, группы пользователей и счетчики, данные по которым будут отображены в отчете. Можно выбирать их все вместе. То есть в одном отчете могут собирать данные по пользователям, группам и счетчикам.

В отчете отображается следующая информация по каждому выбранному в фильтрах пользователю, группе или счетчику.

- Общий объем входящего трафика.
- Общий объем исходящего трафика.
- Объем трафика, принятого из кэша прокси-сервера.
- Объем входящего почтового трафика.

- Объем исходящего почтового трафика.
- Общая сумма затрат.
- Сумма затрат по трафику.
- Сумма затрат по времени.

Отчет по времени

Графический отчет, предназначенный для просмотра потребления трафика по пользователям, группам пользователей и счетчикам по времени. Отчет по пользователям размещен в разделе **Отчеты -> Трафик -> По времени** консоли администратора. Для настройки отображения отчета используются следующие параметры.

- Интервал дат, за который строится отчет.
- Группировка информации – по дням или по часам.

> ***Замечание!*** *Группировка по часам возможна только при выборе в интервале дат одни сутки.*

- Информация, которая должна включаться в отчет: данные по входящему и исходящему трафику, почтовому трафику и трафику из кэша.
- Отдельные пользователи, группы пользователей и счетчики, данные по которым будут отображены в отчете. Можно выбирать их все вместе. То есть в одном отчете могут собирать данные по пользователям, группам и счетчикам.

Отчет по скорости

Графический отчет, предназначенный для просмотра скорости доступа по пользователям, группам пользователей и счетчикам по времени. Отчет по пользователям размещен в разделе **Отчеты -> Трафик -> По времени** консоли администратора. Для настройки отображения отчет используются следующие параметры. Его настройка полностью аналогична настройке отчета по времени.

Отчёты

15

Отчёты по сетевой статистике

В Traffic Inspector реализовано два отчета по сетевой статистике:

- **Сетевая статистика** – для детального анализа трафика по хостам, IP-адресам, протоколам и портам для пользователей и счетчиков;
- **Текущие соединения** – отображает текущую сетевую статистику пользователей и счетчиков.

Сетевая статистика

Табличный отчет, который применяется для детального анализа трафика по хостам, IP-адресам, протоколам и портам для пользователей и счетчиков. При формировании используется журнал сетевой статистики, куда запись данных для пользователей и счетчиков должна быть специально разрешена (подробнее см. в разделе Управление сетевой статистикой). Отчет по сетевой статистике размещен в разделе **Отчеты -> Сетевая статистика** консоли администратора. Для настройки отображения отчета используются следующие параметры.

- Интервал дат, за который строится отчет.
- Фильтр для отображения статистики – тип фильтра (пользователь, контролируемый счетчик, информационный счетчик или нарушение политик) и его значение.

В отчете отображается следующая информация по каждой записи в сетевой статистике.

- IP-адрес и имя хоста.
- Протокол, по которому происходил обмен трафиком.
- Объем входящего и исходящего трафика.
- Объект (пользователь или счетчик).
- Период соединения.

Текущие соединения

Табличный отчет, который текущую сетевую статистику пользователей и счетчиков. Он размещен в разделе **Отчеты -> Текущие соединения** консоли администратора. Для настройки отображения отчета используются следующие параметры.

- Фильтр для отображения статистики – тип фильтра (пользователь, контролируемый счетчик, информационный счетчик или нарушение политик) и его значение.

В отчете отображается та же информация, что и в отчете **Сетевая статистика** (см. выше).

Отчёты по прокси-серверу

В Traffic Inspector реализовано два отчета по прокси-серверу:

- **Биллинг** – отчет для просмотра событий, связанных с тарификацией пользователей;
- **Прокси-сервер** – отчет для детального анализа сетевого контента, проходящего через прокси-сервер.

Биллинг

Табличный отчет, в котором отображаются события, связанные с изменением тарификации пользователей, их состояния и активности. При формировании используются записи журнала пользователей. Отчет по биллингу размещен в разделе **Отчеты -> Биллинг** консоли администратора. Для настройки отображения отчета используются следующие параметры.

- Интервал дат, за который строится отчет.
- Группа, по пользователям которой строится отчет.
- Конкретный пользователь, по событиям которого строится отчет.
- Конкретное событие (например, остановка или запуск сессии биллинга, изменение тарифа, работа в кредит и пр.), по которому строится отчет.

В отчете отображается следующая информация по каждому событию, удовлетворяющему заданным фильтрам.

- Дата и время события.

- Пользователь программы.
- Наименование события.
- Баланс пользователя после события.
- Сумма, начисленная на лицевой счет.
- Сумма, списанная с лицевого счета за трафик.
- Сумма, списанная с лицевого счета за время подключения.
- Администратор, выполнивший операцию (для операций, связанных с управлением биллингом, тарифами и пр.).
- Комментарий администратора.

При просмотре отчета по биллингу можно перемещаться по нему, открывая группы и просматривая данные по входящих в их состав пользователей, и возвращаясь на верхний уровень для просмотра суммарных данных по группам.

Прокси-сервер

Табличный отчет, который используется для детального анализа сетевого контента, проходящего через прокси-сервер.Он размещен в разделе **Отчеты -> Прокси-сервер** консоли администратора. Для настройки отображения отчета используются следующие параметры.

- Интервал дат, за который строится отчет.
- Группа, по пользователям которой строится отчет.
- Конкретный пользователь, по которому строится отчет.
- Конкретный хост, по которому строится отчет.

В отчете отображается следующая информация по каждому запросу, удовлетворяющему заданным фильтрам.

- Дата и время запроса.
- Пользователь.
- Количество байтов, принятых и отправленных в рамках данного запроса.
- Запрос.

Отчёт по активности пользователей

Отчет по активности пользователей – графический отчет, который отражает активность пользователей за указанный период времени. Он размещен в разделе **Отчеты -> Активность** консоли администратора. Для настройки отображения отчета используются следующие параметры.

- Интервал дат, за который строится отчет.
- Группа, по пользователям которой строится отчет.
- Конкретный пользователь, по которому строится отчет.

Отчёты по работе SMTP шлюза

Отчет по работе SMTP-шлюзом – табличный отчет, с помощью которого можно просмотреть журналов по работе с письмами, полученными SMTP-шлюзом. Он размещен в разделе **Отчеты -> Письма** консоли администратора. Для настройки отображения отчета используются следующие параметры.

- Интервал дат, за который строится отчет.
- Отправитель, по которому строится отчет.
- Отправитель, по которому строится отчет.
- Тема, по которой строится отчет.
- Тип писем, по которому строится отчет (все, заблокированные, отправленные).

В отчете отображается следующая информация по каждому письму, удовлетворяющему заданным фильтрам.

- Адрес отправителя.

- Адрес получателя.
- Тема письма.
- Размер письма.
- IP-адрес SMTP-сервера отправителя.
- Дата и время получения письма.
- Статус письма.

Отчёты по работе дополнительных модулей

В Traffic Inspector реализованы следующие отчеты по работе дополнительных модулей:

- **Контекстная фильтрация** – отображает данные о категоризации HTTP-запросов;
- **Антиспам** – предназначен для манипуляций с письмами, прошедшими через антиспам-фильтр;
- **Антивирус** – предназначен для просмотра информации о найденных вирусах и вредоносном программном обеспечении.

Контекстная фильтрация

Табличный отчет, который отображает данные о категоризации HTTP-запросов и позволяет просмотреть причины блокировки ресурсов. Он размещен в разделе **Отчеты -> Контекстная фильтрация** консоли администратора. Для настройки отображения отчета используются следующие параметры.

- Интервал дат, за который строится отчет.
- Группа, по пользователям которой строится отчет.
- Конкретный пользователь, по которому строится отчет.
- Категория модуля контекстной фильтрации, по которому строится отчет.

В отчете отображается следующая информация по каждому хосту, удовлетворяющему

заданным фильтрам.

- Дата и время обращения к хосту.
- Имя хоста.
- Используемый для категоризации дополнительный модуль.
- Имя пользователя.
- Категория, к которой отнесен данный хост.
- Статус запроса.
- Правило, которое сработало по данной категории.
- Объем загруженной с хоста информации.

Антиспам

Табличный отчет, который предназначен для манипуляций с письмами, прошедшими через антиспам-фильтр. Он размещен в разделе **Отчеты -> Антиспам** консоли администратора. Для настройки отображения отчета используются следующие параметры.

- Интервал дат, за который строится отчет.
- Отправитель, по которому строится отчет.
- Отправитель, по которому строится отчет.
- Тема, по которой строится отчет.
- Тип писем, по которой строится отчет.

В отчете отображается следующая информация по каждому письму, удовлетворяющему заданным фильтрам.

- Отправитель.
- Тема письма.

- Получатель.
- Дата и время получения.

В сформированном отчете можно отмечать письма и указывать, являются они спамом или нет. Это позволяет исправлять ошибки модуля антиспама и способствовать более качественному его обучению.

Антивирус

Табличный отчет, который представляет собой перечень найденных вирусов и другого нежелательного контента. Он размещен в разделе **Отчеты -> Антивирус** консоли администратора. Для настройки отображения отчета используются следующие параметры.

- Интервал дат, за который строится отчет.
- Группа, по пользователям которой строится отчет.
- Конкретный пользователь, по которому строится отчет.

В отчете отображается следующая информация по каждому случаю обнаружения вирусов и вредоносного программного обеспечения, удовлетворяющему заданным фильтрам.

- Дата и время инцидента.
- Пользователь.
- Антивирусный модуль, обнаруживший вирус.
- Тип, вид и имя вредоносного программного обеспечения.
- Выполненное антивирусным модулем действие.
- Источник вредоносного программного обеспечения.

HTTP прокси-сервер и SOCKS работает на всех IP-адресах внутренних интерфейсов, в том числе на локальном (127.0.0.1). С внешних сетей он всегда недоступен.

16 Прокси-сервер, настройки и возможности

Прокси-сервер, входящий в Traffic Inspector – это классический HTTP/FTP прокси-сервер. Учитывая наличие NAT, где производительность работы существенно выше, служба, на первый взгляд, необязательная. Но его применение во многих случаях целесообразно, поскольку обеспечивает следующие возможности.

- Фильтрация на уровне приложений HTTP и FTP работает только через прокси-сервер.
- Кэширование, которое позволяет реально экономить 10-25% трафика. Возможен и больший процент, но могут возникнуть некоторые неудобства для пользователей – им придется иногда управлять режимами кэширования, хотя имеющиеся возможности гибкой тарификации трафика из кэша позволяют сделать это для них экономически выгодным.
- Возможность работы в активном режиме с FTP. Работа через NAT в активном режиме возможна не всегда.
- Возможность перенаправления (редиректа) запросов.
- Использование SOCKS обеспечивает динамическое открытие входящих TCP- и UDP-соединений.

Прокси-сервер поддерживает туннельные TCP-соединения методом CONNECT, позволяя работать с протоколом SSL.

Если требуется работа через прокси-сервер с приложениями, которые используют входящие TCP- и UDP-соединения со стороны пользователя, то использование SOCKS-сервера – единственная возможность это сделать. Текущая версия программы поддерживает SOCKS версии 4 и 5.

Для ограничения доступа пользователей по протоколу SOCKS используются правила (подробнее см. в п. Виды и предназначение правил, наборы правил), но при этом условия уровня приложений не работают. Для вторичных соединений, как входящих, так и исходящих, правила на запрещение не применяются – любой трафик с хостом, на который установлено первичное соединение, не блокируется.

Прокси-сервер, настройки и возможности

16

Особенности реализации протокола HTTP/1.1

Прокси-сервер оптимизирован для работы с протоколом HTTP/1.1, полностью соответствует стандарту RFC 2616, в нем реализованы механизмы Keep-Alive и Pipelining.

Keep-Alive – процедура удержания и повторного использования TCP-соединений. Все современные браузеры и большинство веб-серверов ее поддерживают, но для них могут потребоваться особые настройки. Использование Keep-Alive существенно экономит трафик, что особенно заметно при загрузке страниц с большим количеством объектов. В некоторых случаях это приводит к ускорению загрузки страниц.

Pipelining – возможность в рамках одного TCP-соединения передавать запросы, не дожидаясь принятого ответа от сервера. Если на странице объектов много, то браузер отправляет сразу все запросы на сервер через одно TCP-соединение. В прокси-сервере Traffic Inspector реализована параллельная асинхронная обработка запросов и ответов: данные запросов также сразу отправляются на сервер, при этом количество запросов в очереди не ограничено.

Функция Pipelining поддерживается не всем веб-серверами и не всеми браузерами. Кроме того, в некоторых браузерах она по умолчанию отключена (подробнее см. документацию на соответствующие браузеры). Нужно учитывать, что если исходящий канал медленный или время отклика сервера большое (большие задержки в каналах связи), то использование Pipelining существенно ускоряет загрузку данных.

Все эти функции работают и в режиме каскадирования на другой прокси-сервер, но здесь все зависит от поддержки данных функций на вышестоящем прокси. Наиболее распространенные прокси-сервера – ISA и Squid – в полном объеме Pipelining не поддерживают.

Особенности реализации кэширования

Кэширование в прокси-сервере выполняется путем сохранением загруженных страниц в кэше для их повторного использования при последующих обращениях к данным ресурсам.

Это позволяет экономить трафик и ускоряет загрузку страниц при медленных каналах связи. Обратной стороной использования кэша является проблема получения всегда достоверных данных для сохраненных ресурсов – необходимо проверять, обновились ли они на веб-сервере. Стандарты на HTTP/1.1 и другие подробно регламентируют работу серверов, но реалии сети Интернет таковы, что не все им следуют. Задача получить реальную экономию за счет кэширования и при этом передать на пользователя достоверные данные оказывается весьма сложной и противоречивой.

Прокси-сервер Traffic Inspector позволяет произвести настройку кэша достаточно тонко в соответствии с поставленными задачами. При установке эти настройки включены в режим небольшого сбережения трафика, при этом пользователи практически всегда получают достоверные данные от сервера.

Алгоритм работы программы при кэшировании следующий.

При сохранении ресурса в кэше запоминается время его получения с сервера и время создания (модификации) на самом сервере. Правда, этот атрибут может и отсутствовать – сервер по какой-то причине может его не выдать. Если далее на прокси-сервер поступает запрос на доступ к этому ресурсу, а он есть в кэше, то производится вычисление параметра TTL – прогнозируемого времени жизни. Он берется как процент от времени, в течение которого ресурс существовал с момента его записи в кэш. Смысловым значением данного параметра является прогноз: если ресурс не изменялся какое-то время, то он и в дальнейшем не будет меняться.

Следует отметить, что серверы для некоторых ресурсов выдают атрибут времени существования объекта. Если он был выдан, то тдже сохраняется при кэшировании. При его наличии прогноз вычисляться не будет; TTL же определяется на основании этого атрибута. Использование времени существования объекта, полученного от сервера, может быть отключено. Причина в том, что данный параметр довольно часто по вине небрежности программистов и администраторов веб-сервера выдается некорректным, и для определения TTL лучше полагаться на собственную логику.

На полученное значение TTL дополнительно накладываются ограничения по минимуму и максимуму. Если на момент запроса текущее время не превысило TTL, то ресурс считается

непросроченным, в этом случае он берется из кэша. Иначе ресурс будет считаться просроченным. А значит его потребуется перепроверить на сервере, для чего посылается соответствующий запрос с условиями проверки. Если сервер такие запросы поддерживает, и ресурс за последнее время не изменен, то после ответа сервера ресурс будет взят из кэша. Такой ответ по размеру данных гораздо меньше полного ответа с самим объектом, но для экономии трафика желательно минимальное количество подобных проверок.

Вычисление TTL и прогнозирование можно совсем отключить – прокси-сервер перепроверяет ресурсы всегда. Экономия трафика сведется к минимуму, зато пользователи будут иметь гарантированно свежие данные.

Данные могут быть отмечены и как личные – иметь HTTP-атрибут private. Они будут кэшироваться, но в дальнейшем доступны из кэша только тому пользователю, кто их сохранил. Cookie с сервера также сохраняются в кэше и выдаются в будущем пользователю. Но, если данные отмечены как личные и имеют cookie, то в кэш они не записываются. Подразумевается, что они могут нести важные личные сведения. Плюс к тому отметим, что кэшируются только запросы типа GET.

Таким образом видно, что для увеличения реальной экономии трафика за счет кэширования следует увеличивать параметры, связанные с вычислением TTL. Для того чтобы при этом можно было нормально просматривать быстроменяющиеся ресурсы, в Traffic Inspector предусмотрена возможность оперативного переключения режимами кэширования самим пользователем с помощью агента (подробнее об агентах см. в п. Клиентский агент Windows).

Для большего сбережения трафика можно рекомендовать следующие параметры: TTL – 70-150%, минимум 12-24 часа, максимум 15-30 дней. При таких настройках можно экономить до 25-35% трафика, но придется переключать режимы кэширования агентом при посещении быстрообновляемых ресурсов.

Для облегчения этой работы есть возможность для отдельных ресурсов задавать собственные правила кэширования. В них для соответствующих сайтов задаются индивидуальные параметры кэширования.

Данные кэша хранятся в одном большом файле, он имеет постоянный размер и сразу создается при конфигурировании прокси-сервера. Это позволяет полностью исключить фрагментацию файловой системы. Внутри кэша данные фрагментации не подвержены. Алгоритм размещения объектов в кэше очень эффективен и позволяет без ухудшения производительности работать с большим количеством объектов. Данные в кэше не имеют ограничений по времени хранения. Если лимит свободного места в кэше исчерпан, то по необходимости будут удаляться объекты, имеющие наибольший срок хранения.

Индекс кэша реализован в виде SQL-базы данных, файл proxy.db3. В случае потери или порчи файла индекса данные в кэше будут потеряны.

Подробно настройка кэширования и правила кэширования описаны в п. Кэширование и правила кэширования.

Особенности преобразования и анализа контента

Прокси-сервер может работать с различным типом контента и форматом получаемых данных. В процессе передачи данных от сервера пользователю во время работы сервера данные могут быть преобразованы.

- Chanked – специальный потоковый контент. Прокси-сервер всегда преобразует такой контент в обычный, удаляя данные форматирования chanked-формата. Иными словами, пользователь никогда данные chanked-формата не получает.
- Компрессия данных – позволяет сильно экономить трафик для некоторых типов данных.

Компрессию должен поддерживать, прежде всего, веб-сервер. Он обычно настраивается так, чтобы сжимать не все типы данных, а только те, для которых это имеет смысл (например, картинки типа gif, jpeg или архивы сжимать бессмысленно). Сервер будет выдавать сжатые данные, только если в пользовательском запросе есть HTTP-атрибут, заявляющий о поддержке клиентом соответствующих форматов компрессии данных. Компрессия обычно применяется в запросах по протоколу HTTP/1.1.

Прокси-сервер поддерживает форматы компрессии gzip и deflate, т.е. он может их при

необходимости распаковывать. Если браузер сам поддерживает компрессию, то прокси-сервер будет распаковывать сжатые данные только по необходимости. Имеется режим, позволяющий использовать компрессию в том случае, если браузер ее не поддерживает.

В кэш могут записываться как сжатые данные, так и несжатые. При выборке сжатых данных из кэша прокси-сервер также будет их распаковывать по необходимости.

Если браузер запросил сжатые данные и сервер выдал их в формате компрессии, который прокси-сервер не поддерживает, то такие данные будут прозрачно переданы пользователю.

В прокси-сервере предусмотрено два режима передачи контента от сервера пользователю – потоковый и с предварительной загрузкой. В первом режиме данные с сервера передаются пользователю порциями прозрачно, сразу по мере их приема. Во втором режиме данные передаются пользователю только после получения всего объекта с сервера. Для небольших объектов большой разницы для пользователя нет, но для больших второй режим может вызывать проблемы – пользователь не видит процесса загрузки данных с сервера. Прокси-сервер использует второй режим только при необходимости, например, когда требуется распаковка сжатых данных или для антивирусной проверки.

Для данных, размер которых более двух гигабайт, может использоваться только потоковый метод. Такие файлы никогда не кэшируются, а антивирусная проверка для них недоступна. Кроме того, они не могут быть распакованы прокси-сервером.

Антивирусная проверка HTTP- и FTP-контента позволяет выявлять данные, зараженные вирусами, а также имеющие нежелательные составляющие: программы-шпионы, скрипты и т.д. Проверка данных выполняется антивирусными сканерами, которые являются дополнительными модулями программы (подробнее см. в п. Дополнительные модули).

С точки зрения антивирусной проверки оптимальным вариантом является использование режима с предварительной загрузкой (то есть проверка осуществляется только после полной загрузки объекта). В этом случае, если в объекте антивирусом найден вредоносное ПО, а файл лечению не поддается, то будет произведена фильтрация объекта аналогично срабатыванию правила на запрещение – выдано стандартное сообщение прокси-сервера о блокировке с отчетом антивирусного сканера, а для картинок и флеш-файлов –

"пустышка".

При загрузке больших файлов использование этого режима может вызвать проблемы. Поэтому предусмотрен режим антивирусной проверки "по последнему пакету". В этом случае данные передаются пользователю прозрачно, антивирусная проверка производится только тогда, когда с сервера пришел последний пакет. Если в данных антивирус что-то найдет, последний пакет пользователю передаваться не будет, т.е. файлы будут неполные, архивы повреждены.

Лечение зараженных данных в этом режиме уже невозможно. Также существует вероятность того, что даже не полностью загруженный зараженный файл будет представлять опасность. На браузер пользователя в этом случае никакого предупреждающего сообщения не выдается. Поэтому в настройках прокси-сервера предусмотрено много настроек, позволяющих гибко задавать условия выбора этих режимов (подробнее см. в п. Основные настройки прокси-сервера).

Все данные о выявлении вирусов записываются в отдельный общий журнал, плюс отправляется сообщение на агент пользователя.

Реализация режимов перенаправления трафика на прокси-сервер

Работа через прокси-сервер позволяет реализовать более тонкий контроль за HTTP-трафиком, т.к. доступна информация прикладного уровня. Со стороны пользователя с помощью настроек браузера можно выбрать, использовать прокси-сервер или нет. И у администратора не всегда имеет возможность выставить эти настройки принудительно.

Для принудительного перенаправления HTTP-трафика на прокси-сервер в Traffic Inspector реализована специальная функция, реализованная на уровне драйвера программы. Перенаправление на прокси-сервер программы происходит в момент начала TCP-соединения. Однако в данный момент еще неизвестно, какой протокол уровня приложений (HTTP или другой) будет использоваться. Поэтому перенаправление может быть произведено только для TCP/80, причем в данном случае перенаправляется любой TCP-трафик.

Аутентификация браузера с прокси-сервером здесь невозможна, т.к. браузер "не знает", что работает через прокси. Для этого при авторизации по имени придется обязательно использовать агента (подробнее см. в п. Способы авторизации пользователей).

Следует учитывать возникновение в этом режиме некоторых других проблем, связанных с тем, что браузер при работе через прокси-сервер "не знает", как именно он работает. Поэтому стоит рассматривать режим только как меру пресечения работы пользователя мимо прокси-сервера. Оптимальным вариантом является настройка браузеров пользователей для работы с прокси-сервером.

В дополнение к этому в Traffic Inspector реализована функция блокирования любого другого HTTP-трафика, идущего мимо прокси-сервера, что позволит гарантированно пресечь работу пользователя мимо прокси-сервера. Применение этих функций задается отдельно для пользователей (авторизованный трафик) и "неавторизованного пользователя". Они настраиваются в общих настройках пользователей (подробнее см. в п. Общие настройки пользователей), свойствах групп (подробнее см. в п. Создание и настройка групп) и свойствах отдельных пользователей (подробнее см. в п. Создание и настройка пользователей).

Данные функции никогда не применяются для трафика:

- на все IP-адреса всех интерфейсов сервера;
- на IP-сети, заданные в настройках LAT (Local Address Table) прокси-сервера.

Также в Traffic Inspector реализована функция перенаправления любых TCP-соединений со стороны пользователей, с помощью которой можно гибко реализовать Transparent Proxy для любого HTTP-трафика на любой прокси-сервер (подробнее см. в п. Перенаправление запросов).

Особенности реализации протокола FTP

Обычно для FTP лучше всего использовать NAT. Но могут быть случаи, когда полезны и другие варианты работы.

Для работы с FTP-серверами в режиме только чтения такими браузерами, как Mozilla или Opera, используется метод GET. В этом случае прокси-сервер будет генерировать HTML-страницы каталогов FTP-сервера. Активный или пассивный режим при этом может выбираться автоматически. Достоинство этого метода – наличие фильтрации по контенту.

Полноценную работу с FTP обеспечивает SOCKS. Доступны все режимы активный и пассивный.

Особенности тарификации и учет трафика в прокси-сервере и SOCKS

В программе предусмотрено два метода съема трафика с целью учета при работе пользователя через прокси-сервер и SOCKS.

1. **Kernel**. Драйвер ведет списки TCP всех сессий, и для каждой учитывается трафик. Эти данные запрашиваются и используются для учета трафика в прокси-сервере и SOCKS. Данный метод имеет абсолютную точность по причине учета всех пакетов TCP-сессии.
2. **Application**. В этом случае учитывается только полезный трафик, передаваемый в службе прокси-сервера и SOCKS. Итоговые данные занижаются, т.к. не учитываются заголовки пакетов и служебные пакеты TCP-протокола. Обращаем внимание: именно так работает учет трафика всех "классических" прокси-серверов.

Режим учета в каждой сессии прокси-сервера и SOCKS отображается в консоли с целью диагностики работы программы.

Режимы выбираются автоматически. Логика выбора режима учета такова, что application-режим выбирается только тогда, когда kernel использовать возможности нет.

Для HTTP-прокси в kernel-режиме трафик снимается на интерфейсе, через который идет соединение между прокси-сервером и веб-сервером. Если этот интерфейс в программе не назначен, то используется режим application.

Для FTP через HTTP используется режим application.

Для SOCKS всегда используется kernel-режим, но трафик снимается между пользователем и SOCKS-сервером.

Во время работы через спутник пакеты TCP-сессии передаются и принимаются на разных интерфейсах. Для того, чтобы корректно работал kernel-режим, при конфигурировании надо обязательно указать интерфейс, на котором принимаются пакеты, иначе входящий трафик учитываться не будет (подробнее см. в п. Конфигуратор).

Основные настройки прокси-сервера

Основная информация о работе прокси-сервера приводится в разделе **Сервисы -> Прокси-сервер** консоли администратора. В нем отображается одноименный блок, состоящий из двух вкладок. На вкладке **Информация** основные данные о работе службы. На вкладке **Действия** размещены ссылки на некоторые операции с прокси-сервером. Аналогичный блок, только с меньшим количеством отображаемых данных, размещен также в разделе **Сервисы** консоли администратора.

Для настройки прокси-сервера выполните следующие действия.

1. Откройте окно свойств прокси-сервера. Сделать это можно из блока **Прокси-сервер** в одноименном разделе консоли администратора.

2. На вкладке **HTTP прокси** включите или выключите принудительное блокирование кэширования браузерами пользователей. Эта функция работает путем добавления ко всему HTTP-трафику атрибута no-cashe, что, согласно спецификациям стандарта, должно предотвратить кэширование информации браузером. Также включите или выключите игнорирование атрибута no-cache в запросах пользователя. Рекомендуется включить эту функцию в том случае, если пользователи используют переключение режимов кэширования с помощью агента.

   На этой же вкладке настройте параметры распаковки сжатых данных и формата передачи chunked (подробное описание см. в разделе **Особенности преобразования и анализа контента** в п. Прокси-сервер, настройки и возможности. Для этого включите или выключите возврат статуса 501, который определяет действия программы в тех случаях, когда формат передаваемого контента не поддерживается. В первом случае такой контент будет прозрачно передаваться пользователю, при этом он не будет

кэшироваться, а также проверяться антивирусом. Поэтому, если используется антивирусная проверка, отключать опцию не рекомендуется. Также включите или отключите принудительную поддержку HTTP-компрессии. При включении функции, если браузер пользователя компрессию не поддерживает, то прокси-сервер будет отдавать на него распакованные данные. Если же ее отключить, то с сервера всегда будет запрашиваться контент без компрессии, независимо от того, запрашивает браузер компрессию или нет.

> ***Замечание!*** *Декомпрессия дополнительно нагружает процессор, и отключение этой настройки может иметь смысл в случае нехватки ресурсов процессора. После отключения настройки желательно очистить кэш прокси-сервера, т.к. в нем могут оказаться сжатые данные. А это, в случае отдачи их браузеру, не поддерживающему компрессию, приведет к ошибке отображения данных.*

3. На вкладке **HTTP кэш** включите или выключите использование кэширования HTTP-трафика. При включении настройте следующие параметры.

   - Выберите способ проверки объектов кэша – безусловный или условный. В первом случае все запрашиваемые пользователями объекты, присутствующие в кэше, будут проверяться на веб-сервере на предмет их "свежести" – не обновились ли они. Это послужит гарантией того, что пользователь всегда получит правильные данные, но экономия трафика будет минимальной. Во втором случае такая проверка будет выполняться только при выполнении условий, которые определяются прогнозируемым временем жизни объекта в процентах (TTL), а также минимальное (в часах) и максимальное (в днях) время жизни объектов в кэше (подробно логика работы кэширования и перечисленные условия описаны в разделе **Особенности реализации кэширования** в п. Кэширование и правила кэширования).

   - Включите или выключите кэширование объектов с неизвестным временем создания. В большинстве случаев имеет смысл включить эту функцию, поскольку в Интернете много веб-серверов, которые не передают сведения о времени создания объектов.

   - Включите или выключите кэширование динамических объектов. Под

динамическими объектами в данном случае объекты, получаемые с веб-страниц, строка запроса которых содержит параметры после символа "?", или объекты, для которых используется специальный тип HTTP-контента chunked.

- Включите или выключите возврат ошибки, если по каким-то причинам проверить "свежесть" объекта на веб-сервере не удается (например, веб-сервер недоступен). Если эту функцию включить, то пользователю будет показано сообщение об ошибке. В противном случае будет отображен объект из кэша.
- Установите максимальный размер кэшируемых объектов (по умолчанию 8192 килобайта).
- Включите или выключите игнорирование времени жизни объекта, полученного от сервера. По умолчанию данная функция отключена, т.е. если сервер возвращает срок жизни объекта, то прогнозирование TTL не используется, а используются рекомендации сервера. Но они зависят от настроек серверов, которые часто из-за небрежности администраторов или программистов бывают совсем неправильными. При включении функции будет использоваться собственная логика с использованием прогнозирования TTL.
- Включите или выключите постоянный возврат из кэша всего объекта целиком. В первом случае прокси-сервер всегда возвратит весь объект, даже если браузер запрашивает только обновление объекта при его наличии в своем собственном кэше. Это оптимальный вариант в тех случаях, когда внутреннего трафика никакого значения не имеет (кэш браузера не всегда работает корректно). Если же трафик из кэша для пользователей не бесплатне, то логичнее эту функцию отключить.

4. На вкладке настройте параметры работы FTP-прокси через HTTP/GET. Для этого укажите таймаут команд (время ожидания отклика от сервера, по истечению которого соединение автоматически закрывается) и таймаут начала передачи данных (время ожидания начала передачи данных после открытия активного режима, для режима FTP через HTTP по истечении этого времени будет предпринята попытка использовать пассивный режим). Здесь же при необходимости включите или выключите принудительное использование пассивного режима (при выключении режим

выбирается автоматически) и установите интервал передачи команды NOOP, которая используется для удержания соединения с FTP-сервером.

5. На вкладке **Пользователи** настройте параметры автоматического конфигурирования браузеров пользователей для использования прокси-сервера. Механизм автоконфигурирования следующий. Браузер при загрузке запрашивает у прокси-сервера файл автоконфигурирования. Это обычный Java-скрипт с некоторыми стандартными функциями. Браузер на каждом запросе вызывает функцию FindProxyForURL() из этого скрипта, которая выдает ему инструкции, использовать прокси-сервер или работать напрямую и, если использовать, то какой именно. Все современные браузеры это поддерживают.

   Для того чтобы браузер запросил скрипт, его URL надо прописать в соответствующих настройках. Прокси-сервер поддерживает выдачу скрипта при запросе имен файлов wpad.dat и config.script. URL запроса скрипта может иметь вид: http://server/config.script или http://server/wpad.dat.

   Кроме настроек прокси-сервера, в скрипт также добавляется информация о том, для каких ресурсов прокси-сервер использовать не следует. Это называется LAT (Local Address Table). По умолчанию в LAT всегда заносятся следующие ресурсы:

   - localhost (127.0.0.1) и обращение по коротким именам хостов (считается, что это ресурсы локальной сети);
   - IP-адреса самого сервера и его имя.

   Дополнительно в LAT можно вносить следующие ресурсы.

   - IP сети. Для этого сформируйте список конкретных IP-адресов или диапазонов IP-адресов, для которых не будет использоваться прокси-сервер. Сделать это можно вручную или импортировать из буфера обмена или предварительно созданного текстового файла.

     Замечание! *Обработка условий в LAT, где описаны IP-адреса и сети, использует DNS для преобразования выделяемых из запросов имен хоста в IP-адрес. Поэтому требуется обязательная правильная настройка DNS у*

пользователя, иначе загрузка страниц у браузера будет сопровождаться большими задержками. Если в мастере конфигурирования программы был установлен режим "DNS не используется", то IP-адреса и сети в LAT выдаваться не будут (подробнее см. в п. Конфигуратор).

- Имена хостов. Для этого сформируйте список имен хостов, для которых не будет использоваться прокси-сервер. Имена содержат выражения вроде Regular Expressions. Синтаксис выражений определяется браузером. При их обработке анализируется строка запроса в необработанном виде, DNS-преобразование не используется.

Дополнительно на этой же вкладке настройте следующие параметры автоконфигурирования.

- Включите или выключите указание в скрипте SOCKS-сервера. При включении для браузера в качестве альтернативного варианта будет указан SOCKS-сервер. Обратите внимание, что включение данной опции может иметь некоторые нежелательные последствия. Если браузер при попытке работать через HTTP-прокси получит ошибку, то он переключится на SOCKS, и в дальнейшем будет работать через эту службу, больше не проверяя доступность HTTP-прокси.

- Включите или выключите указание в скрипте FTP-сервера. При включении для браузера при FTP-запросе будет указан прокси-сервер. Иначе с FTP он будет работать напрямую (подробнее см. в разделе **Особенности реализации протокола FTP** в п. Прокси-сервер, настройки и возможности).

- Включите или выключите принудительное конфигурирование браузеров пользователей через клиентские агенты. При включении этой функции при старте агента в браузер будет прописан скрипт автоматического конфигурирования. Кроме этой общей настройки также есть возможность задать ее отдельно для пользователей (подробнее см. в п. Создание и настройка пользователей) и групп (подробнее см. в п. Создание и настройка групп).

6. На вкладке **Антивирус** включите или выключите антивирусную проверку трафика. Антивирусная проверка возможна только в том случае, если установлен один или

несколько дополнительных антивирусных модулей (подробнее см. в п. Дополнительные модули). При включении настройте следующие параметры анализа.

- Укажите максимальный размер проверяемых объектов (по умолчанию 200 мегабайт). Объекты с размером больше этого лимита проверяться не будут. Данное ограничение следует устанавливать в соответствии с имеющимся лимитом свободной физической памяти, а также размером файла подкачки. С точки зрения быстродействия сервера, наилучший вариант – наличие в системе свободной физической памяти в двойном размере относительно максимального размера проверяемого файла, и, как минимум, доступной виртуальной памяти.

  Замечание! *Файлы более 2 гигабайт, независимо от имеющейся памяти, проверяться не могут.*

- Включите или выключите проверку объектов, извлекаемых из кэша прокси-сервера. Включение этой функции, в целом, полезно, так как в кэш может попасть вирус, не известный сканеру на момент записи данных в кэш. Однако если на сервере есть проблемы с системными ресурсами, то ее можно отключить.

- Включите или отключите проверку основного контента. Под основным контентом в данном случае понимается такой контент, который всегда будет проверяться с полной загрузкой (как правило, текстовый контент, составляющий основное содержимое страниц). При включении можно изменить состав типов данных, относящихся к основному контенту.

- Включите или отключите проверку дополнительного контента. Под дополнительным контентом в данном случае понимается такой контент, для которого может быть выбран режим проверки по последнему пакету (подробнее о режимах антивирусной проверки см. в разделе **Особенности преобразования и анализа контента** в п. Прокси-сервер, настройки и возможности). При включении можно изменить состав типов данных, относящихся к дополнительному контенту (включая типы контента, не заданные в файле определения типов контента cntgrp.ini), и указать максимальный размер объектов для предварительной проверки. В этом случае все объекты размером меньше указанного лимита будут проверяться с полной

загрузкой, а больше него – по последнему пакету.

- Определите, что будет делать прокси-сервер с неполным контентом (объекты при частичной закачке или докачке) – не проверять его или вообще блокировать. В первом случае антивирус такие данные проверять не будет, т.к. не может гарантировать обнаружение в них вирусов, а распаковка фрагмента архива невозможна в принципе. Во втором случае неполный контент будет отфильтровываться.

- Включите или выключите отправку сообщений с отчетами о найденных вирусах. Письма отправляют адреса электронной почты, описанные в настройках SMTP службы отправки (подробнее см. в п. Служба отправки).

7. На вкладке **Журнал** настройте параметры записи в журнал статистики работы прокси-сервера. В первую очередь выберите режим записи, который будет использоваться при работе пользователей по умолчанию. При необходимости для отдельных групп и пользователей можно использовать индивидуальные настройки (подробнее см. в п. Создание и настройка групп и в п. Создание и настройка пользователей).

   - **Запись отключена** – в этом режиме никакие данные с прокси-сервера в журнале не сохраняются. Для анализа посещаемости ресурсов можно использовать только записи сетевой статистики (подробнее см. в п. Управление сетевой статистикой).

   - **Нормальный режим** – режим, используемый по умолчанию. В нем пишется минимальный набор данных, который нужен для формирования отчетов о посещаемых ресурсах. Для минимизации размера базы данных можно задать минимальный размера объектов, данные о которых будут записывать в журнал (по умолчанию 10 килобайт), то есть информация об объектах меньше установленного лимита сохраняться не будет. В этом режиме сохраняются данные только для авторизованных пользователей.

   - **Детальный режим** – при выборе данного режима можно отдельно включить или отключить запись в журнал запросов неавторизованных пользователей (по сути, анонимный трафик, который не привязан к конкретному пользователю программы),

заблокированные запросы (может быть полезно для отладки правил, так как в журнал попадут и отфильтрованные запросы) и подробную информацию обо всех запросах (будет записываться дополнительная информация, полезная для отладки фильтрации, тарификации, кэширования и т.д.).

8. На вкладке **Дополнительно** настройте следующие параметры работы прокси-сервера.

- Если при приеме трафика через прокси-сервер с DVB-карты не учитывается входящий трафик, то включите принудительный режим учета трафика на прием Application.
- Задайте таймаут соединения с прокси-сервером.
- Включите или выключите авторизацию в фоновом режиме. Эта функция понижает приоритет процессов прокси-сервера до момента авторизации. Можно включить для исключения ситуации перегрузки процессора при обработке большого количества запросов на прокси-сервер (флуде).
- Укажите размер объектов, при превышении которого будет использоваться буферизация в файле (по умолчанию 1024 килобайта). В этом случае данные будут храниться и обрабатываться не в оперативной памяти, а в виде временного файла. Уменьшение лимита приведет к более экономному использованию оперативной памяти, а увеличение – к росту быстродействия. Однако задавать в качестве лимита очень большие значения не рекомендуется, т.к. даже при достаточном объеме оперативной и виртуальной памяти системы имеется лимит виртуальной памяти для процесса – 2 гигабайта. И при интенсивной работе прокси-сервера может появиться вероятность появления ошибок по причине нехватки памяти.
- Включите или выключите асинхронный режим для базы данных индекса кэша прокси-сервера. В обычном режиме при операциях обновления данных кэша программа ждет, пока данные не будут физически записаны на диск. Это гарантирует их целостность при различных сбоях работы операционной системы (например, при отключении питания и т.д.), но несколько замедляет работу. При очень большой нагрузке на кэш прокси-сервера (десятки запросов в секунду и более) для увеличения

производительности можно включить асинхронный режим. В этом случае при сбоях в работе операционной системы возможна ситуация повреждения данных кэша, что может привести к полной или частичной потери данных в нем.

9. Сохраните внесенные изменения.

Кэширование и правила кэширования

Логика и принципы работы кэширования прокси-сервера подробно описаны в разделе **Особенности реализации кэширования** в п. Прокси-сервер, настройки и возможности.

Настройка основных параметров кэширования осуществляется на вкладке **HTTP кэш** окна свойств прокси-сервера (подробнее см. в п. Основные настройки прокси-сервера).

В рамках управления кэшем прокси-сервера в Traffic Inspector реализованы следующие возможности:

- управление кэшем;
- операции по управлению правилами кэширования.

Управление кэшем

В рамках управления кэшем в Traffic Inspector реализованы следующие операции, которые выполняются с помощью специального мастера:

- перенос файла кэша в другое место;
- изменение размера кэша;
- проверка целостности данных в кэше;
- быстрая очистка кэша.

Для переноса файла кэша выполните следующие действия.

1. Запустите мастер настройки кэша. Сделать это можно из блока **Прокси-сервер** в разделах **Сервисы** или **Сервисы -> Прокси-сервер** консоли администратора.
2. На вкладке **Выберите действие** выберите желаемое действие – **Перенос файла кэша**.

3. На вкладке **Опции переноса** выберите способ переноса:

- **С проверкой** – при выборе этого способа создается новый файл кэша, куда пообъектно переносятся данные, начиная с самых последних (поздних). Если размер нового файла кэша меньше размера данных в старом, то будут отброшены самые старые данные. Если данные были повреждены (например, антивирусом), они также будут отброшены. Полный отчет об операции заносится в журнал системных событий. Старый файл кэша удаляется только в самом конце операции. Поэтому если операция была прервана (например, выгрузкой сервиса), данные не потеряются. Следует учесть, что для этой операции на диске требуется дополнительное свободное место – для старого и нового файла кэша одновременно. Выполнение операции может занять длительное время.

- **С очисткой данных** – при выборе данного способа создается новый пустой файл кэша, а старый удаляется. Также выполняется очистка индексной таблицы. Операция осуществляется быстро, но при этом вся информация из кэша теряется.

4. В ходе переноса файла кэша можно изменить его размер. Для этого на вкладке **Размер файла кэша** укажите новое значение.

5. На вкладке **Размещение файла** введите местоположение нового файла кэша.

6. Запустите операцию и дождитесь ее завершения.

Операция изменения размера файла кэша, по сути, аналогична операции переноса. При ее выполнении также создается новый файл, только в том же самом месте. Поэтому выполняется операция, как и описано выше, только вкладка **Размещение файла** отсутствует.

Операция проверки целостности данных в кэше выполняется аналогично предыдущим двум, однако при ее выполнении не изменяется ни размер файла кэша, ни его местоположение. Однако в ходе проверки из кэша удаляются все поврежденные данные.

При выполнении быстрой очистки кэша выполняется очистка только индексной таблицы, а сам файл кэша остается нетронутым. Это быстрая операция, которая выполняется практически моментально.

При всех операциях обслуживания кэша база данных индекса кэша создается заново – это наилучший способ решения различных проблем с ней (повреждения файла и т.д.). Если данные в индексе повреждены не до конца, то они по возможности будут сохранены.

До и после операций настоятельно рекомендуется произвести дефрагментацию файловой системы.

Операции по управлению правилами кэширования

Правила кэширования позволяют более тонко настроить работу прокси-сервера в плане максимальной экономии трафика, а также более корректного отображения ресурсов. С их помощью можно задавать свои собственные правила кэширования для разных ресурсов. Список правил кэширования размещен в разделе **Сервисы -> Прокси-сервер -> Правила кэширования** консоли администратора.

В рамках управления правилами кэширования в Traffic Inspector реализованы следующие операции:

- создание/изменение правила кэширования;
- удаление правила кэширования.

Для создания нового или изменения существующего правила кэширования выполните следующие действия.

1. Откройте окно свойств нового или существующего правила кэширования. Сделать это можно с помощью контекстного меню в разделе **Сервисы -> Прокси-сервер -> Правила кэширования** консоли администратора.
2. На вкладке **Правило** введите уникальное наименование правила кэширования и, при необходимости, произвольные примечания. Здесь же можно временно отключить правило, не удаляя его из системы.
3. На вкладке **Применение** задайте условия для отбора пользователей, на которых будет распространяться данное правило кэширования. По умолчанию оно работает для всех пользователей. При необходимости можно указать, на какие группы пользователей

распространяется правило, а также при каком состоянии счета пользователя оно будет работать (например, только для пользователей из определенной группы, работающих в кредит).

4. На вкладке **Проверка IP** укажите IP-адреса получателей, для которых будет работать данное правило кэширования. Для этого введите конкретный IP-адрес или диапазон IP-адресов или укажите предварительно созданную IP-сеть (подробнее про IP-сети см. в п. IP-сети). Здесь же можно указать сетевой порт, при соединении по которому будет срабатывать правило кэширования (по умолчанию 80).

5. На вкладке **Проверка URL** задайте параметры отбора сайтов, для которых будет действовать данное правило кэширование на основе их URL-адресов. Здесь может быть три варианта.

   - **Не проверять** – условия к URL-адресам не предъявляются. Это значит, что правило будет действовать для всех сайтов при соблюдении условий по IP-адресам получателей, типу контента и расписанию.
   - **URL запрос или строка в формате регулярных выражений** – конкретный URL-адрес или регулярное выражение, которое задает ряд определенных URL-адресов. При выборе этого варианта правило кэширование будет действовать только для сайтов, адрес которой соответствуют заданной строке.
   - **Список** – предварительно созданный в системе URL-список (подробнее про URL-списки см. в п. URL-списки). При выборе этого варианта можно прямо с данной вкладки перейти непосредственно к редактированию выбранного или созданию нового URL-списка.

   При выборе второго и третьего вариантов можно проверить соответствие произвольного запроса заданным условиям.

6. На вкладке **Анализ контента** определите типы контента, которые будут кэшироваться согласно данному правилу кэширования. По умолчанию правило работает для всех типов. При необходимости можно указать конкретные типы из числа возможных.

7. На вкладке **Расписание** настройте расписание действия правила кэширования. Работа

на вкладке аналогична работе на вкладке **Расписание** в окне свойств пользователя (подробнее о работе на вкладке см. в п. Общие настройки пользователей).

8. На вкладке **Действия** настройте правила кэширования для ресурсов, удовлетворяющих заданным ранее условиям. Для этого включите принудительную проверку "свежести" всех объектов или задайте условия выполнения такой проверки, включите или выключит кэширование динамических объектов и игнорирование HTTP-атрибутов кэширования, полученных с веб-сервера (эти настройки аналогичны общим настройкам кэширования, подробнее см. описание вкладки **HTTP кэш** окна свойств кэша прокси-сервера в п. Основные настройки прокси-сервера).

9. Сохраните внесенные изменения.

Удаление правил кэширования осуществляется с помощью контекстного меню в разделе **Сервисы -> Прокси-сервер -> Правила кэширования** консоли администратора.

Прокси-каскад

Перенаправление запросов с прокси-сервера Traffic Inspector на другие прокси-сервера реализуется с помощью правил построения каскадов. В этих правилах описываются условия, при которых они применяются, а также настройки для вышестоящих HTTP-прокси и SOCKS-сервера.

При обработке запроса привила проверяются последовательно от начала списка вниз. Применено будет первое правило, где все условия совпадут. Поэтому порядок правил в списке имеет значение, его можно менять. Если правило описано только для одного типа трафика (HTTP или SOCKS), то для другого типа трафика оно срабатывать не будет – последует проверка следующего в списке.

Список правил построения каскадов размещен в разделе **Сервисы -> Прокси-каскад** консоли администратора.

В рамках управления правилами построения каскадов в Traffic Inspector реализованы следующие операции:

- создание/изменение правила построения каскадов;

- удаление правила построения каскадов.

Создание/изменение правила построения каскадов

Для создания нового или изменения существующего правила построения каскадов выполните следующие действия.

1. Откройте окно свойств нового или существующего правила построения каскадов. Сделать это можно с помощью контекстного меню в разделе **Сервисы -> Прокси-каскад** консоли администратора.
2. На вкладке **Правило** введите уникальное наименование правила построения каскадов и, при необходимости, произвольные примечания. Здесь же можно временно выключить правило, не удаляя его из системы.
3. На вкладке **Применение** укажите пользователей, для которых будет действовать данное правило построения каскадов. По умолчанию оно работает для всех пользователей. При необходимости можно указать, на какие группы пользователей распространяется правило, а также при каком состоянии счета пользователя оно будет работать (например, только для пользователей из определенной группы, работающих в кредит).
4. На вкладке **Проверка IP** укажите IP-адреса получателей, для которых будет работать данное правило построения каскадов. Для этого введите конкретный IP-адрес или диапазон IP-адресов или укажите предварительно созданную IP-сеть (подробнее про IP-сети см. в п. IP-сети). Здесь же можно указать сетевой порт, при соединении по которому будет срабатывать правило кэширования (по умолчанию 80).
5. На вкладке **Проверка URL** задайте параметры отбора сайтов, для которых будет действовать данное правило построения каскадов на основе их URL-адресов. Здесь может быть три варианта.
   - **Не проверять** – условия к URL-адресам не предъявляются. Это значит, что правило будет действовать для всех сайтов при соблюдении условий по IP-адресам получателей, типу контента и расписанию.

- **URL запрос или строка в формате регулярных выражений** – конкретный URL-адрес или регулярное выражение, которое задает ряд определенных URL-адресов. При выборе этого варианта правило кэширование будет действовать только для сайтов, адрес которой соответствуют заданной строке.

- **Список** – предварительно созданный в системе URL-список (подробнее про URL-списки см. в п. URL-списки). При выборе этого варианта можно прямо с данной вкладки перейти непосредственно к редактированию выбранного или созданию нового URL-списка.

При выборе второго и третьего вариантов можно проверить соответствие произвольного запроса заданным условиям.

6. На вкладке **Анализ контента** определите типы контента, для которых будет работать данное правило построения каскадов. По умолчанию правило работает для всех типов. При необходимости можно указать конкретные типы из числа возможных.

7. На вкладке **Расписание** настройте расписание действия правила построения каскадов. Работа на вкладке аналогична работе на вкладке **Расписание** в окне свойств пользователя (подробнее о работе на вкладке см. в п. Общие настройки пользователей).

8. На вкладке **HTTP прокси** задайте действие, выполняемое для HTTP-трафика:

   - **Правило не применять** – правило для HTTP-не применяется трафика (оно может использоваться для SOCKS-трафика), осуществляется проверка следующих правил каскадирования в списке.

   - **Перенаправлять все запросы на вышестоящий прокси сервер** – HTTP-трафик перенаправляется на указанный прокси-сервер. При выборе этого варианта введите IP-адрес или имя хоста этого прокси-сервера и номер сетевого порта, на котором он работает. Если вышестоящий прокси-сервер требует авторизации, то укажите необходимые логин и пароль (для NTLM-авторизации логин задается в формате "*domaim\username*").

   - **Использовать прямое соединение** – для HTTP-трафика, соответствующего заданным условиям, каскадирование применяться не будет (трафик по следующим в

списке правилам построения каскадов не проверяется).

9. На вкладке **SOCKS прокси** задайте действие, выполняемое для SOCKS-трафика. Она аналогична описанной выше вкладке **HTTP прокси**. Единственными отличиями являются параметры вышестоящего SOCKS-сервера. При их настройке необходимо выбрать тип SOCKS-прокси.

10. Сохраните внесенные изменения.

Удаление правила построения каскадов

Удаление правил построения каскадов осуществляется с помощью контекстного меню в разделе **Сервисы -> Прокси-каскад** консоли администратора.

Монитор работы: возможности и управление

Монитор работы располагается в разделе **Учет трафика -> Монитор работы** консоли администратора. Он используется для решения большого количества задач, связанных как с мониторингом работы пользователей, так и с управлением ими. В частности, в мониторе доступны следующие операции:

- мониторинг работы пользователей и коллективных счетов;
- управление состоянием пользователей и коллективных счетов;
- выполнение различных действий с пользователями и коллективными счетами;
- управление уровнями фильтрации и кэширования пользователей через их агенты.

Монитор работы состоит из двух частей. В левой отображается список пользователей и коллективных счетов с информацией по каждому из них: группа, текущее состояние, способ авторизации, тариф, потребленный трафик, данные по абонентской плате и т.д. Количество и положение колонок можно настраивать в обычном порядке (подробнее см. в п. Консоль администратора). Правая часть представляет собой панель операций, с помощью которой можно выполнять те или иные действия по управлению пользователями и коллективными счетами. Также часть операций продублирована в контекстном меню монитора.

Мониторинг работы пользователей 17

Мониторинг работы пользователей

Для просмотра актуальной информации о работе пользователей используется левая часть монитора работы. Данные в ней отображаются в режиме реального времени, что обеспечивает администратора Traffic Inspector всей необходимой информацией о работе пользователей.

В левой части монитора работы есть специальная панель, в которой отображается более подробная информация о выбранном пользователе или коллективном счете. Она состоит из следующих вкладок.

- **Состояние** – на вкладке отображается основная информация о состоянии пользователя или коллективного счета - текущая скорость, количество открытых TCP-соединений, баланс, текущее состояние, тип доступа и пр.
- **Тарификация** – на вкладке отображается список используемых для данного пользователя или коллективного счета тарифов с объемом потребленного трафика и начисленными суммами по каждому из них.
- **Авторизация** – вкладка используется для вывода подробной информации об авторизации пользователя (для коллективных счетов не отображается). На ней показываются тип авторизации, логин пользователя, IP- и MAC-адреса места последней авторизации и пр.
- **Сетевая статистика** – на вкладке отображается сетевая статистика для данного пользователя или коллективного счета.
- **Прокси-сервер** – на вкладке отображается список запросов на прокси-сервер для данного пользователя или коллективного счета.
- **Поисковые запросы** – на вкладке отображается список поисковых запросов для данного пользователя или коллективного счета.

По умолчанию в мониторе работы отображаются все пользователи и коллективные счета, работа которым разрешена. Однако при необходимости можно использовать для вывода

списка и другие фильтры. Для этого в правой панели откройте раздел **Фильтрация** и выберите тип пользователей и коллективных счетов, список которых нужно просмотреть (например, всех активных в данный момент по трафику, всех авторизованных на сервере, всех с отрицательным балансом и пр.).

Также можно включать и отключать отображение в списке коллективных счетов, пользователей вне групп и пользователей из каждой группы по отдельности. Отметим, что фильтрации по типу и группам дополняют друг от друга. Можно, к примеру, оставить в списке только авторизованных пользователей из одной или нескольких определенных групп.

Управление состоянием пользователей и коллективных счетов

Управление состоянием пользователей и коллективных счетов осуществляется в разделе **Состояние** правой панели монитора работы или с помощью контекстного меню. В рамках этих операций выполняется перевод состояния одного или нескольких пользователей или коллективных счетов в следующие состояния.

- **Работа разрешена** – пользователь или коллективный счет активен, работа в Интернете разрешена.
- **Пауза** – работа пользователя или коллективного счета временно приостановлена с возможностью возобновления в рамках той же сессии биллинга.
- **Стоп** – работа пользователя или коллективного счета заблокирована. При этом все данные об операциях по счету будут удалены. При его включении в будущем начнется новая сессия биллинга.

Пользователи и коллективные счета со статусом **Работа разрешена** отображаются в списке с помощью фильтра **Разрешена работа** (см. выше), со всеми остальными статусами – с помощью фильтра **Заблокированы**.

При изменении статуса введите комментарий, поясняющий причину выполнения данной операции. При необходимости включите его показ пользователям. В этом случае данный комментарий будет виден пользователям в отчетах.

Если пользователь переводится из состояния **СТОП**, то у него будет начинаться новая сессия биллинга. При этом выводится окно ввода оплаты. При необходимости введите в нем сумму, зачисляющуюся на счет, а также сумму начального состояния счета (по умолчанию эта сумма загружается из настроек тарифа пользователя, подробнее см. в п. Тарифы).

Выполнение различных действий с пользователями и коллективными счетами

В мониторе работы реализованы следующие операции с пользователями и коллективными счетами:

- добавление оплаты;
- рестарт сессии биллинга;
- отправка сообщения.

Для добавления оплаты на счет пользователя или коллективный счет выполните следующие действия.

1. Выделите одного или нескольких пользователей или коллективных счетов (выбирать можно либо одних пользователей, либо одни коллективные счета) и с помощью правой панели или контекстного меню запустите операцию добавления оплаты.
2. В открывшемся окне на вкладке **Добавление оплаты** введите сумму оплаты. Если был выбран один пользователь или коллективный счет, то при необходимости здесь же измените сумму всех предыдущих оплат, на основании которой вычисляется текущий баланс.
3. При необходимости на вкладке **Комментарий администратора** введите произвольный комментарий, поясняющий причину выполнения данной операции. Здесь же можно включить его показ пользователям. В этом случае введенный текст будет виден пользователям в отчетах
4. Сохраните оплату.

Для рестарта сессии биллинга выполните следующие действия.

1. Выделите одного или нескольких пользователей или коллективных счетов (выбирать можно либо одних пользователей, либо одни коллективные счета) и с помощью правой панели или контекстного меню запустите операцию рестарта сессии биллинга.

2. В открывшемся окне на вкладке **Выберите действие** выберите один из двух способов рестарта сессии биллинга.

   - **Рестарт сессии биллинга** – открывает новый отчетный период с обнулением существующего баланса лицевого счета.
   - **Рестарт сессии биллинга с переносом остатков** – открывает новый отчетный период, в который переносится актуальный на данный момент остаток с лицевого счета.

   Здесь же включите или выключите добавление к лицевому счету в новой сессии биллинга оплаты по умолчанию, которая задается в настройках тарифа (подробнее см. в п. Тарифы).

3. При необходимости на вкладке **Комментарий администратора** введите произвольный комментарий, поясняющий причину выполнения данной операции. Здесь же можно включить его показ пользователям. В этом случае введенный текст будет виден пользователям в отчетах.

4. Запустите процесс рестарта.

Отправка сообщений возможна одному, нескольким или всем пользователям сразу. Отправленное сообщение запоминается службой программы. Доставляется оно через агента пользователя, а также отображается на главной страничке веб-сервера статистики пользователя. Если пользователь авторизован на сервер в момент отправки сообщения, то он получит его сразу, а если нет, то получит после авторизации. Сообщение удаляется автоматически после доставки или при истечении его срока хранения. То есть, если пользователь так и не авторизовался на сервере, а у сообщения закончился срок хранения, то он его не получит. Также отправленное, но не полученное пользователем сообщение можно отменить вручную (с помощью контекстного меню). Очередь сообщений в программе не реализована, запоминается для отправки только одно сообщение. Если оно

не было доставлено, а администратор создал новое, то старое сообщение будет удалено автоматически.

Для отправки сообщения выполните следующие действия.

5. Выделите одного или нескольких пользователей или коллективных счетов (выбирать можно либо одних пользователей, либо одни коллективные счета) и с помощью правой панели или контекстного меню запустите операцию отправки сообщения.
6. На вкладке **Параметры отправки** укажите, кому должно быть отправлено сообщение – только выбранным или вообще всем пользователям программы. Здесь же выберите срок хранения сообщения на сервере: указанное количество часов, до перезагрузки сервера или без ограничений по времени.
7. На вкладке **Сообщение** введите текст сообщения.
8. Отправьте сообщение.

Управление уровнями фильтрации и кэширования пользователей через их агенты

В мониторе работы можно управлять уровнями фильтрации и кэширования, которые установлены в агентах пользователей. Для этого выберите одного или нескольких пользователей, и в разделе **Настройки агента** установите нужные значения (описание значений см. в п. Клиентский агент Windows). Установленные параметры будут автоматически транслированы в агенты выбранных пользователей.

Активные пользователи прокси

В Traffic Inspector предусмотрена возможность мониторинга активных пользователей прокси-сервера. Осуществляется он в разделе **Сервисы -> Прокси-сервер -> Активные пользователи консоли администратора**. В нем отображаются все активные сессии прокси-сервера, SOCKS и встроенного веб-сервера с полной информацией по каждой из них.

Для удобства администратора с помощью контекстного меню можно быстро перейти на URL-адрес произвольной сессии, скопировать его или имя хоста в буфер обмена.

Обслуживание и автоматизация 18

Резервное копирование

В Traffic Inspector реализовано резервное копирование всей значимой информации. Задача копирует все файлы конфигурации, файлы баз данных, а также некоторые другие данные, например, от дополнительных модулей. Главная цель копирования – быстрое восстановление работы программы при сбое, а также откат к старым настройкам. Процедура восстановления данных средствами Traffic Inspector не предусмотрена. Восстановление осуществляется путем копированием файлов из резервной копии в папку установки Traffic Inspector при остановленной службе программы.

Информация о состоянии задачи резервного копирования и статусе последнего резервирования информации размещена в блоке **Обслуживание БД** в разделе **Настройки** и в блоке **Задачи обслуживания БД** в разделе **Настройки -> Обслуживание БД** консоли администратора. Более подробные данные

По умолчанию резервное копирование выключено. Для его включения и настройки выполните следующие действия.

1. Запустите окно настройки резервного копирования. Сделать это можно из блока **Обслуживание БД** в разделе **Настройки** или в разделе **Настройки -> Обслуживание БД** консоли администратора.
2. На вкладке **Резервное копирование** включите операцию резервного копирования. Если она должна выполняться автоматически, то включите запуск резервирования по расписанию и настройте расписание.
3. На вкладке **Настройки копирования** укажите папку, в которую будет копироваться информация (если такой папки на диске нет, она будет создана автоматически). Здесь же настройте параметры копирования журналов Traffic Inspector (все журналы хранятся в одном файле db3.log, как правило, этот файл имеет значительный объем).
   - **Копировать все** – в резервную копию включается файл db3.log целиком. Эта операция выполняется относительно быстро, поскольку, по сути, является простым копированием файла.
   - **Копировать выборочно** – в резервную копию включаются только те записи из

журналов, которые соответствуют заданным на вкладе **Выборочное копирование** настройкам (см. ниже). Эта операция связана с анализом файла с журналами и выборочным извлечением из него данных, а поэтому при большом объеме базы может занимать продолжительное время. Однако выборочное копирование позволяет во многих случаях значительно уменьшить объем резервной копии.

- **Не копировать** – не включать в резервные копии информацию из журналов. В этом случае после восстановления данных построение отчетов за период времени будет невозможным (данные биллинга будут сохранены).

На этой же вкладке включите или выключите копирование индекса кэша прокси-сервера (по умолчанию отключено). Резервное копирование самого кэша прокси-сервера из-за его очень большого размера не предусмотрено. Однако файл индекса может быть скопирован, а впоследствии восстановлен. При включении данной функции необходимо учитывать, что данные в кэше прокси-сервера с могут быть изменены и не соответствовать индексу. Тем не менее, в некоторых случаях эта опция может быть полезна. Механизм чтения данных из кэша защищен от чтения неверных данных, поэтому на его корректности работы это никак не скажется.

4. На вкладке **Настройки копирования** выберите режим резервного копирования:

   - **Переписывать данные** – новые данные в архиве пишутся поверх старых. Для XML-файлов конфигурации создаются bak-файлы, а остальные файлы просто переписываются поверх старых. В этом режиме в случае сбоя операции может получиться так, что архив будет неполным.

   - **Для каждого архива создавать новую папку** – в этом случае каждый раз создается отдельный архив в отдельной папке. В этом режиме надо позаботится о том, чтобы не произошло переполнение диска, автоочистка диска для этой операции пока не предусмотрена.

5. Если на вкладке **Настройки копирования** было выбрано выборочное копирование журналов, то на вкладке **Выборочное копирование** настройте параметры отбора записей журналов для резервирования. Для этого укажите, за сколько последних дней

будут копироваться записи. При необходимости этот параметр можно настроить отдельно для каждого большого по объему журнала (журнал прокси-сервера, журнал сетевой статистики, журналы блокировки и трассировки SMTP-сервера).

6. Сохраните внесенные изменения.

Также настроить резервное копирование можно в процессе настройки операция обслуживания базы данных (подробнее см. в п. Обслуживание БД).

После включения и настройки операция резервного копирования будет выполняться автоматически в соответствии с заданным расписанием. Также ее можно запустить вручную из блока **Задачи обслуживания БД** в разделе **Настройки -> Обслуживание БД** консоли администратора.

Обслуживание БД

В рамках обслуживания БД в Traffic Inspector реализованы следующие операции:

- отслеживание наличия свободного места на дисках сервера;
- резервное копирование базы данных;
- очистка встроенной базы данных.

Все операции настраиваются с помощью единого окна настройки операций обслуживания. Кроме того, настройка резервного копирования и очистки встроенной базы данных могут быть выполнены в отдельных окнах. Также очистка встроенной базы может быть настроена в рамках настройки синхронизации встроенной базы данных с внешней (подробнее см. в п. Синхронизация с внешней БД).

Для настройки операций обслуживания выполните следующие действия.

1. Откройте окно настройки операций обслуживания. Сделать это можно из блока **Обслуживание БД** в разделе **Настройки** или в разделе **Настройки -> Обслуживание БД** консоли администратора.
2. На вкладке **Задачи обслуживания** выберите задачи, которые будут настраиваться в рамках данного мастера.

3. Если на вкладке **Задачи обслуживания** была выбрана задача **Файлы и диски**, то на одноименной вкладке настройте следующие параметры этой операции.

   - Укажите, при каком объеме свободного пространства на дисках сервера Traffic Inspector прекращает запись данных. Программа в этом случае остается работоспособной, но ситуация требует немедленного разрешения, так как возможна потеря данных. В журнале программы фиксируется критическая ошибка, а также создается замечание (подробнее см. в п. Журналы событий).

   - При необходимости включите оповещение администратора, при каком объеме свободного пространства будет отправляться предупреждение по электронной почте (оповещение отправляется на адрес, указанные в параметрах службы отправки, подробнее см. в п. Служба отправки).

   - При необходимости включите автоматическое удаление файлов с данными старше указанного возраста.

   - Укажите размер базы данных журналов, при превышении которого будет отправляться предупреждение по электронной почте (оповещение отправляется на адрес, указанные в параметрах службы отправки, подробнее см. в п. Служба отправки).

4. Если на вкладке **Задачи обслуживания** была выбрана задача **Резервное копирование**, то на одноименной вкладке настройте параметры выполнения этой операции (настройка полностью аналогична настройке резервного копирования в отдельном окне, подробнее см. в п. Резервное копирование).

5. Если на вкладке **Задачи обслуживания** была выбрана задача **Очистка данных**, то на одноименной вкладке разрешите очистку встроенной базы данных и, при необходимости, настройте расписание автоматического запуска этой операции. Затем на вкладке **Настройки** укажите максимальный возраст данных, после которого они будут удаляться в ходе очистки. При необходимости этот параметр можно настроить отдельно для каждого большого по объему журнала (журнал прокси-сервера, журнал сетевой статистики, журналы блокировки и трассировки SMTP-сервера).

На этой же вкладке включите или выключите сжатие очищенного файла базы данных.

6. Сохраните внесенные изменения.

Задачи: виды и назначение

Задачи представляют собой средства для автоматизации выполнения различных операций. Они могут выполняться автоматически по заданному расписанию или запускаться вручную (если это разрешено в настройках программы). Перечень задач размещен в разделе **Настройки -> Задачи** консоли администратора.

В настоящее время в Traffic Inspector реализованы следующие типы задач.

- **Пользователи – оплата и сброс сессии биллинга** – задачи этого типа могут использоваться для выполнения периодически повторяющихся операций со счетами пользователей, как индивидуальными, так и коллективными: рестарта сессии биллинга с обнулением или переносом текущего остатка, добавление оплаты.
- **Внешние счетчики – сброс** – данные задачи предназначены для обнуления собранной статистики на одном или нескольких внешних счетчиках (подробнее про внешние счетчики см. в п. Счётчики трафика).
- **Запуск внешней программы** – задачи этого типа используются для запуска произвольных внешних программ и сценариев.
- **Запуск скрипта** – эти задачи применяются для запуска предварительно созданных в Traffic Inspector скриптов автоматизации (подробнее про скрипты см. в документации SDK).

В рамках управления задачами в Traffic Inspector реализованы следующие операции.

- создание/изменение задач типа **Пользователи – оплата и сброс сессии биллинга**;
- создание/изменение задач типа **Внешние счетчики – сброс**;
- создание/изменение задач типа **Запуск внешней программы**;
- создание/изменение задач типа **Запуск скрипта**;

- удаление задач.

Создание/изменение задач типа Пользователи – оплата и сброс сессии биллинга

Для создания новой или изменения существующей задачи типа **Пользователи – оплата и сброс сессии биллинга** выполните следующие действия.

1. Откройте окно свойств новой или существующей задачи. Сделать это можно с помощью контекстного меню в разделе **Настройки -> Задачи** консоли администратора.
2. На вкладке **Задача** введите уникальное имя задачи и, при необходимости, произвольные примечания. Здесь же можно разрешить или запретить выполнение задачи, не удаляя ее из системы.
3. На вкладке **Задача** выберите тип задачи из списка возможных (список реализованных в Traffic Inspector типов задач приведен выше). При этом в окне свойств задачи будет сформирован список вкладок для настройки именно выбранного типа.

   Замечание! *Отредактировать тип существующей задачи нельзя, он выбирается при создании и сменить его в последующем невозможно.*

4. На вкладке **Настройка запуска** разрешите или запретите ручной запуск данной задачи и, при необходимости, настройте расписание ее автоматического запуска.
5. На вкладке **Выбор счетов** определите, для каких счетов будет выполняться данная задача. Сделать это можно, выбрав отдельных пользователей программы, целые их группы и коллективные счета.
6. На вкладке **Сброс сессии биллинга** настройте действия, выполняемые данной задачей. Для этого включите или выключите операцию рестарта сессии биллинга. При ее включении укажите, будет или нет при рестарте переноситься существующий остаток в новую сессию, а также будет или нет добавляться на счета пользователей оплата по умолчанию (она берется из настроек тарифа, подробнее см. в п. Тарифы). При необходимости укажите сумму, которая будет добавлена к счетам пользователей или списана с них (независимо от рестарта сессии биллинга).

На этой же вкладке включите или выключите применение задачи для пользователей в состоянии **Запрещен** и для пользователей и коллективных счетов в состоянии **Стоп**.

7. При необходимости на вкладке **Комментарий администратора** введите произвольный комментарий, поясняющий причину выполнения данной операции. Здесь же можно включить его показ пользователям. В этом случае введенный текст будет виден пользователям в отчетах.
8. Сохраните внесенные изменения.

Создание/изменение задач типа Внешние счетчики – сброс

Для создания новой или изменения существующей задачи типа **Внешние счетчики – сброс** выполните следующие действия.

1. Выполните шаги 1-4 операции создания/изменения задачи типа **Пользователи – оплата и сброс сессии биллинга** (см. выше), выбрав на вкладке **Задача** тип **Внешние счетчики – сброс**.
2. На вкладке **Сброс внешних счетчиков** укажите счетчики трафика, данные которых будут обнулены. Выбирать можно сразу все контролируемые или информационные счетчики или указывать только конкретные счетчики трафика.
3. Сохраните внесенные изменения.

Создание/изменение задач типа Запуск внешней программы

Для создания новой или изменения существующей задачи типа **Запуск внешней программы** выполните следующие действия.

1. Выполните шаги 1-4 операции создания/изменения задачи типа **Пользователи – оплата и сброс сессии биллинга** (см. выше), выбрав на вкладке **Задача** тип **Запуск внешней программы**.
2. На вкладке **Запуск задачи** укажите внешнюю программу или сценарий, которые будут запущены. При необходимости введите строку параметров запуска и рабочую папку

программы (по умолчанию используется подпапка *script* в папке установки Traffic Inspector).

Здесь же включите или отключите запись вывода консольного приложения в файл. При включении этой функции весь вывод консольной программы будет сохраняться в отдельном файле в подпапке *script\output* папки установки Traffic Inspector. Именем файла будет являться имя задачи. Если функция отключена, то вывод будет доступен для просмотра до первой перезагрузки службы программы.

На этой же вкладке укажите таймаут выполнения (по умолчанию 120 секунд) или значение "0" (без ограничений). Задачу всегда можно прервать с консоли вручную, кроме того выполнение всех задач прерывается при остановке службы программы.

3. Сохраните внесенные изменения.

Создание/изменение задач типа Запуск скрипта

Для создания новой или изменения существующей задачи типа **Запуск скрипта** выполните следующие действия.

1. Выполните шаги 1-4 операции создания/изменения задачи типа **Пользователи – оплата и сброс сессии биллинга** (см. выше), выбрав на вкладке **Задача** тип **Запуск скрипта**.
2. На вкладке **Запуск скрипта** выберите предварительно созданный скрипт автоматизации. Здесь же включите или выключите запись вывода скрипта в файл и укажите таймаут выполнения (параметры работают аналогично записи вывода внешнего приложения, см. выше). При необходимости здесь же задайте скрипт запуска скрипта автоматизации (если его не указать, то будет запущена процедура Main() скрипта автоматизации, подробнее см. в документации по SDK).
3. Сохраните внесенные изменения.

Удаление задач

Удаление задач осуществляется с помощью контекстного меню в разделе **Настройки -> Задачи** консоли администратора.

Общая настройка программы осуществляется в специальном окне, запустить которое можно из блока **Настройки Traffic Inspector** в разделе **Настройки** консоли администратора.

Окно общих настроек состоит из целого ряда вкладок:

- **Сетевой драйвер**;
- **Параметры очередей**;
- **Сетевая статистика**;
- **Распознавание имен**;
- **Журналы**;
- **Оповещение**;
- **Автоматизация**;
- **Счетчики скорости**;
- **Дополнительно**.

Вкладка Сетевой драйвер

На вкладке **Сетевой драйвер** настраиваются основные параметры работы сетевого драйвера Traffic Inspector. На ней можно включить или выключить учет трафика заголовков сетевых пакетов (14 байт в каждом сетевом пакете). В первом случае эти 14 байт каждого сетевого пакета будут учитываться в потребляемом пользователями трафике. Это может привести к завышению внешнего трафика, если вышестоящий провайдер ведет учет только чистого трафика. Поэтому в большинстве случаев имеет смысл этот параметр привести в соответствии с принятой системой учета вышестоящего провайдера.

Также здесь можно включить или выключить блокировку фрагментов IP-пакетов. Она

позволяет отфильтровывать неполные сетевые пакеты.

На этой же вкладке можно включить или выключить блокировку внешних сетей при остановке службы программы. Если эту функцию включить, то при возникновении каких-либо сбоев, приводящих к остановке службы программы, работа пользователей в Интернет будет остановлена, что не позволит им получить неучтенный трафик. Кроме того, доступ на сервер извне будет закрыт. При выключении функции в случае остановки службы доступ работа пользователей в Интернете может быть продолжена, однако весь получаемый ими трафик не будет учтен.

Вкладка Параметры очередей

На вкладке **Параметры очередей** можно настроить размер внутреннего буфера данных (в пакетах), передаваемых драйвером для обработки программой. Если в статистике интерфейсов появляются пропущенные пакеты, увеличение размера буфера поможет это исключить. Рекомендуется производить при достаточных свободных ресурсах процессора. Для ситуации, когда ресурсы процессора на пределе, буфер следует уменьшать. Появятся потерянные пакеты, зато устранится более опасная ситуация остановки обработки всей очереди данных и перегрузка всей системы.

Также здесь можно настроить лимит очередей шейпера, который используется для ограничения скорости работы пользователей в Интернете. Для этого нужно указать размер очереди (в пакетах) и максимальный предел задержки. Больший размер очереди требует больших ресурсов процессора и, при наличии последних, эти параметры можно немного увеличить. Но до разумных пределов, т.к. перебор приведет к обратному результату – ухудшению работы приложений. Если же каналы скоростные и ресурсы процессора на пределе, то очередь можно уменьшить, предпочтительнее за счет уменьшения времени жизни.

Параметры шейпера можно настраивать отдельно для пользователей и групп. При оптимизации работы шейпера для группы размер очереди можно задать большим, чем для пользователя.

Вкладка Сетевая статистика

На вкладке **Сетевая статистика** настраиваются параметры сбора информации с сетевых интерфейсов (подробнее см. в п. Управление сетевой статистикой). Здесь можно включить группировку сетевых портов с номерами больше 1023. В этом случае трафик по всем этим портам будет записываться вместе. Это имеет смысл, так как согласно стандартами порты с номерами больше 1023 являются динамическими. Если же их группировку выключить, то для каждого такого порта будет создаваться своя запись в сетевой статистике, а это приведет к значительному увеличению ее размеров и ухудшению наглядности. При необходимости можно добавить исключения группировки – порты, для которых информация будет сохраняться отдельной строкой. Это позволяет отслеживать трафик от отдельных приложений, использующих динамические порты.

Здесь же можно включить запись всего трафика. В этом случае в сетевую статистику будет попадать не только тарфицируемый, но и бесплатный трафик. Учет бесплатного трафика увеличит нагрузку на сервер, но даст более подробную статистику. Использовать эту функцию имеет смысл в целях диагностики, например, при настройке правил на бесплатные сети. Если требуется анализ для прямого трафика, то также следует включить функцию **Анализировать весь трафик** в общих настройках пользователей (иначе будет доступен бесплатный трафик только через прокси-сервер).

Вкладка Распознавание имен

На вкладке **Распознавание имен** можно включить использование DNS для обратного преобразования имен (вычисление имени хоста по IP-адресу). В этом случае в сетевой статистике будут отображаться не только IP-адреса, но и имена доменов. Обратите внимание, что достоверность обратного преобразования не гарантирована, поскольку по одному IP-адресу может располагаться несколько хостов. Поэтому возможны ошибки, то есть отображение не тех имен, на которые на самом деле обращались пользователи.

Отдельно можно включить использование DNS для сетевой статистики у пользователей. Однако эта операция весьма ресурсоемкая. Не рекомендуется включать ее при количестве

пользователей более 300, поскольку это может привести к нехватке системных ресурсов сервера и отказу работы Traffic Inspector.

> ***Замечание!*** *Для преобразования имен сервер обращается к служ бе DNS, что мож ет привести к росту служ ебного трафика самого сервера.*

Также на данной вкладке можно включить распознавание имен хостов в HTTP-запросах. Эта функция работает на уровне драйвера Traffic Inspector для трафика мимо прокси-сервера. Она позволяет отображать в отчетах реальные имена хостов из запрашиваемых URL.

Вкладка Журналы

На вкладке **Журналы** можно задать максимальное количество записей системных логов, хранимых в программе. В силу того, что запись логов производится также в системный журнал событий Windows, это ограничение распространяется только на записи, которые доступны для просмотра в консоли администратора.

Вкладка Оповещение

На вкладке **Оповещение** можно включить или выключить автоматическое отображение списка предупреждений при открытии консоли администратора (подробнее о предупреждениях см. в п. Журналы событий). Эта функция позволит администратору не пропустить важную информацию.

Здесь же можно включить или выключить рассылку оповещений о системных ошибках. При включении Traffic Inspector при появлении в журнале системных ошибок новой записи будет дублировать ее путем отправки сообщения по электронной почте. Для работы функции необходима настройка службы отправки (подробнее см. в п. Служба отправки). Список рассылки задается в свойствах этой службы.

Также на вкладке **Оповещение** можно включить или выключить запись в журнал попыток нарушения правил фильтрации. Включение этой функции может привести к значительному увеличению размеров журнала, зато позволит отследить все попытки

доступа пользователей к запрещенному для них контенту и/или заблокированным сетевым службам.

Вкладка Автоматизация

На вкладке **Автоматизация** задаются общие настройки работы скриптов автоматизации (подробнее о скриптах см. в документации по SDK). Здесь можно включить вывод скрипта в файл, а также указать местоположение этого файла (по умолчанию используется подпапка *script\output* в папке установки Traffic Inspector).

Вкладка Счетчики скорости

Для пользователей программы и внешних счетчиков имеются специальные счетчики, в которых хранится история из ста последних значений текущей скорости. Они используются для оперативного отображения информации о сетевой активности объекта. На вкладке **Счетчики скорости** можно настроить их отображение, в частности, выбрать шаг анализа скорости (по умолчанию 10 секунд), то есть время, через которое выполняется замер скорости. Он может быть выбран в интервале от 2 до 60 секунд. Чем этот шаг больше, тем за больший период времени будут отображаться данные.

Здесь же выбирается способ определения скорости за шаг на основе значения текущей скорости. Текущая скорость вычисляется каждую секунду. Если задать определение по максимуму (по умолчанию), то на графиках будут более наглядно отображаться кратковременные всплески скорости; по среднему – отображаемое значение скорости будет более объективно.

Также на этой вкладке можно указать количество шагов измерения скорости, на основе которых система вычисляет самые активные счетчики скорости.

Вкладка Дополнительно

На вкладке **Дополнительно** можно включить использование вышестоящего прокси-сервера и настроить параметры подключения к нему: указать его имя или IP-адрес и номер

порта и, при необходимости, данные для авторизации. Данные настройки являются едиными в пределах всей программы. Они используются самой программой в служебных целях (для активации, загрузки обновлений и пр.), а также дополнительными модулями для своей работы (подробнее см. в п. Дополнительные модули).

> ***Замечание!*** *К настройке каскадирования прокси данный прокси-сервер никакого отношения не имеет. При каскадировании прокси-сервера указываются непосредственно в правилах каскадирования.*

Журналы событий

В Traffic Inspector реализован лог сообщений сервера. В него записываются все сообщения сервера об ошибках или с предупреждениями. Лимит хранимых сообщений можно задать в окне главных настроек программы (подробнее см. в п. Общие настройки программы). Все эти сообщения также пишутся в журнал системных событий операционной системы. В нем они могут быть просмотрены в полном объеме стандартными средствами.

Журналы событий размещены в разделе **События** консоли администратора. В разделе **События -> Ошибки** отображаются сообщения об ошибках, возникших при выполнении разных операций. В разделе **События -> Предупреждения** отображаются сообщения с предупреждениями администратору, например, о скором окончании срока действий лицензий, ошибках в настройках Traffic Inspector и пр. Сообщения в этих разделах показываются в виде списка. Для подробного просмотра сообщения дважды кликните на нем левой кнопкой мыши.

В **События -> Замечания** отображаются подробные сообщения о недостатках настройки Traffic Inspector, требующих исправления. Например, это может быть предупреждение о возможности доступа к консоли администратора всех локальных пользователей (функция включена сразу после установки и требует настройки), об отключенной службе резервного копирования и т.д. В отличие от журналов с предупреждениями об ошибках, замечания могут автоматически показываться администратору в консоли при подключении к серверу Traffic Inspector (эта возможность включается в общих настройках программы, подробнее см. в п. Общие настройки программы).

Диагностика работы 20

Параметры работы драйверов

В разделе **Настройки -> Настройки сети -> Драйвер** консоли администратора можно просмотреть перечень всех установленных на сервере Traffic Inspector сетевых интерфейсов.

Также у каждого интерфейса в этом разделе консоли администратора есть собственный подраздел, в котором приводится подробная статистика его работы, информация о работе шейпера и потерянных пакетах.

Отображение сетевых настроек

В консоли администратора есть возможность просмотра текущих сетевых настроек сервера Traffic Inspector. При локальной работе администратора сделать это можно и встроенными средствами операционной системы. Однако при удаленной работе удобнее воспользоваться средствами консоли администратора.

В разделе **Настройки -> Настройки сети -> Сетевые настройки** показывается полная информация обо всех текущих настройках (полный аналог команды *ipconfig -all*).

В разделе **Настройки -> Настройки сети -> Таблица маршрутов** показывается полная информация обо всех текущих маршрутах (полный аналог команды *route print*).