SMART-SOFT

ХАРАКТЕРИСТИКИ TRAFFIC INSPECTOR

Минимальные системные требования

- Процессор Intel® Core i5.
- 4096 Мб оперативной памяти.
- 1000 Мб свободного места на жестком диске (для дальнейшей работы потребуется дополнительное место под файлы кэша и статистики).
- Монитор и видеоадаптер с разрешением 1024 на 768.
- Операционная система Microsoft Windows 7/2008 R2 или выше (ОС x86 и x64).
- Подключение к сети Интернет.

Внутренние и внешние сети - протоколы и топология

- Сервер может работать с несколькими внутренними интерфейсами в сложной по топологии сети.
- Поддерживаются интерфейсы 802.3 (Ethernet), 802.11 (Radio Ethernet), WAN PPP, WAN VPN (PPTP, L2TP).
- Работает совместно с NAT от Windows. Поддерживается RAS (Dial-out), VPN (PPTP, L2TP), PPPoE.
- Работает с RAS сервером (Dial-In клиенты), поддерживаются как модемные соединения, так и VPN (PPTP, L2TP).
- Внутренние сети могут быть описаны как локальные (например внутриофисная сеть) или публичные (например домовая). Для разных сетей могут использоваться разные политики доступа.
- Для съема трафика пользователей через другие сервера внутренней сети может также использоваться специальный режим сниффера («прослушки»).
- Сервер может работать с несколькими внешними интерфейсами, т.е. может быть несколько подключений к сети Интернет.
- Для работы с динамическими внешними интерфейсами имеется режим автоматического их выбора.
- Обеспечивается корректная работа при разделении входящего и исходящего трафика на внешних интерфейсах (например, при работе через спутник).
- Для персонального режима работы используется внутренний IP интерфейс (127.0.0.1). В этом случае назначение других внутренних интерфейсов запрещено.
- Реализована возможность работы клиентов на терминальном сервере.
- Имеется поддержка протокола IEEE 802.1Q (Tag based VLAN).

Авторизация пользователей

- Авторизация по сетевому адресу - IP, MAC или вместе. Также можно задать диапазон IP адресов.

- Авторизация по имени и паролю. Может использоваться при работе с прокси сервером или через клиентского агента с использованием как собственных паролей, так и через домен сети Windows. Поддерживается авторизация с разных доменов.
- Запись MAC клиентов авторизации в таблицу статических ARP операционной системы.
- Авторизация по адресам электронной почты - используется в SMTP шлюзе.
- В качестве дополнительно параметра авторизации можно использовать Vlan ID.
- Авторизация через API. Позволяет использовать сторонние программы.
- Контроль нарушений правил авторизации. В программе ведется учет нарушений доступа, производится запись этих событий в сетевую статистику и журнал, а также есть возможность оповещать администраторов по электронной почте.
- Поддерживается 8192 пользователей и 256 групп.
- Автоматическое перенаправление неавторизованных пользователей на специальную информационную страницу встроенного Веб-сервера (удобно для Wi-Fi сетей и подключении новых клиентов в домовых сетях).
- Аутентификация пользователей через ЕСИА (Единая система идентификации и аутентификации).

СМС-Идентификация

В 2014 году правительство РФ приняло постановление, вносящее изменения в федеральный закон «Об информации, информационных технологиях и о защите информации». Согласно поправкам, оператор публичного сервиса доступа к сети Интернет обязан хранить данные пользователя (номер мобильного телефона, MAC-адрес устройства, а также время и объем пользования услугами) в течении полугода с момента предоставления услуги. Данные пользователя могут быть предоставлены в правоохранительные органы в ситуациях, предусмотренных законом.

Traffic Inspector предлагает механизм SMS-идентификации для выполнения требований законодательства Российской Федерации (Постановление Правительства РФ № 758) в сфере предоставления публичного доступа к сети Интернет. В наиболее общем случае, учреждение настраивает общедоступный, открытый Wi-Fi хотспот. Мобильное устройство пользователя свободно ассоциируется с Wi-Fi точкой доступа. При попытке обратится к веб-сайту, пользователь перенаправляется на captive портал (страницу регистрации / авторизации) Traffic Inspector, где вводит свой номер телефона. Для подтверждения, на мобильный телефон пользователя высылается SMS-сообщение с кодом проверки. Получив данное сообщение, пользователь вводит код проверки на портале. Происходит регистрация пользователя в программе Traffic Inspector, после чего он получает доступ к сети Интернет. Traffic Inspector хранит идентификационные данные пользователя в течение необходимого периода времени.

Ограничения работы пользователей

- По датам.
- По расписанию. Может быть задано индивидуально для пользователя, для группы или сразу для всех.
- По доступу к ресурсам. Имеются групповые и общие фильтры на запрещение и разрешение. Фильтры применяются на IP уровне для любого трафика (IP адреса, протоколы и порты), так и на уровне приложений при работе через прокси (HTTP, FTP, URL, типы данных, regular expressions). Вместо IP адресов всегда можно

задавать и имена хостов, что описание фильтра делает независимым от изменений адресов ресурсов.
- По IP и MAC адресам клиента. Для пользователей с авторизацией по имени это может использоваться для введения дополнительных ограничений.
- По доступу к службам (NAT, роутинг, прокси-сервер, SOCKS-сервер).
- По количеству TCP сессий. Это ограничение работает, как через прокси (SOCKS), так и для прямого трафика.
- Защита от перегрузки сети и сервера Virus Flood Protect. Используется анализ трафика пользователя и блокирует его при переполнении сетевой статистики, свойственной при заражениях компьютера пользователя сетевыми вирусами.
- Реализована возможность отключения порта управляемого оборудования по SNMP-протоколу с помощью скриптов при измении состояния клиента.

Layer 7 фильтрация (nDPI)

Система глубокой инспекции пакетов обеспечивает интеллектуальное распознование протоколов прикладного (седьмого) уровня за счет сигнатурного анализа. С точки зрения пользователя, данная система – простое решение для блокировки приложений вроде Skype и BitTorrent.

Тарификация

- Возможен различный вид учета трафика: по входящему, исходящему, сумме входящего и исходящего и максимальному значению от входящего и исходящего.
- Есть возможность задания предоплаченного (бесплатного) трафика.
- Есть возможность тарифицировать время работы клиентов. При этом абонентская плата может начисляться посуточно или поминутно за время реальной работы.
- Тарифы могут быть изменены задним числом - любое их изменение влечет немедленный пересчет всех данных по билингу. Дополнительно могут задаваться скидки на трафик из кэша, почтовый или любой другой в соответствии заданным в фильтрах критериям.
- Работа в кредит. При работе клиента в кредит до момента блокировки могут быть применены отдельные политики доступа.
- Все настройки тарификации могут быть сделаны индивидуальными, групповыми или общими, что позволяет иметь различные тарифные планы.
- Текущий статус клиента со всеми его параметрами тарификации отображается в реальном времени.
- Все изменения статуса клиентов могут записываться в журнал для последующей обработки и формирования отчетов.
- Реализована возможность создания групповых счетов - единый счет для нескольких групп и клиентов.
- В настройках тарифов есть возможность задать лимиты трафика на сутки, неделю, месяц.

Контроль внешнего трафика

- Для учета общего трафика, потребляемого у провайдера, имеются контролируемые счетчики, которые описываются как IP сети. С их помощью можно учитывать трафик от провайдера. Несколько таких счетчиков позволяют вести раздельный учет разного вида трафика (льготный или бесплатный).
- Для контролируемых счетчиков задаются лимиты - предупреждения, перерасхода и ежедневный, при превышении которых выдается оповещение администратора или (и) данное направление (трафик) может быть заблокировано.

- При срабатывании блокировок на внешних счетчиках может быть запущено любое внешнее приложение.
- Для дополнительного анализа общего потребляемого трафика могут быть заданы и внешние информационные счетчики, где есть дополнительная возможность анализировать трафик по IP протоколам и портам.
- Данные по внешним счетчикам могут отображаться как в реальном времени и записываться в журнал для формирования отчетов.

Сетевая статистика

- Для пользователей и внешних счетчиков может быть включен сбор сетевой статистики в контексте IP адресов, протоколов, портов и DNS-имен.
- Есть возможность индивидуально или для всех задавать степень детализации - интервал анализа и количество активных соединений.
- Текущая статистика может отображаться в реальном времени и записываться в журнал для последующего анализа и формирования отчетов.
- Для дополнительного анализа хостов и сетей используется сервис WhoIs и NetGeo.
- Предусмотрена возможность записи сетевой статистики во внутреннюю СУБД программы, а также синхронизация внутренней СУБД с внешней базой на MSSQL 2005, либо MySQL, либо PosrgreSQL.

Прокси-сервер

- Протоколы - HTTP/1.1, FTP, SOCKS 4/5.
- Аутентификация - BASIC (открытым паролем) или интегрированная через домен Windows (NTLM v. 1/2).
- Кэширование - есть много настроек для выбора оптимальных параметров с точки зрения экономии трафика.
- Индивидуальная гибкая настройка параметров кэширования для отдельных ресурсов.
- Кэш хранится в одном файле СУБД, при этом полностью исключена его внутренняя фрагментация. Все индексы кэша хранятся в оперативной памяти, что обеспечивает высокую скорость работы с кэшем.
- Фильтрация контента - прокси сервер использует общие с IP фильтрами списки, но для него есть возможность также задавать тип контента и вести анализ протокола и URL вплоть до контекстного поиска с помощью выражений regular expressions. Это позволяет, например, легко реализовать эффективную фильтрацию баннеров.
- Есть поддержка метода HTTP CONNECT - через прокси сервер в этом режиме может работать SSL, FTP или любое другое TCP приложение, позволяющее работать через HTTP туннель.
- FTP через HTTP (метод GET) - прокси сервер генерирует HTML страницы, позволяя работать с FTP серверами в режиме чтения. При этом работает автоматическое переключение между активным и пассивным режимами для протокола FTP.
- Авторизация - сквозная. Если пользователь не авторизовался, то по необходимости запрашивается аутентификация через прокси или SOCKS сервер.
- Автоматическое конфигурирование броузеров, в соответствии принятым стандартам. Прокси сервер выдает клиентам стандартный WPAD.DAT JAVA скрипт для их конфигурирования. Есть возможность задания в нем LAT (таблицы локальных адресов). Также может быть использовано принудительное конфигурирование броузеров через клиентского агента.
- Форвардинг HTTP запросов на другой прокси сервер.
- Блокировка HTTP трафика мимо прокси сервера.

- Оперативное управление режимами фильтрации и кэширования со стороны клиента.
- Имеется возможность выборочно включить запись в журнал всех запросов через прокси сервер.
- Анализ SSL/TLS.

SMTP-шлюз

- Публикует один внутренний SMTP-сервер для доступа из Интернета.
- Запрещает открытые relay (пересылки), что позволяет использовать внутри сети самые простые почтовые сервера.
- Есть проверка адресов отправителей на достоверность их домена.
- Есть проверка хостов отправителей с помощью служб RBL, базирующихся на DNS. Многопоточная реализация позволяет задействовать большое количество служб без внесения дополнительных задержек. Через RBL также могут проверяться и все промежуточные SMTP-сервера анализом заголовков сообщений.
- Имеются «черные списки» хостов отправителей, которые могут заполняться как автоматически, так и вручную. Автоматическое занесение в «черные» списки хостов, отфильтрованных через RBL, позволяет существенно экономить трафик при массовой рассылке спама с них за счет исключения последующих запросов на RBL службы.
- Есть «белые» списки, описывающие отправителей, для которых фильтрация сообщений применяться не будет.
- Для анализа отфильтрованной почты ведется подробный журнал, а также может использоваться почтовая рассылка администраторам.
- Тарифицирует входящую почту для известных получателей - пользователей Traffic Inspector. Для экономии трафика прием почты для неизвестных получателей может быть запрещен.
- Может быть запрещен также прием почты для отключенных или заблокированных пользователей.
- Поддерживается интеграция модуля защиты от нежелательной почты Traffic Inspector AntiSpam.
- Фильтрация по MIME-типам объектов.
- Поддержка StartTLS.

Межсетевой экран (firewall)

- По умолчанию закрывает все запросы извне, при этом прозрачно разрешая исходящие TCP, UDP и ICMP данные, в связи с чем настройка службы практически не требуется.
- Динамическая UDP-фильтрация - позволяет корректно отличать входящие UDP запросы от исходящих, прозрачно разрешая исходящие UDP данные.
- Динамическая фильтрация FTP-DATA. Производится анализ FTP команд PORT и PASV и выставление временных разрешений в firewall. Это позволяет без проблем работать с активным режимом (клиент), так и пассивным (публикуемый сервер).
- Для разрешения работы различных серверных приложений или других протоколов можно отдельно задать список разрешающих и запрещающих правил.
- На информационных счетчиках можно вести раздельный учет и анализ отфильтрованного входящего трафика (анализ флуда, сканирования портов и др.).
- Для защиты самого сервера изнутри сети также может быть включен внутренний firewall. Его функциональность аналогична внешнему. Имеются отдельные настройки этого firewall для локальных и публичных внутренних сетей.
- Реализована возможность запрета неавторизованого трафика с самого сервера.

- Блокировка по географической локации.

Система обнаружения / предотвращения вторжений

Система IDS/IPS значительно увеличивает безопасность, выявляет и предотвращает широкий диапазон атак:

- эксплуатирование уязвимостей в сетевых протоколах (DNS, FTP, ICMP, IMAP, POP3, HTTP, NetBIOS, DCERPC, SNMP, TFTP, VOIP-протоколах)
- DOS-атаки
- сетевое сканирование
- работа ботнетов и скомпрометированных хостов
- работа хостов, зараженных троянским ПО и сетевыми червями
- защита от спам-сетей
- использование скомпрометированных SSL-сертификатов

Bandwidth control (шейпер)

- Служба работает по любому трафику, проходящему через сервер. В том числе через прокси-сервер и SOCKS.
- Ограничение индивидуальной скорости работы клиента с отдельной настройкой на прием и передачу.
- Динамическое ограничение - назначение суммарной максимальной скорости для группы, отдельно на прием и передачу.
- Ограничение по количеству пакетов. Полезная функция для предотвращения перегрузки сети при эпидемиях вирусов.
- Назначение в фильтрах типа трафика, который надо исключить из контроля.
- Выставление отдельных ограничений скорости для конкретного типа трафика.
- Выставление приоритетов на определенный тип трафика. Эта настройка позволяет менять очередность обработки пакетов во внутренней очереди шейпера и передавать эти данные с минимальными задержками.
- Для всех правил может быть назначено расписание, что позволяет динамически изменять настройки службы этой в зависимости от времени.
- При работе через прокси сервер имеется возможность настроить полосу отдельно для разного типа контента.
- Данные из кэша прокси сервера, а также с локального веб сервера (сервер статистики) ограничениям по скорости не подвергаются.

Advanced routing и перенаправление TCP-соединений

Расширяет функции роутера Windows. Также эта функция известна как «policy routing» или «source routing».

- Перенаправление трафика через заданный внешний интерфейс для группы пользователей.
- Перенаправление трафика через заданный внешний интерфейс для пользователя индивидуально.
- Применение перенаправления для заданного типа трафика. При работе через прокси можно задать также тип HTTP контента.
- В фильтрах также можно задать в качестве условия факт перенаправления трафика.

- Реализован редирект исходящих от клиента TCP-соединений. Редирект удобно использовать, если в локальной сети есть сторонний прокси-сервер или требуется перенаправление клиента на другой интернет-ресурс.

Клиентский агент

С помощью специальной программы - клиентского агента - пользователь может самостоятельно:

- видеть текущий баланс, также можно настроить оповещение, когда средства на счету подходят к концу.
- переключать уровни фильтрации контента - работать в режиме «сбережения» трафика.
- переключать режимы кэширования прокси сервера. Это позволяет без проблем просматривать быстро обновляемые ресурсы, имея при этом хорошие показатели экономии трафика за счет кэширования.
- быстрый доступ в личный кабинет с помощью контекстного меню агента.
- менять пароль через агент. Администратор может отключить возможность смены пароля в Traffic Inspector.
- Несколько протоколов авторизации с помощью агента (UDP, HTTP, SSL). При возникновении проблем авторизации по UDP в WiFi сетях можно использовать HTTP или SSL.
- Встроеный Веб-агент во многом аналогичный по функционалу клиентскому агенту. Установка Веб-агента не требуется, т.к. он запускается из главной страницы встроеного Веб-сервера.
- Настраиваемые предупреждения в клиентском агенте о блокировке по лимитам групповых счетов.

Кроме того, администратор может разослать быстрое оповещение пользователям, у которых используется клиентский агент.

Встроенный веб сервер с поддержкой запуска скриптов и формирования динамического контента позволяет обеспечить клиентам доступ для просмотра различных отчетов по их работе. Этот сервис полностью задокументирован и может быть легко самостоятельно доработан.

Администрирование

- Удаленное управление - для удаленного доступа используется стандартная технология DCOM, консоль управления выполнена как MMC Snap-In, что позволяет ее легко интегрировать с другими инструментами администратора.
- Ограничение доступа - можно задать группу администраторов в домене Windows или использовать встроенную аутентификацию по паролю.
- Распределение доступа - можно создать администраторов с ограниченными правами, например, только для добавления клиентов, только для пополнения счетов, только для работы с определенной группой клиентов.
- Мониторинг работы клиентов и сетевой статистики в реальном времени.
- Просмотр статистики клиентов и пополнение счета через веб-интерфейс.
- В случае, когда компьютеры клиентов не в сети Windows, клиенты могут самостоятельно загрузить или обновить агента через встроенный веб сервер.
- Автоматическое добавление клиентов - если сеть работает с доменом Windows. Также имеется возможность ограничить это для отдельной группы домена, а также

сразу помещать новых клиентов в разные группы Traffic Inspector с привязкой к группам домена.
- Часть настроек клиентов программы доступна через веб интерфейс.
- Тройка активности по счетчикам.
- Тройка активности по клиентам.

Отчеты

- Может быть сформировано несколько десятков видов разных отчетов трафику, билингу и сетевой статистике. Все отчеты могут быть импортированы и сохранены в различных видах и форматах - табличных и графических.
- Набор отчетов может быть расширен использованием интерфейса автоматизации.

Дополнительные плагины и программные продукты

- **AdGuard**. Фильтрация рекламы, всплывающих окон в трафике, проходящем через прокси-сервер.
- **Dr. Web Secuirty Suite**. Антивирусная проверка. Проверяется HTTP-трафик, проходящий через прокси-сервер, и SMTP-трафик, проходящий через SMTP-шлюз.
- **NetPolice для Traffic Inspector**. Фильтрация по URL-категориям для трафика, проходящего через прокси-сервер. Используется онлайн база NetPolice.
- **RAS Dialer**. Модуль-дозвонщик. Устанавливает VPN (PPTP, L2TP/IPsec, SSTP, PPPoE) и Dial-Up (PPP) подключения с удаленными серверами.
- **RBL SMTP Filter**. Фильтрация почтовых сообщений, проходящих через SMTP-шлюз, с проверкой email адресов в он-лайн базах данных DNSBL.
- **Traffic Inspector Antivirus Powered by Kaspersky**. Антивирусная проверка. Проверяется HTTP-трафик, проходящий через прокси-сервер, и SMTP-трафик, проходящий через SMTP-шлюз.
- **Traffic Inspector Anti-Spam Powered by Kaspersky**. Фильтрация почтовых сообщений (спама), проходящих через SMTP-шлюз.

Интерфейс автоматизации

- Открытое API для сторонних разработчиков.
- Встроенная поддержка скриптов автоматизации.
- Сообщество разработчиков на форуме.

Производительность

Возможности сервера с Traffic Inspector зависят от мощности используемого оборудования, но планируемая нагрузка при пропускании трафика через сервер не должна превышать следующих рекомендуемых значений:

- емкость сети не более 200 абонентов при работе через прокси и 2000 при работе через NAT.
- прохождение трафика через сервер не более 5000 пакетов в секунду.
- пропускная способность драйвера до 600 Мбит/сек.