Kaspersky®
Web Traffic Security

Функциональные возможности

Состав и развертывание продукта

Программное обеспечение

Решение в виде исполняемых двоичных файлов для различных операционных систем на базе Linux. Управление осуществляется только через веб-интерфейс (интерфейс командной строки недоступен)

Поддержка установки на виртуальные машины

Можно устанавливать на виртуальные машины вместе с операционной системой.

Локализации

RU/EN/FR/DE/JP.

Управление несколькими узлами, поддержка кластеров

Продукт поддерживает управление несколькими узлами, причем каждый узел может устанавливаться вместе с клиентом ICAP либо отдельно. Это позволяет реализовать разные схемы развертывания и интеграции.

Схема развертывания выглядит так: Центральный управляющий узел – резервные управляющие узлы – рабочие узлы (см. схему).

Сбор данных

Интеграция с ICAP

Продукт поддерживает интеграцию с прокси-серверами и хранилищем по протоколу ICAP.

Поддержка контроля шифрованного трафика

При включении контроля корпоративного трафика (corporate traffic surveillance) решение Kaspersky Web Traffic Security может отслеживать трафик с SSL-шифрованием и анализировать объекты, проходящие через защищенный канал (такие как объекты веб-трафика HTTPS). Для этого требуется дополнительная настройка существующего корпоративного прокси-сервера.

Методики обнаружения

Антивирусный движок

Проверенная временем многоуровневая система защиты, включающая как высокоточные технологии обнаружения, так и основанные на машинном обучении проактивные методы блокировки вредоносных угроз, включая ботов, троянцев, червей, клавиатурных шпионов и вредоносное ПО для мобильных устройств и совершения преступлений.

Новинка **Репутационный анализ файлов и веб-адресов**	Технология репутационной фильтрации обнаруживает подозрительные и нежелательные файлы или веб-адреса на основе данных о репутации из баз KSN/KPSN.
Новинка **Обнаружение скриптов**	Решение обнаруживает вредоносные элементы на веб-страницах и в документах Microsoft Office и PDF-файлах, блокируя их открытие.
Новинка **Фильтрация содержимого**	Возможность блокировать загруженные из интернета файлы. Фильтрация по имени, расширению (используется распознаватель форматов), размеру, типу содержимого и контрольным суммам.
Новинка **Веб-контроль с категориями**	Огромная база данных веб-адресов, разделенная на 40 категорий, позволяет гибко ограничить доступ к веб-ресурсам.

Интеграция с внешними системами

Интеграция с Active Directory	Огромная база данных веб-адресов, разделенная на 40 категорий, позволяет гибко ограничить доступ к веб-ресурсам.

Интеграция с базами данных об угрозах

Новинка **KSN (Kaspersky Security Network)**	Возможность делать запросы в облачную базу данных о подозрительных объектах, что обеспечивает мгновенную реакцию на неизвестные угрозы.
Новинка **KPSN (Kaspersky Private Security Network)**	Интеграция с локальной репутационной базой позволяет использовать все преимущества облачной базы знаний в изолированных сетях, без передачи данных в облако. Через KPSN осуществляется интеграция с Kaspersky Anti Targeted Attack Platform: решение KWTS может использовать вердикты KATA, загруженные в KPSN.

Управляемость

Веб-панель мониторинга	Представление в режиме реального времени всех событий безопасности, связанных с нарушением установленных политик безопасности. Благодаря этому IT-специалисты могут своевременно реагировать на происходящее и изучать различные виды активности в сети.
Новинка **Распределение задач по ролям**	Решение позволяет определять роли для ограничения прав различных категорий администраторов. Роль системного администратора задается заранее.
Управление событиями	Результаты анализа угроз представляются исходя из событий и с отображением активности в режиме реального времени. Кроме того, решение позволяет анализировать поведение пользователей в интернете.
Новинка **Интеграция с SIEM**	Системы управления данными и инцидентами безопасности (SIEM) могут собирать информацию об инцидентах через системный журнал, в том числе в формате событий CEF.
Новинка **Поддержка рабочих областей**	Специальный режим для поставщиков услуг и компаний и предприятий с распределенной структурой позволяет назначать специальные рабочие области для различных компаний-клиентов или подразделений для управления доступом пользователей в интернет.

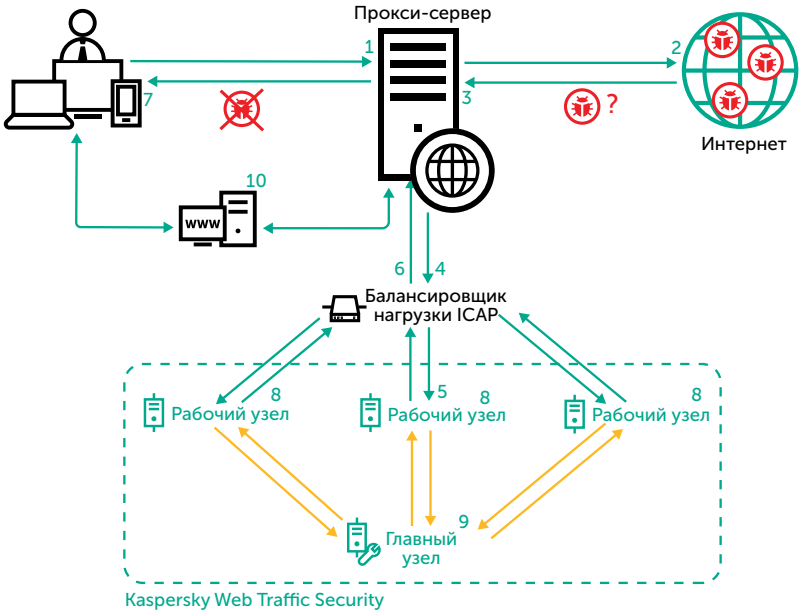
Лицензирование

Новинка **Гибкая модель лицензирования по объему трафика или числу пользователей. Также доступно лицензирование по модели с помесячной оплатой.**

Kaspersky Web Traffic Security можно приобрести в составе следующих решений:

1. Kaspersky Security для бизнеса
2. Kaspersky Security для интернет-шлюзов
3. Kaspersky Total Security для xSP
4. Kaspersky Anti-Virus for xSP

Также решение поддерживает интеграцию с Kaspersky Security для систем хранения данных



1 – Пользователь запрашивает информацию из интернета] через корпоративный прокси-сервер (трафик http(s), ftp)

2 – Прокси-сервер ищет запрошенный веб-ресурс

3 – Запрошенные ресурсы отправляются на прокси-сервер

4 – Прокси-сервер через балансировщик нагрузки отправляет объекты в нашу систему, используя ICAP

5 – Балансировщик нагрузки выбирает рабочий узел и передает объекты для проверки

6 – Рабочий узел возвращает вердикт на прокси-сервер

7 – Прокси-сервер доставляет пользователю проверенные безопасные веб-страницы и объекты, а также вердикты о найденных угрозах

8 – Рабочие узлы представляют серверы ICAP для сканирования объектов на основе правил обработки трафика. Правило по умолчанию включает антивирусную и антифишинговую проверки. Также доступны категории веб-адресов и фильтрация содержимого

9 – Центральный (главный) узел собирает данные о событиях и управляет ими. Здесь размещается веб-интерфейс решения для управления настройками, а также панели мониторинга для оперативного отслеживания событий безопасности и состояния системы.

10 – Контроллер домена Windows проводит аутентификацию пользователя или устройства на прокси-сервере через Kerberos или NTLM

Схема работы Kaspersky Web Traffic Security

Системные требования

Поддерживаемые платформы:

Приложение может использоваться как безопасный веб-шлюз (с прокси-сервером)

Минимальные аппаратные требования:

- Процессор Intel® Xeon 3040 или Core 2 Duo с частотой 1,86 ГГц или выше
- 8 ГБ ОЗУ и минимум 4 ГБ для подкачки
- 100 ГБ на жестком диске для установки приложения и хранения временных файлов и журналов

При установке Управляющего и Обрабатывающего сервера на одном физическом сервере:

- 2 процессора Intel® Xeon 3040 или Core 2 Duo с частотой 1,86 ГГц или выше
- 16 ГБ ОЗУ и минимум 4 ГБ для подкачки
- 200 ГБ на жестком диске для установки приложения и хранения временных файлов и журналов

Поддерживаемые операционные системы

- Red Hat Enterprise Linux версии 7.5 x64
- CentOS версии 7.5 x64
- SUSE Linux Enterprise Server 12 SP3
- Debian 9.5
- Ubuntu 18.04.1 LTS

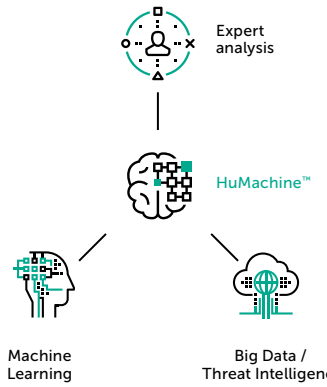
Дополнительные требования

- Ngnix версий 1.10.3, 1.12.2 и 1.14.0.
- HAProxy для балансировки нагрузки версии 1.5.
- Squid версии 3.5.20, если вы устанавливаете сервис Squid на Обрабатывающий сервер.

Поддерживаемые браузеры (для использования веб-интерфейса):

- Mozilla Firefox 39 и выше
- Internet Explorer 11 и выше
- Google Chrome 43 и выше
- Microsoft Edge 40 и выше

Для обработки сетевого трафика программой Kaspersky Web Traffic Security необходимо, чтобы в сети был установлен и настроен прокси-сервер HTTP(S) с поддержкой ICAP-протокола и служб Request Modification (REQMOD) и Response Modification (RESPMOD). Для этого можно использовать отдельный прокси-сервер или, например, установить сервис Squid на Обрабатывающий сервер Kaspersky Web Traffic Security.Suggested software balancer:



#ИстиннаяБезопасность
#HuMachine

www.kaspersky.ru