Traffic Inspector®

Дополнительные модули для Traffic Inspector

Anti-Virus powered by Kaspersky

Дополнительный антивирусный модуль для Traffic Inspector, который обеспечивает безопасность трафика, проходящего через прокси-сервер и почтовый шлюз программы, лечение зараженных файлов, блокировку вредоносных программ, запрет потенциально опасного содержимого.

Принцип работы антивирусного модуля:

- Сканируется весь HTTP-, HTTPS- и FTP-трафик, проходящий через прокси-сервер, а также почтовый трафик, передаваемый через SMTP-шлюз программы Traffic Inspector.
- Зараженные объекты лечатся, неизлечимые и вредоносные программы удаляются и блокируются.
- С помощью механизмов эвристического анализа запрещается получение файлов, которые могут нанести ущерб пользователям.

Достоинством модуля является его совместимость с любыми другими антивирусами, которые установлены в сети, а также возможность двойной проверки трафика, что повышает степень защиты от новых вирусов при сетевых эпидемиях.

Высокая скорость проверки обеспечивает незаметное для пользователей сканирование всего проходящего трафика.

Поддерживается как полное, так и частичное обновление антивирусных баз, что существенно экономит трафик. Доступно как ручное, так и гибко настраиваемое автоматическое обновление.

Настройка работы антивирусного модуля происходит в привычном для администраторов интерфейсе консоли программы Traffic Inspector.

По всем обнаруженным вирусам или иным вредоносным программам создается подробный отчет.

При обнаружении вируса модуль оповещает пользователя о зараженном файле и действиях антивируса через клиентского агента, прокси-сервер или вложенный отчет в почтовом сообщении - в зависимости от вида угрозы.

Модуль использует передовую технологию от популярного производителя (сканер, разработанный «Лабораторией Касперского»), что обеспечивает высокое качество антивирусной безопасности и оперативность работы.

Traffic Inspector Anti-Spam powered by Kaspersky

Антиспам модуль Traffic Inspector Anti-Spam powered by Kaspersky интегрируется в почтовый шлюз программы Traffic Inspector и анализирует сообщения, приходящие на внутренний почтовый сервер.

Traffic Inspector Anti-Spam powered by Kaspersky - гибкий инструмент для работы с корпоративной почтой. Функционал программы позволяет задавать правила и настройки, фильтровать или сортировать письма по папкам, помечая тему, добавляя в заголовки и изменяя весовой коэффициент для сообщений, распознанных как спам, для обычных и сомнительных писем. Предусмотрены установка уровня агрессивности проверки и размера проверяемых сообщений.

В основу программного продукта легли уникальные исследования в области методик определения спама от «Лаборатории Касперского».

Модуль встроен в каждое комплексное решение Traffic Inspector, активируется на необходимое количество лицензий (учетных записей), которые могут распределяться по отдельным пользователям и по группам.

В основе модуля:

- **Фильтрация по SPF и SURBL**

В процессе фильтрации может учитываться авторизация отправителя по технологии SPF (Sender Policy Framework). В дополнение к спискам DNSBL, выявляющим спамерские IP-адреса, используется также технология SURBL (Spam URI Realtime Block List), распознающая спамерские URL в теле сообщения.

- **Сигнатурный анализ**

Использование круглосуточно обновляемой базы лексических сигнатур позволяет распознавать модифицированные варианты исходного спам-письма, создаваемые для обхода спам-фильтров.

- **Графические сигнатуры**

Используя базу графических сигнатур, приложение блокирует спам-письма, которые содержат информацию в виде изображений, а не в виде текста.

- **Белый список адресов отправителей**

В случае если адрес занесен администратором в белый список, то сообщение принимается, минуя все этапы анализа.

- **Черные списки**

Модуль Traffic Inspector Anti-Spam powered by Kaspersky способен анализировать почтовую корреспонденцию с использованием методики проверки сообщения по спискам. Модуль проверяет IP-адрес отправителя по черным спискам провайдеров и общественных организаций (DNSBL — DNS-based Blackhole List).

- **Анализ формальных признаков письма**

Программа отсеивает спам по таким типичным для него признакам как модификация адреса отправителя или отсутствие его IP-адреса в системе доменных имен (DNS), неоправданно

большое количество получателей или сокрытие их адресов. Кроме того, оцениваются размер и формат сообщения.

- **Лингвистические эвристики**

Программа проверяет наличие и расположение в тексте письма слов и фраз, типичных для спама. Анализу подвергается как текст самого письма, так и содержание вложенных файлов.

- **UDS-запросы в режиме реального времени**

Технология UDS (Urgent Detection System) позволяет получать данные о последних спамерских рассылках уже через секунду после их обнаружения. Эта информация используется для дополнительной проверки тех сообщений, которые не получили однозначной оценки (спам/не-спам).

Модуль Traffic Inspector Anti-Spam powered by Kaspersky использует спам-базу, разрабатываемую и распространяемую «Лабораторией Касперского». Одно из основных преимуществ такого подхода - модуль готов к выполнению своей задачи сразу после обновления базы.

Adguard для Traffic Inspector

Adguard для Traffic Inspector — дополнительный модуль Traffic Inspector для фильтрации на компьютерах корпоративной сети рекламы, всплывающих окон и другого нецелевого контента. Технология Displace убирает ненужное содержимое непосредственно из тела страницы, в любом браузере и на любой платформе.

Adguard для Traffic Inspector — серверный плагин и не требует установки на компьютеры всех пользователей сети. Модуль использует все способы фильтрации: по маскам URL, HTML-фрагментам, характерным размерам, JavaScript-вызовам, CSS-селекторам. Плагин удаляет с веб-страниц рекламу и нежелательные элементы, не ломая верстку.

Не требует обучения и настроек. Автоматически обновляется для поддержания алгоритмов фильтрации в актуальном состоянии, в том числе при появлении новых форматов рекламы. За счет фильтрации ускоряет время загрузки веб-страниц, снижает вирусную опасность, экономит внимание сотрудников, не давая им повода отвлекаться от работы. Убирает рекламу не только на компьютерах и ноутбуках, но и на планшетах, смартфонах и любых других устройствах, подключенных к локальной сети организации.

Плагин поддерживает 4 листа фильтрации, имеющих различное назначение:

- Стандартный лист. Фильтрует рекламу и баннерные сети.
- Лист блокировки счетчиков интернет-статистики.
- Лист блокировки социальных виджетов (Facebook Connect, Like, Tweet и др.).
- Фильтр для иностранных сайтов (английских, немецких, испанских, японских и т.д.).

Разделение позволяет гибко настраивать режим фильтрации. Например, можно оставить показ счетчиков для отдельных сотрудников, если это необходимо им для работы.

NetPolice для Traffic Inspector

NetPolice для Traffic Inspector - модуль контентной фильтрации на основе категорий веб-ресурсов. Плагин интегрирует возможности программ NetPolice, разработанные ЦАИР, в Traffic Inspector.

Основная функция модуля - обеспечение безопасного и эффективного доступа в интернет на уровне шлюза для детей и подростков. Он позволяет установить необходимый уровень доступа к ресурсам интернета в учебных заведениях, обеспечивая фильтрацию контента, не совместимого с задачами образования и воспитания.

База NetPolice включает 100+ категорий (в том числе по спискам категорий, рекомендованным Минобрнауки РФ). По запросу «Лиги безопасного интернета» специально для учебных учреждений были добавлены категории «Белый список» и «Безопасные для детей».

NetPolice применяется и в офисах для запрета нецелевого использования интернета сотрудниками.

Модуль NetPolice производит проверку каждого запрашиваемого ресурса и присваивает ему категорию контента в соответствии с заданными в нем правилами. В программе можно создать фильтры или правила клиента, условиями срабатывания которых может быть наличие у ресурса присвоенной категории. Такой подход позволяет гибко реализовать различные виды фильтрации.

Для достижения высокого уровня безопасности в плагине реализованы две технологии фильтрации:

- URL-фильтрация;
- динамическая фильтрация.

Фильтр проверяет, к какой категории (запрещенной или разрешенной) относится запрашиваемый сайт, а также анализирует его содержимое. Настраивать фильтрацию можно самостоятельно по категориям классификации, предоставленным ЦАИР, или с использованием списка «стоп-слов». Имеется возможность дополнить список «стоп-слов», предоставленный ЦАИР. Количество «стоп-слов» для добавления в список фильтрации неограниченно.

При попытке перехода на небезопасный сайт в браузере открывается страница с предупреждением — «страница блокировки». Пользователи могут заменить стандартную страницу блокировки на любой интернет-ресурс. Главное – удостовериться в его безопасности и полезности.

В модуле есть страница проверки запроса, на ней можно произвести проверку любого ресурса и проверить логику присвоения типа рейтинга.

Также в модуле есть возможность просматривать отчеты по заблокированным ресурсам.