kaspersky

Kaspersky Web Traffic Security

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 6.2.0.155

kaspersky

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Дата редакции документа: 30.09.2025

https://www.kaspersky.ru
https://support.kaspersky.ru

О "Лаборатории Касперского" https://www.kaspersky.ru/about/company

kaspersky

Содержание

kaspersky

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Web Traffic Security" (далее также "программа", "приложение").

Подготовительные процедуры изложены в разделах "Установка и первоначальная настройка приложения", "Начало работы с приложением" и "Процедура приемки" и содержат процедуры безопасной установки и первоначальной настройки приложения, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе "Требования" приведены минимально необходимые системные требования для безопасной установки приложения.

Остальные разделы этого документа представляют собой руководство по эксплуатации. Руководство по эксплуатации содержит сведения о том, как осуществлять безопасное администрирование приложения, а также инструкции и указания по безопасному использованию приложения.

В документе также содержатся разделы с дополнительной информацией о приложении.

Документ адресован техническим специалистам, в обязанности которых входит установка, эксплуатация и администрирование Kaspersky Web Traffic Security, а также поддержка организаций, использующих Kaspersky Web Traffic Security.

kaspersky

Источники информации о приложении

Указанные источники информации о приложении (в частности, электронная справка) созданы для удобства пользователя и не являются полноценным эквивалентом этого документа.

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Web Traffic Security:

- страница Kaspersky Web Traffic Security на веб-сайте "Лаборатории Касперского";
- страница Kaspersky Web Traffic Security на веб-сайте Службы технической поддержки (База знаний);
- электронная справка;
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского".
Для использования источников информации на веб-сайтах требуется подключение к интернету.

Страница Kaspersky Web Traffic Security на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Web Traffic Security (https://www.kaspersky.com/small-to-medium-business-security/proxy-web-traffic) вы можете получить общую информацию о приложении, его возможностях и особенностях работы.

Страница Kaspersky Web Traffic Security содержит ссылку на интернет-магазин. В нем вы можете приобрести приложение или продлить право пользования приложением.

Страница Kaspersky Web Traffic Security в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Web Traffic Security в Базе знаний https://support.kaspersky.com/kwts/6.2?page=kb вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Web Traffic Security, но и к другим приложениям "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Электронная справка Kaspersky Web Traffic Security (справка веб-интерфейса)

С помощью веб-интерфейса вы можете управлять Kaspersky Web Traffic Security через браузер. Справка содержит информацию о том, как управлять защитой, настраивать параметры программы и решать основные задачи пользователя через веб-интерфейс Kaspersky Web Traffic Security (далее также "веб-интерфейс").

Обсуждение программ "Лаборатории Касперского" на форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории

Касперского" и с другими пользователями на нашем Форуме (https://forum.kaspersky.com/forum/%D1%80%D1%83%D1%81%D1%81%D0%BA%D0%BE%D1%8F%D0%B7%D1%8B%D1%87%D0%BD%D1%8B%D0%B9-%D1%84%D0%BE%D1%80%D1%83%D0%BC-162/).

На Форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

kaspersky

О Kaspersky Web Traffic Security

Программное изделие Kaspersky Web Traffic Security представляет собой средство антивирусной защиты и предназначено для применения на серверах информационных систем. Основными угрозами, для противостояния которым используется Kaspersky Web Traffic Security, являются угрозы, связанные с внедрением в информационные системы из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и /или съемных машинных носителей информации, вредоносных компьютерных программ (вирусов) (КВ). В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению программой;
- управление работой программы;
- управление параметрами программы;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных компьютерных программ (вирусов) (БД ПКВ);
- аудит безопасности программы;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия;
- сигнализация программы;
- фильтрация сообщений протокола ICAP;
- идентификация и аутентификация.

Kaspersky Web Traffic Security – это решение для защиты HTTP-, HTTPS- и FTP-трафика, проходящего через прокси-сервер.

Приложение обеспечивает защиту пользователей корпоративной сети при работе с веб-ресурсами: удаляет вредоносные программы и другие программы, представляющие угрозу, из потока данных, поступающего в корпоративную сеть из интернета по протоколам HTTP(S) и FTP, блокирует зараженные и фишинговые веб-сайты, а также контролирует доступ к веб-ресурсам на основании категорий веб-ресурсов и типов контента.

Приложение разработано для корпоративных пользователей.

Kaspersky Web Traffic Security позволяет:

- Защищать IT-инфраструктуру вашей организации от большинства современных вредоносных программ и программ-шифровальщиков благодаря использованию алгоритмов машинного обучения и технологии эмуляции данных в операционных системах.
- Блокировать доступ к зараженным и фишинговым сайтам.
- Использовать данные Kaspersky Security Network для получения информации о репутации файлов и веб-ресурсов, обеспечения более высокой скорости реакции приложений "Лаборатории Касперского" на угрозы, не дожидаясь обновления баз приложения, а также снижения вероятности ложных срабатываний.
- Интегрироваться с приложением "Лаборатории Касперского" Kaspersky Private Security Network (далее также "KPSN"), чтобы получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в Kaspersky Security Network со своих

компьютеров.

- Проверять зашифрованный трафик при замене сертификата на стороне прокси-сервера.
- Выполнять контентную фильтрацию входящих и исходящих файлов по URL-адресу, имени файла, MIME-типу, размеру, типу исходного файла (приложение позволяет определять истинный формат и тип файла, независимо от его расширения), контрольной сумме (MD5 или SHA256).
- Ограничивать доступ к различным категориям веб-ресурсов (далее также "веб-категории"), например: Азартные игры, лотереи, тотализаторы; Для взрослых; Детский интернет; Запрещено законодательством Российской Федерации.
- Настраивать параметры приложения и управлять приложением через веб-интерфейс.
- Осуществлять мониторинг состояния работы приложения, веб-трафика, обрабатываемого приложением, количества проверенных и обнаруженных объектов, последних угроз, заблокированных пользователей и URL-адресов в веб-интерфейсе приложения.
- Создавать рабочие области для настройки индивидуальных правил обработки трафика подразделений организаций или управляемых организаций (для интернет-провайдеров).
- Настраивать права доступа администраторов для работы с управляемыми организациями.
- Расследовать инциденты доступа в интернет с помощью поиска и просмотра событий.
- Корректировать условия обработки трафика в случаях, если обработка трафика не соответствует заданным правилам.
- Обновлять базы приложения с серверов обновлений "Лаборатории Касперского" или настраиваемых ресурсов (HTTP-серверов, разделяемых сетевых папок) по расписанию или по требованию.

  Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

- Интегрироваться с Microsoft® Active Directory® для назначения ролей и управления правилами доступа и защиты. Реализована поддержка NTLM- и Kerberos-аутентификации в Active Directory для доступа к веб-интерфейсу.
- Получать доступ к информации о приложении по протоколу SNMP.
- Публиковать события программы в SIEM-систему, которая уже используется в вашей организации, по протоколу Syslog. Информация о каждом событии передается как отдельное syslog-сообщение.

Kaspersky Web Traffic Security соответствует Общему регламенту по защите данных (General Data Protection Regulation, GDPR) и применимым законам Европейского союза о конфиденциальной информации, персональных данных и защите данных.

В этом разделе

kaspersky

Интерфейс Kaspersky Web Traffic Security

Работа с приложением осуществляется через веб-интерфейс.

Окно веб-интерфейса приложения содержит следующие элементы:

- разделы в левой части окна веб-интерфейса приложения;
- вкладки в верхней части окна веб-интерфейса приложения для некоторых разделов приложения;
- рабочую область в нижней части окна веб-интерфейса приложения.

Разделы окна веб-интерфейса приложения

Веб-интерфейс приложения содержит следующие разделы:

- **Мониторинг**. Содержит данные мониторинга Kaspersky Web Traffic Security.
- **Отчеты**. Позволяет формировать отчеты о работе приложения.
- **События**. Содержит информацию о событиях, обнаруженных в сетевом трафике.
- **Правила**. Позволяет работать с правилами обработки трафика.
- **Рабочие области**. Позволяет работать с рабочими областями и распределять сетевой трафик.
- **Пользователи**. Позволяет управлять пользователями приложения.
- **Узлы**. Позволяет управлять узлами кластера.
- **Параметры**. Содержит разделы **Общие**, **Внешние службы**, **Журналы и события**, **Доступ к программе**, в которых вы можете настраивать параметры приложения.

Рабочая область окна веб-интерфейса приложения

В рабочей области отображается информация, просмотр которой вы выбираете в разделах и на вкладках окна веб-интерфейса приложения, а также элементы управления, с помощью которых вы можете настроить отображение информации.

Принцип работы приложения

Kaspersky Web Traffic Security проверяет HTTP-, HTTPS- и FTP-трафик пользователей, проходящий через прокси-сервер. Если по результатам проверки исходящий запрос к запрашиваемому веб-ресурсу разрешен и в трафике не содержится вирусов и других угроз, то запрос передается через прокси-сервер на веб-сервер. Аналогичным образом обрабатывается ответ веб-сервера.

При установке приложения Kaspersky Web Traffic Security используется внешний прокси-сервер. Он может быть установлен на одном физическом сервере с приложением или на отдельном физическом сервере. Администрирование и настройка внешнего прокси-сервера осуществляется средствами операционной системы.

Принцип работы приложения Kaspersky Web Traffic Security представлен на рисунке ниже.

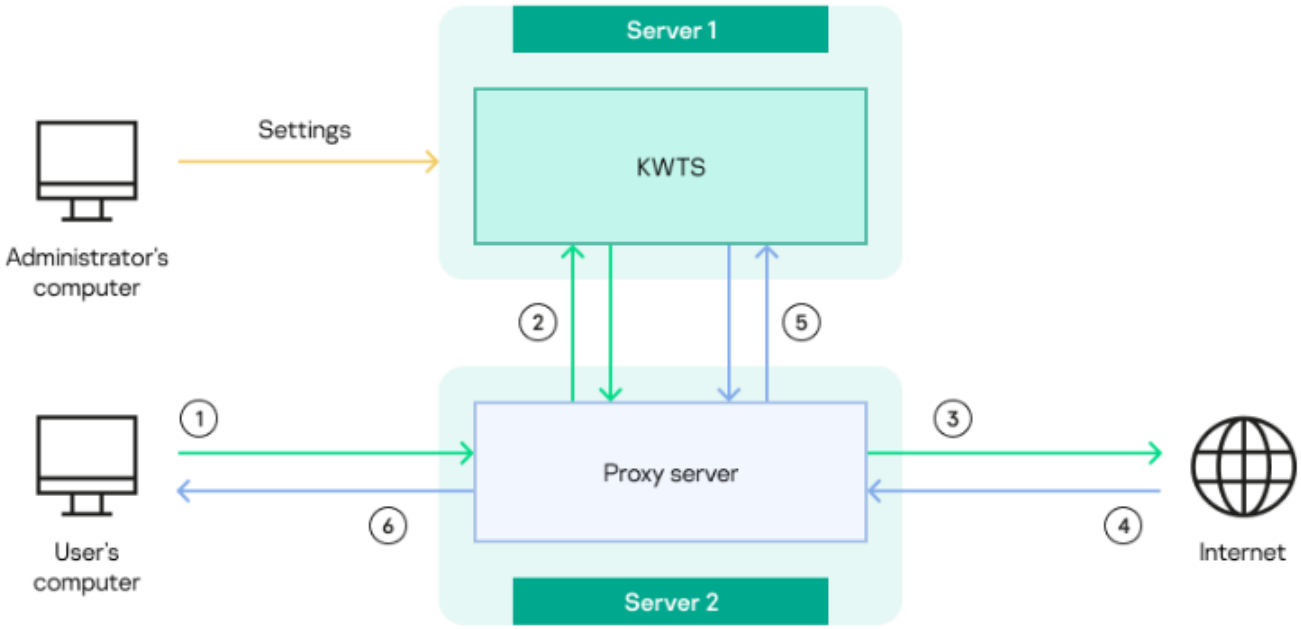

Рисунок 1. Принцип работы приложения Kaspersky Web Traffic Security

Нумерация на рисунке соответствует следующим этапам обработки трафика:

1. Пользователь запрашивает доступ к веб-ресурсу. Этот запрос передается на прокси-сервер.
2. Прокси-сервер передает запрос на узел кластера, обрабатывающий трафик. Приложение проверяет запрос по правилам обработки трафика (см. раздел "Работа с правилами обработки трафика" на стр. 80), полученным от Управляющего узла. После этого результат проверки передается прокси-серверу.
3. Если доступ к веб-ресурсу разрешен, то прокси-сервер отправляет запрос на веб-сервер для доступа к запрашиваемому веб-ресурсу.
4. Веб-сервер, на котором располагается запрашиваемый веб-ресурс, отправляет ответ прокси-серверу.
5. Ответ также отправляется на узел кластера для проверки по правилам обработки трафика.
6. После проверки прокси-сервер направляет ответ на компьютер пользователя. В зависимости от

заданных в приложении действий пользователю могут отобразиться следующие страницы:

- Если доступ к веб-ресурсу разрешен, отображается запрошенная веб-страница.
- Если доступ к веб-ресурсу запрещен, отображается страница блокировки (на стр. 160).
- Если было применено действие **Перенаправить**, отображается веб-страница, на которую выполнено перенаправление.

Рекомендуется дополнительно настроить обработку HTTPS-трафика (см. раздел "Настройка SSL Bumping в сервисе Squid" на стр. 256) на внешнем прокси-сервере.

При обработке трафика приложение может использовать информацию об учетных записях пользователей и их принадлежности к доменным группам. Для этого нужно настроить интеграцию Kaspersky Web Traffic Security с Active Directory. Интеграция с Active Directory позволяет использовать автоподстановку учетных записей при работе с ролями пользователей в приложении, а также распознавать учетные записи пользователей при создании рабочих областей и правил обработки трафика. Первичная аутентификация пользователей будет осуществляться на прокси-сервере. Информацию, полученную от Active Directory, прокси-сервер передает приложению вместе с исходным запросом пользователя. При этом прокси-сервер и узлы приложения будут взаимодействовать с сервером Active Directory независимо друг от друга. Принцип работы приложения при настроенной интеграции с Active Directory представлен на рисунке ниже.

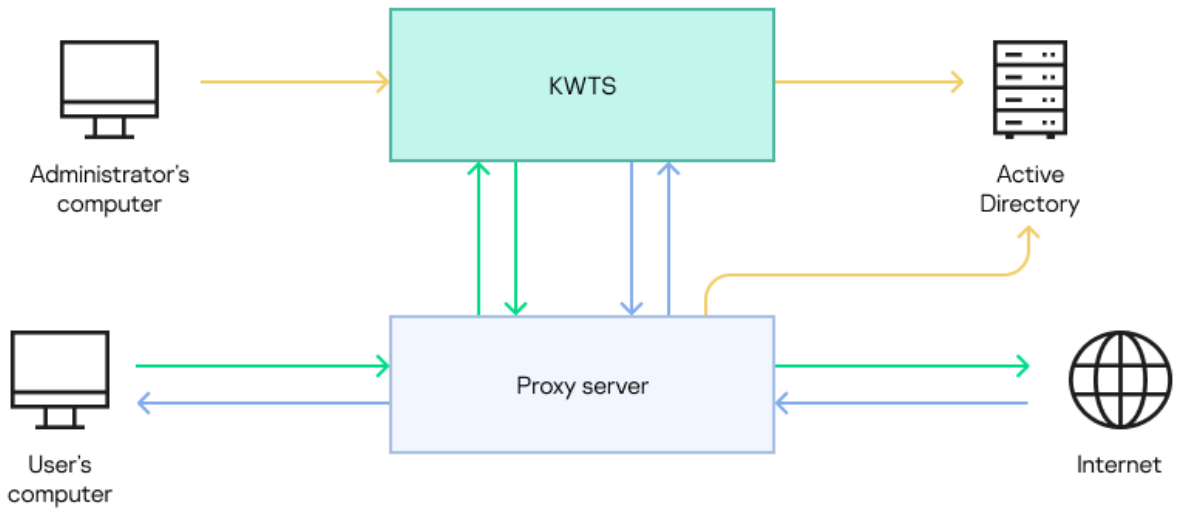

Рисунок 2. Принцип работы приложения при настроенной интеграции с Active Directory

В этом разделе

Работа приложения в кластере

Если для обработки трафика требуется два и более сервера с установленным приложением, то все серверы объединяются в *кластер*. В кластере необходимо назначить одному из серверов роль *Управляющий узел*. Остальные серверы получат роль *Подчиненный узел*. Вы можете настроить обработку трафика на всех узлах, в том числе и на Управляющем узле. Отличие Управляющего узла от Подчиненных узлов состоит в том, что на Управляющем узле вы можете изменять параметры приложения. С Управляющего узла они распространяются на все Подчиненные узлы в кластере. После этого каждый узел кластера обменивается данными с сервером Active Directory независимо от Управляющего узла и других Подчиненных узлов. Схема взаимодействия компонентов представлена на рисунке ниже.

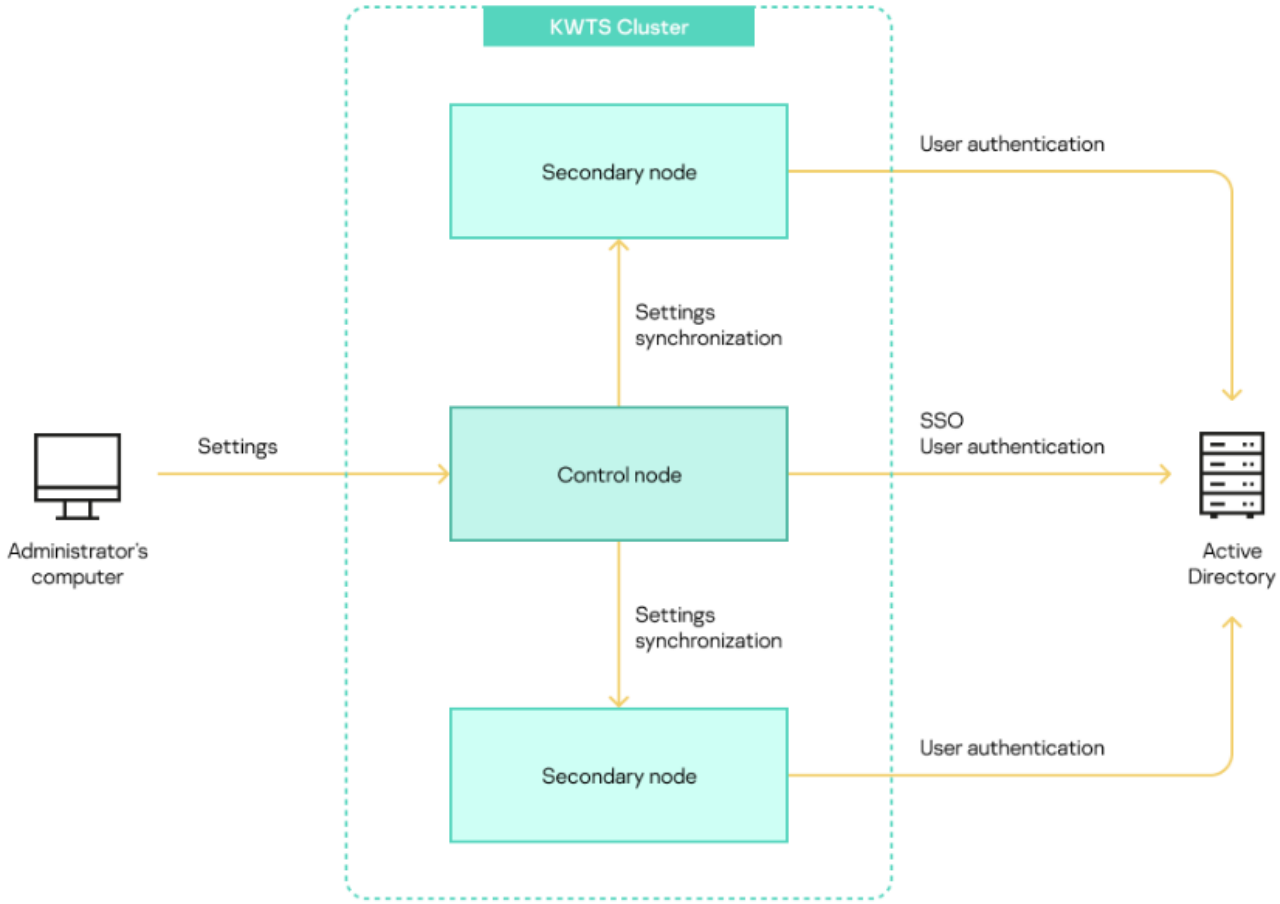

Рисунок 3. Схема взаимодействия компонентов приложения

Если Управляющий узел выходит из строя, приложение переходит в аварийный режим (см. раздел "Работа приложения в аварийном режиме" на стр. 137). В этом случае администратору требуется назначить одному из Подчиненных узлов роль Управляющего узла. При этом обработка трафика не будет прервана. Все узлы продолжают обрабатывать сетевой трафик в соответствии с последними значениями параметров, полученными от Управляющего узла до перехода приложения в аварийный режим. Последующая настройка значений параметров осуществляется на новом Управляющем узле. Схема смены ролей при переходе приложения в аварийный режим представлена на рисунке ниже.

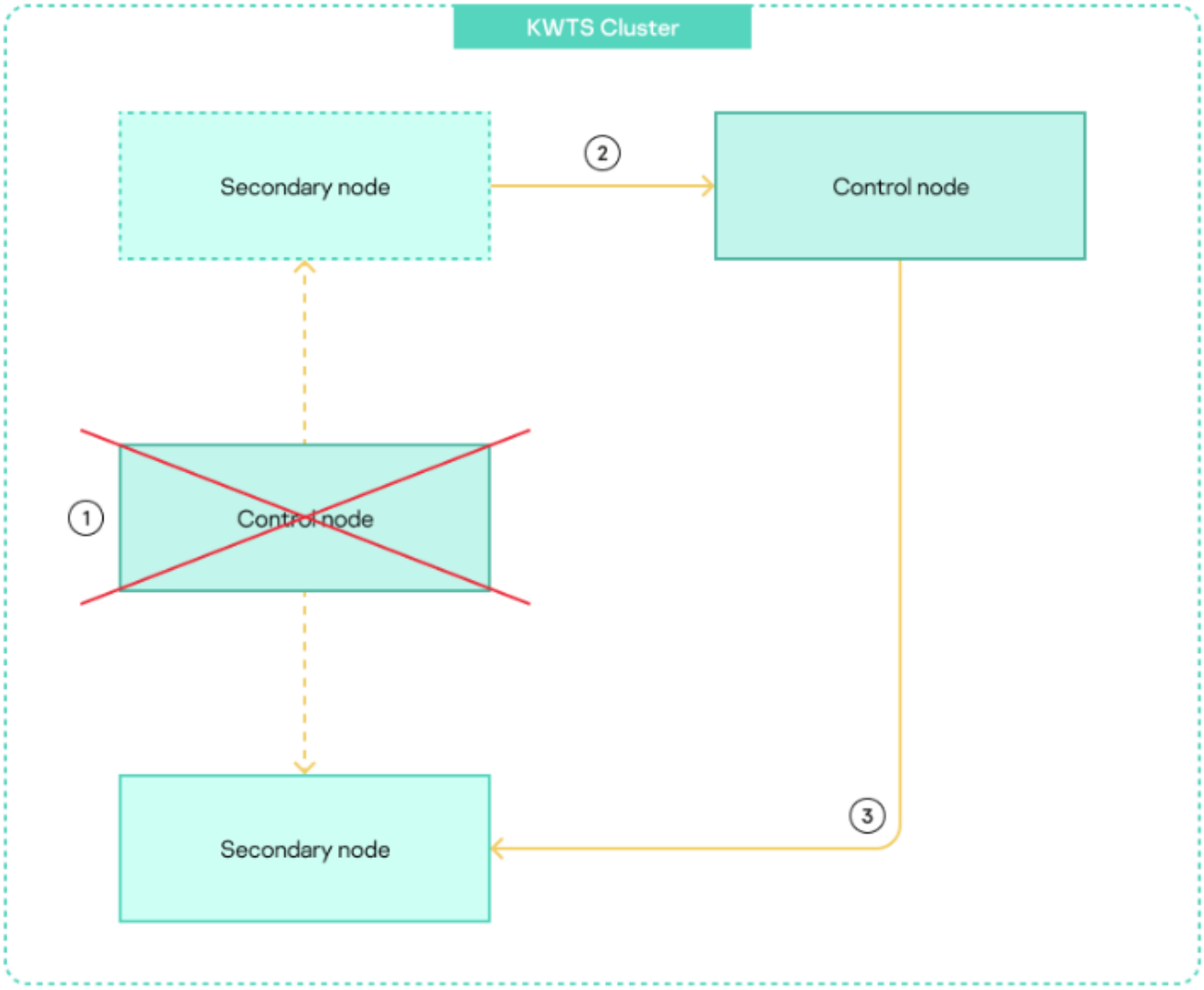

Рисунок 4. Схема смены ролей при переходе приложения в аварийный режим

Если объем обрабатываемого трафика предполагает большое количество узлов кластера, рекомендуется использовать балансировку нагрузки (см. раздел "Работа приложения с балансировщиком нагрузки" на стр. 19).

Работа приложения с балансировщиком нагрузки

При наличии нескольких узлов в кластере необходимо использовать внешний балансировщик для равномерного распределения нагрузки между узлами и обеспечения общей отказоустойчивости обработки

пользовательского трафика. Балансировщик контролирует доступность отдельных узлов кластера и определяет, на какой сервер направить запрос на проверку в соответствии с заданным способом балансировки.

При использовании внешнего прокси-сервера узлы Kaspersky Web Traffic Security выступают в роли ICAP-сервера, а прокси-сервер выступает в роли ICAP-клиента. В таком сценарии необходим балансировщик ICAP-трафика, например, вы можете использовать балансировщик нагрузки HAProxy (см. раздел "Приложение 5. Настройка балансировки ICAP с помощью HAProxy" на стр. 244). Схема подключения балансировщика представлена на рисунке ниже.

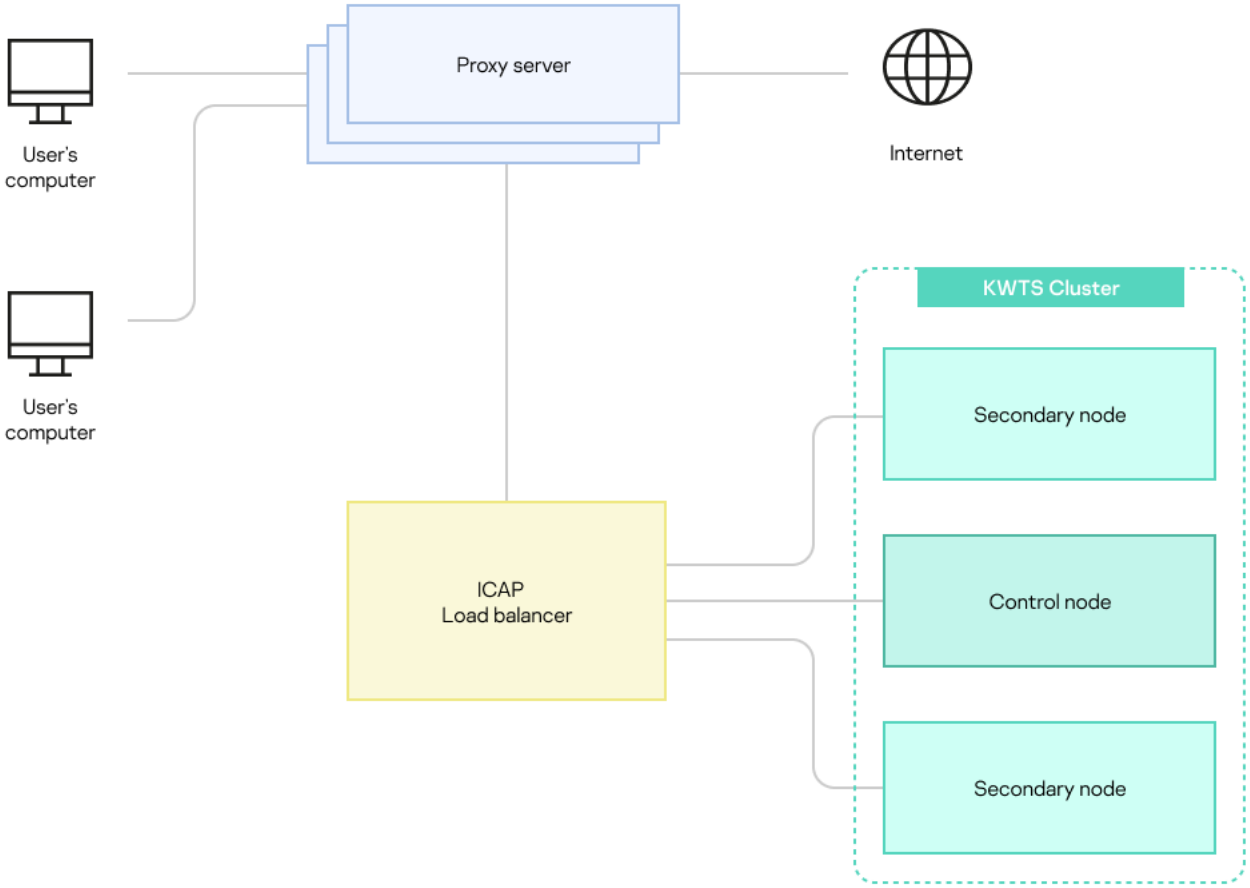

Рисунок 5. Схема подключения балансировщика при использовании внешнего прокси-сервера

Вместо внешнего прокси-сервера вы можете установить прокси-сервер Squid локально на каждом узле кластера, и использовать его для проверки пользовательского трафика. При такой схеме использования компьютеры пользователей подключаются к балансировщику, который обеспечивает перераспределение HTTP-запросов между узлами кластера. Принцип работы приложения с балансировщиком нагрузки представлен на рисунке ниже.

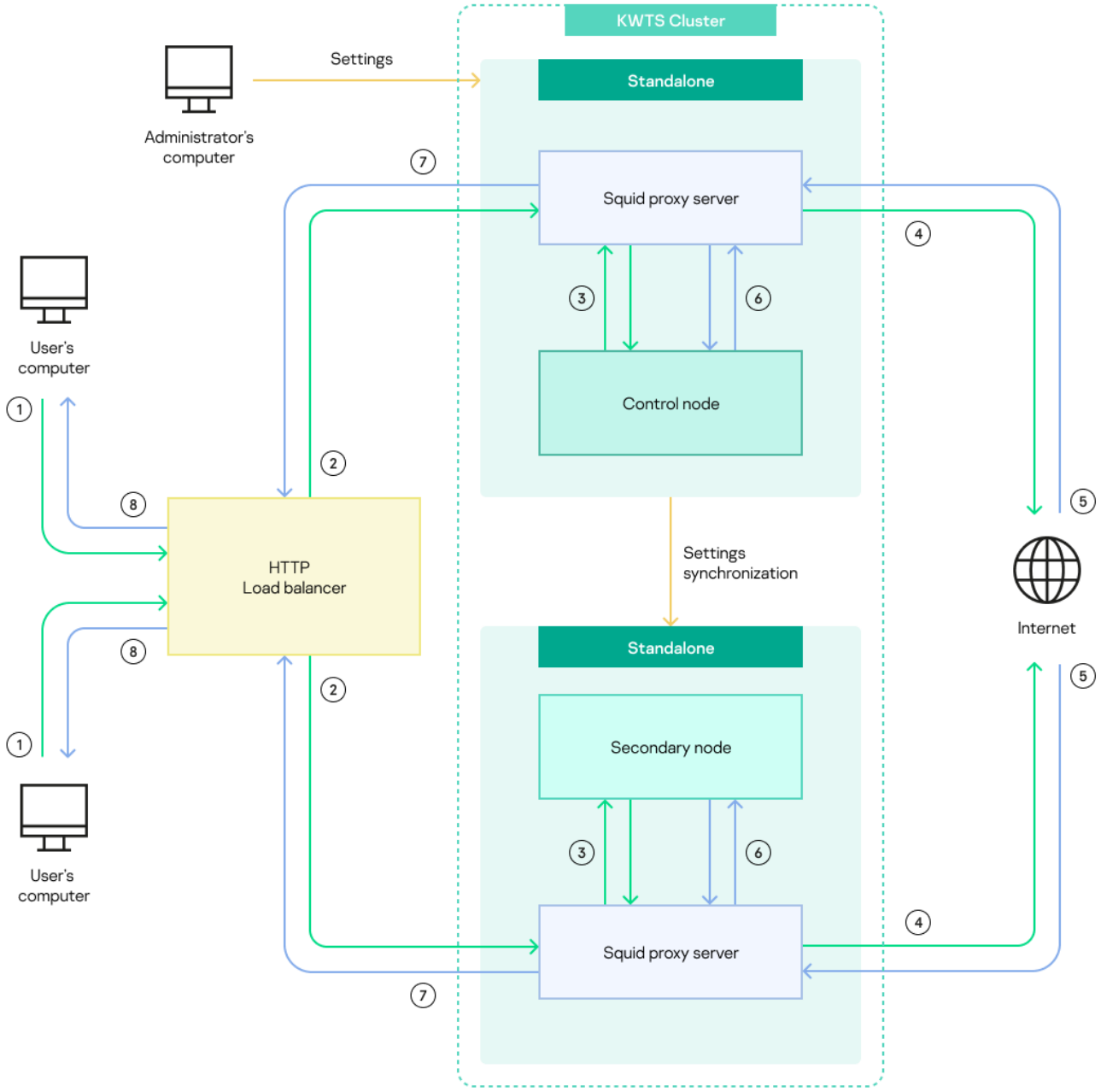

Рисунок 6. Схема подключения балансировщика при использовании локального прокси-сервера

Нумерация на рисунке соответствует следующим этапам обработки трафика:

1. Пользователь запрашивает доступ к веб-ресурсу. Этот запрос передается балансировщику нагрузки.
2. Балансировщик нагрузки выбирает узел кластера согласно заданному способу балансировки и

передает этому узлу запрос пользователя.

3. Прокси-сервер Squid выбранного узла принимает запрос и передает его ICAP-серверу приложения на проверку по правилам обработки трафика (см. раздел "Работа с правилами обработки трафика" на стр. 80).
4. Если по результатам проверки доступ к веб-ресурсу разрешен, прокси-сервер Squid отправляет запрос на веб-сервер в интернет.
5. Веб-сервер, на котором располагается запрашиваемый веб-ресурс, отправляет ответ прокси-серверу Squid.
6. Прокси-сервер Squid передает ответ веб-сервера ICAP-серверу приложения для проверки по правилам обработки трафика. Результат проверки возвращается на прокси-сервер Squid.
7. Прокси-сервер Squid передает ответ балансировщику нагрузки.
8. Балансировщик нагрузки направляет ответ на компьютер пользователя. В зависимости от заданных в приложении действий пользователю могут отобразиться следующие страницы:
   - Если доступ к веб-ресурсу разрешен, отображается запрошенная веб-страница.
   - Если доступ к веб-ресурсу запрещен, отображается страница блокировки (на стр. 160).
   - Если было применено действие **Перенаправить**, отображается веб-страница, на которую выполнено перенаправление.

Известные ограничения

В версии 6.2 известны следующие ограничения:

- Для Kaspersky Web Traffic Security 6.2 не поддерживается обновление с предыдущей версии. Доступна миграция с версии 6.1 на версию 6.2 (см. раздел "Миграция приложения с версии 6.1 на версию 6.2" на стр. 168).
- Подключение к веб-интерфейсу Подчиненного узла возможно только под учетной записью с правом **Создавать/изменять/удалять узлы**.
- В правиле обхода bypass по умолчанию установлен максимальный размер проверяемого файла 10 Мб. Для изменения значения необходимо отредактировать или отключить правило. Файлы больше указанного размера будут пропущены без проверки.

kaspersky

Требования

Этот раздел содержит аппаратные и программные требования для установки и работы приложения, а также указания по эксплуатации и требования к среде.

В этом разделе

Аппаратные и программные требования

Минимальные аппаратные требования к серверам для установки Kaspersky Web Traffic Security

- 8 ядер процессора.
- 16 ГБ оперативной памяти.
- Раздел подкачки объемом не менее 8 ГБ.
- 200 ГБ на жестком диске, из которых:
  - 25 ГБ для хранения временных файлов;
  - 25 ГБ для хранения файлов журналов.

Программные требования

Указанные ниже программные требования содержат минимальные проверенные версии программных продуктов, необходимых для установки Kaspersky Web Traffic Security.

Операционная система сервера для установки Kaspersky Web Traffic Security:

- Astra Linux Special Edition РУСБ.10015-01 (уровень защиты "Смоленск"), с оперативным обновлением 1.7.6.UU2 (БЮЛЛЕТЕНЬ № 2024-1127SE17MD), ядро generic.
- Astra Linux Special Edition РУСБ.10015-01 (уровень защиты "Смоленск"), с оперативным обновлением 1.8.3 (БЮЛЛЕТЕНЬ № 2025-0811SE18), ядро generic.

На всех серверах, на которые планируется установка Kaspersky Web Traffic Security, должны быть выполнены следующие условия:

- В операционной системе установлена локаль en_US.UTF-8.
- Установлены пакеты sudo, less.
- В параметрах операционной системы настроена синхронизация времени и установлен один и тот же часовой пояс на всех серверах.
- Установлен веб-сервер Apache минимальной версии 2.4.57.
- При установке на операционную систему Astra Linux Special Edition 1.7: установлен пакет postgresql минимальной версии 11.22.
- При установке на операционную систему Astra Linux Special Edition 1.8: установлен пакет postgresql минимальной версии 15.13.

Дополнительные требования:

- HAProxy версии 1.8 или выше для балансировки нагрузки (устанавливается на отдельном сервере, не входит в комплект поставки).
- Если вы устанавливаете сервис Squid и приложение Kaspersky Web Traffic Security на одном сервере, требуется пакет squid-openssl версии не ниже 6.13. Если пакета требуемой версии нет на установочном диске операционной системы, вы можете выполнить установку из сетевого репозитория.

  Для обработки пользовательского веб-трафика приложением Kaspersky Web Traffic Security необходимо, чтобы в вашей сети был установлен и настроен прокси-сервер HTTP(S) с поддержкой ICAP-протокола и служб Request Modification (REQMOD) и Response Modification (RESPMOD). В качестве прокси-сервера рекомендуется использовать Squid. Совместимость с другим программным обеспечением не гарантируется.

- Если вам необходима функциональность SSL Bumping, убедитесь в том, что прокси-сервер Squid из сертифицированного репозитория Astra Linux SE 1.7 поддерживает эту функциональность.
- Если вам необходима обработка сетевых запросов с ненулевыми мандатными метками (см. раздел "Включение и выключение обработки сетевого трафика с ненулевой мандатной меткой" на стр. 156), а используемая версия сервиса Squid не поддерживает обработку таких сетевых запросов, вам требуется настроить механизм privsock в Astra Linux таким образом, чтобы Squid игнорировал мандатные метки. Подробнее о поддержке обработки мандатных меток сервисом Squid вы можете узнать в документации Astra Linux или обратившись в техническую поддержку Astra Linux.

  Если сервис Squid настроен таким образом, чтобы игнорировать мандатные метки, конфиденциальность передаваемых данных может быть нарушена. Такая настройка создает потенциальную угрозу информационной безопасности.

Программные требования к компьютерам интернет-пользователей:

- Windows® 10 (22H2).
- Windows 11 (23H2).

Программные требования к серверам для интеграции с LDAP-каталогом и настройки Kerberos- или NTLM-аутентификации с помощью технологии SSO:

- Windows Server® 2016 Standard.
- Windows Server 2019 Standard.
- Windows Server 2022 Standard.

На компьютере администратора для работы с Kaspersky Web Traffic Security через веб-интерфейс должен быть установлен один из следующих браузеров:

- Mozilla™ Firefox™ 127.0.2 или выше.
- Microsoft Edge 139.0.3405 или выше.
- Google Chrome™ 139.0.7258 или выше.

kaspersky

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление приложением должны осуществляться в соответствии с эксплуатационной документацией.
2. Приложение должно эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации приложения необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ приложения ко всем объектам информационной системы, которые необходимы приложению для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость приложения с контролируемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы приложения со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.
7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлено приложение.
8. Должна быть обеспечена синхронизация по времени между компонентами приложения, а также между приложением и средой его функционирования.
9. Персонал, ответственный за функционирование приложения, должен обеспечивать надлежащее функционирование приложения, руководствуясь эксплуатационной документацией.
10. Должна быть обеспечена доверенная связь между приложением и уполномоченными субъектами информационной системы (администраторами безопасности).
11. Функционирование приложения должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности приложения.
12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
13. Должна быть обеспечена защищенная область для выполнения функций безопасности приложения.
14. Управление атрибутами безопасности, связанными с доступом к функциям и данным приложения, должно предоставляться только уполномоченным ролям (администраторам приложения и информационной системы).
15. Администратор должен установить в среде ИТ максимальное число попыток неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.
16. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.

kaspersky

Лицензирование приложения

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием приложения Kaspersky Web Traffic Security.

В сертифицированной версии Kaspersky Web Traffic Security допускается активация только кодом активации. Иные способы активации ведут к выходу из безопасного состояния приложения.

В этом разделе

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать приложение.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с приложением.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Web Traffic Security.
- Прочитав документ license.txt. Этот документ включен в комплект поставки приложения.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки приложения. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку приложения и не должны использовать приложение.

kaspersky

О лицензии

Лицензия – это ограниченное по времени право на использование Kaspersky Web Traffic Security, предоставляемое вам на условиях заключенного Лицензионного договора (Лицензионного соглашения).

Список доступных функций и срок использования приложения зависят от лицензии, по которой используется приложение.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с приложением.

  Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Web Traffic Security прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

  Вы можете использовать приложение по пробной лицензии только в течение одного срока пробного использования.

- *Коммерческая* – платная лицензия.

  По истечении срока действия коммерческой лицензии приложение прекращает выполнять свои основные функции. Для продолжения работы Kaspersky Web Traffic Security вам нужно продлить срок действия коммерческой лицензии. После истечения срока действия лицензии вы не можете далее использовать приложение и должны удалить его с устройства.

  Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить непрерывность защиты устройства от угроз компьютерной безопасности.

О лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- идентификатор лицензии или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о приложении, которое можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать приложение по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать приложение в соответствии с условиями Лицензионного соглашения. Лицензионный ключ

создается специалистами "Лаборатории Касперского".

Для добавления ключа в приложение необходимо ввести *код активации*.

Ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если ключ заблокирован, для работы приложения требуется добавить другой ключ.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ, активирующий Kaspersky Web Traffic Security. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Web Traffic Security или после заказа пробной версии Kaspersky Web Traffic Security.

Чтобы активировать приложение с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Если код активации был потерян после активации приложения, свяжитесь с партнером "Лаборатории Касперского", у которого вы приобрели лицензию.

О предоставлении данных

Для работы приложения используются данные, на отправку и обработку которых требуется согласие администратора Kaspersky Web Traffic Security.

Вы можете ознакомиться с перечнем данных и условиями их использования, а также дать согласие на обработку данных в следующих соглашениях между вашей организацией и "Лабораторией Касперского":

- В Лицензионном соглашении.

  Согласно условиям принятого Лицензионного соглашения, вы соглашаетесь в автоматическом режиме предоставлять "Лаборатории Касперского" информацию, которая требуется для повышения уровня защиты IT-инфраструктуры организации. Эта информация перечислена в Лицензионном соглашении в пункте Условия обработки данных:

  - тип, версия и локализация приложения;
  - версии установленных обновлений приложения;
  - идентификатор компьютера;
  - идентификатор установки приложения;
  - код активации и уникальный идентификатор активации текущей лицензии;
  - тип, версия и разрядность операционной системы;
  - название виртуальной среды;
  - идентификаторы компонентов приложения, активных на момент предоставления информации.

  Вы можете в любой момент просмотреть текст Лицензионного соглашения в директории /opt/kaspersky/kwts/share/htdocs/<код языка>/eula.

- В Политике конфиденциальности.

- В Положении о Kaspersky Security Network и в Дополнительном Положении о Kaspersky Security Network.

  При участии в Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network и использование Kaspersky Private Security Network" на стр. 173) и при отправке KSN-статистики в "Лабораторию Касперского" может передаваться информация, полученная в результате работы приложения. Перечень передаваемых данных указан в Положении о Kaspersky Security Network и в Дополнительном Положении о Kaspersky Security Network. Вы можете просмотреть эти Положения в веб-интерфейсе в разделе **Параметры** → **Внешние службы** → **KSN/KPSN** → **Kaspersky Security Network (KSN)**.

Содержимое памяти и доступ учетных записей к персональным данным пользователей

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

Оперативная память Kaspersky Web Traffic Security может содержать любые обрабатываемые данные пользователей приложения. Администратору Kaspersky Web Traffic Security необходимо обеспечить безопасность этих данных самостоятельно.

По умолчанию доступ к персональным данным пользователей имеют следующие учетные записи:

- Учетные записи операционной системы:
  - Пользователь с привилегиями root.
  - kluser.
  - Пользователи, от имени которых запускаются процессы приложения:
    - Squid (далее – пользователь Squid);
    - Apache (далее – пользователь Apache).
  - Учетные записи, входящие в одну из следующих групп:
    - klusers.
    - kl_web_users.
    - kl_var_users.
- Учетная запись локального администратора Kaspersky Web Traffic Security.

Ограничение прав учетных записей

Учетные записи пользователей операционной системы не являются частью приложения. Эти учетные записи создаются на компьютере администратора, когда он самостоятельно устанавливает стороннее программное обеспечение (например, Squid).

Приложение не предоставляет возможностей для ограничения прав учетных записей пользователей операционной системы, на которой установлено приложение. Доступ к месту хранения данных ограничен средствами файловой системы. Администратору рекомендуется контролировать доступ к персональным данным других пользователей любыми системными средствами на его усмотрение.

Пользователь приложения, имеющий разрешение на создание и изменение учетных записей и ролей, может предоставить доступ к веб-интерфейсу. Доступ к персональным данным предоставляется согласно правам доступа для роли, которая привязана к учетной записи.

Передача данных между узлами кластера, подключение к Active Directory, обработка сетевого трафика, работа с приложением

Данные передаются между узлами кластера по зашифрованному каналу (по протоколу HTTPS с использованием авторизации с помощью сертификата безопасности). Данные передаются в веб-интерфейс по зашифрованному каналу по протоколу HTTPS. Локальный администратор авторизуется с помощью пароля, остальные пользователи веб-интерфейса проходят авторизацию по протоколу Kerberos или NTLM.

Подключение к Active Directory выполняется по зашифрованному каналу (SASL) с авторизацией по протоколу Kerberos.

При работе из командной строки сервера, на котором установлено приложение Kaspersky Web Traffic Security, администратор операционной системы может управлять параметрами дампа. Дамп формируется при сбоях приложения и может понадобиться при анализе причины сбоя. В дамп могут попасть любые данные, фрагменты анализируемого сетевого трафика или файлов.

Доступ к этим данным может быть осуществлен из командной строки сервера, на котором установлено приложение, под учетной записью администратора операционной системы.

При передаче диагностической информации в Службу технической поддержки "Лаборатории Касперского" администратору Kaspersky Web Traffic Security необходимо обеспечить безопасность дампов и файлов трассировки самостоятельно. Администратор Kaspersky Web Traffic Security несет ответственность за доступ к этой информации.

Получение диагностической информации с помощью утилиты collect_diag_info.py

В состав Kaspersky Web Traffic Security 6.2 входит утилита collect_diag_info.py (см. раздел "Получение информации с помощью утилиты collect_diag_info.py" на стр. 237), с помощью которой можно получить диагностическую информацию о состоянии Kaspersky Web Traffic Security в случае, если веб-интерфейс приложения недоступен. Утилита находится в директории /opt/kaspersky/kwts/bin. Утилиту следует запускать от имени пользователя root.

В результате работы утилиты создается архив с диагностической информацией. Архив располагается по пути, который указывает администратор при вызове утилиты. Созданному архиву утилита назначает следующие права:

- Для пользователя root: только на чтение и запись.
- Для остальных пользователей: запрет на чтение, запись и запуск.

В архиве с диагностической информацией могут содержаться следующие данные:

- Информация из сетевого трафика:
  - Имена учетных записей пользователей, инициировавших HTTP-запрос.
  - IP-адреса компьютеров, с которых был отправлен HTTP-запрос.
  - Клиентское приложение, инициировавшее HTTP-запрос.
  - URL-адреса веб-ресурсов, доступ к которым запрашивал пользователь.
  - Имена и размер проверяемых объектов, входящих в HTTP-сообщение.

- Данные об обновлениях приложения:
  - IP-адреса, используемые для скачивания обновлений.
  - IP-адреса источников обновлений.
  - Информация о скачиваемых файлах и скорости скачивания.
- Информация об учетных записях пользователей:
  - Имена учетных записей администраторов и пользователей веб-интерфейса приложения.
  - Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты.

После предоставления диагностической информации сотрудникам Службы технической поддержки "Лаборатории Касперского" администратору необходимо самостоятельно удалить архив, созданный утилитой.

Состав данных, которые могут храниться в приложении

Для ознакомления с полным перечнем данных пользователей, которые могут храниться в Kaspersky Web Traffic Security, см. таблицу ниже.

Таблица 1. Данные пользователей, которые могут храниться в Kaspersky Web Traffic Security

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
Основная функциональность приложения				
• Имена учетных записей администратора и пользователей приложения. • Права доступа учетных записей приложения. • Имя учетной записи и пароль подключения приложения к прокси-серверу. • Keytab-файлы и параметры подключения к LDAP-серверу.	Конфигурация приложения	/var/opt/kaspersky/kwts	Бессрочно.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
• Keytab-файлы для подключения по SSO Kerberos и параметры для подключения к NTLM-серверу. • Комментарии. • Код активации или ключ активации (используется для активации добавляемых узлов кластера, передается на сервер активации). • Публичные сертификаты веб-серверов узлов кластера.				• Пользователи веб-интерфейса приложения, имеющие права на просмотр параметров приложения и права на просмотр учетных записей.
Приватные сертификаты для установки TLS соединений.	Конфигурация приложения	/var/opt/kaspersky/kwts/certs/	Бессрочно.	• Пользователь root имеет доступ к месту хранения информации. • Пользователи kluser имеют доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их обработке.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
• Хеш пароля локального администратора. • Параметры интеграции с KATA.	Конфигурация приложения	/var/opt/kaspersky/kwts	Бессрочно.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их передаче между узлами.
• Имена учетных записей пользователей и контактов в LDAP и другие LDAP-атрибуты. • IP-адреса инициаторов сетевых запросов. • Комментарии.	Правила обработки трафика	/var/opt/kaspersky/kwts	Бессрочно.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие права на просмотр правил обработки трафика.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
• IP-адреса инициаторов сетевых запросов. • Имена учетных записей пользователей. • URL-адреса веб-ресурсов, к которым запрашивается доступ.	Статистика работы приложения	/var/opt/kaspersky/kwts	Бессрочно.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие права на просмотр отчетов и раздела **Мониторинг**. Если в настройках приложения включено использование SNMP, то к статистике работы приложения имеет доступ сервис snmpd, а также пользователь, от имени которого запущен сервис snmpd.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
Информация из запросов доступа к веб-ресурсам: • IP-адреса и User Agent инициаторов сетевых запросов. • URL-адреса веб-ресурсов, к которым запрашивается доступ. • Имена скачиваемых файлов. • Имена учетных записей пользователей в LDAP, контактов в LDAP и другие	Журнал событий обработки трафика	/var/opt/kaspersky/kwts	Согласно параметрам, заданным пользователем приложения. По умолчанию устанавливается срок хранения 3 дня или максимальный размер журнала 1 ГБ. При достижении этого ограничения более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие право на просмотр событий обработки почтового трафика.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
LDAP-атрибуты.		Зависит от параметров подсистемы журналирования из состава операционной системы. Пример места хранения: /var/log/messages.	Зависит от параметров подсистемы журналирования из состава операционной системы.	Пользователь root имеет доступ к месту хранения информации. Окончательный список пользователей зависит от прав доступа, выданных на файлы с сообщениями подсистемы журналирования. Права доступа выдает администратор операционной системы. Если будет выдан доступ на чтение пользователю kluser, информация станет доступна для просмотра следующим пользователям: • Пользователь Apache будет иметь доступ к данным при их передаче между узлами кластера, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие право на получение диагностической информации.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
• Имя учетной записи пользователя, инициировавшего событие. • IP-адрес и порт узла, на котором произошло событие. • Параметры события.	Журнал системных событий	/var/opt/kaspersky/kwts	Согласно параметрам, заданным пользователем приложения. По умолчанию устанавливается срок хранения 1100 дней или максимальный размер журнала 1 ГБ. При достижении этого ограничения более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие право на просмотр событий приложения.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
		Зависит от параметров подсистемы журналирования из состава операционной системы. Пример места хранения /var/log/messages.	Зависит от параметров подсистемы журналирования из состава операционной системы.	Пользователь root имеет доступ к месту хранения информации. Окончательный список пользователей зависит от прав доступа, выданных на файлы с сообщениями подсистемы журналирования. Права доступа выдает администратор операционной системы. Если будет выдан доступ пользователю kluser, информация станет доступна для просмотра следующим пользователям: • Пользователь Apache будет иметь доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие право на получение диагностической информации.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
Информация из запросов доступа к веб-ресурсам: • IP-адреса. • Имена учетных записей и домены пользователей. • URL-адреса веб-ресурсов, к которым запрашивается доступ. • Имена скачиваемых файлов. Данные об обновлениях приложения: • IP-адреса, используемые для скачивания	Файлы трассировки	/var/log/kaspersky/kwts	Бессрочно. При достижении объема 150 МБ для каждого потока трассировки более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при получении диагностической информации. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие права на получение диагностической информации.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
обновлений. • IP-адреса источников обновлений. • Информация о скачиваемых файлах и скорости скачивания. Информация об учетных записях пользователей: • Имена учетных записей администраторов и пользователей веб-интерфейса приложения. • Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты.		Зависит от параметров подсистемы журналирования из состава операционной системы. Пример места хранения /var/log/messages.	Зависит от параметров подсистемы журналирования из состава операционной системы.	Пользователь root имеет доступ к месту хранения информации. Окончательный список пользователей зависит от прав доступа, выданных на файлы с сообщениями подсистемы журналирования. Права доступа выдает администратор операционной системы. Если будет выдан доступ пользователю kluser, информация станет доступна для просмотра следующим пользователям: • Пользователь Apache будет иметь доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие право на получение диагностической информации.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
		/var/log/kaspersky/extra	Бессрочно. При достижении объема 400 МБ для каждого файла трассировки более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при получении диагностической информации и при записи событий в журнал. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие право на получение диагностической информации.
Информация из запросов доступа к веб-ресурсам: • Тела HTTP-сообщений, включая тела скачиваемых файлов и содержимое отправляемых веб-форм.	Временные файлы	• /tmp • /tmp/kwtstmp	Зависит от параметров операционной системы.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке.

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
Подключение через веб-интерфейс: • IP-адрес пользователя. • Имя учетной записи пользователя.	Журнал событий авторизации	Зависит от параметров подсистемы журналирования из состава операционной системы. Пример места хранения: /var/log/secure	Зависит от параметров подсистемы журналирования из состава операционной системы.	Окончательный список пользователей зависит от прав доступа, выданных на файлы с сообщениями подсистемы журналирования. Права доступа выдает администратор операционной системы.
Интеграция с приложением Kaspersky Anti Targeted Attack Platform (KATA)				
Информация из запросов доступа к веб-ресурсам: • Файлы пользователей.	Отправка объектов для проверки на сервере KATA	Данные не сохраняются.	Данные не сохраняются.	Нет значения.
Информация из обнаружений KATA: • MD5- или SHA256-хеш файла. • URL-адреса.	Получение объектов, обнаруженных приложением KATA.	/var/opt/kaspersky/kwts/detects.cache	Согласно параметру **Срок хранения кеша (часы)**, заданному пользователем приложения. По умолчанию установлено значение 48 часов.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке.
Интеграция с Active Directory®				

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
Атрибуты User Object: • distinguishedName • sAMAccountName • msDS-PrincipalName • userPrincipalName • canonicalName • displayName • cn • primaryGroupI • memberOf Атрибуты Contacts Object: • distinguishedName • displayName • cn • memberOf Атрибуты Group Object: • distinguishedName • canonicalName • objectSid • memberOf	• Правила обработки трафика. • Аутентификация с помощью технологии единого входа. • Автозаполнение учетных записей при работе с ролями и правами пользователей, а также при настройке правил обработки трафика.	• /var/opt/kaspersky/kwts/ldap/cache.dbm • /var/opt/kaspersky/kwts/ldap/storage	Бессрочно. Данные регулярно обновляются. При отключении интеграции приложения с Active Directory данные удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Пользователь Apache имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса приложения, имеющие права на просмотр разделов приложения, где есть элемент интерфейса с функцией автозаполнения учетных записей.
Взаимодействие между веб-интерфейсом и серверной частью				
• Сертификаты для установки TLS-соединений. • Файлы приватных ключей сертификатов.	Безопасное взаимодействие с серверной частью	/var/opt/kaspersky/kwts/certs/	Бессрочно	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке.

Состав данных, передаваемых в службу Kaspersky Security Network (KSN)

Данные передаются на серверы KSN в зашифрованном виде. По умолчанию доступ к данным имеют специалисты "Лаборатории Касперского", учетная запись root, а также учетная запись kluser, от имени которой работают компоненты приложения.

Для ознакомления с полным перечнем данных пользователей, передаваемых в службу KSN, см. таблицу ниже.

Указанные данные передаются только в случае согласия на участие в Kaspersky Security Network (см. раздел "Настройка участия в Kaspersky Security Network" на стр. 174).

Таблица 2. Данные, передаваемые в службу Kaspersky Security Network

Тип данных	Где используются данные	Место хранения	Срок хранения
Информация о проверяемых объектах: • Имя и размер проверяемого объекта. • Контрольные суммы (MD5, SHA2-256) объекта. • Идентификатор типа файла. • Идентификатор формата файла. • Название обнаруженной угрозы согласно классификации АО "Лаборатория Касперского". • Идентификатор антивирусных баз и идентификатор записи в антивирусных базах, которые использовались для проверки объекта. • Дата и время выпуска антивирусных баз. • URL-адрес, с которого загружается объект. • Имя файла процесса, выполнившего загрузку объекта или получение сообщения или ссылки. • Отпечаток сертификата и контрольная сумма (SHA256) публичного ключа сертификата подписанного файла. Информация для определения репутации файлов и URL-адресов: • Контрольная сумма проверяемого файла (MD5). • URL-адрес, репутация которого запрашивается. • Идентификатор протокола соединения и номер используемого порта.	Отправка KSN-запросов	/var/opt/kaspersky/kwts/	Бессрочно

Тип данных	Где используются данные	Место хранения	Срок хранения
Информация об установленном программном обеспечении (далее также ПО) и компьютере: • Уникальный идентификатор компьютера, на котором установлено ПО. • Уникальный идентификатор установки ПО на компьютере.	KSN-статистика	/var/opt/kaspersky	До отправки статистики в KSN. После отключения отправки KSN-статистики в параметрах приложения данные удаляются при следующей попытке отправки.

Тип данных	Где используются данные	Место хранения	Срок хранения
• Полная версия установленного ПО. • Идентификатор типа ПО. • Информация об операционной системе, установленной на компьютере: тип, версия, редакция, разрядность и параметры режима работы. • Информация об установленных пакетах обновлений. • IP-адрес пользователя, запросившего ресурс. Информация о результатах проверки URL-адресов модулем Антивирус или Анти-Фишинг: • URL-адрес, в котором обнаружены угрозы модулем Антивирус или Анти-Фишинг. • URL-адрес исходной страницы или адрес страницы, с которой пользователь был перенаправлен на данный URL. • Дата и время выпуска баз модулей Антивирус и Анти-Фишинг. • Название организации и веб-сайт, на которые производилась атака. • Информация о результатах проверки модулей Антивирус и Анти-Фишинг: значение уровня доверия, вес и статус решения. • Время события. Информация о проверяемых объектах: • Имя и размер проверяемого объекта. • Контрольные суммы (MD5, SHA2-256) объекта. • Идентификатор типа файла. • Идентификатор формата файла. • Название обнаруженной угрозы согласно классификации АО "Лаборатория Касперского". • Идентификатор антивирусных баз и идентификатор записи в антивирусных базах, которые использовались для проверки объекта.			

Тип данных	Где используются данные	Место хранения	Срок хранения
• Дата и время выпуска антивирусных баз. • URL-адрес, с которого загружается объект. • Имя файла процесса, выполнившего загрузку объекта или получение сообщения или ссылки. Данные об ошибках, возникших в работе компонентов ПО: • Идентификатор компонента ПО, в котором произошла ошибка. • Идентификатор типа ошибки. • Фрагменты отчетов о работе компонентов. Данные об обновлении антивирусных баз и компонентов ПО: • Версия компонента, на котором выполняется обновление баз. • Код ошибки обновления баз в случае ее возникновения. • Статус ПО после выполнения задачи обновления баз. • Количество неуспешных завершений обновления баз и количество аварийных завершений работы компонента, на котором выполнялось обновление баз, за все время его работы. Информация о работе компонента Updater: • Версия компонента Updater. • Статус завершения задачи обновления компонента Updater. • Тип и идентификатор ошибки при обновлении компонента Updater в случае ее возникновения. • Код завершения задачи обновления компонента Updater. • Количество аварийных завершений работы компонента Updater при выполнении задач обновления за время работы этого компонента. • Количество неуспешных завершений задач обновления компонента Updater.			

Обновление баз приложения с серверов "Лаборатории Касперского"

При обновлении баз приложения с серверов "Лаборатории Касперского" передается следующая информация:

- тип и версия приложения;
- уникальный идентификатор действующего лицензионного ключа;
- уникальный идентификатор установки приложения;
- идентификатор сессии обновления.

Просмотр информации о лицензии и активации приложения

► *Чтобы просмотреть информацию о лицензии:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. В блоке **Лицензия** перейдите по ссылке **Подробные сведения**.

   Откроется окно **Лицензия**.

В окне отображается информация о лицензиях на серверах с установленным приложением.

► *Чтобы просмотреть информацию об активации приложения,*

в окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Лицензирование**.

В окне отображается информация об активации приложения или поле для ввода кода активации, если приложение не было активировано.

Активация приложения

Для активации приложения необходимо добавить лицензионный ключ. Для добавления лицензионного ключа необходимо ввести код активации.

► *Чтобы ввести код активации:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Лицензирование**.
2. В поле **Ввести код активации** введите код активации приложения в формате XXXXX-XXXXX-XXXXX-XXXXX, где X может быть буквами латинского алфавита (A-Z, кроме O и I (прописная i)) или цифрами (0-9).
3. Нажмите на кнопку **Активировать**.

Код активации будет отправлен на серверы активации "Лаборатории Касперского" для проверки.

Если введенный код неверен, отобразится сообщение о вводе ошибочного кода. Вы можете повторить попытку ввода кода активации.

Если введенный код верен, отобразится статус **Код активации успешно применен. Проверьте состояние активации программы на узлах кластера**.

Удаление лицензионного ключа

► *Чтобы удалить лицензионный ключ:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Лицензирование**.
2. Нажмите на кнопку **Удалить**.

   Отобразится подтверждение удаления лицензионного ключа.
3. Нажмите на кнопку **Да**.

Лицензионный ключ будет удален.

kaspersky

Установка и первоначальная настройка приложения

Установка и первоначальная настройка приложения состоит из следующих этапов:

1. **Подготовка к установке приложения (на стр. 51)**
2. **Установка пакета приложения (на стр. 53)**
3. **Установка пакета локализации (на стр. 54)**
4. **Настройка приложения с помощью скрипта настройки (см. раздел "Настройка приложения вручную" на стр. 55)**
5. **Установка сервиса Squid (на стр. 255)**

   Этот шаг следует выполнить, если вы не используете отдельный прокси-сервер и хотите установить сервис Squid.
6. **Настройка сервиса Squid (на стр. 255)**

   Этот шаг следует выполнить, если вы установили сервис Squid.
7. **Настройка SSL Bumping в сервисе Squid (на стр. 256)**

   Этот шаг следует выполнить, если вы установили сервис Squid.

После установки приложение начинает записывать информацию, связанную с работой его компонентов, в журнал событий Kaspersky Web Traffic Security (см. раздел "Журнал событий Kaspersky Web Traffic Security" на стр. 76), в журнал событий Syslog (см. раздел "Журнал событий Syslog" на стр. 189), а также в файлы трассировки (см. раздел "Получение информации для Службы технической поддержки" на стр. 235) в соответствии с заданным уровнем трассировки. Более подробную информацию см. в разделе О предоставлении данных (на стр. 28).

После первоначальной настройки приложения вам нужно объединить все узлы в кластер для управления приложением через веб-интерфейс (см. раздел "Управление кластером" на стр. 130).

В этом разделе

kaspersky

Подготовка к установке приложения

► *Чтобы подготовиться к установке приложения Kaspersky Web Traffic Security:*

1. Убедитесь, что сервер удовлетворяет аппаратным и программным требованиям (см. раздел "Аппаратные и программные требования" на стр. 23).
2. Скопируйте следующие файлы из комплекта поставки на сервер:
   - Пакет приложения Kaspersky Web Traffic Security в формате DEB.
   - Пакеты локализации Kaspersky Web Traffic Security в формате DEB.
   - Файл с ключом в формате GPG для работы в режиме замкнутой программной среды (при установке на операционную систему Astra Linux Special Edition).
3. Удалите приложение Kaspersky Web Traffic Security предыдущей версии, следуя инструкции по удалению для этой версии. Установка поверх предыдущей версии не поддерживается.
4. Проверьте, что в операционной системе установлена локаль en_US.UTF-8 (см. раздел "Установка локали en_US.UTF-8 в операционной системе" на стр. 52), и при необходимости установите ее.

   В процессе работы скрипта первоначальной настройки (см. раздел "Настройка приложения вручную" на стр. 55) приложения вам будут показаны тексты Лицензионного соглашения и Политики конфиденциальности. Для их корректного отображения убедитесь в том, что ваш терминал поддерживает отображение символов на языке, который вы выберете для просмотра текстов Лицензионного соглашения и Политики конфиденциальности.
5. При необходимости выполните команды по настройке Astra Linux Special Edition для установки Kaspersky Web Traffic Security в режиме замкнутой программной среды.
6. Убедитесь, что на межсетевом экране открыты необходимые доступы (см. раздел "Настройка сетевых доступов" на стр. 63).
7. Убедитесь, что установлены пакеты sudo и less. При необходимости установите их при помощи пакетного менеджера операционной системы.
8. Убедитесь, что веб-сервер установлен и запущен, а также активированы необходимые модули. Следуйте инструкции по установке веб-сервера (см. раздел "Установка веб-сервера" на стр. 53).
9. Если вы устанавливаете Kaspersky Web Traffic Security на операционную систему Astra Linux Special Edition, убедитесь, что установлен пакет postgresql. При необходимости установите его с помощью пакетного менеджера операционной системы.

В этом разделе

kaspersky

Подготовка к установке в Astra Linux Special Edition в режиме замкнутой программной среды

Администратору требуется выполнить подготовительные действия для установки Kaspersky Web Traffic Security в операционной системе Astra Linux Special Edition 1.7 или 1.8 в режиме замкнутой программной среды.

► *Чтобы установить Kaspersky Web Traffic Security в режиме замкнутой программной среды:*

1. Создайте директорию для ключа Kaspersky Web Traffic Security с помощью команды:

   ```
   mkdir -p /etc/digsig/keys/kaspersky/
   ```

2. Скопируйте файл kaspersky_kwts_pub_key_339cc887.gpg из состава дистрибутива приложения в директорию, созданную на предыдущем шаге, с помощью команды:

   ```
   cp kaspersky_kwts_pub_key_339cc887.gpg /etc/digsig/keys/kaspersky/
   ```

3. Обновите образ initramfs с помощью команды:

   ```
   update-initramfs -u -k all
   ```

4. Перезагрузите сервер.

В результате приложение Kaspersky Web Traffic Security может быть установлено в режиме замкнутой программной среды.

Установка локали en_US.UTF-8 в операционной системе

Для корректной работы Kaspersky Web Traffic Security в операционной системе должна быть установлена локаль en_US.UTF-8. Если этой локали в системе нет, ее необходимо установить.

► *Чтобы проверить наличие локали en_US.UTF-8:*

1. Выполните команду:

   ```
   locale -a
   ```

2. Проверьте, есть ли списке локаль en_US.UTF-8 или en_US.utf8.

Если локаль уже установлена, дополнительных действий не требуется.

► *Чтобы установить локаль en_US.UTF-8:*

1. Выполните следующие команды:

   ```
   apt install locales
   ```

   ```
   dpkg-reconfigure locales
   ```

2. В интерактивном мастере выберите требуемую локаль в списке для установки и подтвердите изменения.

   Локаль будет добавлена в операционную систему.

3. Проверьте, что локаль была успешно добавлена. Для этого выполните команду:

   ```
   locale -a
   ```

kaspersky

Установка веб-сервера

При установке Kaspersky Web Traffic Security на операционную систему Astra Linux Special Edition поддерживается интеграция только с веб-сервером Apache.

► *Чтобы установить и настроить веб-сервер:*

1. Для установки веб-сервера выполните команду:

   ```
   apt install apache2
   ```

2. Настройте автоматический запуск веб-сервера при помощи команды:

   ```
   systemctl enable apache2
   ```

3. Для корректной работы Kaspersky Web Traffic Security требуются дополнительные модули, которые по умолчанию отключены. Включите их при помощи команды:

   ```
   a2enmod headers proxy proxy_http deflate ssl socache_shmcb
   ```

4. Перезапустите службу веб-сервера с помощью команды:

   ```
   systemctl restart apache2
   ```

Веб-сервер будет установлен и настроен.

Kaspersky Web Traffic Security работает в режиме отключенного AstraMode. Если для использования веб-сервисов, отличных от Kaspersky Web Traffic Security, вам нужен Apache с режимом AstraMode, вы можете оставить включенным AstraMode в настройках Apache. Это не влияет на работоспособность Kaspersky Web Traffic Security, Apache и веб-сервисов, работающих под управлением Apache.

Установка пакета приложения

Kaspersky Web Traffic Security распространяется в пакете формата DEB.

Запускать установку Kaspersky Web Traffic Security требуется с правами учетной записи root.

► *Чтобы установить Kaspersky Web Traffic Security из пакета формата DEB, выполните следующую команду:*

```
dpkg -i kwts-se_6.2.0-155_amd64.deb
```

После установки приложения отобразится путь к скрипту настройки setup.py.

Перед запуском скрипта настройки необходимо установить пакеты локализации (см. раздел "Установка пакета локализации" на стр. 54).

kaspersky

Установка пакета локализации

Английская локализация включена в состав приложения. Для остальных языков требуется установка пакета локализации. При необходимости вы можете установить несколько пакетов локализации.

► *Чтобы установить пакет локализации из пакета формата DEB, выполните следующую команду:*

```
dpkg -i kwts-l10n-<код пакета локализации>_6.2.0.155-1_all.deb
```

В таблице ниже приведены коды пакетов локализации.

Таблица 3. Коды пакетов локализации

Язык	Код пакета локализации
Немецкий	de
Испанский	es
Французский	fr
Японский	ja
Португальский (Бразилия)	pt-BR
Русский	ru
Китайский традиционный	zh-TW
Китайский упрощенный	zh-CN

Первоначальная настройка приложения

После установки приложения вам нужно провести первоначальную настройку.

Вы можете выполнить первоначальную настройку приложения вручную (см. раздел "Настройка приложения вручную" на стр. 55) или в автоматическом режиме (см. раздел "Запуск автоматической настройки приложения" на стр. 59), используя файл с сохраненными ответами. Автоматический режим первоначальной настройки позволит избежать повторного ввода параметров и сократить время на развертывание приложения в инфраструктуре организации.

Учетная запись пользователя, выполняющего первоначальную настройку приложения, должна обладать правами суперпользователя.

В этом разделе

kaspersky

Настройка приложения вручную

Запускать процесс первоначальной настройки Kaspersky Web Traffic Security требуется с правами учетной записи root.

► *Чтобы запустить первоначальную настройку Kaspersky Web Traffic Security вручную, выполните следующую команду:*

```
/opt/kaspersky/kwts/bin/setup.py --install
```

Далее скрипт первоначальной настройки по шагам запрашивает информацию для настройки Kaspersky Web Traffic Security.

Чтобы ввести значение по умолчанию, предложенное скриптом, нажмите на клавишу **ENTER**.

Шаг 1. Выбор языка просмотра Лицензионного соглашения и Политики конфиденциальности

На этом шаге вы можете выбрать язык, на котором будут отображаться тексты Лицензионного соглашения и Политики конфиденциальности.

Чтобы выбрать язык, введите номер нужного языка из предложенного списка и нажмите на клавишу **ENTER**.

Шаг 2. Просмотр Лицензионного соглашения

На этом шаге требуется принять или отклонить условия Лицензионного соглашения. Использовать приложение без принятия Лицензионного соглашения невозможно.

► *Чтобы просмотреть Лицензионное соглашение:*

1. Нажмите на клавишу **ENTER**.

   Откроется текст Лицензионного соглашения. Для перемещения по тексту используйте клавиши управления курсором, клавиши **PAGE UP** и **PAGE DOWN**. Для выхода из режима просмотра нажмите на клавишу **Q**.

2. Выполните одно из следующих действий:

   - Если вы хотите принять условия Лицензионного соглашения, введите `yes`.
   - Если вы хотите отклонить условия Лицензионного соглашения, введите `no`.

3. Нажмите на клавишу **ENTER**.

   Если вы отклонили условия Лицензионного соглашения, первоначальная настройка прерывается.

Вы можете в любой момент просмотреть текст Лицензионного соглашения в файле. Файл с текстом Лицензионного соглашения расположен по следующему пути: /opt/kaspersky/kwts/share/doc/LICENSE.<язык>.

Шаг 3. Просмотр Политики конфиденциальности

На этом шаге требуется принять или отклонить условия Политики конфиденциальности. Использовать приложение без принятия Политики конфиденциальности невозможно.

► *Чтобы просмотреть Политику конфиденциальности:*

1. Нажмите на клавишу **ENTER**.

   Откроется текст Политики конфиденциальности.

   Для перемещения по тексту используйте клавиши управления курсором клавиши **PAGE UP** и **PAGE DOWN**. Для выхода из режима просмотра нажмите на клавишу **Q**.

2. Выполните одно из следующих действий:

   - Если вы хотите принять условия Политики конфиденциальности, введите `yes`.
   - Если вы хотите отклонить условия Политики конфиденциальности, введите `no`.

3. Нажмите на клавишу **ENTER**.

   Если вы отклонили условия Политики конфиденциальности, первоначальная настройка прерывается.

Вы можете в любой момент просмотреть текст Политики конфиденциальности в файле. Файл с текстом Политики конфиденциальности расположен по следующему пути: /opt/kaspersky/kwts/share/doc/LICENSE_privacy_policy.<язык>.

Шаг 4. Просмотр информации о параметрах защиты по умолчанию

На этом шаге требуется принять или отклонить значения параметров защиты, устанавливаемых по умолчанию. Использовать приложение без принятия параметров защиты по умолчанию, невозможно.

► *Чтобы просмотреть информацию о параметрах защиты по умолчанию:*

1. Нажмите на клавишу **ENTER**.

   Откроется текст информации о параметрах защиты по умолчанию.

   Для перемещения по тексту используйте клавиши управления курсором клавиши **PAGE UP** и **PAGE DOWN**. Для выхода из режима просмотра нажмите на клавишу **Q**.

2. Выполните одно из следующих действий:

   - Если вы хотите принять параметры защиты, устанавливаемые по умолчанию, введите `yes`.
   - Если вы хотите отклонить параметры защиты, устанавливаемые по умолчанию, введите `no`.

3. Нажмите на клавишу **ENTER**.

   Если вы отклонили параметры защиты, устанавливаемые по умолчанию, первоначальная настройка прерывается.

Вы можете в любой момент просмотреть информацию о параметрах защиты, устанавливаемых по

умолчанию, в файле. Файл с информацией о параметрах защиты, устанавливаемых по умолчанию, расположен по следующему пути: /opt/kaspersky/kwts/share/doc/limited_protection.<язык>.

Шаг 5. Выбор веб-сервера

На этом шаге вы можете выбрать веб-сервер для работы веб-интерфейса Kaspersky Web Traffic Security из списка веб-серверов, автоматически обнаруженных в операционной системе.

► *Чтобы выбрать веб-сервер:*

1. Укажите номер нужного веб-сервера из списка.

   Если нужный веб-сервер не найден, введите цифру, соответствующую опции прерывания настройки **Abort setup**, исправьте проблему обнаружения веб-сервера (например, установите пакет веб-сервера) и запустите скрипт первоначальной настройки Kaspersky Web Traffic Security заново (см. раздел "Настройка приложения вручную" на стр. 55).

2. Нажмите на клавишу **ENTER**.
3. Проверьте параметры веб-сервера и подтвердите предложенную конфигурацию вводом цифры, соответствующей опции **Continue setup**.

   Если параметры веб-сервера определены неверно, введите цифру, соответствующую опции **Abort setup**, измените конфигурацию веб-сервера и повторно запустите скрипт первоначальной настройки Kaspersky Web Traffic Security.

Шаг 6. Ввод параметров узла

На этом шаге вы можете указать IP-адрес узла, номер порта для межмашинного взаимодействия в кластере и номер порта, по которому будет доступен веб-интерфейс Kaspersky Web Traffic Security.

Скрипт предлагает следующие номера портов по умолчанию: 9045 для межмашинного взаимодействия и 443 для веб-интерфейса. Если эти порты заняты, скрипт не будет предлагать значение по умолчанию, вам нужно вручную указать номера свободных портов.

Если вы хотите использовать значения по умолчанию, для каждого параметра нажмите на клавишу **ENTER**.

► *Чтобы указать параметры узла Kaspersky Web Traffic Security:*

1. Укажите IP-адрес узла и нажмите на клавишу **ENTER**.

   По умолчанию используется IP-адрес текущего узла.

   Этот IP-адрес будет использоваться для межмашинного взаимодействия в кластере.

2. Укажите номер порта текущего узла и нажмите на клавишу **ENTER**.

   Этот порт будет использоваться для межмашинного взаимодействия в кластере.

3. Укажите номер порта текущего узла для предоставления доступа к веб-интерфейсу Kaspersky Web Traffic Security и нажмите на клавишу **ENTER**.

   Значение, отличное от номера порта по умолчанию, требуется, если веб-сервер используется для предоставления доступа к веб-интерфейсу разных систем, и стандартный порт уже занят.

kaspersky

Шаг 7. Подтверждение параметров СУБД

Этот шаг отображается только при установке Kaspersky Web Traffic Security на операционную систему Astra Linux Special Edition.

На этом шаге вы можете подтвердить автоматически определенные параметры СУБД.

► *Чтобы подтвердить параметры СУБД:*

1. Проверьте автоматически обнаруженные параметры СУБД.
2. Если все верно, подтвердите конфигурацию вводом цифры, соответствующей значению **Yes**.
3. Если обнаруженные параметры некорректны:
   a. Введите цифру, соответствующую опции **Change utility path**.
   b. Укажите путь к утилите psql и нажмите на клавишу **ENTER**.
   c. Укажите путь к утилите pg_ctl и нажмите на клавишу **ENTER**.
   d. Подтвердите конфигурацию.
4. Если параметры СУБД не удалось определить автоматически:
   a. Укажите путь к утилите psql и нажмите на клавишу **ENTER**.
   b. Укажите путь к утилите pg_ctl и нажмите на клавишу **ENTER**.
   c. Подтвердите конфигурацию.

Шаг 8. Назначение пароля доступа к веб-интерфейсу приложения

На этом шаге вы можете указать пароль учетной записи Administrator для доступа к веб-интерфейсу приложения.

Пароль доступа к веб-интерфейсу Kaspersky Web Traffic Security обязателен. Вы не сможете войти в веб-интерфейс приложения без пароля.

► *Чтобы назначить пароль доступа к веб-интерфейсу:*

1. Введите пароль учетной записи Administrator.

   Пароль должен содержать не менее 15 символов, а также удовлетворять следующим условиям:

   - Содержать хотя бы один символ верхнего регистра.
   - Содержать хотя бы один символ нижнего регистра.
   - Содержать хотя бы один специальный символ.
   - Содержать хотя бы одну цифру.
2. Нажмите на клавишу **ENTER**.
3. Введите пароль повторно.

4. Нажмите на клавишу **ENTER**.

   Если пароль не соответствует требованиям или введенные пароли не совпадают, произойдет возврат к началу текущего шага.

   > Вы можете изменить пароль Локального администратора (см. раздел "Изменение пароля учетной записи Administrator" на стр. 129) после установки приложения в веб-интерфейсе в разделе **Локальный администратор**.

   На этом первоначальная настройка приложения будет завершена, станет доступен веб-интерфейс Kaspersky Web Traffic Security.

После этого вам нужно добавить сервер в кластер (см. раздел "Добавление узла в кластер" на стр. 133) для управления параметрами приложения через веб-интерфейс.

Запуск автоматической настройки приложения

Вы можете выполнять первоначальную настройку Kaspersky Web Traffic Security в автоматическом режиме.

Сценарий выполнения первоначальной настройки в автоматическом режиме состоит из следующих этапов:

1. **Создание конфигурационного файла с ответами на вопросы скрипта первоначальной настройки**

   Для этого используется команда:

   ```
   /opt/kaspersky/kwts/bin/setup.py --create-auto-install=<полный путь к файлу для сохранения параметров>
   ```

   > Создание конфигурационного файла с ответами невозможно запустить на узле, на котором была выполнена первоначальная настройка вручную (см. раздел "Настройка приложения вручную" на стр. 55).

2. **Изменение адреса настраиваемого узла**

   В конфигурационном файле с ответами записаны сетевые параметры того узла, на котором этот файл был создан (см. раздел "Шаг 6. Ввод параметров узла" на стр. 57). Чтобы настроить Kaspersky Web Traffic Security на других узлах, вам нужно вручную в конфигурационном файле изменить IP-адрес текущего узла на значение IP-адреса настраиваемого узла. При необходимости нужно также изменить номера портов узла.

3. **Запуск настройки Kaspersky Web Traffic Security в автоматическом режиме**

   Для этого используется команда:

   ```
   /opt/kaspersky/kwts/bin/setup.py --auto-install=<полный путь к файлу с сохраненными параметрами>
   ```

   Если для учетной записи администратора вы хотите использовать пароль из переменной окружения ADMINISTRATOR_PASSWORD, выполните команду:

   ```
   /opt/kaspersky/kwts/bin/setup.py --auto-install=<полный путь к файлу с сохраненными параметрами> --administrator-password-from-environment
   ```

kaspersky

Настройка PostgreSQL для Astra Linux Special Edition 1.8

Эту настройку требуется выполнять, если вы устанавливаете Kaspersky Web Traffic Security на операционную систему Astra Linux Special Edition 1.8.

► *Чтобы обеспечить корректную работу Kaspersky Web Traffic Security с СУБД PostgreSQL:*

1. Откройте на редактирование файл /var/opt/kaspersky/kwts/postgresql/postgresql.conf.
2. Измените значение параметра **ac_audit_log_only_failures** на **true**.
3. Сохраните изменения в файле.
4. Перезапустите сервис базы данных с помощью команды:

   ```
   systemctl restart kwts.postgresql
   ```

kaspersky

Удаление приложения

► *Чтобы удалить приложение:*

1. Удалите из кластера (см. раздел "Удаление узла из кластера" на стр. 134) узел с удаляемым приложением.
2. Если в Kaspersky Web Traffic Security была включена возможность обработки сетевого трафика с ненулевой мандатной меткой, выключите эту возможность (см. раздел "Включение и выключение обработки сетевого трафика с ненулевой мандатной меткой" на стр. 156) для удаляемого узла кластера.
3. Удалите языковые пакеты с помощью следующих команд:

   ```
   dpkg -r kwts-l10n-de
   dpkg -r kwts-l10n-es
   dpkg -r kwts-l10n-fr
   dpkg -r kwts-l10n-ja
   dpkg -r kwts-l10n-pt-BR
   dpkg -r kwts-l10n-ru
   dpkg -r kwts-l10n-zh-CN
   dpkg -r kwts-l10n-zh-TW
   ```

4. Удалите пакет приложения с помощью команды:

   ```
   dpkg -r kwts-se
   ```

5. Запустите скрипт для удаления данных приложения с помощью команды:

   ```
   /var/opt/kaspersky/kwts/cleanup.sh
   ```

6. Введите `yes`, чтобы подтвердить удаление данных, оставшихся после удаления Kaspersky Web Traffic Security.
7. После завершения работы скрипта выполните команду:

   ```
   dpkg -P kwts-se
   ```

Приложение будет удалено.

kaspersky

Процедура приемки

Перед вводом приложения в эксплуатацию проводится процедура приемки, включающая проверку правильной установки, работоспособности и соответствия безопасной (сертифицированной) конфигурации.

В этом разделе

Безопасное состояние

Программа находится в безопасном состоянии (сертифицированной конфигурации), если выполняются следующие условия:

- Параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу.
- Активный ключ добавлен.
- Базы Антивируса и Анти-Фишинга обновлены.

Проверка работоспособности. Тестовый файл EICAR

Чтобы проверить работоспособность программы, вы можете использовать тестовый файл EICAR.

Тестовый файл EICAR предназначен для проверки работы антивирусных программ. Он разработан организацией The European Institute for Computer Antivirus Research (EICAR).

Тестовый файл EICAR не является вирусом и не содержит программного кода, который может нанести вред вашему компьютеру, но антивирусные программы большинства производителей идентифицируют в нем угрозу.

Вы можете загрузить тестовый файл EICAR со страницы веб-сайта организации EICAR https://secure.eicar.org/eicar_com.zip.

Перед сохранением файла в папке на диске компьютера убедитесь, что постоянная защита файлов в этой папке отключена.

Чтобы проверить антивирусную защиту сообщений с использованием тестового файла EICAR, перейдите по ссылке и попробуйте загрузить файл EICAR с официального веб-сайта организации EICAR: https://secure.eicar.org/eicar_com.zip.

Kaspersky Web Traffic Security сообщит вам об обнаружении угрозы и заблокирует сохранение объекта.

kaspersky

Начало работы с приложением

После завершения установки вы можете работать с приложением с помощью веб-интерфейса через браузер любого компьютера.

Администратору Kaspersky Web Traffic Security требуется самостоятельно обеспечить защиту передачи данных между браузером и Управляющим узлом. Для обеспечения безопасности также рекомендуется настроить Kerberos-аутентификацию с использованием технологии единого входа (см. раздел "Настройка Kerberos-аутентификации" на стр. 222).

Для того чтобы управлять параметрами приложения, вам требуется подключиться к Управляющему узлу. При подключении к Подчиненным узлам вам доступно изменение роли сервера (см. раздел "Изменение роли узла в кластере" на стр. 134) и просмотр состояния других подключенных серверов.

В этом разделе

Настройка сетевых доступов

Для корректной работы Kaspersky Web Traffic Security требуется предварительно настроить порты на серверах с установленным приложением, а также на маршрутизаторах локальной сети организации, через которые проходит трафик.

Информация о необходимых сетевых доступах в соответствии с функциональностью приложения представлена в таблице ниже.

Таблица 4. Сетевые доступы, необходимые для работы приложения

Функциональность	Протокол	Порт	Направление	Назначение соединения
Работа с приложением через веб-интерфейс	TCP	443	Входящее	Компьютер администратора приложения
Взаимодействие между узлами кластера (см. раздел "Управление кластером" на стр. 130)	TCP	По умолчанию 9045 (возможно изменить в веб-интерфейсе приложения)	Входящее и исходящее	Другие узлы кластера
Соединение с ICAP-сервером (см. раздел "Параметры ICAP-сервера" на стр. 154)	TCP	По умолчанию 1344 (возможно изменить в веб-интерфейсе приложения)	Входящее	ICAP-клиенты и балансировщики нагрузки

Функциональность	Протокол	Порт	Направление	Назначение соединения
DNS-запросы	UDP	53	Исходящее	DNS-серверы
Соединение с внешним прокси-сервером (см. раздел "Настройка параметров соединения с прокси-сервером" на стр. 170)	TCP	По умолчанию 8080 (возможно изменить в веб-интерфейсе приложения)	Исходящее	Внешний прокси-сервер
Активация приложения (на стр. 48)	TCP	443	Исходящее	Серверы "Лаборатории Касперского"
Обновление баз приложения (см. раздел "Обновление баз Kaspersky Web Traffic Security" на стр. 171)	TCP	80, 443	Исходящее	Серверы "Лаборатории Касперского"
KSN (см. раздел "Настройка участия в Kaspersky Security Network" на стр. 174)	TCP	443	Исходящее	Серверы "Лаборатории Касперского"
KPSN (см. раздел "Настройка использования Kaspersky Private Security Network" на стр. 174)	TCP	443	Исходящее	Сервер KPSN
Соединение с LDAP-сервером (на стр. 176)	TCP	389	Исходящее	Серверы Active Directory
Kerberos-аутентификация в Active Directory	UDP, TCP	88	Исходящее	Серверы Active Directory
NTLM-аутентификация с помощью технологии единого входа (см. раздел "Настройка NTLM-аутентификации" на стр. 223)	TCP	445	Исходящее	Серверы Active Directory
Интеграция с приложением KATA (см. раздел "Настройка интеграции с приложением Kaspersky Anti Targeted Attack Platform" на стр. 180)	TCP	По умолчанию 443 (возможно изменить в веб-интерфейсе приложения)	Исходящее	Сервер KATA

Функциональность	Протокол	Порт	Направление	Назначение соединения
Работа службы snmpd (см. раздел "Настройка службы snmpd в операционной системе" на стр. 202)	TCP	По умолчанию 705 (возможно изменить в веб-интерфейсе приложения)	Исходящее	SNMP-сервер

Подключение к веб-интерфейсу приложения

Если вы подключаетесь к веб-интерфейсу впервые после установки приложения, перед началом работы вам потребуется создать новый кластер (см. раздел "Создание нового кластера" на стр. 130).

► *Чтобы подключиться к веб-интерфейсу приложения:*

1. В браузере введите следующий адрес:

   `https://<IP-адрес или полное доменное имя (FQDN) Управляющего сервера>`

   Откроется страница авторизации веб-интерфейса с запросом имени и пароля пользователя.
2. В поле **Имя пользователя** введите `Administrator`.
3. В поле **Пароль** введите пароль администратора.

   Если вы введете неверный пароль пять раз, возможность авторизации будет заблокирована на пять минут.
4. Нажмите на кнопку **Войти**.

Откроется главное окно веб-интерфейса приложения.

Проверка работы Kaspersky Web Traffic Security в веб-интерфейсе

► *Чтобы проверить работу Kaspersky Web Traffic Security:*

1. На компьютере администратора войдите в веб-интерфейс приложения и перейдите в раздел **Узлы**.
2. Убедитесь, что все узлы кластера имеют статус **Синхронизирован** и нет ошибок.
3. На компьютере пользователя откройте веб-браузер и перейдите по следующим ссылкам:
   - https://secure.eicar.org/eicar.com
   - https://secure.eicar.org/eicar_com.zip

   Если приложение настроено верно и на прокси-сервере включена расшифровка TLS/SSL-соединений, отобразится сообщение о запрете доступа к этим ресурсам.

4. На компьютере пользователя откройте сайт, доступ к которому не запрещен, например, https://www.kaspersky.ru.

   Если приложение настроено верно, веб-сайт откроется.

5. На компьютере администратора войдите в веб-интерфейс приложения и перейдите в раздел **События → Трафик**.

6. Нажмите на кнопку **Найти**.

   Отобразятся последние события веб-трафика, включая события доступа с компьютера пользователя.

kaspersky

Создание учетных записей пользователей

При установке программы создается учетная запись Administrator с правами суперпользователя. Она является локальной и позволяет входить в систему без использования внешних служб и доменов аутентификации. Вы можете изменить пароль для этой учетной записи после установки в разделе **Параметры**, подразделе **Локальный администратор**.

При первоначальной настройке программы после установки для соответствия требованиям ИТ.САВЗ.Б2.ПЗ рекомендуется создать следующие роли:

- Администратор сервера.
- Администратор безопасности.

Администратору сервера рекомендуется назначить следующие права:

- **Создавать/изменять/удалять узлы**.
- **Получать диагностическую информацию**.

Администратору безопасности рекомендуется назначить следующие права:

- **Создавать/изменять/удалять узлы**.
- **Получать диагностическую информацию**.
- **Проверять целостность данных**.
- **Просматривать информацию об узлах**.
- **Создавать/изменять рабочие области**.
- **Просматривать рабочие области**.
- **Удалять рабочие области**.
- **Создавать/изменять роли**.
- **Просматривать роли**.
- **Удалять роли**.
- **Создавать/изменять правила**.
- **Просматривать правила**.
- **Удалять правила**.
- **Просматривать события обработки трафика**.
- **Просматривать системные события**.
- **Просматривать разделы Мониторинг и Отчеты**.
- **Изменять параметры**.
- **Просматривать параметры**.

kaspersky

Мониторинг работы приложения

В статистике обработанного трафика не учитываются веб-ресурсы, к которым были применены правила обхода (см. раздел "Добавление правила обхода" на стр. 83) или действия **Tunnel** и **Tunnel with SNI check** в рамках обработки SSL-соединений.

Вы можете осуществлять мониторинг работы приложения с помощью графиков и информационных панелей. В окне веб-интерфейса приложения в разделе **Мониторинг** отображается следующая информация:

- **Работоспособность системы**. Диаграмма ошибок в работе кластера. По ссылке **Перейти в раздел Узлы** вы можете перейти в раздел **Узлы** и посмотреть более подробные сведения о работоспособности каждого узла кластера.

  Недоступно в веб-интерфейсе рабочей области.

- **Обнаружения по категории**. Диаграмма обнаруженных объектов по категориям контентной фильтрации, а также график обнаружений по времени. Эта информация позволит вам определить наиболее часто запрашиваемые категории веб-ресурсов в вашей организации.
- **Обработка данных**. График, показывающий объем обработанного входящего и исходящего сетевого трафика в течение времени. Эта информация поможет вам определить часы наибольшей активности пользователей вашей организации, а также оценить количество ресурсов, необходимых для обработки трафика.
- **Антивирус**. Графики, показывающие количество объектов, проверенных модулем Антивирус, и количество найденных угроз.
- **Анти-Фишинг**. Графики, показывающие количество объектов, проверенных модулем Анти-Фишинг, и количество найденных угроз.
- **Фильтр вредоносных ссылок**. Графики, показывающие общее количество проверенных ссылок и количество ссылок, признанных вредоносными.
- **KATA**. Графики, показывающие количество объектов, проверенных на основании информации с сервера KATA, и количество найденных угроз.
- **Последние 10 угроз**. Названия и время обнаружения последних 10 объектов.
- **Последние 10 заблокированных URL-адресов**. URL-адреса последних 10 веб-ресурсов, доступ к которым был заблокирован.
- **Последние 10 пользователей с заблокированными запросами**. IP-адреса последних 10 пользователей, запросы которых были заблокированы приложением.

В общем веб-интерфейсе приложения вы можете фильтровать данные мониторинга (см. раздел "Фильтрация данных мониторинга" на стр. 71) по следующим критериям:

- интервалу времени;
- узлам кластера;
- рабочим областям.

В веб-интерфейсе рабочей области доступна только фильтрация по интервалу времени.

Вы можете создавать новые схемы расположения графиков (см. раздел "Создание новой схемы расположения графиков" на стр. 69), переключаться между сохраненными схемами (см. раздел "Выбор схемы расположения графиков из списка" на стр. 71), а также устанавливать схему, отображаемую по умолчанию (см. раздел "Выбор схемы расположения графиков, отображаемой по умолчанию" на стр. 71).

В этом разделе

Создание новой схемы расположения графиков

► *Чтобы создать новую схему расположения графиков:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку ☰.
3. В раскрывающемся списке выберите **Новая**.

   Отобразится набор графиков по умолчанию.
4. В поле **Название схемы расположения графиков** введите имя новой схемы расположения графиков.
5. Если вы хотите добавить графики в схему, нажмите на кнопку **Графики** и выполните следующие действия:
   a. В появившемся окне **Добавить график** включите переключатели рядом с названиями тех графиков, которые вы хотите добавить на схему расположения графиков.
   b. Нажмите на кнопку ✕.
6. Если вы хотите переместить график на схеме, перетащите график на другое место схемы, нажав и удерживая левую клавишу мыши на верхней части графика.
7. Если вы хотите удалить график со схемы, нажмите на значок ✕ в правом верхнем углу графика.
8. Нажмите на кнопку **Сохранить**.

Новая схема будет добавлена в список схем расположения графиков в разделе **Графики**.

kaspersky

Изменение схемы расположения графиков

Вы не можете изменить предустановленную схему расположения графиков под названием **Схема по умолчанию**.

► *Чтобы изменить схему расположения графиков:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В списке схем расположения графиков выберите схему, которую вы хотите изменить.
3. В верхней части окна нажмите на кнопку ☰.
4. В раскрывающемся списке выберите **Изменить**.
5. Если вы хотите переименовать схему, в поле с текущим именем схемы расположения графиков введите новое имя.
6. Если вы хотите добавить графики в схему, нажмите на кнопку **Графики** и выполните следующие действия:
   a. В появившемся окне **Добавить график** включите переключатели рядом с названиями тех графиков, которые вы хотите добавить на схему расположения графиков.
   b. Нажмите на кнопку ✕.
7. Если вы хотите переместить график на схеме, перетащите график на другое место схемы, нажав и удерживая левую клавишу мыши на верхней части графика.
8. Если вы хотите удалить график со схемы, нажмите на значок ✕ в правом верхнем углу графика.
9. Нажмите на кнопку **Сохранить**.

Схема расположения графиков будет изменена.

Удаление схемы расположения графиков

Вы не можете удалить предустановленную схему расположения графиков под названием **Схема по умолчанию**.

► *Чтобы удалить схему расположения графиков:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В списке схем расположения графиков выберите схему, которую вы хотите удалить.
3. Наведите курсор мыши на название схемы расположения графиков, которую вы хотите удалить.
4. Нажмите на значок 🗑 справа от названия схемы расположения графиков.

   Отобразится подтверждение удаления схемы расположения графиков.
5. Нажмите на кнопку **Удалить**.

Схема расположения графиков будет удалена.

Выбор схемы расположения графиков из списка

► *Чтобы выбрать схему расположения графиков из списка схем расположения графиков:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса приложения в списке схем расположения графиков выберите нужную схему расположения графиков.

Выбранная схема расположения графиков отобразится в окне веб-интерфейса приложения.

Выбор схемы расположения графиков, отображаемой по умолчанию

► *Чтобы выбрать схему расположения графиков, отображаемую по умолчанию:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса приложения раскройте список схем расположения графиков.
3. Выберите схему, которая должна отображаться по умолчанию.
4. Нажмите на значок ☆ слева от названия схемы.

Выбранная схема расположения графиков будет отображаться при выборе раздела **Мониторинг**.

Фильтрация данных мониторинга

► *Чтобы отфильтровать сведения, отображаемые на графиках:*

1. В веб-интерфейсе приложения в разделе переключения между рабочими областями выберите общие параметры или название нужной рабочей области.
2. Выберите раздел **Мониторинг**.
3. Если вы хотите отфильтровать сведения по интервалу времени, в раскрывающемся списке **Прошедший час** выберите один из следующих вариантов:
   - **Прошедший час**.
   - **Прошедшие сутки**.
   - **Прошедшая неделя**.
   - **Прошедший месяц**.
   - **Прошедший год**.

   По умолчанию отображаются сведения за последний час.
4. Если вы хотите отфильтровать сведения по узлам кластера, в раскрывающемся списке **Все узлы** выберите IP-адрес нужного узла.

По умолчанию отображаются сведения обо всех узлах.

> Недоступно в веб-интерфейсе рабочих областей.

5. Если вы хотите отфильтровать сведения по рабочим областям, в раскрывающемся списке **Глобальная** выберите название нужной рабочей области.

   По умолчанию отображаются сведения обо всех рабочих областях.

   > Недоступно в веб-интерфейсе рабочих областей.

Сведения, отображаемые на графиках, будут отфильтрованы по заданным критериям.

kaspersky

Отчеты

Функциональность доступна только при наличии у пользователя права **Просматривать разделы Мониторинг и Отчеты**.

Вы можете создать отчет (см. раздел "Создание отчета" на стр. 73) по заданным критериям на основе статистики из раздела **Мониторинг**. Отчет содержит данные об обработанном трафике выбранной рабочей области за указанный период времени.

После создания отчет доступен для скачивания (см. раздел "Скачивание отчета на компьютер" на стр. 74) в формате PDF.

В этом разделе

Создание отчета

► *Чтобы создать отчет:*

1. В веб-интерфейсе приложения выберите раздел **Отчеты**.
2. Нажмите на кнопку **Создать отчет**.

   Откроется окно **Новый отчет**.
3. В раскрывающемся списке **Период** выберите один из следующих периодов, за который вы хотите сформировать отчет:
   - **Прошедшие сутки**.
   - **Прошедшая неделя**.
   - **Прошедший месяц**.
   - **Прошедший год**.
4. В раскрывающемся списке **Рабочая область** выберите рабочую область, данные о которой вы хотите включить в отчет.

   Если вы хотите получить данные обо всех рабочих областях, выберите **Глобальная**.
5. В раскрывающемся списке **Язык** выберите язык отчета.
6. Нажмите на кнопку **Добавить**.

Отчет будет создан и отобразится в первой строке таблицы отчетов. Вы можете сохранить созданный отчет (см. раздел "Скачивание отчета на компьютер" на стр. 74) на жесткий диск компьютера.

kaspersky

Удаление отчета

► *Чтобы удалить отчет:*

1. В веб-интерфейсе приложения выберите раздел **Отчеты**.
2. В таблице **Последние созданные отчеты** в правой части строки с отчетом, который вы хотите удалить, нажмите на значок .

Отчет будет удален.

Скачивание отчета на компьютер

Вы можете скачать отчет на любой компьютер, с которого вы вошли в веб-интерфейс приложения.

► *Чтобы скачать отчет на компьютер:*

1. В веб-интерфейсе приложения выберите раздел **Отчеты**.
2. В таблице **Последние созданные отчеты** в правой части строки с отчетом, который вы хотите скачать, нажмите на значок .

Файл отчета в формате PDF будет сохранен в папке загрузки браузера.

Просмотр содержимого отчета

PDF-файл сформированного отчета содержит данные об обработке трафика выбранной рабочей области за указанный период времени.

В заголовке отчета содержится следующая информация:

- Период, за который были получены данные.
- Рабочая область, к которой относятся данные об обрабатываемом трафике.

  Если был выбран раздел **Глобальная**, сначала отображаются суммарные данные об обработке всего трафика, а затем данные по каждой рабочей области.

- Язык отчета.

Тело отчета включает в себя следующие блоки информации:

- Количество обработанных объектов (**Обработано объектов**) и объем проверенного трафика (**Трафик**).
- Количество обработанных объектов (**Проверено**) и угроз (**Обнаружено**), обнаруженных следующими технологиями:
  - **Антивирус**.
  - **KATA**.

    - **Фильтр вредоносных ссылок**.
    - **Анти-Фишинг**.
- Количество посещенных URL-адресов, попадающих под следующие веб-категории:
    - **Для взрослых**.
    - **Алкоголь, табак, наркотические и психотропные вещества**.
    - **Культура и общество**.
    - **Программное обеспечение, аудио, видео**.
    - **Информационные технологии**.
    - **Интернет-магазины, банки, платежные системы**.
    - **Ненависть и дискриминация**.
    - **Общение в сети**.
    - **Образование**.
    - **Хобби и развлечения**.
    - **Красота, здоровье и спорт**.
    - **Азартные игры, лотереи, тотализаторы**.
    - **Другие**.
    - **Заблокировано законодательством Российской Федерации**.
    - **Запрещено полицией**.
- **Последние 10 заблокированных URL-адресов**. URL-адреса последних 10 веб-ресурсов, доступ к которым был заблокирован.
- **Последние 10 угроз**. Названия и время обнаружения последних 10 объектов.
- **Последние 10 пользователей с заблокированными запросами**. IP-адреса последних 10 пользователей, запросы которых были заблокированы приложением.

kaspersky

Журнал событий Kaspersky Web Traffic Security

Во время работы Kaspersky Web Traffic Security возникают различного рода события. Они отражают изменение состояния приложения, а также результаты работы правил обработки трафика. Для того чтобы администратор приложения мог самостоятельно проанализировать ошибки, допущенные при настройке параметров приложения, а также для того, чтобы специалисты "Лаборатории Касперского" могли оказать эффективную техническую поддержку, Kaspersky Web Traffic Security записывает информацию об этих событиях в *журнале событий*.

Данные журнала событий хранятся на узлах приложения. Файлы журнала событий автоматически ротируются по достижении максимально разрешенного размера файлов или по истечении максимального срока их хранения (см. раздел "Настройка параметров журнала событий" на стр. 78).

В общем веб-интерфейсе приложения отображаются следующие события:

- События обработки трафика.
- Системные события приложения.
- События KATA, если настроена интеграция с приложением KATA (см. раздел "Настройка интеграции с приложением Kaspersky Anti Targeted Attack Platform" на стр. 180).

Администратор может отфильтровать события по отдельной рабочей области, а также события, которые не относятся к рабочим областям.

В веб-интерфейсе рабочей области отображаются только события обработки трафика текущей рабочей области.

В этом разделе

Просмотр журнала событий

► *Чтобы просмотреть журнал событий Kaspersky Web Traffic Security:*

1. В окне веб-интерфейса приложения выберите раздел **События**.
2. Выберите одну из следующих вкладок в зависимости от типа событий, которые вы хотите просмотреть:
   - **Трафик**;
   - **Система**;
   - **KATA**.
3. В раскрывающемся списке справа от параметра **Максимальное количество событий** выберите

количество записей для просмотра.

4. Нажмите на кнопку **Добавить условие**.
5. Настройте фильтр событий с помощью появившихся раскрывающихся списков:
   a. В левом раскрывающемся списке выберите критерий фильтрации.
   b. В центральном раскрывающемся списке выберите оператор сравнения.

      Для каждого критерия фильтрации доступен свой релевантный набор операторов сравнения. Например, при выборе критерия **Направление** для событий обработки трафика доступны операторы **Равняется** и **Не равняется**.
   c. В зависимости от выбранного критерия фильтрации выполните одно из следующих действий:
      - В поле справа от оператора сравнения введите значение, по которому вы хотите выполнить поиск событий.
      - В раскрывающемся списке справа от оператора сравнения выберите значение, по которому вы хотите выполнить поиск событий.

      Например, для поиска полного совпадения по имени пользователя введите имя пользователя.
6. Нажмите на кнопку **Найти**.

Отобразится таблица событий, удовлетворяющих условиям фильтрации.

Экспорт событий

Вы можете отфильтровать события из журнала событий (см. раздел "Просмотр журнала событий" на стр. 76) приложения и экспортировать их в файл.

► *Чтобы экспортировать события:*

1. В окне веб-интерфейса приложения выберите раздел **События**.
2. Выберите одну из следующих вкладок в зависимости от типа событий, которые вы хотите просмотреть:
   - **Трафик**.
   - **Система**.
   - **KATA**.
3. В раскрывающемся списке справа от параметра **Максимальное количество событий** выберите количество записей для просмотра.
4. Нажмите на кнопку **Добавить условие**.
5. Настройте фильтр событий с помощью появившихся раскрывающихся списков.
6. Нажмите на кнопку **Найти**.

   Отобразится таблица событий, удовлетворяющих условиям фильтрации.
7. В правом верхнем углу окна нажмите на кнопку **Экспортировать**.

Файл экспорта событий в формате CSV будет сохранен в папке загрузки браузера.

kaspersky

Настройка отображения таблицы событий

► *Чтобы настроить отображение таблицы событий:*

1. В окне веб-интерфейса приложения выберите раздел **События**.
2. Нажмите на кнопку **Добавить условие**.
3. Укажите условия фильтрации событий с помощью появившихся раскрывающихся списков.
4. Нажмите на кнопку **Найти**.

   Отобразится таблица событий, удовлетворяющих условиям фильтра.
5. По кнопке  откройте меню отображения таблицы событий.
6. Установите флажки рядом с теми параметрами, которые должны отображаться в таблице.

   Должен быть установлен хотя бы один флажок.

Отображение таблицы событий будет настроено.

Настройка параметров журнала событий

При настройке параметров журнала необходимо учитывать доступное дисковое пространство на серверах с установленным приложением.

Параметры журнала событий не влияют на параметры записи событий по протоколу Syslog (см. раздел "Настройка параметров Syslog" на стр. 189).

► *Чтобы настроить параметры журнала событий:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Журналы и события → События**.
2. В блоке **Трафик** выполните следующие действия:
   a. В раскрывающемся списке **Записывать события обработки трафика** выберите, какие события обработки трафика должны быть записаны в журнал. Вы можете выбрать один из следующих вариантов:
      - **все события**;
      - **после действий Заблокировать/Перенаправить**;
      - **не записывать**.

   Значение по умолчанию – **все события**.

   b. В поле **Максимальный размер журнала событий (МБ)** укажите размер журнала событий, при превышении которого более старые записи будут удалены.

   Значение по умолчанию – 1024 МБ. Минимальное значение – 100 МБ.

   c. В поле **Срок хранения событий в журнале (сут.)** укажите, сколько дней приложение должно

хранить на сервере события обработки сетевого трафика.

Значение по умолчанию – 3 дня. Минимальное значение – 1 день.

3. В блоке **KATA** выполните следующие действия:
   a. В поле **Максимальный размер журнала событий (МБ)** укажите размер журнала событий, при превышении которого более старые записи будут удалены.

      Значение по умолчанию – 1024 МБ. Минимальное значение – 100 МБ.

   b. В поле **Срок хранения событий в журнале (сут.)** укажите, сколько дней приложение должно хранить на сервере события KATA.

      Значение по умолчанию – 3 дня. Минимальное значение – 1 день.

4. В блоке **Система** выполните следующие действия:
   a. В поле **Максимальный размер журнала событий (МБ)** укажите размер журнала записей о событиях Kaspersky Web Traffic Security. При превышении этого значения более старые записи будут удалены.

      Значение по умолчанию – 1 ГБ. Минимальное значение – 100 МБ.

   b. В поле **Срок хранения событий в журнале (сут.)** укажите, сколько дней приложение должно хранить на сервере системные события. При превышении этого значения более старые записи будут удалены.

      Значение по умолчанию – 1100 дней. Минимальное значение – 1 день.

Параметры журнала событий будут настроены.

Работа с правилами обработки трафика

Вы можете регулировать доступ пользователей к веб-ресурсам с помощью правил обработки трафика. Эти правила делятся на правила обхода, правила доступа и правила защиты. Вы можете создавать группы правил доступа и группы правил защиты или добавлять правила вне групп.

Kaspersky Web Traffic Security начинает обработку трафика с проверки правил обхода. Если доступ к веб-ресурсу разрешен, то приложение переходит к проверке трафика с помощью правил доступа. По результатам обработки правил доступа приложение или блокирует веб-ресурс, или переходит к проверке трафика с помощью правил защиты. Алгоритм работы правил обработки трафика показан на рисунке ниже.

Рисунок 7. Алгоритм работы правил обработки трафика

Kaspersky Web Traffic Security применяет правила в порядке их расположения в таблице правил (см. раздел "Просмотр таблицы правил обработки трафика" на стр. 102) сверху вниз. Если заданные в правиле условия не выполняются, приложение переходит к следующему правилу. Как только заданные в очередном правиле условия выполняются, к трафику применяются параметры обработки, заданные в этом правиле, и поиск совпадения условий завершается.

При наличии рабочей области (см. раздел "Управление рабочими областями" на стр. 111) приоритет правил рабочей области определяется положением строки **Правила рабочей области** в таблице общих правил. В этом случае правила также применяются в порядке расположения в таблице сверху вниз. Правила рабочей области будут применены после проверки трафика по всем правилам, расположенным в таблице выше. Если ни одно из правил рабочей области не сработало, приложение переходит к проверке трафика по правилам, расположенным в таблице под строкой **Правила рабочей области**.

При установке приложения создается *правило обхода по умолчанию*. Согласно этому правилу, доступ к веб-ресурсам, для которых значение HTTP-заголовка Content-Length превышает 10240 КБ, разрешается всем пользователям без выполнения проверки модулями Антивирус и Анти-Фишинг. Это значение обеспечивает баланс между производительностью приложения и безопасностью сетевого трафика. Вы можете изменить (см. раздел "Изменение правила обработки трафика" на стр. 94), отключить (см. раздел "Включение и отключение правила обработки трафика" на стр. 96) или удалить (см. раздел "Удаление правила обработки трафика" на стр. 94) правило обхода по умолчанию.

Если ни одно правило не содержит условий, подходящих для данного веб-ресурса, трафик обрабатывается

согласно политике защиты по умолчанию. В этом случае приложение разрешает доступ к веб-ресурсу, который не запрещен в результате проверки модулями Антивирус и Анти-Фишинг. Политика защиты по умолчанию создается во время установки Kaspersky Web Traffic Security и отображается в разделе **Параметры**, в подразделе **Защита**. В параметрах политики защиты по умолчанию вы можете установить действия, которые приложение будет выполнять с объектами разных типов.

В этом разделе

Сценарий настройки доступа к веб-ресурсам

Совокупность правил обработки трафика позволяет выполнять следующие задачи:

- Разграничивать доступ к веб-ресурсам для сотрудников разных подразделений.

  Для этого вы можете использовать существующие доменные группы, если настроена интеграция с Active Directory (см. раздел "Приложение 8. Настройка интеграции сервиса Squid с Active Directory" на стр. 260). Например, вы можете разрешить доступ ко всем веб-ресурсам для группы Администраторы и запретить категории **Социальные сети** или **Программное обеспечение, аудио, видео** для остальных сотрудников.

- Блокировать доступ к веб-ресурсам, запрещенным законами вашей страны.

  Для этого вы можете создать правила для всех рабочих областей, распространяющиеся на всех пользователей.

- Контролировать объем трафика.

  В целях экономии трафика вы можете запретить или ограничить загрузку мультимедийных файлов, а также доступ к веб-ресурсам, не связанным с работой.

- Получать статистику о запрошенных веб-ресурсах в вашей организации.

  Если в правиле обработки трафика выбрано действие **Разрешить**, то пользователь получает доступ к веб-ресурсу, но информация об этом запросе сохраняется в журнал событий (см. раздел "Журнал событий Kaspersky Web Traffic Security" на стр. 76). Вы можете фильтровать события в журнале, например, просмотреть все обращения пользователей к веб-сайту www.kaspersky.ru.

Рекомендуется настраивать правила обработки трафика в следующем порядке:

1. **Создание рабочих областей (см. раздел "Управление рабочими областями" на стр. 111) и / или групп правил обработки трафика (см. раздел "Работа с группами правил обработки трафика" на стр. 97), если требуется**

   Правила обработки трафика проверяются в соответствии с их расположением в таблице правил. Для того, чтобы сработало нужное правило, необходимо заранее продумать способ организации правил. Рекомендуется использовать рабочие области для крупных подразделений организации или для разных клиентов интернет-провайдера. Далее можно объединять правила в группы. Например, вы можете создать рабочие области *Филиал 1* и *Филиал 2*, а внутри рабочих областей добавить группы *Администраторы*, *Бухгалтеры* и т.д.

2. **Добавление правил обхода (см. раздел "Добавление правила обхода" на стр. 83), если требуется**

   С помощью правила обхода вы можете предоставить пользователям доступ к веб-ресурсам, не выполняя их проверку. Например, разрешить скачивание обновлений используемого в вашей организации программного обеспечения с официального сайта производителя. Это позволяет сократить ресурсы приложения, затрачиваемые на обработку трафика из доверенных источников.

3. **Добавление правил доступа и правил защиты**

   Вы можете добавлять правила доступа (см. раздел "Добавление правила доступа" на стр. 84) и правила защиты (см. раздел "Добавление правила защиты" на стр. 86) как для отдельной рабочей области, так и для всех рабочих областей. Кроме того, правила можно объединять в группы или добавлять их вне групп.

4. **Настройка инициатора срабатывания правила (на стр. 87)**

   Для каждого добавленного правила требуется указать пользователя или приложение, сетевые соединения которых будет проверять Kaspersky Web Traffic Security.

5. **Настройка критериев фильтрации трафика (см. раздел "Настройка фильтрации трафика" на стр. 88)**

   С помощью критериев фильтрации необходимо задать условия, при соблюдении которых запрошенный пользователем веб-ресурс будет проверен согласно правилу.

   > Для правил обхода доступны критерии **URL**, **MIME-тип HTTP-сообщения**, **Направление трафика**, **HTTP-метод**, **HTTP Content-Length, КБ**.

6. **Добавление исключения для правила (см. раздел "Добавление исключения для правила обработки трафика" на стр. 91), если требуется**

   Вы можете добавить в исключения инициатора срабатывания правила или критерий фильтрации. Например, вы можете запретить доступ к категории **Программное обеспечение, аудио, видео** для всех сотрудников доменной группы *Бухгалтерия*, кроме руководителя отдела. Или вы можете запретить загрузку файлов размером более 500 МБ, кроме файла с корпоративными стандартами организации и т.д.

7. **Настройка расписания работы правила (см. раздел "Настройка расписания работы правила**

обработки трафика" на стр. 93), если требуется

Расписание позволяет автоматически отключать правило в заданные часы. Например, вы можете настроить работу правил только в рабочие часы организации или отключить правило в определенный день.

8. **Настройка политики защиты по умолчанию (на стр. 99)**

   Если веб-ресурс не удовлетворяет условиям фильтрации ни одного из правил обработки трафика, то применяется политика защиты по умолчанию. Параметры политики защиты по умолчанию распространяются на обработку трафика всех рабочих областей, а также вне рабочих областей.

Добавление правила обхода

Создание правил обхода для отдельных рабочих областей недоступно.

Веб-ресурсы, к которым применяются правила обхода, не учитываются в статистике обработанного трафика в разделе **Мониторинг**.

► *Чтобы добавить правило обхода:*

1. В окне веб-интерфейса приложения в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите вкладку **Обход**.

   Откроется таблица правил обхода.

4. Нажмите на кнопку **Добавить правило**.

   Откроется окно добавления правила.

5. Выберите вкладку **Общие параметры**.
6. В раскрывающемся списке **Действие** выберите один из следующих вариантов:

   - **Разрешить без проверки**, если вы хотите добавить правило разрешения.

     Приложение не будет выполнять проверку объектов на вирусы, фишинг, некоторые легальные программы, которые могут быть использованы злоумышленниками, и другие программы, представляющие угрозу. Доступ к запрашиваемому веб-ресурсу будет разрешен без проверки.

   - **Заблокировать**, если вы хотите добавить правило запрета.
   - **Перенаправить**, если вы хотите добавить правило перенаправления пользователя на указанный URL-адрес.

По умолчанию установлено значение **Заблокировать**.

> Если в запросе веб-ресурса используется HTTP-метод CONNECT и в правиле заданы действия **Заблокировать** или **Перенаправить**, то соединение будет прервано. Пользователь не будет перенаправлен на заданный в правиле веб-ресурс, и ему не будет отображаться страница блокировки. Это применимо ко всем запросам, использующим HTTP-метод CONNECT, независимо от того, указан ли этот метод в критериях фильтрации трафика.

7. В поле **Название правила** введите название правила обхода.

   > Название правила должно быть уникально среди правил в разделе **Глобальная**.

8. Если требуется, в поле **Комментарий** введите комментарий.
9. Если вы хотите применить правило сразу после добавления, переведите переключатель **Статус** в положение **Включено**.
10. Нажмите на кнопку **Добавить**.

Правило обхода будет добавлено.

Добавление правила доступа

► *Чтобы добавить правило доступа:*

1. В окне веб-интерфейса приложения выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   > Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите вкладку **Доступ**.

   Откроется таблица правил доступа.
4. Выполните одно из следующих действий:
   - Если вы хотите добавить правило в группу правил, выберите нужную группу и в открывшемся окне нажмите на кнопку **Добавить правило**.
   - Если вы хотите добавить правило вне группы, в верхней части окна нажмите на кнопку **Добавить правило**.

   Откроется окно добавления правила.
5. Выберите вкладку **Общие параметры**.

6. В раскрывающемся списке **Действие** выберите один из следующих вариантов:
   - **Заблокировать**, если вы хотите запрещать доступ к веб-ресурсам.
   - **Разрешить**, если вы хотите разрешать доступ к веб-ресурсам.
   - **К следующей группе**, если вы хотите пропустить проверку по правилам этой группы.

     Приложение будет выполнять проверку по правилам, которые расположены в таблице после этой группы.
   - **Перенаправить**, если вы хотите добавить правило перенаправления пользователя на указанный URL-адрес.

   По умолчанию установлено значение **Заблокировать**.

   Если в запросе веб-ресурса используется HTTP-метод CONNECT и в правиле заданы действия **Заблокировать** или **Перенаправить**, то соединение будет прервано. Пользователь не будет перенаправлен на заданный в правиле веб-ресурс, и ему не будет отображаться страница блокировки. Это применимо ко всем запросам, использующим HTTP-метод CONNECT, независимо от того, указан ли этот метод в критериях фильтрации трафика.

7. Если вы выбрали вариант **Заблокировать** и хотите, чтобы при попытке открыть ресурс, доступ к которому заблокирован, использовалась страница блокировки, отличная от страницы по умолчанию (см. раздел "Настройка страницы блокировки по умолчанию" на стр. 162), выполните следующие действия:
   a. Установите флажок **Введите текст для отображения на странице блокировки**.
   b. Введите текст сообщения.
8. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из поддерживаемых макросов (см. раздел "Список поддерживаемых макросов" на стр. 160). Если вы выбрали вариант **Разрешить** и хотите удалять HTTP-заголовок Range, установите флажок **Удалять HTTP-заголовок Range**.

   Если флажок установлен, то все объекты будут загружаться целиком для дальнейшей проверки с помощью правил защиты. Загрузка объектов по частям в этом режиме невозможна.
9. Если вы выбрали вариант **Перенаправить**, в поле **URL-адрес перенаправления** укажите URL-адрес, на который будет перенаправлен исходный запрос.
10. В поле **Название правила** введите название правила доступа.

    Название должно быть уникально в рамках рабочей области, если вы создаете правило рабочей области, или среди правил раздела **Глобальная**, если вы создаете правило вне рабочих областей.
11. Если требуется, в поле **Комментарий** введите комментарий.
12. Если вы хотите применить правило сразу после добавления, переведите переключатель **Статус** в положение **Включено**.
13. Нажмите на кнопку **Добавить**.

Правило доступа будет добавлено.

kaspersky

Добавление правила защиты

► *Чтобы добавить правило защиты:*

1. В окне веб-интерфейса приложения выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите вкладку **Защита**.

   Откроется таблица правил защиты.
4. Выполните одно из следующих действий:
   - Если вы хотите добавить правило в группу правил, выберите нужную группу и в открывшемся окне нажмите на кнопку **Добавить правило**.
   - Если вы хотите добавить правило вне группы, в верхней части окна нажмите на кнопку **Добавить правило**.

   Откроется окно добавления правила.
5. Выберите вкладку **Общие параметры**.
6. В блоке параметров **Действия** в раскрывающихся списках выберите одно из действий для каждого из следующих параметров:
   a. **Вредоносная программа**:
      - **Заблокировать**.
      - **Заблокировать, по возможности вылечить**.
      - **Пропустить проверку**.

      По умолчанию установлено значение **Заблокировать, по возможности вылечить**.
   b. **Объекты, обнаруженные KATA**, **Фишинг**, **Вредоносная ссылка**, **Зашифрованный объект** и **Документ с макросом**:
      - **Заблокировать**.
      - **Пропустить проверку**.

      По умолчанию установлено значение **Заблокировать**.

Если в запросе веб-ресурса используется HTTP-метод CONNECT и в правиле заданы действия **Заблокировать** или **Заблокировать, по возможности вылечить**, то соединение будет прервано. Пользователю не будет отображаться страница блокировки. Это применимо ко всем запросам, использующим HTTP-метод CONNECT, независимо от того, указан ли этот метод в критериях фильтрации трафика.

7. Если вы хотите, чтобы при попытке открыть ресурс, доступ к которому заблокирован, использовалась страница блокировки, отличная от страницы по умолчанию (см. раздел "Настройка страницы блокировки по умолчанию" на стр. 162), выполните следующие действия:

   a. Установите флажок **Введите текст для отображения на странице блокировки**.

   b. Введите текст сообщения.

8. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из поддерживаемых макросов (см. раздел "Список поддерживаемых макросов" на стр. 160). В поле **Название правила** введите название правила защиты.

   Название должно быть уникально в рамках рабочей области, если вы создаете правило рабочей области, или среди правил раздела **Глобальная**, если вы создаете правило вне рабочих областей.

9. Если требуется, в поле **Комментарий** введите комментарий.

10. Если вы хотите применить правило сразу после добавления, переведите переключатель **Статус** в положение **Включено**.

11. Нажмите на кнопку **Добавить**.

Правило защиты будет добавлено.

Настройка инициатора срабатывания правила

► *Чтобы настроить инициатора срабатывания правила:*

1. В окне веб-интерфейса приложения выберите один из следующих разделов:

   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.

3. Выберите одну из следующих закладок:

   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.

4. Выберите правило, для которого вы хотите настроить инициатора срабатывания правила.

   Откроется окно с информацией о правиле.

5. Нажмите на кнопку **Изменить**.

6. Нажмите на кнопку  в блоке **Инициатор**.
7. В появившемся раскрывающемся списке выберите один из следующих вариантов:
   - **Имя пользователя**.

     Вы можете выбрать учетную запись пользователя из Active Directory или добавить имя пользователя в формате `username@REALM`.
   - **LDAP: group canonicalName**.

     Вы можете выбрать доменную группу из Active Directory или добавить название группы в формате `domain.com/groups/groupname`.
   - **LDAP: user distinguishedName**.

     Вы можете выбрать отличительное имя (DN, Distinguished Name) пользователя из Active Directory или добавить имя пользователя в формате `cn=username,ou=users,dc=test,dc=ru`.
   - **IP-адрес**.

     Вы можете указать IP-адрес пользователя или диапазон IP-адресов в формате IPv4 или IPv6 (например, `192.168.0.1/32`).
   - **User agent**.

     Вы можете указать название браузера или программы, обрабатывающей веб-трафик (например, `*IE*`).
8. В поле справа от раскрывающегося списка укажите значение выбранного вами параметра.

   Вы можете использовать регулярные выражения.
9. Если вы добавили более одного критерия, в раскрывающемся списке рядом с названием блока **Инициатор** выберите логический оператор:
   - Если вы хотите, чтобы правило срабатывало при соблюдении хотя бы одного из добавленных условий, выберите **любой из**.
   - Если вы хотите, чтобы правило срабатывало только при одновременном соблюдении всех добавленных условий, выберите **все из**.
10. Нажмите на кнопку **Сохранить**.

Инициатор срабатывания правила будет настроен.

Настройка фильтрации трафика

Для корректной обработки HTTPS-трафика требуется настроить перехват SSL-соединений на внешнем прокси-сервере (см. раздел "Настройка SSL Bumping в сервисе Squid" на стр. 256). Если перехват SSL-соединений не настроен, критерии фильтрации трафика не будут применены и проверка веб-ресурса модулями Антивирус и Анти-Фишинг не будет выполняться.

► *Чтобы настроить фильтрацию трафика:*

1. В окне веб-интерфейса приложения выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило, для которого вы хотите настроить критерии фильтрации.

   Откроется окно с информацией о правиле.
5. Нажмите на кнопку **Изменить**.
6. Нажмите на кнопку  в блоке **Фильтрация трафика**.
7. В появившемся раскрывающемся списке выберите один из следующих вариантов:

   Для правил обхода доступны критерии URL, MIME-тип HTTP-сообщения, Направление трафика, HTTP-метод, HTTP Content-Length, КБ.

   - **Категория**.

     С помощью этого критерия вы можете контролировать доступ пользователей к веб-ресурсам какой-либо тематики. Например, вы можете запретить доступ к социальным сетям, выбрав категорию **Социальные сети**. Список веб-категорий, поддерживаемых приложением, см. в Приложении 3 (см. раздел "Приложение 3. Категории сайтов" на стр. 242).
   - **URL**.

     Вы можете добавить в критерии фильтрации не только URL-адреса, но и протокол или порт сетевых соединений.
     - Если вы хотите добавить в критерии фильтрации URL-адреса, введите их в поле в окне **URL** и нажмите на кнопку **Добавить**.

       Если URL-адрес не прошел процесс нормализации (см. раздел "Приложение 2. Нормализация URL-адресов" на стр. 241), он не будет добавлен в список и будет отображаться сообщение об ошибке.

Убедитесь, что любая часть указанного URL-адреса не содержит символы ? и #, а части Домен и Порт не содержат символ @. В противном случае URL-адрес будет импортирован не полностью.

- Если вы хотите добавить в критерии фильтрации протокол или порт сетевых соединений, то в окне **URL** введите в поле любое значение и нажмите на кнопку **Добавить**. В появившихся ниже полях **Протокол** и **Порт** укажите необходимые значения.

  Например, вы можете запретить доступ ко всем веб-ресурсам по протоколу HTTP.

- **Имя файла**.

  Вы можете добавить в критерии фильтрации название конкретного файла или использовать регулярные выражения. Например, вы можете запретить загрузку исполняемых файлов с расширением exe, указав значение `*.exe`.

- **Тип файла**.

  Вирус или другая программа, представляющая угрозу, может распространяться в исполняемом файле, переименованном в файл с другим расширением, например, txt. Если вы выбрали критерий фильтрации **Имя файла** и указали значение `*.exe`, то такой файл не будет обработан приложением. Если же вы выбрали фильтрацию файлов по формату, то приложение проверяет истинный формат файла, вне зависимости от его расширения. Если в результате проверки выясняется, что файл имеет формат EXE, то приложение обрабатывает его в соответствии с правилом.

- **Размер файла, КБ**.

  С помощью этого критерия вы можете контролировать объем сетевого трафика организации. Например, запретить загрузку файлов, размер которых превышает 700 МБ.

- **MIME-тип части HTTP-сообщения**.

  С помощью этого критерия вы можете контролировать доступ к multipart-объектам в соответствии с содержимым их составных частей.

- **MIME-тип HTTP-сообщения**.

  С помощью этого критерия вы можете контролировать доступ к объектам в соответствии с их содержимым. Например, вы можете запретить воспроизведение потокового видео-контента, указав значение `video/*`. Примеры указания MIME-типов объектов см. в Приложении 1 (см. раздел "Приложение 1. MIME-типы объектов" на стр. 240).

  При указании `multipart/*` учитывается общий заголовок Content-Type объекта. Отдельные составные части объекта не обрабатываются. Для фильтрации трафика по составным частям multipart-объекта требуется использовать критерий **MIME-тип части HTTP-сообщения**.

- **MD5**.

  Вы можете запретить доступ к объекту, указав его MD5-хеш. Это может понадобиться, если вы получили информацию о вирусе или другой программе, представляющей угрозу, из сторонней системы и знаете только его MD5-хеш.

- **SHA256**.

  Вы можете запретить доступ к объекту, указав его SHA2-хеш. Это может понадобиться, если вы

получили информацию о вирусе или другой программе, представляющей угрозу, из сторонней системы и знаете только его SHA2-хеш.

- **Направление трафика**.

  С помощью этого критерия вы можете настроить обработку всех входящих или исходящих соединений.

- **HTTP-метод**.

  С помощью этого критерия вы можете контролировать доступ к трафику в зависимости от используемого HTTP-метода.

- **HTTP Content-Length, КБ**.

  С помощью HTTP-заголовка Content-Length вы можете контролировать доступ к трафику в зависимости от длины тела HTTP-сообщения. Если заголовок Content-Length присутствует, то приложение использует его значение для применения критериев фильтрации трафика. Если этот заголовок отсутствует, то значение Content-Length считается пустым и не учитывается при обработке трафика.

  Доступно только для правил обхода.

8. В поле справа от раскрывающегося списка укажите значение выбранного вами параметра.
9. Если вы добавили более одного критерия, в раскрывающемся списке рядом с названием блока **Фильтрация трафика** выберите логический оператор:
   - Если вы хотите, чтобы правило срабатывало при соблюдении хотя бы одного из добавленных условий, выберите **любой из**.
   - Если вы хотите, чтобы правило срабатывало только при одновременном соблюдении всех добавленных условий, выберите **все из**.
10. Нажмите на кнопку **Сохранить**.

Фильтрация трафика будет настроена.

Добавление исключения для правила обработки трафика

► *Чтобы добавить исключение для правила обработки трафика:*

1. В окне веб-интерфейса приложения выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.

3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило обработки трафика, для которого вы хотите добавить исключение.

   Откроется окно с информацией о правиле.
5. Нажмите на кнопку **Изменить**.
6. Выберите вкладку **Исключения**.
7. Нажмите на кнопку **+ Добавить исключение**.

   Появится блок параметров исключения **Исключение**.
8. Добавьте инициатора соединения. Для этого нажмите на кнопку  .
9. Укажите следующие параметры:
   a. В раскрывающемся списке **Инициатор** выберите один из следующих вариантов:
      - **Имя пользователя**.
      - **LDAP: group canonicalName**.
      - **LDAP: user distinguishedName**.
      - **IP-адрес**.
      - **User agent**.

   b. В поле справа от раскрывающегося списка укажите значение выбранного вами параметра.
   c. Если вы хотите добавить нового инициатора соединения, повторите действия по добавлению инициатора соединения.
10. Добавьте критерий фильтрации трафика. Для этого нажмите на кнопку  .
11. Укажите следующие параметры:
    a. В раскрывающемся списке **Фильтрация трафика** выберите один из следующих вариантов:
       - **Категория**.
       - **URL**.
       - **Имя файла**.
       - **Тип файла**.
       - **Размер файла, КБ**.
       - **MIME-тип HTTP-сообщения**.
       - **MIME-тип части HTTP-сообщения**.
       - **MD5**.
       - **SHA256**.
       - **Направление трафика**.

- **HTTP-метод**.

b. В поле справа от раскрывающегося списка укажите значение выбранного вами параметра.

c. Если вы хотите добавить новый критерий фильтрации, повторите действия по добавлению критерия.

12. Нажмите на кнопку **Сохранить**.

Исключение для правила обработки трафика будет добавлено.

Настройка расписания работы правила обработки трафика

► *Чтобы настроить расписание работы правила обработки трафика:*

1. В окне веб-интерфейса приложения выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило обработки трафика, расписание работы которого вы хотите настроить.

   Откроется окно с информацией о правиле.
5. Нажмите на кнопку **Изменить**.
6. Выберите вкладку **Расписание**.
7. Если вы хотите отключить правило после наступления запланированной даты, установите флажок **Отключить правило** и во всплывающем календаре укажите дату и время завершения действия правила.
8. Если вы хотите, чтобы правило действовало в определенные дни недели и часы, выполните следующие действия:
   a. Установите флажок **Задать расписание действия правила**.
   b. Установите флажки рядом с названиями дней недели, в которые будет действовать правило.
   c. Укажите период действия правила.
9. Нажмите на кнопку **Сохранить**.

Расписание работы правила обработки трафика будет настроено.

kaspersky

Изменение правила обработки трафика

► *Чтобы изменить правило обработки трафика:*

1. В окне веб-интерфейса приложения выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило обработки трафика, которое вы хотите изменить.

   Откроется окно с информацией о правиле.
5. В правом нижнем углу окна нажмите на кнопку **Изменить**.

   Откроется окно изменения правила.
6. Внесите необходимые изменения.
7. Нажмите на кнопку **Сохранить**.

Правило обработки трафика будет изменено.

Удаление правила обработки трафика

► *Чтобы удалить правило обработки трафика:*

1. В окне веб-интерфейса приложения выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.

3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило, которое вы хотите удалить.

   Откроется окно с информацией о правиле.
5. Нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения удаления правила обработки трафика.
6. Нажмите на кнопку **Да**.

Правило обработки трафика будет удалено.

Создание копии правила обработки трафика

► *Чтобы скопировать правило обработки трафика:*

1. В окне веб-интерфейса приложения выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило обработки трафика, которое вы хотите скопировать.

   Откроется окно с информацией о правиле обработки трафика.
5. Нажмите на кнопку **Копировать**.

   Откроется окно создания правила обработки трафика. Все параметры правила обработки трафика будут скопированы.
6. Измените имя копии правила обработки трафика.
7. Нажмите на кнопку **Добавить**.

Будет создана копия правила обработки трафика.

kaspersky

Включение и отключение правила обработки трафика

► *Чтобы включить или отключить правило обработки трафика:*

1. В окне веб-интерфейса приложения выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило, которое вы хотите включить или отключить.

   Откроется окно с информацией о правиле.
5. Выполните одно из следующих действий:
   - Если вы хотите включить правило, нажмите на кнопку **Включить**.

     Правило будет включено.
   - Если вы хотите отключить правило, нажмите на кнопку **Отключить**.

     Правило будет отключено.

Изменение порядка применения правил

Правила проверяются в порядке расположения в таблице правил обработки трафика сверху вниз. В рамках группы правила также проверяются по порядку сверху вниз. Изменение порядка применения правил выполняется с помощью перемещения в таблице правил обработки трафика.

► *Чтобы изменить порядок применения правил:*

1. В окне веб-интерфейса приложения выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. В строке с названием правила или группы правил в левой части окна нажмите на значок  и, удерживая левую клавишу мыши, перетащите эту строку в нужное место таблицы.

   Перемещая строку **Правила рабочей области**, вы изменяете приоритет правил рабочей области.
5. Нажмите на кнопку **Сохранить**.

Порядок применения правил будет изменен в соответствии с новым расположением правил в таблице.

Работа с группами правил обработки трафика

Вы можете объединять правила доступа и правила защиты в группы, чтобы задать порядок их проверки. Создание групп для правил обхода недоступно.

Kaspersky Web Traffic Security проверяет группы по списку сверху вниз. Внутри каждой группы правила также проверяются согласно следованию в таблице. Вы можете изменять приоритет группы и правила внутри группы, перемещая их вверх или вниз.

Создание группы правил обработки трафика

► *Чтобы создать группу правил обработки трафика:*

1. В окне веб-интерфейса приложения выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:

- **Доступ**.
- **Защита**.

4. Нажмите на кнопку **Добавить группу**.

   Откроется окно создания группы правил.

5. В поле **Название** введите название новой группы правил.

   > Название должно быть уникально в рамках рабочей области, если вы создаете группу правил рабочей области, или среди групп раздела **Глобальная**, если вы создаете группу правил вне рабочих областей.

6. Нажмите на кнопку **Добавить**.

Группа правил обработки трафика будет создана.

Изменение группы правил обработки трафика

► *Чтобы изменить группу правил обработки трафика:*

1. В окне веб-интерфейса приложения выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   > Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Доступ**.
   - **Защита**.
4. Выберите группу правил, которую вы хотите изменить.

   Откроется окно с информацией о группе правил.

5. Нажмите на кнопку **Изменить**.
6. В поле **Название** введите новое название группы правил.

   > Название должно быть уникально в рамках рабочей области, если вы создаете группу правил рабочей области, или среди групп раздела **Глобальная**, если вы создаете группу правил вне рабочих областей.

7. Нажмите на кнопку **Сохранить**.

Группа правил обработки трафика будет изменена.

Удаление группы правил обработки трафика

► *Чтобы удалить группу правил обработки трафика:*

1. В окне веб-интерфейса приложения выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.
2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Доступ**.
   - **Защита**.
4. Выберите группу правил, которую вы хотите удалить.

   Откроется окно с информацией о группе правил.
5. Нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения удаления группы правил обработки трафика.
6. Нажмите на кнопку **Да**.

Группа правил обработки трафика будет удалена.

Настройка политики защиты по умолчанию

Политика защиты по умолчанию применяется к веб-ресурсам, которые не удовлетворили критериям фильтрации ни одного из правил обработки трафика. В параметрах политики вам требуется установить для каждого типа объекта действие, которое приложение должно выполнять с этим объектом.

► *Чтобы настроить политику защиты по умолчанию:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Защита**.
2. В блоке параметров **Политика защиты по умолчанию** выберите действия, которые приложение должно выполнять с объектами следующих типов:
   - **Вредоносная программа**:
     - **Заблокировать**.
     - **Заблокировать, по возможности вылечить**.
     - **Пропустить проверку**.
   - **Объекты, обнаруженные KATA**:
     - **Заблокировать**.

- **Пропустить проверку**.
- **Фишинг**:
  - **Заблокировать**.
  - **Пропустить проверку**.
- **Вредоносная ссылка**:
  - **Заблокировать**.
  - **Пропустить проверку**.
- **Зашифрованный объект**:
  - **Заблокировать**.
  - **Пропустить проверку**.
- **Документ с макросом**:
  - **Заблокировать**.
  - **Пропустить проверку**.

По умолчанию для **Вредоносная программа** установлено значение **Заблокировать, по возможности вылечить**. Для остальных типов объектов установлено значение **Заблокировать**.

3. Нажмите на кнопку **Сохранить**.

Политика защиты по умолчанию будет настроена. Если по результатам проверки приложение не обнаружит угроз, доступ к веб-ресурсу будет разрешен.

Мониторинг работы правил обработки трафика

После того как правила обработки трафика вступают в силу, вы можете просматривать информацию об их выполнении в разделе **События**. При возникновении вопросов о работе правила вы можете найти это правило в таблице раздела **Правила** и посмотреть заданные в нем параметры.

Обработка запросов пользователей о доступе к веб-ресурсам

Если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно, он может обратиться к администратору локальной сети организации. В этом случае необходимо выяснить, в рамках какого правила обработки трафика был запрещен доступ. Для этого нужно найти событие в журнале по указанным пользователем параметрам.

► *Чтобы выяснить причину блокировки доступа к веб-ресурсу:*

1. В окне веб-интерфейса приложения выберите раздел **События**.
2. Выберите вкладку **Трафик** при ее наличии.
3. Нажмите на кнопку **Добавить условие**.
4. Настройте фильтр по имени обратившегося пользователя:
   a. В левом раскрывающемся списке выберите **Пользователь**.
   b. В центральном раскрывающемся списке выберите **Равняется**.
   c. В правом поле введите имя пользователя.

5. Нажмите на кнопку **Добавить условие**.
6. Настройте фильтр по веб-адресу заблокированного веб-ресурса:
   a. В левом раскрывающемся списке выберите **URL**.
   b. В центральном раскрывающемся списке выберите **Равняется**.
   c. В правом поле введите веб-адрес заблокированного веб-ресурса.
7. Нажмите на кнопку **Найти**.

Отобразится таблица событий, удовлетворяющих условиям фильтрации. В графе **Название правила** вы можете посмотреть правило обработки трафика, согласно которому пользователю запрещен доступ к веб-ресурсу.

Получение статистики о доступе к веб-ресурсам

В целях мониторинга сетевой активности пользователей вам может потребоваться получить статистику о посещении определенного веб-ресурса или о сетевых соединениях конкретных пользователей. Для этого вы можете отфильтровать события в журнале событий и экспортировать полученный результат в файл формата CSV.

► *Чтобы получить статистику о доступе к веб-ресурсам:*

1. В окне веб-интерфейса приложения выберите раздел **События**.
2. Выберите вкладку **Трафик** при ее наличии.
3. Нажмите на кнопку **Добавить условие**.
4. Настройте фильтр событий с помощью появившихся раскрывающихся списков:
   a. В левом раскрывающемся списке выберите критерий фильтрации.
   b. В центральном раскрывающемся списке выберите оператор сравнения.

      Для каждого критерия фильтрации доступен свой релевантный набор операторов сравнения. Например, при выборе критерия **Направление** доступны операторы **Равняется** и **Не равняется**.
   c. В зависимости от выбранного критерия фильтрации выполните одно из следующих действий:
      - Укажите в поле справа от оператора сравнения один или несколько символов, по которым вы хотите выполнить поиск событий.
      - В правом раскрывающемся списке выберите вариант условия, по которому вы хотите выполнить поиск событий.

      Например, для поиска полного совпадения по имени пользователя введите имя пользователя.
5. Нажмите на кнопку **Найти**.

   Отобразится таблица событий, удовлетворяющих условиям фильтрации.
6. Нажмите на кнопку **Экспортировать**.

Файл с отфильтрованными событиями будет сохранен в папке загрузки браузера в формате CSV.

При конвертации полученного файла CSV в другие форматы необходимо учитывать, что в качестве разделителя полей используется точка с запятой.

kaspersky

Просмотр таблицы правил обработки трафика

Таблица правил обработки трафика отображается в разделе **Правила**. Если вы перешли в веб-интерфейс отдельной рабочей области, то в таблице отображаются только правила обработки трафика для этой рабочей области.

В таблице правил обработки трафика содержится следующая информация:

1. **Название**. Название правила обработки трафика.
2. **Действие**. Действие, которое выполняет правило обработки трафика.

   В правилах обхода возможны следующие действия:

   - **Разрешить без проверки**.
   - **Заблокировать**.
   - **Перенаправить**.

   В правилах доступа возможны следующие действия:

   - **Заблокировать**.
   - **Разрешить**.
   - **К следующей группе**.
   - **Перенаправить**.

   В правилах защиты возможны следующие действия:

   - **Заблокировать**.
   - **Заблокировать, по возможности вылечить**.
   - **Пропустить проверку**.
3. **Статус**. Использование правила обработки трафика во время проверки веб-ресурсов.

   Правило обработки трафика может находиться в одном из следующих состояний:

   - **Выключено**.
   - **Включено**.
4. **Комментарий**. Комментарий к правилу обработки трафика.

Просмотр информации о правиле обработки трафика

► *Чтобы просмотреть информацию о правиле обработки трафика:*

1. В окне веб-интерфейса приложения выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило обработки трафика, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о правиле.

Окно содержит следующие вкладки:

1. **Общие параметры**.

   Общие параметры правила обработки трафика:

   a. **Статус** – использование правила обработки трафика при проверке веб-ресурсов.

   b. **Действие** – действие, которое выполняет правило обработки трафика.

   c. **Название правила** – название правила обработки трафика.

   d. **Комментарий** – комментарий к правилу обработки трафика.
2. **Исключения**.

   Информация о каждом исключении из правила обработки трафика отображается в отдельном блоке параметров **Исключение**:

   a. **Инициатор** – инициатор соединения.

   b. **Фильтрация трафика** – фильтр трафика.
3. **Расписание**.

   Расписание работы правила обработки трафика. Отображается дата отключения правила, а также дни недели и периоды работы правила.

Обработка CONNECT-запросов

При обработке трафика, передаваемого по протоколу HTTPS, результат применения действий приложения **Заблокировать** и **Перенаправить** отличается от применения этих действий к трафику, передаваемому по протоколу HTTP. Пользователю не отображается страница блокировки, и не выполняется перенаправление на заданный URL-адрес. Вместо этого соединение обрывается.

Это связано с тем, что для установки шифрованных соединений по протоколу HTTPS компьютер пользователя запрашивает у прокси-сервера соединение с веб-сервером с помощью HTTP-сообщения, содержащего метод CONNECT (далее также "CONNECT-запрос"). Возможности прокси-серверов по обработке CONNECT-запросов и ответу на них ограничены на уровне HTTP-протокола. Прокси-сервер может либо уведомить пользователя об успешной установке соединения, либо прервать соединение.

Чтобы действия **Заблокировать** и **Перенаправить** применялись корректно, вам требуется включить расшифровку TLS/SSL-соединений на прокси-сервере, а также добавить метод CONNECT в исключения или создать для него правило обхода. При отсутствии правил обработки трафика, разрешающих CONNECT-запросы, соединение будет прервано.

Разрешение CONNECT-запросов может привести к снижению защиты IT-инфраструктуры организации. Рекомендуется добавлять метод CONNECT в исключения только в тех правилах обработки трафика, для которых отображение страницы блокировки и выполнение перенаправления являются критичными.

Далее в этой статье приведены особенности и различия в обработке трафика, передаваемого по протоколу HTTP с помощью стандартных HTTP-сообщений, и трафика, передаваемого по протоколу HTTPS, когда для установки шифрованных соединений используются CONNECT-запросы.

Обработка стандартных HTTP-сообщений

Большинство HTTP-методов (например, GET, POST, DELETE, HEAD, OPTIONS, PATCH, PUT, TRACE) предназначено для обмена HTTP-сообщениями между клиентом, то есть компьютером пользователя, и веб-сервером, на котором хранится запрашиваемый веб-ресурс. Kaspersky Web Traffic Security может проверять такие HTTP-сообщения и применять к ним все доступные в приложении действия. Принципы обработки HTTP-сообщений в приложении Kaspersky Web Traffic Security представлены на рисунке ниже.

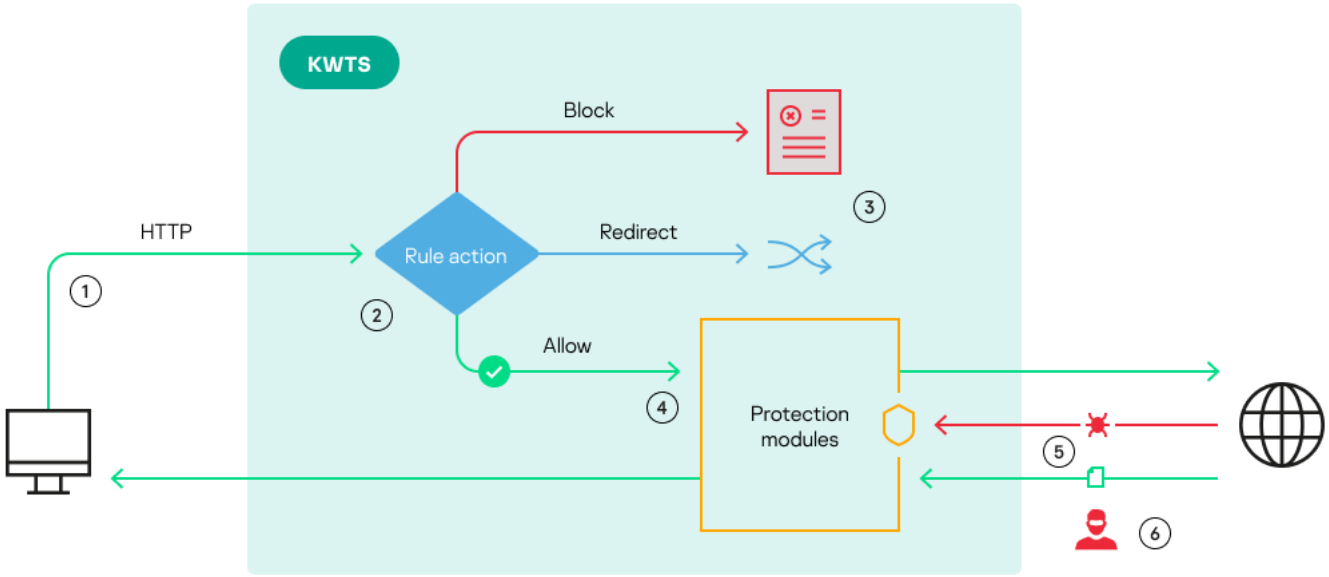

Рисунок 8. Принципы обработки HTTP-сообщений

Нумерация на рисунке соответствует следующим этапам обработки стандартных HTTP-сообщений:

1. Пользователь запрашивает доступ к веб-ресурсу. Этот запрос передается на прокси-сервер.
2. Приложение проверяет, удовлетворяет ли запрошенный веб-ресурс критериям правил доступа.
3. Если в результате применения правила доступа выполняется действие **Заблокировать**, пользователю отображается страница блокировки. Если выполняется действие **Перенаправить**, пользователь перенаправляется на заданный URL-адрес.
4. Если в результате применения правила доступа выполняется действие **Разрешить**, то приложение переходит к проверке трафика с помощью правил защиты или политики защиты по умолчанию. При отсутствии обнаруженных угроз запрос пользователя передается на веб-сервер.

5. Полученный ответ от веб-сервера также проверяется модулями защиты на наличие вирусов и других угроз. При обнаружении угроз приложение блокирует трафик, а при их отсутствии передает ответ веб-сервера на компьютер пользователя.
6. При попытке несанкционированного доступа злоумышленники могут перехватить данные, так как трафик передается в нешифрованном виде.

Особенности обработки CONNECT-запросов

При попытке получить доступ к веб-ресурсу по протоколу HTTPS компьютер пользователя отправляет на прокси-сервер CONNECT-запрос на соединение с веб-сервером. В результате обмена параметрами шифрования и сертификатами безопасности между компьютером пользователя и веб-сервером устанавливается туннелированное защищенное соединение по протоколу TLS. Внутри этого туннеля клиент и веб-сервер обмениваются HTTP-сообщениями с использованием стандартных HTTP-методов (GET, POST и т.д.). По умолчанию прокси-сервер не может анализировать содержимое шифрованного соединения и вмешиваться в обмен сообщениями внутри туннеля. Механизм обработки шифрованных соединений по умолчанию представлен на рисунке ниже.

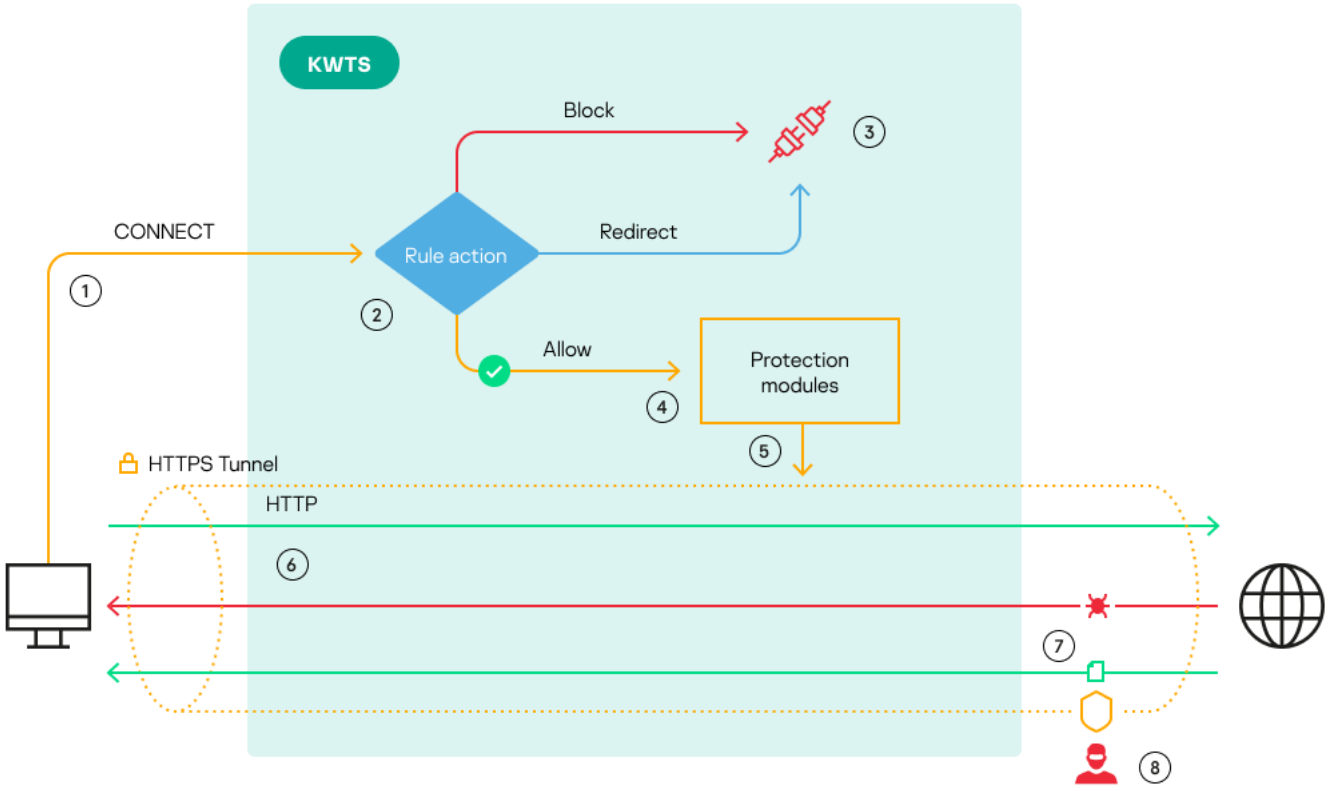

Рисунок 9. Механизм обработки шифрованных соединений по умолчанию

Нумерация на рисунке соответствует следующим этапам обработки шифрованных соединений по умолчанию:

1. Компьютер пользователя при помощи CONNECT-запроса запрашивает у прокси-сервера организацию шифрованного канала связи с веб-сервером.
2. Приложение проверяет, удовлетворяет ли запрошенный веб-ресурс критериям правил доступа.
3. Если в результате применения правил выполняется действие **Заблокировать** или **Перенаправить**,

соединение обрывается. Пользователю не отображается страница блокировки, и он не перенаправляется на заданный URL-адрес.

4. Если в результате применения правила доступа выполняется действие **Разрешить**, приложение передает CONNECT-запрос для дальнейшей обработки модулями защиты.
5. При успешной проверке CONNECT-запроса модулями защиты прокси-сервер формирует шифрованный канал связи между компьютером пользователя и веб-сервером.
6. Внутри шифрованного канала связи компьютер пользователя обменивается с веб-сервером обычными HTTP-сообщениями. При этом прокси-сервер не может получить доступ к этим сообщениям и передать их на проверку модулям защиты, так как передаваемые данные зашифрованы.
7. Ответ веб-сервера также передается компьютеру пользователя напрямую без проверки модулями защиты. Это снижает уровень защиты IT-инфраструктуры организации, так как на компьютер пользователя может поступать трафик, содержащий угрозы.
8. При попытке несанкционированного доступа злоумышленники не могут перехватить данные, так как трафик передается внутри шифрованного канала.

Чтобы приложение могло проверять трафик, передаваемый внутри шифрованного канала связи, модулями защиты, вам требуется настроить расшифровку TLS/SSL-соединений. Механизм обработки шифрованных соединений при включенной расшифровке TLS/SSL-соединений представлен на рисунке ниже.

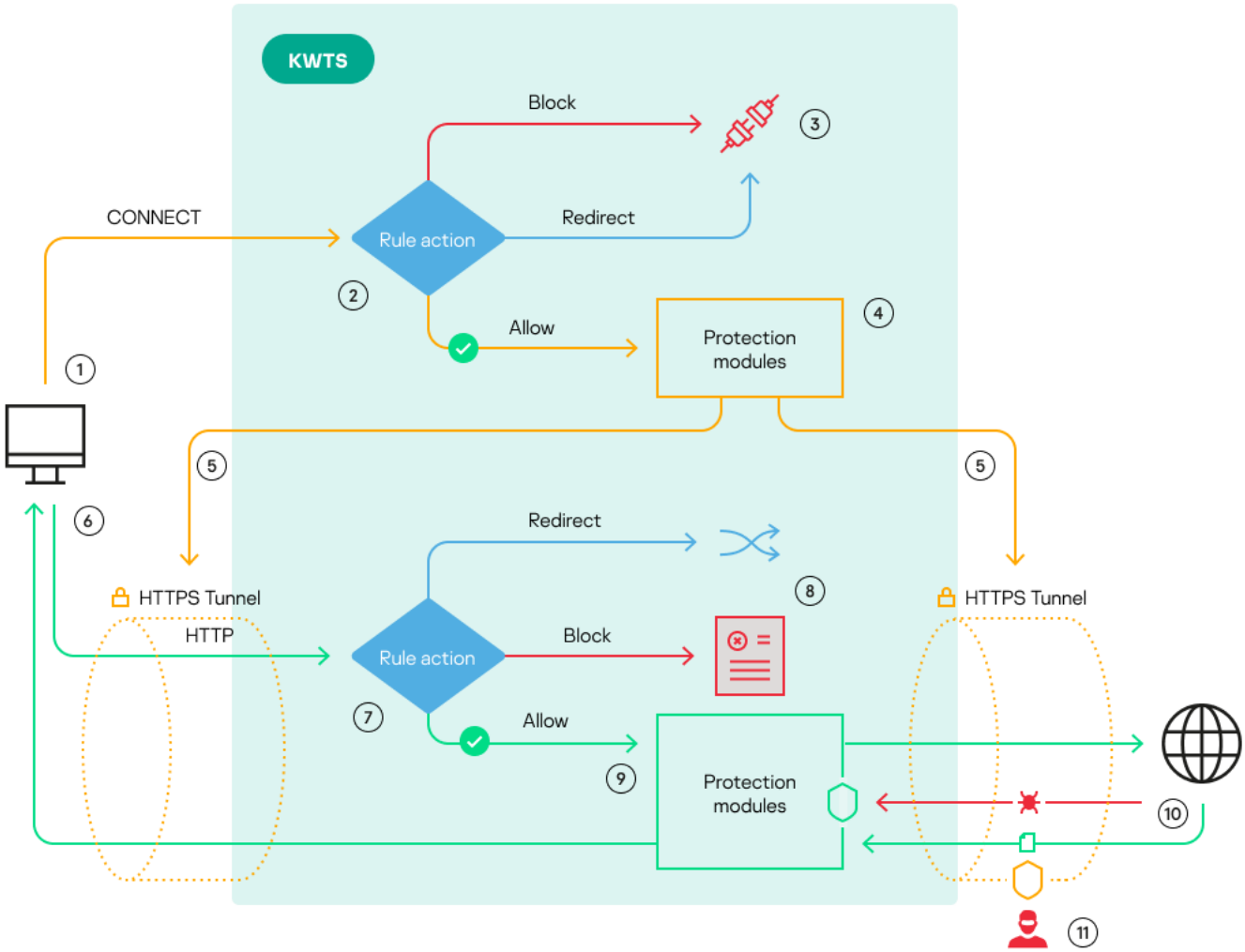

Рисунок 10. Механизм обработки шифрованных соединений при включенной расшифровке TLS/SSL-соединений

Нумерация на рисунке соответствует следующим этапам обработки шифрованных соединений при включенной расшифровке TLS/SSL-соединений:

1. Компьютер пользователя при помощи CONNECT-запроса запрашивает у прокси-сервера организацию шифрованного канала связи с веб-сервером.
2. Приложение проверяет, удовлетворяет ли запрошенный веб-ресурс критериям правил доступа.
3. Если в результате применения правила доступа выполняется действие **Заблокировать** или **Перенаправить**, соединение обрывается. Пользователю не отображается страница блокировки, и он не перенаправляется на заданный URL-адрес.
4. Если в результате применения правила доступа выполняется действие **Разрешить**, приложение передает CONNECT-запрос для дальнейшей обработки модулями защиты.
5. При успешной проверке CONNECT-запроса модулями защиты между компьютером пользователя и прокси-сервером, а также между прокси-сервером и веб-сервером устанавливаются шифрованные каналы связи.
6. Внутри шифрованного канала связи компьютер пользователя обменивается с веб-сервером обычными HTTP-запросами. Приложение получает доступ ко всем передаваемым данным и может применять к ним правила защиты.
7. Приложение проверяет, удовлетворяет ли запрошенный веб-ресурс критериям правил доступа.
8. Если в результате применения правила доступа выполняется действие **Заблокировать**, пользователю отображается страница блокировки. Если выполняется действие **Перенаправить**, пользователь перенаправляется на заданный URL-адрес.
9. Если в результате применения правила доступа выполняется действие **Разрешить**, то приложение переходит к проверке трафика с помощью правил защиты или политики защиты по умолчанию. При отсутствии обнаруженных угроз запрос пользователя передается на веб-сервер.
10. Полученный ответ от веб-сервера также проверяется модулями защиты на наличие вирусов и других угроз. При обнаружении угроз приложение блокирует трафик, а при их отсутствии передает ответ веб-сервера на компьютер пользователя по шифрованному каналу связи.
11. При попытке несанкционированного доступа злоумышленники не могут перехватить данные, так как трафик передается внутри шифрованного канала связи.

В этом разделе

Настройка исключений в правилах обработки трафика

Перед созданием исключений для CONNECT-запросов убедитесь, что вы включили расшифровку TLS/SSL-соединений. В противном случае зашифрованные соединения не будут проверены модулями Антивирус и Анти-Фишинг. Это может привести к заражению компьютеров пользователей.

► *Чтобы настроить исключения для CONNECT-запросов в правилах обработки трафика:*

1. В веб-интерфейсе приложения выберите раздел **Правила**.
2. Выберите вкладку **Доступ**.
3. Выберите правило, для которого требуется корректно отображать страницу блокировки или

выполнять перенаправление пользователя.

Откроется страница **Просмотреть правило**.

4. Нажмите на кнопку **Изменить**.

   Откроется страница **Изменить правило**.

5. Выберите вкладку **Исключения**.
6. Нажмите на кнопку **+ Добавить исключение**.
7. Если вы хотите добавить исключение только для пользователей с заданными критериями, в блоке параметров **Инициатор** нажмите на кнопку **+ Условия правила** и укажите нужные критерии.

   Если критерии не указаны, исключение распространяется на всех пользователей.

8. В блоке параметров **Фильтрация трафика** нажмите на кнопку **+ Условия правила**.
9. В появившемся раскрывающемся списке слева выберите **HTTP-метод**.
10. В раскрывающемся списке справа выберите **CONNECT**.
11. Нажмите на кнопку **Сохранить**.

Исключение будет настроено. Приложение не будет проверять HTTP-сообщения, содержащие метод CONNECT.

Создание правила обхода

Перед созданием правила обхода убедитесь, что вы включили расшифровку TLS/SSL-соединений. Если расшифровка TLS/SSL-соединений не настроена, HTTP-сообщения, содержащие метод CONNECT, не будут проверены модулями Антивирус и Анти-Фишинг. Это может привести к заражению компьютеров пользователей.

► *Чтобы создать правило обхода для CONNECT-запросов:*

1. В веб-интерфейсе приложения выберите раздел **Правила**.
2. Выберите вкладку **Обход**.
3. Нажмите на кнопку **Добавить правило**.

   Откроется окно **Добавить правило**.

4. В раскрывающемся списке **Действие** выберите **Разрешить без проверки**.
5. Если вы хотите добавить правило только для пользователей с заданными критериями, в блоке параметров **Инициатор** нажмите на кнопку **+ Условия правила** и укажите нужные критерии.

   Если критерии не указаны, правило распространяется на всех пользователей.

6. В блоке параметров **Фильтрация трафика** нажмите на кнопку **+ Условия правила**.
7. В появившемся раскрывающемся списке слева выберите **HTTP-метод**.
8. В раскрывающемся списке справа выберите **CONNECT**.
9. В поле **Название правила** введите название правила.
10. Если требуется, в поле **Комментарий** укажите любую дополнительную информацию о правиле.

11. Переведите переключатель **Статус** в положение **Включено**.
12. Нажмите на кнопку **Добавить**.

Правило обхода будет создано и отобразится в таблице правил. Приложение будет пропускать без проверки все HTTP-сообщения, содержащие метод CONNECT.

kaspersky

Управление рабочими областями

Рабочая область – набор параметров и прав доступа, применимых к выделенной группе пользователей. Например, вы можете создавать рабочие области для подразделений компании или для управляемых организаций (если вы являетесь поставщиком услуг).

Использование рабочих областей предоставляет следующие возможности:

- разграничение прав доступа к каждой рабочей области между разными администраторами;
- создание правил обработки трафика, действующих только для пользователей отдельной рабочей области;
- настройка индивидуальной страницы блокировки.

В этом разделе

Сценарий настройки рабочей области

Настройка рабочей области включает в себя следующие этапы.

1. **Добавление рабочей области (на стр. 113)**
2. **Добавление роли администратора рабочей области (см. раздел "Добавление роли" на стр. 125), если требуется**

   В приложении доступны роли по умолчанию (см. раздел "Набор прав для ролей по умолчанию" на стр. 124). Вы можете назначить учетной записи администратора одну из этих ролей. Если набор прав для ролей по умолчанию вам не подходит, вы можете добавить новую роль.
3. **Назначение роли администратора рабочей области (см. раздел "Назначение роли" на стр. 128)**

   После того, как вы назначили пользователю роль администратора рабочей области, он может войти в веб-интерфейс приложения под своей доменной учетной записью. Пользователю будут доступны разделы веб-интерфейса в соответствии с предоставленными ему правами доступа.

   Вы можете добавлять несколько администраторов для одной рабочей области или создавать другие роли с нужным вам набором прав доступа.
4. **Создание правил обработки трафика для этой рабочей области (см. раздел "Сценарий настройки доступа к веб-ресурсам" на стр. 81)**

5. **Изменение страницы блокировки (см. раздел "Настройка страницы блокировки для рабочей области" на стр. 162), если требуется**

   После создания рабочей области пользователям отображается страница блокировки по умолчанию. Вы можете настроить индивидуальную страницу блокировки, которая будет отображаться только пользователям этой рабочей области.

Просмотр таблицы рабочих областей

Таблица рабочих областей отображается в разделе **Рабочие области** окна веб-интерфейса приложения.

В таблице рабочих областей содержится следующая информация:

- **Название** – название рабочей области.
- **Критерии** – критерии для определения трафика рабочей области.
- **Выделено лицензий** – количество лицензий, выделенных для этой рабочей области.
- **Комментарий** – комментарий к рабочей области.

Просмотр информации о рабочей области

► *Чтобы просмотреть информацию о рабочей области:*

1. В окне веб-интерфейса приложения выберите раздел **Рабочие области**.
2. Выберите рабочую область, информацию о которой вы хотите просмотреть.

   Откроется окно с информацией о рабочей области.

Окно содержит следующую информацию:

- Вкладка **Общие**:
  - **Название** – название рабочей области.
  - **Комментарий** – комментарий к рабочей области.
  - **Закрепить клиентские лицензии за рабочей областью** – количество лицензий, выделенных для этой рабочей области.
  - **Критерии** – критерии для определения трафика рабочей области.
- Вкладка **Страница блокировки** – параметры страницы блокировки для рабочей области (см. раздел "Настройка страницы блокировки для рабочей области" на стр. 162).

Настройка отображения таблицы рабочих областей

► *Чтобы настроить отображение таблицы рабочих областей:*

1. В окне веб-интерфейса приложения выберите раздел **Рабочие области**.

   Откроется таблица рабочих областей.

2. По кнопке  откройте меню отображения таблицы рабочих областей.
3. Установите флажки рядом с теми параметрами, которые должны отображаться в таблице рабочих областей.

   Должен быть установлен хотя бы один флажок.

4. Если вы хотите обновить информацию о рабочих областях, нажмите на кнопку **Обновить**.

   Информация о рабочих областях будет обновлена.

Отображение таблицы рабочих областей будет настроено.

Добавление рабочей области

► *Чтобы добавить рабочую область:*

1. В окне веб-интерфейса приложения выберите раздел **Рабочие области**.
2. Нажмите на кнопку **Добавить рабочую область**.

   Откроется окно добавления рабочей области.
3. В поле **Название** укажите название рабочей области.
4. В поле **Комментарий** укажите комментарий к рабочей области.

   Необязательный параметр.
5. Если вы хотите закрепить за этой рабочей областью часть клиентских лицензий, выполните следующие действия:
   a. Установите флажок **Закрепить клиентские лицензии за рабочей областью**.
   b. Укажите количество клиентских лицензий, которые вы хотите закрепить за этой рабочей областью.
6. Добавьте критерий для определения трафика рабочей области. Для этого выполните следующие действия:
   a. В блоке критериев для определения трафика рабочей области **Критерии** в раскрывающемся списке выберите один из следующих вариантов:
      - **LDAP: group canonicalName**.
      - **LDAP: user distinguishedName**.
      - **IP-адрес**.
   b. В поле справа от раскрывающегося списка укажите значение выбранного вами параметра.
7. Если вы хотите добавить новый критерий рабочей области, выполните следующие действия:
   a. Нажмите на кнопку  .
   b. Повторите действия пункта 6 по добавлению критерия рабочей области.
8. Если вы указали несколько критериев рабочей области, по ссылке справа от названия блока **Критерии** вы можете выбрать один из следующих вариантов:
   - **любые из**, если вы хотите, чтобы для определения трафика рабочей области было достаточно

соответствия любому из добавленных критериев.

- **все из**, если вы хотите, чтобы для определения трафика рабочей области требовалось соответствие всем добавленным критериям.

9. Нажмите на кнопку **Добавить**.

Рабочая область будет добавлена.

Изменение параметров рабочей области

► *Чтобы изменить параметры рабочей области:*

1. В окне веб-интерфейса приложения выберите раздел **Рабочие области**.

   Откроется таблица рабочих областей.

2. Выберите рабочую область, параметры которой вы хотите изменить.

   Откроется окно **Просмотреть рабочую область**.

3. В правом нижнем углу окна нажмите на кнопку **Изменить**.

   Откроется окно **Изменить рабочую область**.

4. Внесите необходимые изменения в параметры рабочей области.
5. Нажмите на кнопку **Сохранить**.

Параметры рабочей области будут изменены.

Удаление рабочей области

► *Чтобы удалить рабочую область:*

1. В окне веб-интерфейса приложения выберите раздел **Рабочие области**.

   Откроется таблица рабочих областей.

2. Выберите рабочую область, которую вы хотите удалить.

   Откроется окно с информацией о рабочей области.

3. Нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения удаления рабочей области.

4. Нажмите на кнопку **Да**.

Рабочая область будет удалена.

Переключение между рабочими областями в веб-интерфейсе

Локальный администратор имеет доступ ко всем рабочим областям. Вы также можете предоставить одному пользователю доступ к нескольким рабочим областям.

При создании и настройке рабочих областей, а также впоследствии при работе с неисправностями

приложения пользователю может понадобиться переключаться между рабочими областями. Отображение раздела переключения между рабочими областями в дереве веб-интерфейса определяется по алгоритму, описанному в таблице ниже.

Таблица 5. Алгоритм отображения рабочих областей в веб-интерфейсе приложения

Наличие рабочих областей	Права вне рабочих областей		Права на параметры рабочих областей	Отображение в веб-интерфейсе
	Наличие прав на действия с кластером и с параметрами приложения	Наличие прав на действия с рабочими областями, ролями, правилами, событиями обработки трафика, а также просмотр раздела Мониторинг		
Нет	Не влияет на отображение раздела переключения.	Не влияет на отображение раздела переключения.	Недоступно.	Раздел переключения между рабочими областями не отображается.
Есть	Нет	Есть	Нет.	Раздел переключения между рабочими областями не отображается.
	Нет	Нет	Есть права только в одной рабочей области.	В разделе переключения отображается название рабочей области, но список рабочих областей недоступен.
	Нет	Нет	Есть разрешения в нескольких рабочих областях.	В разделе переключения доступны только те рабочие области, в которых у пользователя есть хотя бы одно разрешение. Раздел **Глобальная** не отображается.
	Нет	Есть	Не влияет на отображение раздела переключения.	В разделе переключения доступен список всех рабочих областей, но не отображается раздел **Глобальная**.

Наличие рабочих областей	Права вне рабочих областей		Права на параметры рабочих областей	Отображение в веб-интерфейсе
	Наличие прав на действия с кластером и с параметрами приложения	Наличие прав на действия с рабочими областями, ролями, правилами, событиями обработки трафика, а также просмотр раздела Мониторинг		
	Есть	Есть	Не влияет на отображение раздела переключения.	В разделе переключения доступен список всех рабочих областей, а также раздел **Глобальная**.

► *Чтобы переключиться между рабочими областями:*

1. В веб-интерфейсе приложения выберите раздел **Глобальная**, если вы находитесь вне рабочих областей, или раздел с названием вашей организации, если вы находитесь в веб-интерфейсе рабочей области.
2. В раскрывшейся панели выберите название рабочей области, в которую вы хотите перейти.

Отобразится веб-интерфейс выбранной рабочей области. В дереве слева будут доступны разделы веб-интерфейса в соответствии с правами доступа текущего пользователя.

kaspersky

Работа с ролями и учетными записями пользователей

Вы можете создавать различные роли для учетных записей пользователей приложения в зависимости от прав, которыми они должны обладать. Таблица ролей и учетных записей пользователей, обладающих этими ролями, отображается в разделе **Пользователи** окна веб-интерфейса приложения.

Для каждой роли вы можете задать набор прав, которыми будет обладать роль. Кроме того, в приложении доступны роли по умолчанию (см. раздел "Набор прав для ролей по умолчанию" на стр. 124), создаваемые во время установки приложения:

- *Superuser* с полным набором прав.
- *Viewer*, обладающая правами только на просмотр информации в веб-интерфейсе приложения.

Удаление и изменение роли по умолчанию недоступно.

Вы можете добавлять роли для рабочей области или вне рабочих областей.

Если пользователю назначена роль для рабочей области, то права этой роли распространяются только на параметры данной рабочей области. Пользователь не сможет выполнять действия с параметрами в других рабочих областях.

Если пользователю назначена роль вне рабочих областей, то разрешения этой роли распространяются на параметры всех рабочих областей.

В этом разделе

Ролевое разграничение доступа к функциям приложения

В зависимости от назначенной роли пользователю будут доступны определенные разделы веб-интерфейса и операции с параметрами приложения.

Описание операций с параметрами приложения в зависимости от назначенного права, приведено в таблице ниже.

Таблица 6. Операции, доступные при назначении прав

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Просматривать разделы Мониторинг и Отчеты	Просмотр всей информации в разделах **Мониторинг** (см. раздел "**Мониторинг работы приложения**" на стр. 68) и **Отчеты** (см. раздел "**Отчеты**" на стр. 73).	Да	Просмотр информации в разделе **Мониторинг** со следующими ограничениями: • не отображается график **Работоспособность системы**; • отсутствует возможность фильтрации по узлам и по рабочим областям. Просмотр, скачивание (см. раздел "Скачивание отчета на компьютер" на стр. 74) и удаление (см. раздел "Удаление отчета" на стр. 74) всех ранее созданных отчетов, а также создание новых отчетов (см. раздел "Создание отчета" на стр. 73) только для текущей рабочей области.
Просматривать события обработки трафика	Просмотр журнала событий (на стр. 76) обработки трафика рабочих областей и вне рабочих областей, а также экспорт событий обработки трафика в разделе **События**.	Да	Просмотр журнала событий (на стр. 76) обработки трафика рабочих областей, а также экспорт событий обработки трафика в разделе **События**.
Просматривать системные события	Просмотр журнала системных событий (см. раздел "Просмотр журнала событий" на стр. 76) приложения, а также экспорт системных событий приложения в разделе **События**.	Нет	Функциональность отсутствует.

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Создавать/изменять правила	Добавление правил обхода (см. раздел "Добавление правила обхода" на стр. 83), правил доступа (см. раздел "Добавление правила доступа" на стр. 84) и правил защиты (см. раздел "Добавление правила защиты" на стр. 86) для рабочих областей и вне рабочих областей, а также изменение их параметров (см. раздел "Изменение правила обработки трафика" на стр. 94) в разделе **Правила**.	Да	Добавление правил обхода (см. раздел "Добавление правила обхода" на стр. 83), правил доступа (см. раздел "Добавление правила доступа" на стр. 84) и правил защиты (см. раздел "Добавление правила защиты" на стр. 86) для текущей рабочей области, а также изменение их параметров (см. раздел "Изменение правила обработки трафика" на стр. 94) в разделе **Правила**.
Просматривать правила	Просмотр таблицы правил обработки трафика (на стр. 102) для рабочих областей и вне рабочих областей в разделе **Правила**. При назначении этого права пользователь не сможет добавлять или удалять правила, а также изменять их параметры.	Да	Просмотр таблицы правил обработки трафика (на стр. 102) для текущей рабочей области в разделе **Правила**. При назначении этого разрешения пользователь не сможет добавлять или удалять правила, а также изменять их параметры.
Удалять правила	Удаление правил обработки трафика (см. раздел "Удаление правила обработки трафика" на стр. 94) для рабочих областей и вне рабочих областей в разделе **Правила**.	Да	Удаление правил обработки трафика (см. раздел "Удаление правила обработки трафика" на стр. 94) для текущей рабочей области в разделе **Правила**.

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Создавать/изменять рабочие области	Добавление рабочих областей (см. раздел "Добавление рабочей области" на стр. 113) и изменение параметров рабочих областей (см. раздел "Изменение параметров рабочей области" на стр. 114) в разделе **Рабочие области**.	Да	Функциональность отсутствует.
Просматривать рабочие области	Просмотр таблицы рабочих областей (на стр. 112) в разделе **Рабочие области**. При назначении этого права пользователь не сможет добавлять и удалять рабочие области, а также изменять их параметры.	Да	Функциональность отсутствует.
Удалять рабочие области	Удаление рабочих областей (см. раздел "Удаление рабочей области" на стр. 114) в разделе **Рабочие области**.	Да	Функциональность отсутствует.
Создавать/изменять роли	Добавление ролей (см. раздел "Добавление роли" на стр. 125) для рабочих областей и вне рабочих областей, а также изменение их параметров (см. раздел "Изменение параметров роли" на стр. 126) в разделе **Пользователи**.	Да	Добавление ролей (см. раздел "Добавление роли" на стр. 125) для текущей рабочей области, а также изменение их параметров (см. раздел "Изменение параметров роли" на стр. 126) в разделе **Пользователи**.

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Просматривать роли	Просмотр списка ролей для рабочих областей и вне рабочих областей в разделе **Пользователи**. При назначении этого права пользователь не сможет добавлять или удалять роли, а также изменять их параметры.	Да	Просмотр списка ролей для текущей рабочей области в разделе **Пользователи**. При назначении этого разрешения пользователь не сможет добавлять или удалять роли, а также изменять их параметры.
Удалять роли	Удаление ролей (см. раздел "Удаление роли" на стр. 127) для рабочих областей и вне рабочих областей в разделе **Пользователи**.	Да	Удаление ролей (см. раздел "Удаление роли" на стр. 127) для текущей рабочей области в разделе **Пользователи**.
Создавать/изменять/удалять узлы	Добавление (см. раздел "Добавление узла в кластер" на стр. 133) и удаление узлов кластера (см. раздел "Удаление узла из кластера" на стр. 134), а также изменение их параметров (см. раздел "Изменение параметров узла" на стр. 133) в разделе **Узлы**.	Нет	Функциональность отсутствует.
Получать диагностическую информацию	Запуск трассировки (на стр. 235), изменение уровня трассировки (на стр. 236), а также просмотр журналов трассировки (на стр. 236) узлов кластера. При назначении этого права пользователь сможет также просматривать информацию об узлах, добавлять и удалять узлы, а также изменять их параметры.	Нет	Функциональность отсутствует.

Право	Доступная функциональность вне рабочих областей		Доступная функциональность в рабочей области
	Описание права	Возможность переключения между рабочими областями	
Проверять целостность данных	Проверка целостности данных (на стр. 135) на узлах кластера. При назначении этого права пользователь сможет также просматривать информацию об узлах, добавлять и удалять узлы, а также изменять их параметры.	Нет	Функциональность отсутствует.
Просматривать информацию об узлах	Просмотр информации об узлах (см. раздел "Просмотр информации об узле кластера" на стр. 131) в разделе **Узлы**. При назначении этого права пользователь не сможет добавлять и удалять узлы, а также изменять их параметры.	Нет	Функциональность отсутствует.
Изменять параметры	Изменение параметров приложения в разделе **Параметры**.	Нет	Функциональность отсутствует.
Просматривать параметры	Просмотр параметров приложения в разделе **Параметры**. Это право не разрешает пользователю изменять параметры приложения.	Нет	Функциональность отсутствует.
Управлять доступом SSH	Добавление и удаление открытого ключа SSH.	Нет	Функциональность отсутствует.
Создавать/изменять страницу блокировки	Функциональность отсутствует.	Нет	Изменение страницы блокировки (см. раздел "Настройка страницы блокировки для рабочей области" на стр. 162) для текущей рабочей области.
Просматривать страницу блокировки	Функциональность отсутствует.	Нет	Просмотр страницы блокировки для текущей рабочей области.

Соответствие между доступными разделами веб-интерфейса приложения и назначенными пользователю правами представлено в таблице ниже.

Таблица 7. Доступ к разделам веб-интерфейса в зависимости от назначенных прав

Область применения	Право	Раздел веб-интерфейса, к которому предоставляется доступ	
		вне рабочих областей	в рабочей области
Вне рабочих областей	**Просматривать разделы Мониторинг и Отчеты**	**Мониторинг**	**Мониторинг**
	Просматривать события обработки трафика	**События**	**События**
	Просматривать системные события	**События**	Недоступно
	Создавать/изменять правила	**Правила**	**Правила**
	Просматривать правила		
	Удалять правила		
	Создавать/изменять рабочие области	**Рабочие области**	**Параметры рабочей области**
	Просматривать рабочие области		
	Удалять рабочие области		
	Создавать/изменять роли	**Пользователи**	**Пользователи**
	Просматривать роли		
	Удалять роли		
	Создавать/изменять/удалять узлы	**Узлы**	Недоступно
	Получать диагностическую информацию		
	Проверять целостность данных		
	Просматривать информацию об узлах		
	Изменять параметры	**Параметры**	Недоступно
	Просматривать параметры		
	Управлять доступом SSH		
В рабочей области	**Просматривать разделы Мониторинг и Отчеты**	Недоступно	**Мониторинг**

Область применения	Право	Раздел веб-интерфейса, к которому предоставляется доступ	
		вне рабочих областей	в рабочей области
	Просматривать события обработки трафика	Недоступно	**События**
	Создавать/изменять правила	Недоступно	**Правила**
	Просматривать правила		
	Удалять правила		
	Создавать/изменять роли	Недоступно	**Пользователи**
	Просматривать роли		
	Удалять роли		
	Создавать/изменять страницу блокировки	Недоступно	**Параметры рабочей области**
	Просматривать страницу блокировки		

Набор прав для ролей по умолчанию

После установки приложения в разделе **Пользователи** отображаются две роли по умолчанию. Кроме того, роли по умолчанию создаются в рамках каждой рабочей области. При удалении рабочей области роли по умолчанию, созданные в этой рабочей области, также удаляются.

Набор прав для ролей по умолчанию вне рабочих областей и в рабочей области представлен в таблице ниже.

Таблица 8. Набор прав для ролей по умолчанию

Право	Вне рабочих областей		В рабочей области	
	Superuser	Viewer	Superuser	Viewer
Просматривать разделы Мониторинг и Отчеты	Есть	Есть	Есть	Есть
Просматривать события обработки трафика	Есть	Есть	Есть	Есть
Просматривать системные события	Есть	Есть	Недоступно	Недоступно
Создавать/изменять правила	Есть	Нет	Есть	Нет
Просматривать правила	Есть	Есть	Есть	Есть
Удалять правила	Есть	Нет	Есть	Нет

Право	Вне рабочих областей		В рабочей области	
	Superuser	Viewer	Superuser	Viewer
Создавать/изменять рабочие области	Есть	Нет	Недоступно	Недоступно
Просматривать рабочие области	Есть	Есть	Недоступно	Недоступно
Удалять рабочие области	Есть	Нет	Недоступно	Недоступно
Создавать/изменять роли	Есть	Нет	Есть	Нет
Просматривать роли	Есть	Есть	Есть	Есть
Удалять роли	Есть	Нет	Есть	Нет
Создавать/изменять/удалять узлы	Есть	Нет	Недоступно	Недоступно
Получать диагностическую информацию	Есть	Нет	Недоступно	Недоступно
Проверять целостность данных	Есть	Нет	Недоступно	Недоступно
Просматривать информацию об узлах	Есть	Есть	Недоступно	Недоступно
Изменять параметры	Есть	Нет	Недоступно	Недоступно
Просматривать параметры	Есть	Есть	Недоступно	Недоступно
Управлять доступом SSH	Есть	Нет	Недоступно	Недоступно
Создавать/изменять страницу блокировки	Недоступно	Недоступно	Есть	Нет
Просматривать страницу блокировки	Недоступно	Недоступно	Есть	Есть

Добавление роли

► *Чтобы добавить роль:*

1. В окне веб-интерфейса приложения в разделе переключения между рабочими областями выберите один из следующих вариантов:
   - Название рабочей области, если вы хотите добавить роль для одной рабочей области.
   - **Глобальная**, если вы хотите добавить роль вне рабочих областей.

2. Выберите раздел **Пользователи**.
3. Откроется список ролей и учетных записей.
4. Нажмите на кнопку **Добавить**.

   Откроется окно добавления роли.
5. В поле **Имя** введите имя роли.
6. В списке **Права** установите флажки рядом с теми правами, которыми должна обладать роль (см. раздел "Ролевое разграничение доступа к функциям приложения" на стр. 117).
7. Нажмите на кнопку **Добавить**.

Роль будет добавлена.

Просмотр информации о роли

► *Чтобы просмотреть информацию о роли:*

1. В окне веб-интерфейса приложения в разделе переключения между рабочими областями выберите один из следующих вариантов:
   - Название рабочей области, если вы хотите просмотреть информацию о роли конкретной рабочей области.
   - **Глобальная**, если вы хотите просмотреть информацию о роли вне рабочих областей.
2. Выберите раздел **Пользователи**.

   Откроется список ролей и учетных записей.
3. В левой части окна выберите роль, информацию о которой вы хотите просмотреть.

Отобразится следующая информация:

- На вкладке **Учетные записи** отображается список учетных записей пользователей, которым назначена выбранная роль. Вы можете отзывать роль (см. раздел "Отзыв роли" на стр. 128) или назначать ее (см. раздел "Назначение роли" на стр. 128) новым пользователям.
- На вкладке **Права** отображается набор прав, которые получает пользователь при назначении ему этой роли. Вы можете изменять список прав (см. раздел "Изменение параметров роли" на стр. 126) для выбранной роли.

Изменение параметров роли

Изменение роли Superuser недоступно.

Вы можете изменить параметры роли: название роли, а также набор прав, которыми она обладает.

► *Чтобы изменить параметры роли:*

1. В веб-интерфейсе приложения в разделе переключения между рабочими областями выберите один из следующих вариантов:
   - Название рабочей области, если вы хотите изменить параметры роли для одной рабочей

области.

- **Глобальная**, если вы хотите изменить параметры роли вне рабочих областей.

2. Выберите раздел **Пользователи**.

   Откроется список ролей и учетных записей.

3. В блоке параметров **Роли** выберите роль, параметры которой вы хотите изменить, и нажмите на кнопку  .

4. В раскрывающемся списке выберите вариант **Изменить**.

   Откроется окно **Изменить роль**.

5. Если требуется, измените название роли в поле **Имя**.

6. Если требуется, измените набор прав, которыми обладает роль. Для этого снимите или установите флажки в блоке параметров **Права**.

7. Нажмите на кнопку **Сохранить**.

Параметры роли будут изменены.

Удаление роли

Удаление роли Superuser недоступно.

► *Чтобы удалить роль:*

1. В веб-интерфейсе приложения в разделе переключения между рабочими областями выберите один из следующих вариантов:

   - Название рабочей области, если вы хотите удалить роль для одной рабочей области.
   - **Глобальная**, если вы хотите удалить роль вне рабочих областей.

2. Выберите раздел **Пользователи**.

   Откроется список ролей и учетных записей.

3. В списке **Роли** выберите роль, которую вы хотите удалить.

4. Нажмите на кнопку  .

5. В раскрывающемся списке выберите вариант **Удалить**.

   Отобразится окно подтверждения удаления роли.

6. Нажмите на кнопку **Да**.

Роль будет удалена.

kaspersky

Назначение роли

► *Чтобы назначить роль для учетной записи:*

1. В веб-интерфейсе приложения в разделе переключения между рабочими областями выберите один из следующих вариантов:
   - Название рабочей области, если вы хотите предоставить пользователю разрешения на параметры одной рабочей области.
   - **Глобальная**, если вы хотите предоставить пользователю разрешения на параметры всех рабочих областей.
2. Выберите раздел **Пользователи**.

   Откроется список ролей и учетных записей.
3. В списке **Роли** выберите роль, которую вы хотите назначить для учетной записи.
4. Нажмите на кнопку **Назначить роль**.

   Откроется окно **Назначить роль**.
5. В поле **Учетная запись (домен\имя для NTLM или user@REALM для Kerberos; значение чувствительно к регистру)** введите доменное имя учетной записи, которой вы хотите назначить роль.
6. Нажмите на кнопку **Сохранить**.

Роль будет назначена выбранной учетной записи.

Отзыв роли

► *Чтобы отозвать роль у пользователя:*

1. В веб-интерфейсе приложения в разделе переключения между рабочими областями выберите один из следующих вариантов:
   - Название рабочей области, если вы хотите отозвать у пользователя разрешения на параметры одной рабочей области.
   - **Глобальная**, если вы хотите отозвать у пользователя разрешения на параметры всех рабочих областей.
2. Выберите раздел **Пользователи**.

   Откроется список ролей и учетных записей.
3. В левой части окна выберите роль, которую вы хотите отозвать.
4. На вкладке **Учетные записи** установите флажки напротив тех пользователей, у которых вы хотите отозвать роль.
5. Нажмите на кнопку **Отозвать роль**.
6. В окне подтверждения нажмите на кнопку **Да**.

Роль будет отозвана у пользователя. Пользователь больше не сможет совершать действия с параметрами приложения, которые были ему доступны в соответствии с правами этой роли.

kaspersky

Изменение пароля учетной записи Administrator

Учетная запись Administrator с правами суперпользователя позволяет входить в систему без использования внешних служб. Пароль этой учетной записи действует в течение одного года. После истечения срока действия пароля при попытке входа в веб-интерфейс приложения администратору отобразится запрос на смену пароля. Аутентификация с учетной записью Administrator будет возможна только после смены пароля.

► *Чтобы изменить пароль учетной записи Administrator:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Доступ к программе**.
2. Перейдите в раздел **Локальный администратор**.
3. В поле **Старый пароль** введите текущий пароль учетной записи Administrator.

   В первый раз этот пароль задается во время установки приложения.

4. В поле **Новый пароль** введите новый пароль, удовлетворяющий требованиям к паролю.

   Требования к паролю приведены под полем.

   Повторное использование пароля не допускается. Kaspersky Web Traffic Security сравнивает новый пароль с последними 24 паролями, которые использовались ранее. При полном совпадении с одним из использовавшихся ранее паролей отображается ошибка.

5. В поле **Подтвердите пароль** введите новый пароль повторно.
6. Нажмите на кнопку **Сохранить**.

Пароль будет изменен.

kaspersky

Управление кластером

После установки и первоначальной настройки (см. раздел "Установка и первоначальная настройка приложения" на стр. 50) вы можете настраивать параметры в веб-интерфейсе приложения. Для этого требуется объединить все узлы с установленным приложением Kaspersky Web Traffic Security в кластер. Вы можете добавлять узлы в кластер (см. раздел "Добавление узла в кластер" на стр. 133) и удалять узлы из кластера (см. раздел "Удаление узла из кластера" на стр. 134). Вы можете назначить роль Управляющего узла (см. раздел "Изменение роли узла в кластере" на стр. 134) любому из узлов, входящих в кластер. Остальные серверы в кластере получат роль Подчиненный узел. Независимо от роли все узлы кластера будут осуществлять обработку трафика.

Объединять в кластер можно только узлы с Kaspersky Web Traffic Security одинакового типа – только установленные из ISO-файла или только установленные из DEB-пакета.
IP-адрес узлов кластера должен быть в одинаковом формате: только IPv4 или только IPv6.

В разделе **Узлы** окна веб-интерфейса приложения отображается таблица узлов кластера, а также следующая информация об узлах:

- **Состояние соединения с KSN/KPSN**.
- **Состояние баз**.
- **Лицензия**.

В этом разделе

Создание нового кластера

После установки приложения требуется создать кластер для управления узлами через веб-интерфейс приложения. Кроме того, вы можете создать несколько кластеров, чтобы управлять разными группами серверов отдельно друг от друга.

► *Чтобы создать новый кластер:*

1. В веб-интерфейсе узла, которому вы хотите назначить роль Управляющий узел, нажмите на кнопку **Создать новый кластер**.
2. Через несколько минут обновите страницу браузера.

   Откроется веб-интерфейс Управляющего узла.

Кластер будет создан. После этого вы можете добавлять в кластер Подчиненные узлы (см. раздел "Добавление узла в кластер" на стр. 133).

Настройка отображения таблицы узлов кластера

► *Чтобы настроить отображение таблицы узлов кластера:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.

   Откроется таблица узлов кластера.
2. По кнопке  откройте меню отображения таблицы узлов кластера.
3. Установите флажки рядом с теми параметрами, которые должны отображаться в таблице.

   Должен быть установлен хотя бы один флажок.

Отображение таблицы узлов кластера будет настроено.

Просмотр информации об узле кластера

► *Чтобы просмотреть информацию об узле кластера:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. Выберите узел, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об узле.

Окно содержит следующую информацию в зависимости от типа сервера:

1. Блок параметров **Информация об узле**:
   - **Отпечаток сертификата** – отпечаток сертификата сервера.
   - **Комментарий** – дополнительная информация об узле. Необязательный параметр.
   - **Роль текущего узла** – роль текущего узла в кластере.
2. Блок параметров **Обработка трафика**:
   - **Количество потоков проверки** – количество одновременных потоков обработки трафика ICAP-сервером.
   - **Дата окончания срока действия лицензии**.
   - **Лицензия** – информация о лицензии и количестве дней до окончания срока действия лицензии.

- **Тип лицензии** – тип лицензии (пробная или коммерческая).
- **Серийный номер** – серийный номер лицензии.
- **Состояние подключения к KSN/KPSN** – состояние соединения со службами KSN / KPSN.
- **Антивирус** – состояние баз модуля Антивирус.
- **Анти-Фишинг** – состояние баз модуля Анти-Фишинг.
- **Отправка файлов в KATA** – наличие или отсутствие ошибок при отправке файлов в KATA (отображается только при включенном режиме **Отправлять файлы** (см. раздел "**Выбор режима интеграции**" на стр. 183)).
- **Получение объектов из KATA** – наличие или отсутствие ошибок при получении объектов, обнаруженных KATA (отображается только при включенном режиме **Получать объекты** (см. раздел "**Выбор режима интеграции**" на стр. 183)).
- **Обновление баз** – состояние баз приложения, а также результат и время их последнего успешного обновления.

3. Блок параметров **Кеш LDAP** (отображается только при настроенной интеграции с доменом Active Directory):
   - **Подключение** – дата и время последнего успешного подключения к контроллеру домена Active Directory.
   - **Данные для подбора правил** – дата и время последнего успешного обновления данных об учетных записях, используемых для подбора правил обработки трафика.
   - **Автозаполнение учетных записей** – дата и время последнего успешного обновления данных, используемых для автозаполнения имен пользователей в веб-интерфейсе приложения.

   Если хотя бы на одном из этих этапов возникла ошибка, в таблице узлов кластера отображается сообщение об ошибке.
4. Блок параметров **Параметры**:
   - Для Управляющего узла:
     - **Применены** – время последнего успешного применения параметров к модулям приложения.
   - Для Подчиненного узла:
     - **Синхронизированы** – время последнего успешного получения параметров от Управляющего узла. Если параметры получены, вы можете назначить этому Подчиненному узлу роль Управляющего без потери заданных параметров.
     - **Применены** – время последнего успешного применения параметров к модулям приложения.
     - **Время** – состояние синхронизации времени с сервером, на котором установлен Управляющий узел.

   Если статус имеет значение *Ошибка*, вы можете скопировать информацию об ошибке в буфер обмена по ссылке **Копировать** справа от статуса.

kaspersky

Добавление узла в кластер

► *Чтобы добавить узел в кластер:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. Нажмите на кнопку **Добавить узел**.

   Откроется окно **Добавить узел**.
3. В поля **IP-адрес** и **Порт** введите IP-адрес и порт сервера с установленным приложением, который вы хотите добавить в качестве узла кластера.
4. Если требуется, в поле **Комментарий** укажите дополнительную информацию о добавляемом узле.
5. В поле **Количество потоков проверки** укажите, сколько потоков трафика может обрабатывать ICAP-сервер одновременно.

   Допустимые значения: целые числа от 4 до 1024. Рекомендуемое значение: количество ядер процессора плюс один.
6. Нажмите на кнопку **Далее**.
7. Сравните отпечатки сертификата в окне **Подтвердить узел** и в файле сертификата в папке /var/opt/kaspersky/kwts/certs/controlapi.crt. Если отпечатки сертификата совпадают, нажмите на кнопку **Подтвердить**.

   Вы можете получить отпечаток сертификата с помощью следующей команды:

   ```
   openssl x509 -noout -fingerprint -sha256 -inform pem -in
   /var/opt/kaspersky/kwts/certs/controlapi.crt
   ```

Узел будет добавлен в кластер и отобразится в таблице узлов на странице **Узлы**.

Изменение параметров узла

Вы не можете изменить IP-адрес и порт сервера, на котором установлено приложение. При необходимости удалите узел из кластера (см. раздел "Удаление узла из кластера" на стр. 134) и добавьте в кластер новый узел (см. раздел "Добавление узла в кластер" на стр. 133) с нужным адресом.

► *Чтобы изменить параметры узла:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. В таблице узлов кластера выберите узел, параметры которого вы хотите изменить.

   Откроется окно параметров узла.
3. В правом нижнем углу окна нажмите на кнопку **Изменить**.

   Откроется окно **Изменить узел**.
4. Если требуется, измените следующие параметры:
   - Дополнительную информацию об узле в поле **Комментарий**.
   - Количество одновременных потоков обработки трафика ICAP-сервером в поле **Количество**

потоков проверки.

Допустимые значения: целые числа от 4 до 1024. Рекомендуемое значение: количество ядер процессора плюс один.

5. Нажмите на кнопку **Сохранить**.

Если вы изменили параметр **Количество потоков проверки**, прокси-сервер будет перезагружен. До завершения перезагрузки обработка трафика будет приостановлена.

Параметры узла будут изменены.

Удаление узла из кластера

Удаление Управляющего узла недоступно.

При удалении узла из кластера приложение не удаляется с сервера. Вы можете в любой момент добавить узел обратно в кластер и продолжить управление параметрами приложения для этого узла.

► *Чтобы удалить узел из кластера:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Подчиненный узел, который вы хотите удалить из кластера.

   Откроется окно параметров узла.
3. В левом нижнем углу окна нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения удаления узла из кластера.
4. Нажмите на кнопку **Да**.

Узел будет удален из кластера. Информация об узле не будет отображаться в таблице узлов кластера.

Изменение роли узла в кластере

Вы можете назначить любому узлу кластера роль Управляющий узел. Остальные узлы будут иметь роль Подчиненный узел. Например, смена ролей может понадобиться при выходе из строя Управляющего узла или при необходимости удалить приложение с этого сервера.

► *Чтобы назначить Управляющему узлу роль Подчиненный узел:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Управляющий узел.

   Откроется окно параметров узла.
3. Нажмите на кнопку **Назначить роль Подчиненный узел**.

Управляющий узел станет Подчиненным узлом. Откроется веб-интерфейс Подчиненного узла.

► *Чтобы назначить Подчиненному узлу роль Управляющий узел:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Подчиненный узел.

   Откроется окно параметров узла.
3. Нажмите на кнопку **Перейти к управлению узлом**.

   В новом окне браузера откроется страница авторизации.
4. Введите имя и пароль администратора приложения.

   Откроется веб-интерфейс Подчиненного узла.
5. Нажмите на кнопку **Назначить роль Управляющий узел**.
6. В окне подтверждения нажмите на кнопку **Да**.

Подчиненный узел станет Управляющим узлом.

Удаление кластера

Удаление кластера возможно только при отсутствии Подчиненных узлов.

► *Чтобы удалить кластер:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Управляющий узел.

   Откроется окно параметров узла.
3. В левом нижнем углу окна нажмите на кнопку **Удалить кластер**.

   Отобразится окно подтверждения удаления узла из кластера.
4. Нажмите на кнопку **Да**.

Кластер будет удален. Отобразится веб-интерфейс сервера с установленным приложением, не входящего в кластер.

Проверка целостности данных

Чтобы убедиться, что компоненты приложения установлены корректно, не изменены и не повреждены, вы можете запустить проверку целостности данных. При этом будут проверены MD5-хеши исполняемых файлов Kaspersky Web Traffic Security.

► *Чтобы проверить целостность данных:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. По кнопке  откройте меню раздела **Узлы**.

3. Выберите пункт **Проверить целостность данных**.

   Откроется окно **Выбор узлов для проверки целостности данных**.

4. В таблице узлов кластера установите флажки напротив тех узлов, для которых вы хотите запустить проверку целостности.

5. Нажмите на кнопку **Запустить**.

   После окончания проверки отобразится таблица с результатами. Вы можете скачать список исполняемых файлов, в которых обнаружено нарушение целостности.

kaspersky

Работа приложения в аварийном режиме

Kaspersky Web Traffic Security переходит в аварийный режим, если в системе два и более Управляющих узла. Например, Управляющий узел стал недоступен, и эта роль была назначена другому узлу в кластере. Через некоторое время первый Управляющий узел снова стал доступен, и в системе оказалось два Управляющих узла.

Аварийный режим приложения не влияет на обработку сетевого трафика. Все узлы продолжают обрабатывать сетевой трафик в соответствии с последними значениями параметров, полученными от Управляющего узла до перехода приложения в аварийный режим.

Управляющий узел

В окне аварийного режима на Управляющем узле отображается следующая информация:

- IP-адрес текущего узла.
- Роль текущего узла.
- Таблица узлов, входящих в кластер.

Таблица узлов содержит следующие графы:

- **IP-адрес:порт** – IP-адрес и порт подключения к узлу.
- **Роль** – роль текущего узла в приложении.
- **Управляющий узел** – IP-адрес Управляющего узла.

  Доступно только для Подчиненного узла.
- **Синхронизированы** – время последней синхронизации значений параметров.
- **Состояние соединения с Управляющим узлом** – доступность Управляющего узла по сети.

Значок  в строке таблицы означает, что в работе этого узла возникла проблема. Например, Подчиненный узел ошибочно стал Управляющим, или сервер недоступен по сети.

Если вы хотите передать управление приложением другому узлу, вы можете назначить текущему Управляющему узлу роль Подчиненный узел с помощью кнопки **Назначить роль Подчиненный узел**.

Подчиненный узел

В окне аварийного режима на Подчиненном узле отображается следующая информация:

- IP-адрес текущего узла.
- Роль текущего узла.
- IP-адрес и доступность Управляющего узла.
- Дата и время последней синхронизации значений параметров.
- Таблица узлов, входящих в кластер.

Таблица узлов содержит следующие графы:

- **IP-адрес:порт** – IP-адрес и порт подключения к узлу.

- **Роль** – роль узла в приложении.

Если вы хотите управлять параметрами приложения на этом узле, вы можете назначить ему роль Управляющий узел с помощью кнопки **Назначить роль Управляющий узел**.

Управление SSL-сертификатом узла кластера

По умолчанию Kaspersky Web Traffic Security в качестве SSL-сертификата узла кластера использует самоподписанный сертификат, который генерируется автоматически при развертывании узла кластера. При входе в веб-интерфейс приложения с этим сертификатом в браузере отображается предупреждение о том, что соединение небезопасно. Для повышения удобства и безопасности при работе в веб-интерфейсе приложения вы можете заменить сертификат узла, который используется по умолчанию, на сертификат, выписанный доверенным центром сертификации.

Для замены SSL-сертификата узла кластера вам потребуются следующие файлы:

- Файл сертификата формата X.509 с расширением PEM или файл-контейнер с цепочкой сертификатов формата X.509 с расширением PEM.
- Файл приватного ключа RSA с расширением PEM (без парольной фразы).

Вы можете подготовить файл приватного ключа и сертификат для подписи самостоятельно или можете получить готовые файлы от удостоверяющего центра.

Этапы замены SSL-сертификата узла кластера при самостоятельном создании файлов приватного ключа и сертификата

1. **Создание файла приватного ключа и запроса на подпись сертификата (Certificate Signing Request) (см. раздел "Создание файла запроса на подпись SSL-сертификата" на стр. 139)**

   Вы получите от удостоверяющего центра один из следующих файлов:

   - файл подписанного сертификата формата X.509 с расширением CER или CRT;
   - файл цепочки сертификатов в формате PKCS#7 с расширением P7B. Файл включает подписанный по вашему запросу сертификат сайта и сертификаты промежуточных центров сертификации.

2. **Конвертация полученных файлов в PEM-кодировку**

   В зависимости от типа файла, полученного на предыдущем этапе, следует выполнить одно из следующих действий:

   - Конвертировать сертификат из кодировки DER в PEM-кодировку (см. раздел "Конвертация сертификата из кодировки DER в PEM-кодировку" на стр. 140).
   - Извлечь цепочку сертификатов из контейнера PKCS#7 (см. раздел "Извлечение цепочки сертификатов из контейнера PKCS#7" на стр. 141).

3. **Замена SSL-сертификата узла кластера (см. раздел "Замена SSL-сертификата узла кластера с веб-сервером Apache" на стр. 142)**

Этапы замены SSL-сертификата узла кластера при предоставлении файлов приватного ключа и сертификата удостоверяющим центром

1. **Получение файлов приватного ключа и сертификата от удостоверяющего центра**

   Приватный ключ и сертификат предоставляются в виде PFX-контейнера (формат PKCS#12, файл с расширением PFX или P12).

Если в качестве удостоверяющего центра в вашей организации используется стандартная служба Active Directory Certification Services, следует использовать шаблон **Web Server** для создания сертификата. Вам нужно сохранить результат в виде цепочки сертификатов (certificate chain) в DER-кодировке.

2. **Извлечение файлов сертификата и приватного ключа из PFX-контейнера (на стр. 141)**
3. **Замена SSL-сертификата узла кластера (см. раздел "Замена SSL-сертификата узла кластера с веб-сервером Apache" на стр. 142)**

В этом разделе

Создание файла запроса на подпись SSL-сертификата

Вы можете создать файл запроса на подпись сертификата (Certificate Signing Request) самостоятельно с помощью утилиты *openssl* или воспользоваться онлайн-сервисами.

► *Чтобы создать файл запроса на выписку сертификата самостоятельно с помощью утилиты openssl:*

1. Подготовьте текстовый файл request.config следующего содержания (примеры параметров см. в таблице ниже):

```
[req]
default_bits=2048
prompt=no
default_md=sha256
req_extensions=req_ext
distinguished_name=dn
[dn]
C=<двухбуквенный код страны>
ST=<регион>
L=<город>
O=<название организации>
OU=<название отдела организации>
emailAddress=<адрес электронной почты администратора>
CN=<доменное имя управляющего узла кластера>
```

```
[req_ext]
subjectAltName=@alt_names
[alt_names]
DNS.1=<доменное имя управляющего узла кластера>
DNS.2=<доменное имя подчиненного узла кластера>
DNS.3=<доменное имя подчиненного узла кластера>
```

2. Создайте приватный ключ RSA с расширением PEM (без парольной фразы) с помощью команды:

   ```
   openssl genrsa -out key.pem 2048
   ```

3. Создайте файл запроса на подпись сертификата с помощью команды:

   ```
   openssl req -new -sha256 -key key.pem -out request.csr -config
   request.config
   ```

В результате будут созданы следующие файлы:

- key.pem – файл приватного ключа RSA с расширением PEM. Вам нужно сохранить этот файл, чтобы использовать его для замены сертификата на узле кластера (см. раздел "Замена SSL-сертификата узла кластера с веб-сервером Apache" на стр. 142).
- request.csr – файл запроса на подпись сертификата в формате PKCS#10. Вам нужно передать этот файл в удостоверяющий центр.

Примеры параметров конфигурационного файла request.config

Параметр	Пример
C	RU
ST	Moscow
L	Moscow
O	Organization name
OU	IT department
emailAddress	administrator@example.com
CN	kwts01.example.com
DNS.1	kwts01.example.com
DNS.<номер>	kwts<номер>.example.com

Конвертация сертификата из кодировки DER в PEM-кодировку

После выполнения запроса на выписку сертификата удостоверяющий центр может предоставить подписанный сертификат в формате X.509 (файл с расширением CER или CRT).

Файл сертификата в формате X.509 может быть представлен в двух кодировках:

- DER encoded (DER-кодировка).
- Base64 encoded (PEM-кодировка).

Если сертификат представлен в DER-кодировке, необходимо конвертировать его в кодировку PEM. Конвертацию можно выполнить с помощью утилиты *openssl*.

► *Чтобы конвертировать сертификат из кодировки DER в PEM-кодировку, используйте команду:*

```
openssl x509 -in source.cer -inform DER -out cert.pem
```

Полученный файл cert.pem можно использовать для замены сертификата веб-интерфейса (см. раздел "Замена SSL-сертификата узла кластера с веб-сервером Apache" на стр. 142).

Извлечение цепочки сертификатов из контейнера PKCS#7

После выполнения запроса на выписку сертификата удостоверяющий центр может предоставить цепочку сертификатов в формате PKCS#7 (файл с расширением P7B). Цепочка включает подписанный по вашему запросу сертификат сайта, а также сертификаты промежуточных центров сертификации.

Файл в формате PKCS#7 может быть представлен в двух кодировках:

- DER encoded (DER-кодировка).
- Base64 encoded (PEM-кодировка).

Для дальнейшего использования необходимо извлечь сертификаты из контейнера и получить файл в кодировке PEM. Конвертацию можно выполнить с помощью утилиты *openssl*.

► *Чтобы конвертировать файл формата PKCS#7 в DER-кодировке, используйте команду:*

```
openssl pkcs7 -in source.p7b -inform DER -print_certs -out cert.pem
```

► *Чтобы конвертировать файл формата PKCS#7 в PEM-кодировке, используйте команду:*

```
openssl pkcs7 -in source.p7b -inform PEM -print_certs -out cert.pem
```

Полученный файл cert.pem можно использовать для замены сертификата веб-интерфейса (см. раздел "Замена SSL-сертификата узла кластера с веб-сервером Apache" на стр. 142).

Извлечение файлов сертификата и приватного ключа из PFX-контейнера

Если удостоверяющий центр предоставил сертификат в форме PFX-контейнера (формат PKCS#12, файл с расширением PFX или P12), необходимо самостоятельно извлечь из него файлы сертификата и приватного ключа в PEM-кодировке.

Извлечение файлов сертификата и приватного ключа можно выполнить с помощью утилиты openssl. В процессе извлечения файлов потребуется ввести парольную фразу от PFX-контейнера.

► *Чтобы извлечь файл приватного ключа, в зависимости от версии openssl используйте одну из следующих команд:*

- Для openssl версии ниже 3.0 используйте команду:

```
openssl pkcs12 -in source.pfx -nocerts -nodes -out key.pem
```

- Для openssl версии 3.0 и выше используйте команду:

```
openssl pkcs12 --legacy -in source.pfx -nocerts -nodes -out key.pem
```

► *Чтобы извлечь файл сертификата, в зависимости от версии openssl используйте одну из следующих команд:*

- Для openssl версии ниже 3.0 используйте команду:

```
openssl pkcs12 -in source.pfx -clcerts -nokeys -out cert.pem
```

- Для openssl версии 3.0 и выше используйте команду:

```
openssl pkcs12 --legacy -in source.pfx -clcerts -nokeys -out cert.pem
```

В результате вы получите следующие файлы:

- key.pem – файл приватного ключа RSA в PEM-кодировке (без парольной фразы);
- cert.pem – файл сертификата формата X.509 в PEM-кодировке.

Полученные файлы приватного ключа и сертификата можно использовать для замены сертификата веб-интерфейса (см. раздел "Замена SSL-сертификата узла кластера с веб-сервером Apache" на стр. 142).

Замена SSL-сертификата узла кластера с веб-сервером Apache

► *Чтобы заменить SSL-сертификат узла кластера с веб-сервером Apache:*

1. Запустите командную оболочку операционной системы на узле кластера для выполнения команд с полномочиями суперпользователя (администратора системы).
2. Поместите файлы сертификата (cert.pem) и приватного ключа (key.pem) в директорию `/root`.
3. Перейдите в директорию с конфигурационными файлами веб-сервера с помощью команды:

```
cd /var/opt/kaspersky/kwts/certs
```

4. Создайте резервные копии файлов действующего сертификата и приватного ключа с помощью команд:

```
cp -p webapi.crt webapi.crt.backup
cp -p webapi.key webapi.key.backup
cp -p webapi-with-dhparam.crt webapi-with-dhparam.crt.backup
```

5. Замените содержимое файлов сертификата и приватного ключа с помощью команд:

```
cat /root/cert.pem > webapi.crt
cat /root/key.pem > webapi.key
```

6. Сгенерируйте параметры DH с помощью команды:

```
openssl dhparam -out dhparam.pem 4096
```

> Генерация параметров DH может занять 10–20 минут. Дождитесь окончания выполнения операции.

7. Добавьте параметры DH к сертификату с помощью команды:

   ```
   cat webapi.crt dhparam.pem > webapi-with-dhparam.crt
   ```

8. Укажите права доступа к измененным файлам с помощью команд:

   ```
   chown root:root webapi.crt
   chmod 644 webapi.crt
   chown kluser:root webapi.key
   chmod 600 webapi.key
   chown root:root dhparam.pem
   chmod 644 dhparam.pem
   chown root:root webapi-with-dhparam.crt
   chmod 644 webapi-with-dhparam.crt
   ```

9. Перезапустите сервис Apache с помощью команды:

   ```
   systemctl restart apache2
   ```

10. Проверьте статус сервиса Apache с помощью команды:

    ```
    systemctl status apache2
    ```

    Для сервиса должен быть статус *running*.

11. Откройте в браузере веб-интерфейс узла кластера. В случае успешной замены сертификата предупреждение о небезопасном соединении не отображается.

12. Если замена завершилась успешно, удалите исходные файлы сертификата и приватного ключа из директории `/root` с помощью команды:

    ```
    rm -f /root/cert.pem /root/key.pem
    ```

Замена SSL-сертификата узла кластера будет завершена. Если вы хотите заменить сертификат на нескольких узлах кластера, вам требуется выполнить шаги инструкции на каждом узле.

Изменение сетевых параметров узла кластера

В этом разделе содержатся инструкции по изменению сетевых параметров узла кластера Kaspersky Web Traffic Security, а также описаны предварительные и заключительные действия, обязательные для корректного выполнения изменений.

kaspersky

В этом разделе

Порядок изменения сетевых параметров узлов кластера

IP-адрес и номер порта, которые приложение Kaspersky Web Traffic Security использует для межмашинного взаимодействия в кластере, указываются при первоначальной настройке приложения (см. раздел "Шаг 6. Ввод параметров узла" на стр. 57). Если вам нужно изменить IP-адрес сервера, на котором установлено приложение, после изменения сетевых настроек операционной системы потребуется выполнить процедуру изменения IP-адреса узла кластера. Эту же процедуру потребуется выполнить, если нужно изменить номер порта, используемого для межмашинного взаимодействия в кластере.

Изменение номера порта для веб-интерфейса не влияет на работу остальных узлов и всего кластера и выполняется отдельно от изменения IP-адреса и номера порта для межмашинного взаимодействия (см. раздел "Изменение номера порта для веб-интерфейса" на стр. 148).

Чтобы сохранить целостность и управляемость кластера Kaspersky Web Traffic Security, нужно менять адреса узлов в определенном порядке. Последовательность действий зависит от количества узлов в кластере и от того, скольким из них планируется изменить адреса. Возможны следующие варианты:

- Требуется изменить адреса части узлов в кластере (см. раздел "Сценарий изменения сетевых параметров части узлов" на стр. 144).
- Требуется изменить адреса всех узлов в кластере (см. раздел "Сценарий изменения сетевых параметров всех узлов" на стр. 145). Этот сценарий также используется в случае, если кластер состоит из одного узла.

Сценарий изменения сетевых параметров части узлов

Администратору требуется обеспечить сетевую связность между узлами с новыми и старыми адресами.

Сценарий изменения сетевых параметров части узлов кластера состоит из следующих этапов:

1. **Изменение роли узла с Управляющего на Подчиненный (см. раздел "Изменение роли узла в кластере" на стр. 134)**

   Этот этап нужно выполнить, если в число узлов, адреса которых планируется изменить, входит Управляющий узел. Временно назначьте роль Управляющего тому узлу, адрес которого менять не планируется.

2. **Отключение обработки сетевого трафика на выбранных узлах**

   Если используется балансировщик нагрузки для сетевого трафика, в параметрах балансировщика

отключите нагрузку на узлы, адреса которых планируете менять. Если балансировщика нагрузки нет, отключите обработку трафика на выбранных узлах средствами сетевого оборудования.

3. **Изменение адресов Подчиненных узлов**

   Последовательно измените адреса выбранных Подчиненных узлов. Для этого для каждого узла выполните следующие действия:

   1. Измените сетевые параметры средствами операционной системы: IP-адреса сетевых адаптеров, сетевые маршруты, адреса DNS-серверов, доменное имя узла.
   2. Проверьте настроенные сетевые параметры операционной системы узла (см. раздел "Проверка сетевых параметров операционной системы узла" на стр. 147).

      Этот шаг позволяет убедиться, что новые сетевые параметры были применены.
   3. Измените A- и PTR-записи на DNS-сервере для Подчиненного узла, чтобы они соответствовали новому IP-адресу и доменному имени узла.

      Это требуется для корректной работы Kerberos-аутентификации с помощью технологии единого входа (см. раздел "Настройка Kerberos-аутентификации" на стр. 222).
   4. Измените адрес узла для межмашинного взаимодействия (см. раздел "Изменение адреса узла в Kaspersky Web Traffic Security" на стр. 147).

      Этот шаг нужно выполнить, если был изменен IP-адрес сетевого адаптера, использовавшийся для межмашинного взаимодействия, или если требуется изменить номер порта для межмашинного взаимодействия.

4. **Замена Подчиненных узлов со старыми адресами на Подчиненные узлы с новыми адресами в кластере через веб-интерфейс приложения**

   Узлы, на которых был изменен адрес, нужно удалить из кластера (см. раздел "Удаление узла из кластера" на стр. 134), затем эти узлы с новыми адресами нужно добавить в кластер (см. раздел "Добавление узла в кластер" на стр. 133).

5. **Изменение роли узла с Подчиненного на Управляющий (см. раздел "Изменение роли узла в кластере" на стр. 134)**

   Этот шаг нужно выполнить, если роль Управляющего узла была временно назначена другому узлу.

6. **Проверка доступности и работоспособности всех узлов кластера**

   Вы можете просмотреть статусы узлов кластера (см. раздел "Управление кластером" на стр. 130) в веб-интерфейсе Управляющего узла.

7. **Включение обработки сетевого трафика на узлах**

   Последовательно введите узлы кластера в обработку сетевого трафика под их новыми адресами. Убедитесь, что обработка трафика происходит без ошибок.

Сценарий изменения сетевых параметров всех узлов

Сценарий изменения сетевых параметров всех узлов кластера состоит из следующих этапов:

1. **Отключение обработки сетевого трафика на выбранных узлах**

   Если используется балансировщик нагрузки для сетевого трафика, в параметрах балансировщика отключите нагрузку на узлы, адреса которых планируете менять. Если балансировщика нагрузки нет, отключите обработку трафика на выбранных узлах средствами сетевого оборудования.

2. **Изменение адреса Управляющего узла**

Для этого на Управляющем узле выполните следующие действия:

1. Измените сетевые настройки средствами операционной системы: IP-адреса сетевых адаптеров, сетевые маршруты, адреса DNS-серверов, доменное имя узла.
2. Проверьте настроенные сетевые параметры операционной системы узла (см. раздел "Проверка сетевых параметров операционной системы узла" на стр. 147).

   Этот шаг позволяет убедиться, что новые сетевые параметры были применены.
3. Измените A- и PTR-записи на DNS-сервере для Управляющего узла, чтобы они соответствовали новому IP-адресу и доменному имени узла.

   Это требуется для корректной работы Kerberos-аутентификации с помощью технологии единого входа (см. раздел "Настройка Kerberos-аутентификации" на стр. 222).
4. Измените адрес узла для межмашинного взаимодействия.

   Этот шаг нужно выполнить, если был изменен IP-адрес сетевого адаптера, использовавшийся для межмашинного взаимодействия, или если требуется изменить номер порта для межмашинного взаимодействия.

3. **Удаление Подчиненных узлов из кластера (см. раздел "Удаление узла из кластера" на стр. 134)**

   Нужно войти в веб-интерфейс по новому адресу Управляющего узла и удалить все Подчиненные узлы из кластера.

   Если узел в кластере один, то пропустите этот этап и перейдите к этапу 6.
4. **Изменение адресов Подчиненных узлов**

   Последовательно измените адреса всех Подчиненных узлов. Для этого для каждого узла выполните следующие действия:

   1. Измените сетевые параметры средствами операционной системы: IP-адреса сетевых адаптеров, сетевые маршруты, адреса DNS-серверов, доменное имя узла.
   2. Проверьте настроенные сетевые параметры операционной системы узла (см. раздел "Проверка сетевых параметров операционной системы узла" на стр. 147).

      Этот шаг позволяет убедиться, что новые сетевые параметры были применены.
   3. Измените A- и PTR-записи на DNS-сервере для Подчиненного узла, чтобы они соответствовали новому IP-адресу и доменному имени узла.

      Это требуется для корректной работы Kerberos-аутентификации с помощью технологии единого входа (см. раздел "Настройка Kerberos-аутентификации" на стр. 222).
   4. Измените адрес узла для межмашинного взаимодействия (см. раздел "Изменение адреса узла в Kaspersky Web Traffic Security" на стр. 147).

      Этот шаг нужно выполнить, если был изменен IP-адрес сетевого адаптера, использовавшийся для межмашинного взаимодействия, или если требуется изменить номер порта для межмашинного взаимодействия.
5. **Добавление Подчиненных узлов в кластер (см. раздел "Добавление узла в кластер" на стр. 133)**

   Нужно войти в веб-интерфейс по новому адресу Управляющего узла и добавить в кластер Подчиненные узлы с новыми адресами.
6. **Проверка доступности и работоспособности всех узлов кластера**

   Вы можете просмотреть статусы узлов кластера (см. раздел "Управление кластером" на стр. 130) в

веб-интерфейсе Управляющего узла.

7. **Включение обработки сетевого трафика на узлах**

   Последовательно введите узлы кластера в обработку сетевого трафика под их новыми адресами. Убедитесь, что обработка трафика происходит без ошибок.

Проверка сетевых параметров операционной системы узла

Перед изменением адреса узла в приложении Kaspersky Web Traffic Security рекомендуется проверить, что были применены новые сетевые параметры операционной системы.

► *Чтобы проверить сетевые параметры операционной системы узла кластера:*

1. Выполните следующие команды:
   - Для проверки параметров сетевых адаптеров:

     ```
     ip address
     ```

   - Для проверки маршрута по умолчанию и статического маршрута:

     ```
     ip route
     ```

   - Для проверки параметров DNS-сервера:

     ```
     cat /etc/resolv.conf
     ```

   - Для проверки доменного имени:

     ```
     hostname -f
     ```

2. Проверьте, что на DNS-сервере существует запись для нового доменного имени узла, с помощью команды:

   ```
   host <доменное имя узла>
   ```

   Если для доменного имени узла не найдена запись на DNS-сервере, проверьте правильность указанных сетевых параметров. При необходимости измените сетевые параметры операционной системы.

Сетевые параметры операционной системы узла будут проверены.

Изменение адреса узла в Kaspersky Web Traffic Security

Перед изменением адреса узла в приложении Kaspersky Web Traffic Security рекомендуется проверить, что новые сетевые параметры операционной системы были применены (см. раздел "Проверка сетевых параметров операционной системы узла" на стр. 147).

► *Чтобы изменить IP-адрес или порт узла кластера:*

1. Запустите мастер изменения сетевых параметров узла кластера с помощью команды:

   ```
   /opt/kaspersky/kwts/bin/setup.py --update-address
   ```

2. Укажите следующие ответы на вопросы мастера:
   - Для вопроса **Before changing network settings of a cluster node, you must ensure network connectivity between nodes with new and old addresses. Continue?** укажите ответ `yes`.
   - Для вопроса **Specify IP address of the current node** укажите новый IP-адрес, который будет использоваться для межмашинного взаимодействия.

     Если менять IP-адрес не требуется, нажмите на клавишу **ENTER**.
   - Для вопроса **Specify the port number of the current node** укажите новый номер порта, который будет использоваться для межмашинного взаимодействия.

     Если менять IP-адрес не требуется, нажмите на клавишу **ENTER**.
   - Для вопроса **Specify the port number of the current node for web interface** нажмите на клавишу **ENTER**.

     Номер порта для веб-интерфейса следует менять отдельно, см. инструкцию в разделе Изменение номера порта для веб-интерфейса (на стр. 148).
3. После завершения работы мастера и перезапуска всех служб перезагрузите узел кластера с помощью команды:

   ```
   shutdown -r
   ```

Адрес узла кластера будет изменен. Перейдите к настройке узлов кластера Kaspersky Web Traffic Security в веб-интерфейсе (см. раздел "Порядок изменения сетевых параметров узлов кластера" на стр. 144).

Изменение номера порта для веб-интерфейса

Вы можете изменить номер порта для веб-интерфейса Управляющего или Подчиненного узла кластера. Изменение номера порта для веб-интерфейса отдельного узла не влияет на работу других узлов и всего кластера.

► *Чтобы изменить порт для веб-интерфейса узла кластера:*

1. Запустите мастер изменения сетевых параметров узла кластера с помощью команды:

   ```
   /opt/kaspersky/kwts/bin/setup.py --update-address
   ```
2. Укажите следующие ответы на вопросы мастера:
   - Для вопроса **Before changing network settings of a cluster node, you must ensure network connectivity between nodes with new and old addresses. Continue?** укажите ответ `yes`.
   - Для вопроса **Specify IP address of the current node** нажмите на клавишу **ENTER**.
   - Для вопроса **Specify the port number of the current node** нажмите на клавишу **ENTER**.
   - Для вопроса **Specify the port number of the current node for web interface** укажите новый номер порта для веб-интерфейса и нажмите на клавишу **ENTER**.

После завершения работы мастера и перезапуска всех служб веб-интерфейс узла кластера будет готов к использованию на новом порте.

Вы можете проверить доступность веб-интерфейса по адресу `https://<IP-адрес или полное доменное имя (FQDN) узла>:<новый порт подключения к веб-интерфейсу>`.

kaspersky

Защита сетевого трафика

Kaspersky Web Traffic Security выполняет следующие действия по защите сетевого трафика:

- Проверяет сетевой трафик на вирусы, фишинг, вредоносные ссылки, некоторые легальные программы (см. раздел "О защите трафика от некоторых легальных программ" на стр. 149), которые могут быть использованы злоумышленниками, и другие программы, представляющие угрозу.
- Лечит зараженные объекты с использованием информации текущей (последней) версии антивирусных баз.

В этом разделе

О защите трафика от некоторых легальных программ

Легальные программы – программы, разрешенные к установке и использованию на компьютерах пользователей и предназначенные для выполнения задач пользователя. Однако легальные программы некоторых типов при использовании злоумышленниками могут нанести вред компьютеру пользователя или компьютерной сети организации. Если злоумышленники получат доступ к таким программам или внедрят их на компьютер пользователя, они могут использовать некоторые функции таких программ для нарушения безопасности компьютера пользователя или компьютерной сети организации.

Среди таких программ – IRC-клиенты, программы автодозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

Подобные программы описаны в таблице ниже.

Таблица 9. Легальные программы

Тип	Название	Описание
Client-IRC	Клиенты интернет-чатов	Пользователи устанавливают эти программы, чтобы общаться в ретранслируемых интернет-чатах (Internet Relay Chats). Злоумышленники используют их для распространения вредоносных программ.
Dialer	Программы автодозвона	Могут устанавливать телефонные соединения через модем в скрытом режиме.
Downloader	Программы-загрузчики	Могут загружать файлы с веб-страниц в скрытом режиме.
Monitor	Программы-мониторы	Позволяют наблюдать за активностью на том компьютере, на котором они установлены (видеть, какие приложения работают, и как они обмениваются данными с приложениями на других компьютерах).

Тип	Название	Описание
PSWTool	Восстановители паролей	Позволяют просматривать и восстанавливать забытые пароли. С этой же целью их скрыто внедряют на компьютеры злоумышленники.
RemoteAdmin	Программы удаленного администрирования	Широко используются системными администраторами; позволяют получать доступ к интерфейсу удаленного компьютера, чтобы наблюдать за ним и управлять им. С этой же целью злоумышленники скрыто внедряют их на компьютеры для наблюдения за компьютерами и управления ими. Легальные программы удаленного администрирования отличаются от троянских программ удаленного администрирования Backdoor. Троянские программы обладают функциями, которые позволяют им самостоятельно проникать в систему и устанавливать себя; легальные программы этих функций не имеют.
Server-FTP	FTP-серверы	Выполняют функции FTP-сервера. Злоумышленники внедряют их на компьютеры, чтобы открыть к ним удаленный доступ по протоколу FTP.
Server-Proxy	Прокси-серверы	Выполняют функции прокси-сервера. Злоумышленники внедряют их на компьютеры, чтобы от их имени рассылать спам.
Server-Telnet	Telnet-серверы	Выполняют функции Telnet-сервера. Злоумышленники внедряют их на компьютеры, чтобы открыть к ним удаленный доступ по протоколу Telnet.
Server-Web	Веб-серверы	Выполняют функции веб-сервера. Злоумышленники внедряют их на компьютеры, чтобы открыть к ним удаленный доступ по протоколу HTTP.
RiskTool	Инструменты для работы на виртуальной машине	Дают пользователю дополнительные возможности при работе на компьютере (позволяют скрывать файлы или окна активных приложений, закрывать активные процессы).
NetTool	Сетевые инструменты	Дают пользователю компьютера, на котором установлены, дополнительные возможности при работе с другими компьютерами в сети (позволяют перезагружать их, находить открытые порты, запускать установленные на них программы).
Client-P2P	Клиенты пиринговых сетей	Позволяют работать в пиринговых (Peer-to-Peer) сетях. Могут использоваться злоумышленниками для распространения вредоносных программ.
Client-SMTP	SMTP-клиенты	Отправляют сообщения электронной почты в скрытом режиме. Злоумышленники внедряют их на компьютеры, чтобы от их имени рассылать спам.

Тип	Название	Описание
WebToolbar	Веб-панели инструментов	Добавляют в интерфейс других приложений панели инструментов для использования поисковых систем.
FraudTool	Псевдопрограммы	Выдают себя за другие программы. Например, существуют псевдоантивирусы, которые выводят на экран сообщения об обнаружении вредоносных программ, но на самом деле ничего не находят и не лечат.

Настройка параметров модуля Антивирус

► *Чтобы настроить параметры модуля Антивирус:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Защита**.
2. В блоке параметров **Антивирус** включите или отключите использование эвристического анализа при антивирусной проверке сетевого трафика с помощью переключателя **Использовать эвристический анализ**.
3. Если вы включили использование эвристического анализа, в списке **Уровень эвристического анализа** выберите один из следующих уровней эвристического анализа:
   - **Поверхностный** – максимально быстрый эвристический анализ.
   - **Средний** – эвристический анализ средней скорости и глубины.
   - **Глубокий** – максимально глубокий эвристический анализ.

   По умолчанию выбран уровень эвристического анализа **Средний**.
4. Включите или отключите блокировку объектов, во время проверки которых произошли ошибки, с помощью переключателя **Блокировать объекты с ошибками проверки**.
5. В поле **Максимальная длительность проверки (сек.)** укажите ограничение длительности антивирусной проверки объектов сетевого трафика в секундах.

   По умолчанию установлено значение 120.
6. В поле **Максимальная глубина проверки архивов** укажите максимальный уровень вложенности проверяемых архивов.

   По умолчанию установлено значение 32.
7. Если требуется, установите флажок **Блокировать архивы при превышении уровня вложенности**.

   Если флажок снят, архив будет пропущен без выполнения антивирусной проверки. В журнал событий для этого объекта будет записан статус *Проверка не завершена*.
8. Включите или отключите обнаружение некоторых легальных программ с помощью переключателя **Обнаруживать некоторые легальные программы**.

К таким легальным программам (см. раздел "О защите трафика от некоторых легальных программ" на стр. 149) относятся, например, коммерческие утилиты удаленного администрирования, программы-клиенты IRC, программы дозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями.

Если переключатель включен, то в случае обнаружения таких программ, они будут обработаны согласно правилам для зараженных объектов.

9. Нажмите на кнопку **Сохранить**.

Параметры модуля Антивирус будут настроены.

Настройка параметров модуля Анти-Фишинг

► *Чтобы настроить параметры модуля Анти-Фишинг:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Защита**.
2. В блоке параметров **Анти-Фишинг** включите или отключите использование эвристического анализа при проверке сетевого трафика на фишинг с помощью переключателя **Использовать эвристический анализ**.
3. Включите или отключите обнаружение рекламных ссылок с помощью переключателя **Отмечать рекламные ссылки как вредоносные**.

   Программы рекламного характера связаны с показом пользователю рекламной информации. Они отображают в интерфейсе других программ рекламные баннеры, перенаправляют поисковые запросы на рекламные веб-страницы. Некоторые из них собирают и переправляют своему разработчику маркетинговую информацию о пользователе: например, сведения о том, какие тематические веб-сайты он посещает, какие поисковые запросы делает. В отличие от троянских программ-шпионов, программы рекламного характера передают эту информацию разработчику с разрешения пользователя.

   Если переключатель включен, приложение отмечает такие ссылки как вредоносные и обрабатывает их согласно параметрам, установленным для вредоносных ссылок.
4. Включите или отключите обнаружение ссылок, связанных с некоторыми легальными программами (см. раздел "О защите трафика от некоторых легальных программ" на стр. 149), с помощью переключателя **Отмечать ссылки, связанные с некоторыми легальными программами, как вредоносные**.

   Легальные программы могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. Такие программы сами по себе не имеют вредоносных функций, но эти программы могут быть использованы в качестве вспомогательного компонента вредоносной программы.

   Если переключатель включен, приложение отмечает такие ссылки как вредоносные и обрабатывает их согласно параметрам, установленным для вредоносных ссылок.
5. В поле **Максимальная длительность проверки (сек.)** укажите ограничение длительности

проверки объектов сетевого трафика на фишинг в секундах.

По умолчанию установлено значение 120.

6. Нажмите на кнопку **Сохранить**.

Параметры модуля Анти-Фишинг будут настроены.

Настройка обработки архивов

Во время проверки на вирусы, фишинг, некоторые легальные программы, которые могут быть использованы злоумышленниками, и другие программы, представляющие угрозу, Kaspersky Web Traffic Security по умолчанию распаковывает архивы во временную директорию /tmp/kwtstmp. Вы можете изменить директорию, в которую будут распаковываться проверяемые архивы.

► *Чтобы настроить директорию для распаковки архивов:*

1. Откройте файл /var/opt/kaspersky/apps/2022 в текстовом редакторе на узле кластера.
2. В секции `[paths]` укажите путь к директории в качестве значения параметра `tmp`.

   Пример:

   ```
   tmp=</path/to/tmp/for/archives>
   ```

   Убедитесь, что указанная директория существует. Необходимо предоставить доступ к директории пользователю kluser и группе klusers.

3. Перезапустите Kaspersky Web Traffic Security.

Архивы будут распаковываться в указанную директорию.

kaspersky

Параметры ICAP-сервера

Чтобы выполнять проверку трафика, а также регулировать доступ пользователей вашей сети к веб-ресурсам, требуется фильтровать и изменять данные HTTP-сообщений (HTTP-запросов и HTTP-ответов). Для этого необходимо настроить интеграцию вашего прокси-сервера с Kaspersky Web Traffic Security по протоколу ICAP.

При использовании локального сервиса Squid менять параметры ICAP-сервера не требуется. Если вы хотите использовать внешний прокси-сервер или если требуется обработка трафика с ненулевой мандатной меткой, настройте параметры ICAP-сервера (см. раздел "Настройка параметров подключения к ICAP-серверу" на стр. 154).

При использовании внешнего прокси-сервера Kaspersky Web Traffic Security выступает в роли ICAP-сервера, а прокси-сервер выступает в роли ICAP-клиента. Значения параметров, настраиваемых на вашем прокси-сервере, должны соответствовать значениям параметров в Kaspersky Web Traffic Security. В качестве внешнего прокси-сервера рекомендуется использовать Squid, совместимость с другим программным обеспечением не гарантируется.

По умолчанию Kaspersky Web Traffic Security начинает передачу содержимого объекта только после его полной проверки. В некоторых случаях это может привести к обрыву соединения со стороны браузера из-за превышения времени ожидания. Это поведение Kaspersky Web Traffic Security можно изменить в параметрах обработки трафика на ICAP-сервере (см. раздел "Настройка параметров обработки трафика на ICAP-сервере" на стр. 158).

В этом разделе

Настройка параметров подключения к ICAP-серверу

Если вы хотите использовать внешний прокси-сервер, для корректного обслуживания запросов требуется настроить параметры ICAP-сервера, в роли которого выступает Kaspersky Web Traffic Security. Если вы хотите использовать сервис Squid, установленный локально на узле кластера, в параметрах ICAP-сервера установите значения по умолчанию.

Если вы используете отдельный прокси-сервер, по умолчанию Kaspersky Web Traffic Security не обеспечивает шифрование ICAP-трафика и аутентификацию ICAP-клиентов. Администратору приложения необходимо самостоятельно обеспечить безопасное сетевое соединение между вашим прокси-сервером и Kaspersky Web Traffic Security с помощью туннелирования трафика или средствами iptables.

► *Чтобы настроить параметры подключения к ICAP-серверу:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры → Общие → ICAP-сервер**.
2. В раскрывающемся списке **Тип сокета для ICAP-сервера** выберите, какой сокет должен быть использован для подключения к ICAP-серверу.

   Если прокси-сервер Squid поддерживает обработку сетевых запросов с ненулевыми мандатными метками и будет направлять в ICAP-сервер сетевой трафик с ненулевой мандатной меткой, выберите **UDS**. В остальных случаях оставьте значение по умолчанию **TCP**. Подробнее о поддержке обработки мандатных меток сервисом Squid вы можете узнать в документации Astra Linux или обратившись в техническую поддержку Astra Linux.

   Если вы меняете тип сокета на **UDS**, предварительно исключите узел из обработки трафика. После изменения типа сокета включите возможность обрабатывать сетевой трафик с ненулевой мандатной меткой (см. раздел "Включение и выключение обработки сетевого трафика с ненулевой мандатной меткой" на стр. 156).

3. В списке **Адрес ICAP-сервера** выберите одно из следующих значений:

   - 127.0.0.1 (адрес IPv4), если прокси-сервер и приложение Kaspersky Web Traffic Security установлены на одном сервере. Приложение будет обрабатывать трафик только с текущего сервера.
   - 0.0.0.0 (адрес IPv4), если вы используете отдельный прокси-сервер. Приложение будет обрабатывать трафик с любых серверов.
   - ::1 (адрес IPv6, аналог адреса 127.0.0.1), если прокси-сервер и приложение Kaspersky Web Traffic Security установлены на одном сервере. Приложение будет обрабатывать трафик только с текущего сервера.
   - :: (адрес IPv6, аналог адреса 0.0.0.0), если вы используете отдельный прокси-сервер. Приложение будет обрабатывать трафик с любых серверов.

4. Введите порт подключения к ICAP-серверу.

   Допустимые значения – от 1 до 65535, кроме портов 22, 80, 443, 705 и 9045.

5. В поле **Максимальное количество соединений про протоколу ICAP** установите ограничение на количество одновременных подключений к ICAP-серверу.

   Вы можете указать значение от 1000 до 10 000. По умолчанию установлено значение 5000.

6. В поле **Заголовок, содержащий IP-адрес клиента** введите заголовок, который прокси-сервер использует для передачи IP-адреса пользователя прокси-сервера.

   По умолчанию установлено значение `X-Client-IP`.

   Если заголовок, указанный в этом поле, отличается от заголовка на прокси-сервере, приложение не сможет корректно определять пользователей при проверке правил обработки трафика.

7. В поле **Заголовок, содержащий имя пользователя** введите заголовок, который прокси-сервер использует для передачи имени пользователя прокси-сервера.

По умолчанию установлено значение `X-Client-Username`.

> Если заголовок, указанный в этом поле, отличается от заголовка на прокси-сервере, приложение не сможет корректно определять пользователей при проверке правил обработки трафика.

8. Если прокси-сервер передает имена пользователей в кодировке Base64, установите флажок **Имя пользователя в кодировке Base64**.
9. В поле **Путь службы модификации запросов** укажите путь службы Request Modification (REQMOD), которая обрабатывает исходящий трафик.
10. В поле **Путь службы модификации ответов** укажите путь службы Response Modification (RESPMOD), которая обрабатывает входящий трафик.
11. Нажмите на кнопку **Сохранить**.

Параметры подключения к ICAP-серверу будут настроены.

Включение и выключение обработки сетевого трафика с ненулевой мандатной меткой

Инструкцию по включению обработки сетевого трафика с ненулевой мандатной меткой следует выполнять, если прокси-сервер Squid поддерживает обработку сетевых запросов с ненулевыми мандатными метками и будет направлять на ICAP-сервер сетевой трафик со значением мандатной метки больше 0. Подробнее о поддержке обработки мандатных меток сервисом Squid вы можете узнать в документации Astra Linux или обратившись в техническую поддержку Astra Linux.

> Необходимо выполнить шаги инструкций на каждом узле кластера Kaspersky Web Traffic Security.

► *Чтобы включить возможность обработки сетевого трафика с ненулевой мандатной меткой:*

1. В разделе **Параметры** → **Общие** → **ICAP-сервер** измените тип сокета ICAP-сервера (см. раздел "Настройка параметров подключения к ICAP-серверу" на стр. 154) на **UDS**.
2. В директории /usr/lib/systemd/system/ создайте файл kwts_klbp.service следующего содержания:

```
[Unit]
Description=kwts klbp
Wants=local-fs.target
After=local-fs.target
Requires=kwts.create-runtime-dir.service
After=kwts.create-runtime-dir.service
```

```
[Service]
CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
Type=simple
User=kluser
Group=klusers
UMask=007
TimeoutSec=5sec
SyslogIdentifier=kwts_klbp
EnvironmentFile=/etc/opt/kaspersky/kwts/klbp.conf
ExecStart=/bin/sh -c '/opt/kaspersky/kwts/libexec/klbp
--downstream_socket=$downstream_socket
--upstream_socket=$upstream_socket'

[Install]
WantedBy=multi-user.target
```

3. Назначьте файлу kwts_klbp.service следующие права:
   - Владелец: root.
   - Группа: root.
   - Права владельца: rw.
   - Права группы и others: r.
4. В конфигурационном файле /etc/opt/kaspersky/kwts/klbp.conf укажите следующие значения.
   - `downstream_socket=<порт, на который Squid обращается к ICAP-серверу>`

     Порт должен совпадать с портом, который указан в конфигурационном файле Squid (см. раздел "Настройка сервиса Squid" на стр. 255) в параметрах `icap_service kwts_req reqmod_precache` и `icap_service kwts_res respmod_precache`.
   - `upstream_socket=unix:/var/run/kwts/icap_server.sock`
5. С помощью утилит для управления systemd выполните следующие действия:
   a. Выполните перезагрузку systemd с помощью команды:

      ```
      systemctl daemon-reload
      ```

   b. Активируйте сервис kwts_klbp с помощью команды:

      ```
      systemctl start kwts_klbp.service
      ```

   c. Добавьте сервис kwts_klbp в автозапуск операционной системы с помощью команды:

      ```
      systemctl enable kwts_klbp.service
      ```

   d. Перезапустите сервис Squid с помощью команды:

      ```
      systemctl restart squid
      ```
6. Повторите шаги инструкции на каждом узле кластера Kaspersky Web Traffic Security.

Возможность обработки сетевого трафика с ненулевой мандатной меткой будет включена.

► *Чтобы выключить возможность обработки сетевого трафика с ненулевой мандатной меткой:*

1. С помощью утилит для управления systemd выполните следующие действия:
   a. Остановите сервис kwts_klbp с помощью команды:
      ```
      systemctl stop kwts_klbp
      ```
   b. Удалите сервис kwts_klbp из автозапуска операционной системы с помощью команды:
      ```
      systemctl disable kwts_klbp
      ```

   Остановка и удаление сервиса kwts_klbp – обязательный для выполнения шаг на каждом узле кластера.

2. Удалите файл kwts_klbp.service из директории /usr/lib/systemd/system/ с помощью команды:
   ```
   rm -f /usr/lib/systemd/system/kwts_klbp.service
   ```
3. В разделе **Параметры** → **Общие** → **ICAP-сервер** измените тип сокета ICAP-сервера (см. раздел "Настройка параметров подключения к ICAP-серверу" на стр. 154) на **TCP**.
4. Перезапустите сервис Squid с помощью команды:
   ```
   systemctl restart squid
   ```
5. Повторите шаги инструкции на каждом узле кластера Kaspersky Web Traffic Security.

Возможность обработки сетевого трафика с ненулевой мандатной меткой будет выключена.

Настройка параметров обработки трафика на ICAP-сервере

По умолчанию Kaspersky Web Traffic Security начинает передачу содержимого объекта только после его полной проверки. В некоторых случаях это может привести к обрыву соединения со стороны браузера из-за превышения времени ожидания.

Если вы хотите, чтобы браузер пользователя не прерывал соединение с ошибкой превышения времени ожидания при загрузке объектов большого размера, выполните шаги инструкции ниже.

► *Чтобы настроить параметры обработки трафика на ICAP-сервере:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **ICAP-сервер**.
2. Переведите переключатель **Начинать передачу HTTP-сообщений до окончания их проверки** в положение **Включено**.

   Если этот параметр включен, а проверка объекта занимает продолжительное время, Kaspersky Web Traffic Security передает часть объекта браузеру, не дожидаясь завершения проверки. Kaspersky Web Traffic Security продолжает проверять объект по правилам обработки трафика. Если по результатам проверки доступ к объекту разрешен, то объект передается браузеру полностью. Если доступ к объекту запрещен, то сессия браузера прерывается и оставшаяся часть объекта не передается. В этом случае загрузка запрещенного объекта прерывается без объяснения причин. Пользователю не выводится сообщение о запрете загрузки, и не производится перенаправление на другую страницу.

3. В поле **Скорость передачи данных (КБ/с)** укажите количество байт, которое будет передаваться браузеру каждую секунду до завершения проверки HTTP-сообщения приложением.

   Вы можете указать целое число от 1 до 1024.

4. В поле **Задержка отправки (сек.)** укажите время задержки в секундах. Приложение начнет передавать объект браузеру через указанное количество секунд.

   Вы можете указать целое число от 1 до 3600.

5. Нажмите на кнопку **Сохранить**.

Параметры обработки трафика на ICAP-сервере будут настроены.

kaspersky

Страница блокировки

Если в результате проверки веб-ресурса по правилам обработки трафика доступ заблокирован, пользователю отображается страница блокировки.

Вы можете использовать следующие шаблоны страницы блокировки:

- по умолчанию (см. раздел "Настройка страницы блокировки по умолчанию" на стр. 162);
- для рабочих областей (см. раздел "Настройка страницы блокировки для рабочей области" на стр. 162);
- для правил обработки трафика (см. раздел "Настройка страницы блокировки для правила обработки трафика" на стр. 163).

Алгоритм выбора страницы блокировки представлен на рисунке ниже.

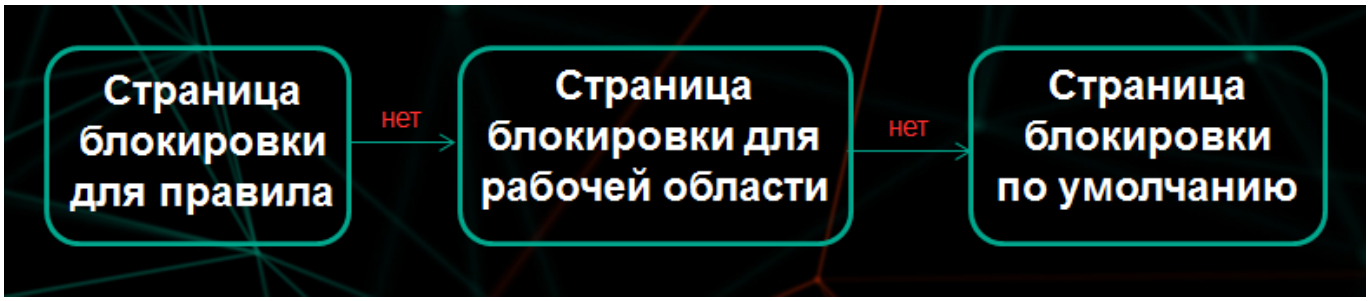

Рисунок 11. Алгоритм применения шаблона для страницы запрета доступа

Если веб-ресурс заблокирован по правилу обработки трафика, в параметрах которого настроена страница блокировки, то пользователю отображается текст, заданный на странице блокировки для этого правила. Если страница блокировки для правила не настроена, то приложение проверяет наличие страницы блокировки для рабочей области. Если страница блокировки для рабочей области настроена, то приложение использует ее. Если не настроена ни одна страница блокировки, то будет использована страница блокировки по умолчанию.

В этом разделе

Список поддерживаемых макросов

Вы можете использовать следующие макросы в тексте страницы блокировки:

- %DATE% – дата и время события.
- %APPLICATION% – название приложения.
- %BUILD% – номер сборки приложения.

- %SERVER_NAME% – имя компьютера, на котором был обработан HTTP-запрос.
- %TYPE% – тип HTTP-сообщению (Request или Response).
- %METHOD% – метод HTTP-сообщения.
- %RULE_NAME% – название правила обработки трафика, согласно которому веб-ресурс был заблокирован.
- %THREAT% – имя обнаруженного вредоносного объекта.
- %CURED_LIST% – список угроз, которые были вылечены.
- %SCAN_RESULT% – тип обнаруженной угрозы, которая представляет наибольшую опасность среди всех угроз, обнаруженных в данном объекте.

  Например, если в одном объекте обнаружены вирус и фишинговая ссылка (`av_status="detected" и ap_status="detected"`), то в качестве значения макроса будет указан вирус.
- %CATEGORY% – категория обработанного веб-ресурса по тематике его содержания.
- %PROCESSING_TIME% – продолжительность обработки HTTP-сообщения.
- %WORKSPACE_NAME% – имя рабочей области, к которой относится обработанный трафик.
- %USER_NAME% – имя учетной записи пользователя, который является источником HTTP-запроса.
- %USER_AGENT% – программа на компьютере пользователя, инициировавшая HTTP-запрос (User Agent).
- %CLIENT_IP% – IP-адрес компьютера, с которого был направлен HTTP-запрос.
- %URL% – URL-адрес веб-сайта, доступ к которому запрещен.
- %MIME_TYPE% – MIME-тип HTTP-сообщения и его частей.
- %FILE_NAME% – имена заблокированных файлов.
- %FILE_TYPE% – тип заблокированных файлов.

kaspersky

Настройка страницы блокировки по умолчанию

► *Чтобы настроить страницу блокировки по умолчанию:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Страница блокировки по умолчанию**.
2. Если требуется, измените текст страницы в поле **Макрос %TEXT%** и / или разметку страницы в поле **HTML-код**.
3. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из поддерживаемых макросов (см. раздел "Список поддерживаемых макросов" на стр. 160).

   Вы также можете использовать макрос %TEXT% – содержимое поля **Макрос %TEXT%** (доступен только для поля **HTML-код**).

   При наличии нескольких значений в одном макросе эти значения отображаются через запятую.
4. Нажмите на кнопку **Просмотреть**, чтобы проверить внесенные изменения.
5. Нажмите на кнопку **Сохранить**.

Страница блокировки по умолчанию будет настроена. Эта страница будет отображаться, если не настроены страницы блокировки для рабочей области и для сработавшего правила обработки трафика.

Настройка страницы блокировки для рабочей области

Настройка страницы блокировки для рабочей области доступна в общем веб-интерфейсе, а также в веб-интерфейсе рабочей области.

► *Чтобы настроить страницу блокировки для рабочей области:*

1. Перейдите в раздел настройки страницы блокировки в общем веб-интерфейсе или в веб-интерфейсе рабочей области. Для этого выполните следующие действия:
   - В общем веб-интерфейсе.
     1. В окне веб-интерфейса программы в разделе переключения между рабочими областями выберите общие параметры.
     2. Выберите раздел **Рабочие области**.

        Выберите рабочую область, для которой вы хотите настроить отдельную страницу блокировки.
     3. Откроется окно с информацией о рабочей области.
     4. Выберите закладку **Страница блокировки**.
     5. В правом нижнем углу нажмите на кнопку **Изменить**.
   - В веб-интерфейсе рабочей области.
     1. В веб-интерфейсе программы в разделе переключения между рабочими областями выберите название нужной рабочей области.

2. Выберите раздел **Параметры рабочей области**.

2. Выберите вариант **Создать индивидуальную страницу блокировки**.
3. Если вы хотите скопировать текст и разметку страницы блокировки по умолчанию (см. раздел "Настройка страницы блокировки по умолчанию" на стр. 162), заданной в общих параметрах, нажмите на ссылку **Скопировать из страницы блокировки по умолчанию** в правом нижнем углу окна.
4. Измените текст страницы в поле **Макрос %TEXT%** и / или разметку страницы в поле **HTML-код**.
5. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из поддерживаемых макросов (см. раздел "Список поддерживаемых макросов" на стр. 160).

   Вы также можете использовать макрос %TEXT% – содержимое поля **Макрос %TEXT%** (доступен только для поля **HTML-код**).

   При наличии нескольких значений в одном макросе эти значения отображаются через запятую.
6. Нажмите на кнопку **Просмотреть**, чтобы проверить внесенные изменения.
7. Нажмите на кнопку **Сохранить**.

Страница блокировки для рабочей области будет настроена. Пользователям, входящим в эту рабочую область, будет отображаться заданный текст. Остальным пользователям будет отображаться страница блокировки по умолчанию.

Если сработало правило, в котором настроена страница блокировки, то используется страница блокировки для правила (см. раздел "Настройка страницы блокировки для правила обработки трафика" на стр. 163), а не страница для рабочей области или страница по умолчанию.

Настройка страницы блокировки для правила обработки трафика

Вы можете изменить только текст страницы блокировки для отдельного правила обработки трафика. Разметка страницы определяется параметрами страницы блокировки по умолчанию (см. раздел "Настройка страницы блокировки по умолчанию" на стр. 162).

► *Чтобы изменить текст страницы блокировки для правила обработки трафика:*

1. В окне веб-интерфейса приложения выберите один из следующих разделов:
   - для действий с правилами отдельной рабочей области в разделе переключения между рабочими областями выберите название этой рабочей области;
   - для действий с правилами, применимыми во всех рабочих областях, в разделе переключения между рабочими областями выберите **Глобальная**.

   Применимо только при наличии прав доступа к нескольким рабочим областям.

2. Выберите раздел **Правила**.
3. Выберите одну из следующих закладок:
   - **Обход**.
   - **Доступ**.
   - **Защита**.

   Откроется таблица правил обработки трафика.
4. Выберите правило обработки трафика, для которого вы хотите настроить страницу блокировки.

   Откроется окно с информацией о правиле.
5. В правом нижнем углу окна нажмите на кнопку **Изменить**.

   Откроется окно **Изменить правило**.
6. Установите флажок **Введите текст для отображения на странице блокировки**.
7. Введите текст сообщения.
8. Если вы хотите добавить в текст сообщения макрос, в раскрывающемся списке **Вставить макрос** выберите один из поддерживаемых макросов (см. раздел "Список поддерживаемых макросов" на стр. 160).

   При наличии нескольких значений в одном макросе эти значения отображаются через запятую.
9. Нажмите на кнопку **Сохранить**.

Страница блокировки для правила обработки трафика будет настроена.

kaspersky

Экспорт и импорт параметров

Функциональность доступна при наличии у пользователя права **Изменять параметры**.

Экспорт и импорт параметров Kaspersky Web Traffic Security может быть использован для следующих целей:

- Резервное копирование параметров приложения.

  Если Управляющий узел выйдет из строя, вы сможете импортировать ранее экспортированные параметры после повторной установки приложения.

- Развертывание приложения на новом сервере.

  Вы можете настроить параметры на одном сервере, затем экспортировать их и создать одинаковую конфигурацию приложения на всех серверах.

- Миграция приложения на новую версию.

  Перед обновлением приложения вы можете экспортировать параметры из старой версии и импортировать их в новую версию.

  Миграция с более новой на более старую версию не поддерживается.

При экспорте параметров (см. раздел "Экспорт параметров Kaspersky Web Traffic Security" на стр. 166) создается конфигурационный файл со следующей информацией:

- Версия приложения.
- Параметры приложения вне рабочих областей:
  - правила защиты и доступа, не относящиеся к рабочим областям;
  - роли и права пользователей;
  - учетные записи пользователей, имеющих роли вне рабочих областей;
  - страницы блокировки;
  - параметры защиты.
- Параметры рабочих областей:
  - критерии принадлежности трафика к рабочей области;
  - правила защиты и доступа, созданные в рамках рабочей области;
  - роли и права пользователей, относящиеся ко всем рабочим областям.

Созданный конфигурационный файл сохраняется локально на Управляющем узле.

При импорте конфигурационного файла (см. раздел "Импорт параметров Kaspersky Web Traffic Security" на стр. 166) вы можете выбрать, какие параметры должны быть применены:

- отдельные параметры приложения вне рабочих областей;
- рабочие области, для которых будут применены все параметры.

При импорте правил защиты из версии 6.1 в версию 6.2 для типа объектов **Вредоносная ссылка** устанавливается действие **Заблокировать**.

Значения остальных параметров не будут изменены после завершения импорта.

В этом разделе

Экспорт параметров Kaspersky Web Traffic Security

► *Чтобы экспортировать параметры Kaspersky Web Traffic Security:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Экспорт/импорт**.
2. Выберите вкладку **Экспорт**.
3. Нажмите на кнопку **Экспортировать**.

   В блоке **Последние операции экспорта конфигурации** отобразится текущее состояние операции экспорта. После успешного завершения операции отобразится строка с датой и временем экспорта.
4. Нажмите на значок  в нужной строке.

Конфигурационный файл с экспортированными параметрами будет сохранен в папке загрузки браузера.

Импорт параметров Kaspersky Web Traffic Security

Не рекомендуется импортировать несколько конфигурационных файлов одновременно. В этом случае будут применены параметры только из одного файла.

► *Чтобы импортировать параметры Kaspersky Web Traffic Security:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Экспорт/импорт**.
2. Выберите вкладку **Импорт**.
3. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
4. Выберите файл с ранее экспортированными параметрами.

   Откроется окно **Выберите параметры для импорта**.
5. Установите флажки напротив тех параметров, которые вы хотите импортировать.

6. Установите флажок под таблицей параметров, подтверждающий согласие на импорт.
7. Нажмите на кнопку **Импортировать**.

Отобразится сообщение о результате запуска операции импорта.

Настройка хранения экспортированных файлов

Вы можете ограничить количество экспортированных конфигурационных файлов, которые хранятся на сервере. В случае превышения установленного ограничения ранее экспортированные файлы будут удалены.

► *Чтобы настроить хранение экспортированных файлов:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Общие** → **Экспорт/импорт**.
2. Выберите вкладку **Экспорт**.
3. В поле **Максимальное количество хранимых конфигурационных файлов** укажите максимальное количество экспортированных файлов, сохраняемых на сервере.

Количество экспортированных файлов будет ограничено заданным значением.

kaspersky

Миграция приложения с версии 6.1 на версию 6.2

Установка Kaspersky Web Traffic Security 6.2 поверх предыдущей версии не предусмотрена. Миграция на версию 6.2 выполняется путем развертывания отдельного кластера с новой версией и постепенного переключения пользователей на работу через новый кластер.

Аппаратные характеристики серверов для нового кластера, такие как количество ядер процессора, размер оперативной памяти, свободное место на жестком диске, должны соответствовать характеристикам серверов старого кластера. В процессе миграции можно постепенно удалять узлы из старого кластера и развертывать узлы с новой версией приложения с использованием освободившихся аппаратных ресурсов и IP-адресов.

Миграция на версию 6.2 состоит из следующих этапов:

1. **Подготовка ресурсов**

   Этот этап включает в себя следующие действия:

   1. Выделение дополнительных аппаратных ресурсов для двух узлов кластера с новой версией Kaspersky Web Traffic Security
   2. Выделение статических IP-адресов и доменных имен для двух узлов кластера с новой версией Kaspersky Web Traffic Security
   3. Подготовка keytab-файлов (см. раздел "Создание keytab-файла" на стр. 218), включающих доменные имена для новых узлов (в случае использования Kerberos SSO)
   4. Экспорт параметров правил и рабочих областей из предыдущей версии Kaspersky Web Traffic Security (см. раздел "Экспорт параметров Kaspersky Web Traffic Security" на стр. 166).

2. **Развертывание и настройка минимального кластера из двух узлов**

   Этот этап включает в себя следующие действия:

   1. Развертывание одного Управляющего и одного Подчиненного узла (см. раздел "Установка и первоначальная настройка приложения" на стр. 50)
   2. Объединение узлов в кластер (см. раздел "Создание нового кластера" на стр. 130)
   3. Активация приложения (на стр. 48)
   4. Настройка обновления баз приложения (см. раздел "Настройка расписания и параметров обновления баз" на стр. 172)
   5. Настройка участия в Kaspersky Security Network (на стр. 174)

      Если вы хотите иметь доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в Kaspersky Security Network со своих компьютеров, вы можете настроить использование Kaspersky Private Security Network.

   6. Настройка интеграции с сервером KATA (см. раздел "Настройка интеграции с приложением Kaspersky Anti Targeted Attack Platform" на стр. 180)

      Этот этап следует выполнять, если в вашей организации развернуто приложение KATA

   7. Настройка интеграции с внешней службой каталогов по протоколу LDAP (см. раздел "Соединение с LDAP-сервером" на стр. 176)
   8. Настройка экспорта событий во внешнюю SIEM-систему (см. раздел "Публикация событий

приложения в SIEM-систему" на стр. 224)

9. Настройка мониторинга работы приложения по протоколу SNMP (см. раздел "Работа с приложением по протоколу SNMP" на стр. 202)
10. Настройка общих параметров защиты и политики защиты по умолчанию (см. раздел "Защита сетевого трафика" на стр. 149)
11. Импорт файла с настройками правил и рабочих областей из предыдущей версии приложения (см. раздел "Импорт параметров Kaspersky Web Traffic Security" на стр. 166)
12. Настройка ролевого доступа к управлению приложением (глобальная область) и к управлению рабочими областями (см. раздел "Работа с ролями и учетными записями пользователей" на стр. 117)

3. Ввод в работу нового кластера

Этот этап включает в себя следующие действия:

1. Перераспределение части нагрузки на узлы нового кластера
2. Мониторинг работы нового кластера под нагрузкой в течение нескольких рабочих дней
3. Выявление и устранение проблем в работе нового кластера

4. Миграция Подчиненных узлов

Этот этап включает в себя следующие действия:

1. Снятие нагрузки с Подчиненного узла кластера со старой версией приложения
2. Вывод из эксплуатации Подчиненного узла со старой версией приложения (см. раздел "Удаление узла из кластера" на стр. 134)
3. Освобождение аппаратных ресурсов и IP-адресов
4. Развертывание Подчиненного узла с новой версией приложения (см. раздел "Установка и первоначальная настройка приложения" на стр. 50)
5. Добавление нового Подчиненного узла в кластер с новой версией приложения (см. раздел "Добавление узла в кластер" на стр. 133)
6. Перераспределение нагрузки на новый Подчиненный узел кластера с новой версией приложения

5. Удаление кластера со старой версией приложения

Этот этап включает в себя следующие действия:

1. Перенос всей нагрузки на узлы нового кластера
2. Вывод из эксплуатации оставшихся узлов кластера со старой версией приложения

kaspersky

Настройка параметров соединения с прокси-сервером

Заданные параметры прокси-сервера будут использованы для обновления баз, активации приложения и работы внешних служб.

► *Чтобы настроить параметры соединения с прокси-сервером:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **Соединение с прокси-сервером**.
2. Включите переключатель рядом с параметром **Использовать прокси-сервер**.
3. В блоке параметров **Адрес прокси-сервера** введите адрес и порт прокси-сервера.
4. Если вы не хотите использовать прокси-сервер для внутренних адресов вашей организации, установите флажок **Не использовать прокси для локальных адресов**.
5. Если вы хотите использовать аутентификацию при подключении к прокси-серверу, в полях **Имя пользователя (необязательно)** и **Пароль (необязательно)** введите имя пользователя и пароль подключения к прокси-серверу.
6. Нажмите на кнопку **Сохранить**.

kaspersky

Обновление баз Kaspersky Web Traffic Security

Базы модулей Антивирус и Анти-Фишинг (далее также "базы") представляют собой файлы с записями, которые позволяют обнаруживать в проверяемых объектах вредоносный код. Эти записи содержат информацию о контрольных участках вредоносного кода и алгоритмы лечения объектов, в которых содержатся угрозы.

Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают множество новых угроз, создают для них идентифицирующие записи и включают их в *пакет обновлений баз* (далее также "пакет обновлений"). Пакет обновлений представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента выпуска предыдущего пакета обновлений. Чтобы свести риск заражения защищаемого сервера к минимуму, рекомендуется регулярно получать пакеты обновлений.

В течение срока действия лицензии вы можете получать пакеты обновлений, загружая их с веб-сайта "Лаборатории Касперского".

Во время установки Kaspersky Web Traffic Security получает текущие базы с одного из серверов обновлений "Лаборатории Касперского". Это специальные интернет-сайты, на которые выкладываются обновления баз и программных модулей для всех приложений "Лаборатории Касперского". Если для доступа в интернет вы используете прокси-сервер, вам нужно настроить параметры соединения с прокси-сервером (см. раздел "Настройка параметров соединения с прокси-сервером" на стр. 170).

Чтобы уменьшить интернет-трафик, вы можете выбрать *пользовательский источник обновлений (см. раздел "Выбор источника обновлений баз" на стр. 171)*. Это могут быть указанные вами HTTP- или FTP-серверы, а также локальные папки на вашем компьютере.

В этом разделе

Выбор источника обновлений баз

► *Чтобы выбрать источник обновлений баз:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **Обновление баз**.
2. В раскрывающемся списке **Источник обновлений** выберите один из следующих источников обновлений:
   - **Серверы "Лаборатории Касперского" (безопасное соединение)**.
   - **Серверы "Лаборатории Касперского" (небезопасное соединение)**.
   - **Пользовательский**.
3. Если на предыдущем шаге вы выбрали **Пользовательский**, в поле **Пользовательский источник** укажите URL-адрес пользовательского источника, из которого вы хотите получать пакеты обновлений.

   Вы также можете установить флажок **При недоступности использовать серверы "Лаборатории**

Касперского", если вы хотите получать пакеты обновлений с серверов обновлений "Лаборатории Касперского", когда ваш источник обновлений недоступен.

4. Нажмите на кнопку **Сохранить**.

Настройка расписания и параметров обновления баз

Приложение загружает обновления баз из выбранного источника обновлений на все узлы кластера.

► *Чтобы настроить расписание и параметры обновления баз:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **Обновление баз**.
2. В блоке параметров **Расписание** в раскрывающемся списке выберите один из вариантов и выполните следующие действия:
   - **Вручную**.
   - **Один раз**. В появившемся поле укажите дату и время запуска обновления баз.
   - **Ежедневно**. В появившемся поле укажите время ежедневного запуска обновления баз.
   - **Еженедельно**. В появившихся полях укажите день недели и время запуска обновления баз.
   - **Ежемесячно**. В появившихся полях укажите день месяца и время запуска обновления баз.
   - **Запускать каждые**. В появившихся полях укажите периодичность запуска обновления баз в минутах, часах или днях.

     Первое обновление баз запустится сразу после сохранения внесенных изменений.
3. В поле **Случайное отклонение (мин)** укажите интервал отклонения от заданного расписанием времени в минутах. Приложение будет запускать обновление баз не на всех узлах одновременно, а случайным образом в течение заданного интервала. Рекомендуется использовать эту опцию для распределения нагрузки на сеть при большом количестве узлов в кластере.
4. В поле **Максимальная длительность (мин)** укажите максимальное время выполнения обновления баз в минутах, по истечении которого обновление баз должно быть остановлено.
5. Переведите переключатель **Запускать пропущенные задачи** в положение **Включено**, если вы хотите запускать пропущенные задачи обновления баз при последующем запуске приложения.

   Если запуск пропущенных задач выключен, то пропущенные задачи обновления баз не будут запущены при последующем запуске приложения. Следующий запуск обновления баз будет выполнен согласно расписанию.
6. Нажмите на кнопку **Сохранить**.

Запуск обновления баз вручную

► *Чтобы запустить обновление баз вручную:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **Обновление баз**.
2. В верхней части окна **Параметры** нажмите на кнопку **Обновить базы**.

   Появится сообщение о запуске обновления баз.

kaspersky

Участие в Kaspersky Security Network и использование Kaspersky Private Security Network

Использование Kaspersky Security Network приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Kaspersky Private Security Network.

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Web Traffic Security использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (далее также "KSN") – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Web Traffic Security на объекты, информация о которых еще не вошла в базы антивирусных программ, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Участие в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках объектов, информация о которых еще не вошла в базы антивирусных программ, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний приложения.

Во время участия в Kaspersky Security Network определенная статистика, полученная в результате работы Kaspersky Web Traffic Security, автоматически отправляется в "Лабораторию Касперского". Также для дополнительной проверки в "Лабораторию Касперского" могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда компьютеру или данным.

Сбор, обработка и хранение персональных данных пользователя не производится. О данных, которые Kaspersky Web Traffic Security передает в Kaspersky Security Network, вы можете прочитать в Положении о KSN.

Участие в Kaspersky Security Network добровольное. Решение об участии в Kaspersky Security Network принимается на этапе установки Kaspersky Web Traffic Security, его можно изменить в любой момент.

Если вы не хотите участвовать в KSN, вы можете использовать Kaspersky Private Security Network (далее также "KPSN") – решение, позволяющее пользователям получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в Kaspersky Security Network со своих компьютеров.

По вопросам приобретения приложения Kaspersky Private Security Network вы можете связаться со специалистами компании-партнера "Лаборатории Касперского" в вашем регионе.

kaspersky

В этом разделе

Настройка участия в Kaspersky Security Network

► *Чтобы настроить участие в Kaspersky Security Network:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **KSN/KPSN**.
2. Выберите один из следующих вариантов:
   - **Не использовать KSN/KPSN**, если вы не хотите участвовать в Kaspersky Security Network или использовать Kaspersky Private Security Network.
   - **Kaspersky Security Network (KSN)**, если вы хотите участвовать в Kaspersky Security Network.
3. Если вы выбрали участие в Kaspersky Security Network, в блоке **Положение о KSN** просмотрите Положение о Kaspersky Security Network и выполните следующие действия:
   - Если вы согласны с условиями, установите флажок **Я согласен участвовать в KSN**.
   - Если вы не согласны с условиями, снимите флажок **Я согласен участвовать в KSN**.
4. Если вы хотите участвовать в Kaspersky Security Network и согласны отправлять статистику вашего использования Kaspersky Security Network в "Лабораторию Касперского", установите флажок **Отправлять KSN-статистику для повышения уровня обнаружения угроз**.
5. Если вы выбрали участие в Kaspersky Security Network и согласны отправлять статистику вашего использования Kaspersky Security Network в "Лабораторию Касперского", в блоке **Дополнительное Положение о KSN** просмотрите Дополнительное Положение о Kaspersky Security Network и выполните следующие действия:
   - Если вы согласны с условиями, установите флажок **Я согласен отправлять KSN-статистику**.
   - Если вы не согласны с условиями, снимите флажок **Я согласен отправлять KSN-статистику**.
6. Нажмите на кнопку **Сохранить**.

Участие в Kaspersky Security Network будет настроено.

Настройка использования Kaspersky Private Security Network

Конфигурационный файл Kaspersky Private Security Network в формате ZIP больше не поддерживается. Для получения конфигурационного файла в формате PKCS7 обратитесь в Службу технической поддержки "Лаборатории Касперского".

► *Чтобы настроить использование Kaspersky Private Security Network:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **KSN/KPSN**.
2. Выберите один из следующих вариантов:
   - **Не использовать KSN/KPSN**, если вы не хотите участвовать в Kaspersky Security Network или использовать Kaspersky Private Security Network.
   - **KPSN**, если вы хотите использовать Kaspersky Private Security Network.
3. Если вы выбрали использование Kaspersky Private Security Network, в блоке **Конфигурационный файл KPSN** загрузите конфигурационный файл KPSN. Для этого выполните следующие действия:
   a. Нажмите на кнопку **Загрузить**.
   b. В окне выбора файлов укажите конфигурационный файл KPSN в формате PKCS7, который вы хотите добавить.
4. Нажмите на кнопку **Open**.

   Окно выбора файлов закроется.
5. Нажмите на кнопку **Сохранить**.

Использование Kaspersky Private Security Network будет настроено.

kaspersky

Соединение с LDAP-сервером

Kaspersky Web Traffic Security позволяет подключаться к серверам внешних служб каталогов, используемых в вашей организации, по протоколу LDAP.

Соединение с внешней службой каталогов по протоколу LDAP предоставляет администратору Kaspersky Web Traffic Security следующие возможности:

- добавлять пользователей из внешней службы каталогов в правила обработки трафика (см. раздел "Работа с правилами обработки трафика" на стр. 80);
- использовать учетные записи пользователей (см. раздел "Работа с ролями и учетными записями пользователей" на стр. 117) из внешней службы каталогов для работы с Kaspersky Web Traffic Security.

Вы можете включить поддержку леса доменов Active Directory (см. раздел "Включение и отключение поддержки леса доменов" на стр. 178). После включения поддержки леса доменов произойдет синхронизация с контроллерами доменов Active Directory. В результате в LDAP-кеше появятся данные о кросс-доменных связях между группами и их членами.

В этом разделе

Создание keytab-файла

Keytab-файл создается на сервере контроллера домена или на компьютере под управлением Windows Server, входящем в домен, под учетной записью с правами доменного администратора.

► *Чтобы создать keytab-файл:*

1. В оснастке **Active Directory Users and Computers** создайте отдельную учетную запись пользователя, которая будет использоваться для подключения приложения к LDAP-серверу (например, с именем `kwts-ldap`).

   При создании пользователя требуется выбрать опцию **Password never expires**.

2. Для использования алгоритма шифрования AES256-SHA1 в оснастке **Active Directory Users and Computers** в свойствах созданной учетной записи на вкладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.

3. Создайте keytab-файл для пользователя `kwts-ldap` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ kwts-ldap@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass <пароль пользователя kwts-ldap> -out <путь к файлу>\<имя файла>.keytab
   ```

   Вы можете использовать символ * в качестве значения параметра -pass, чтобы не указывать пароль в тексте команды. В этом случае утилита запросит пароль в процессе выполнения команды.

   Пример:

   ```
   C:\Windows\system32\ktpass.exe -princ kwts-ldap@COMPANY.COM -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out C:\Keytabs\kwts-ldap.keytab
   ```

Keytab-файл будет создан. В случае изменения пароля учетной записи потребуется сгенерировать новый keytab-файл.

Добавление соединения с LDAP-сервером

Вы можете добавить соединение с одним или несколькими LDAP-серверами.

Если вы настраиваете интеграцию с доменом, в названии которого содержится корневой домен `.local`, то для успешного соединения с LDAP-сервером требуется выполнить предварительные действия в операционной системе.

1. Проверьте состояние службы avahi-daemon. Для этого выполните команду:

   ```
   systemctl status avahi-daemon
   ```

2. Если служба запущена, остановите ее. Для этого выполните команду:

   ```
   systemctl stop avahi-daemon
   ```

3. Отключите автоматический запуск службы. Для этого выполните команду:

   ```
   systemctl disable avahi-daemon
   ```

► *Чтобы добавить соединение с LDAP-сервером:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **Соединение с LDAP-сервером**.
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Добавить соединение**.
3. В поле **Имя** введите имя LDAP-сервера, которое будет отображаться в веб-интерфейсе Kaspersky Web Traffic Security.
4. В блоке параметров **Keytab-файл** нажмите на кнопку **Загрузить**, чтобы загрузить keytab-файл.

Откроется окно выбора файла.

5. Выберите keytab-файл и нажмите на кнопку **Open**.
6. В поле **База поиска** введите *DN* (*Distinguished Name* – уникальное имя) объекта каталога, начиная с которого Kaspersky Web Traffic Security осуществляет поиск записей.

   Вводите суффикс каталога в формате `ou=<название подразделения>` (если требуется), `dc=<имя домена>, dc=<имя родительского домена>`.

   Например, вы можете ввести `ou=people, dc=example, dc=com`.

   Здесь `people` – уровень в схеме каталога, начиная с которого Kaspersky Web Traffic Security осуществляет поиск записей (поиск осуществляется на уровне `people` и ниже. Объекты, расположенные выше этого уровня, исключаются из поиска), `example` – доменное имя каталога, в котором Kaspersky Web Traffic Security осуществляет поиск записей, `com` – имя родительского домена, в котором находится каталог.
7. Нажмите на кнопку **Добавить**.

Соединение с LDAP-сервером будет добавлено.

Включение и отключение поддержки леса доменов

Вы можете включить или выключить поддержку леса доменов Active Directory в Kaspersky Web Traffic Security. После включения поддержки леса доменов произойдет синхронизация с контроллерами доменов Active Directory. В результате в LDAP-кеше появятся данные о кросс-доменных связях между группами и их членами. Для пользователей группы Active Directory, которые относятся к другим доменам леса, начнут работать правила обработки трафика по DN группы.

По умолчанию поддержка леса доменов выключена.

► *Чтобы включить или выключить поддержку леса доменов Active Directory:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **Соединение с LDAP-сервером**.
2. В строке **Лес доменов Active Directory** нажмите **Настроить**.
3. В открывшемся окне включите или выключите переключатель **Лес доменов**.
4. Нажмите на кнопку **Сохранить**.

Поддержка леса доменов будет включена или выключена.

Удаление соединения с LDAP-сервером

► *Чтобы удалить соединение с LDAP-сервером:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **Соединение с LDAP-сервером**.
2. Выберите LDAP-сервер, который вы хотите удалить.

   Откроется окно **Просмотреть параметры соединения**.
3. Нажмите на кнопку **Удалить**.

Откроется окно подтверждения.

4. Нажмите на кнопку **ОК**.

Соединение с LDAP-сервером будет удалено.

Изменение параметров соединения с LDAP-сервером

► *Чтобы изменить параметры соединения с LDAP-сервером:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Внешние службы** → **Соединение с LDAP-сервером**.
2. Выберите LDAP-сервер, параметры соединения с которым вы хотите изменить.

   Откроется окно **Просмотреть параметры соединения**.
3. Нажмите на кнопку **Изменить**.
4. Если требуется, измените следующие параметры:
   - Имя LDAP-сервера, которое отображается в веб-интерфейсе приложения, в поле **Имя**.
   - Keytab-файл, нажав на кнопку **Заменить**.
   - Каталог, начиная с которого приложение осуществляет поиск записей, в поле **База поиска**.
5. Нажмите на кнопку **Сохранить**.

Параметры соединения с LDAP-сервером будут изменены.

Запуск синхронизации с контроллером домена Active Directory вручную

Приложение выполняет автоматическую синхронизацию данных с контроллером домена Active Directory каждые 30 минут. Если вам требуется обновить данные об учетных записях пользователей немедленно (например, при добавлении нового пользователя), вы можете запустить синхронизацию вручную.

► *Чтобы запустить синхронизацию с контроллером домена Active Directory вручную:*

1. В веб-интерфейсе приложения выберите раздел **Параметры** → **Внешние службы** → **Соединение с LDAP-сервером**.
2. Нажмите на кнопку **Синхронизировать**.

   Синхронизация данных с контроллером домена будет запущена. В результате будут обновлены данные об учетных записях пользователей, используемые при подборе правил и при автозаполнении имен пользователей в веб-интерфейсе приложения.

Актуальный статус синхронизации с Active Directory отображается в разделе **Узлы** при просмотре информации об узлах кластера (см. раздел "Просмотр информации об узле кластера" на стр. 131).

kaspersky

Настройка интеграции с приложением Kaspersky Anti Targeted Attack Platform

Настройка интеграции с приложением Kaspersky Anti Targeted Attack Platform (далее также "KATA") доступна только при наличии у пользователя права **Изменять параметры**.

Kaspersky Anti Targeted Attack Platform – решение, предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как, например, атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats.

Приложение KATA позволяет интегрироваться с другими приложениями "Лаборатории Касперского", чтобы получать и обрабатывать проверяемые ими объекты. В качестве такого приложения может выступать Kaspersky Web Traffic Security.

Администратору Kaspersky Web Traffic Security требуется выполнить настройку интеграции KATA (см. раздел "Сценарий настройки интеграции с приложением KATA" на стр. 181) на Управляющем узле. После этого параметры интеграции отправляются на все Подчиненные узлы, входящие в кластер. Далее каждый узел кластера взаимодействует с сервером KATA самостоятельно, независимо от других узлов.

При интеграции с приложением KATA доступно два режима: отправка файлов на сервер KATA и получение объектов, обнаруженных приложением KATA.

Отправка файлов на сервер KATA

Kaspersky Web Traffic Security отправляет на сервер KATA объекты, которые не были заблокированы правилами обработки трафика или политикой защиты по умолчанию. При этом приложение не ожидает от сервера KATA результатов проверки этих объектов.

При обработке каждого файла приложение проверяет необходимость отправки его на сервер KATA. По результатам в журнал событий приложения (см. раздел "Журнал событий Kaspersky Web Traffic Security" на стр. 76) записывается статус проверки. Возможны следующие статусы:

- *Неприменимо. Нет файла для проверки* – HTTP-сообщение не содержит файлов для проверки.
- *Отключено согласно параметрам программы* – режим отправки файлов на сервер KATA отключен в параметрах приложения.
- *Пропущено согласно действию правила* – HTTP-сообщение было заблокировано приложением (применены действия **Заблокировать** или **Перенаправить**) или пропущено по правилу обхода без проверки.
- *Отклонено фильтром KATA* – файл не удовлетворяет условиям отправки на сервер KATA.
- *Запланировано* – отправка файла запланирована.
- *Завершено с ошибкой* – запланировать отправку файла не удалось.

Для файлов со статусами *Запланировано* и *Завершено с ошибкой* в журнал также записывается подробная информация о результате отправки файла.

Все события, связанные с отправкой файлов на сервер KATA, записываются в журнал операционной системы по протоколу Syslog (см. раздел "Содержание syslog-сообщений о событиях отправки файлов на сервер KATA" на стр. 201).

kaspersky

Получение объектов, обнаруженных приложением KATA

Kaspersky Web Traffic Security получает от сервера KATA информацию об объектах, обнаруженных приложением KATA с помощью технологий Sandbox и YARA. Подробнее об этих технологиях см. *Справку Kaspersky Anti Targeted Attack Platform*.

Информация о полученных объектах сохраняется в кеш KATA. Каждый узел кластера хранит свой кеш KATA и получает объекты, обнаруженные приложением KATA, независимо от других узлов. По истечении времени хранения информация об объектах удаляется из кеша. Эти объекты больше не учитываются при применении правил защиты (см. раздел "Добавление правила защиты" на стр. 86) и политики защиты по умолчанию (см. раздел "Настройка политики защиты по умолчанию" на стр. 99).

В правилах защиты и в политике защиты по умолчанию вы можете настроить действия над объектами, информация о которых была получена с сервера KATA. При обнаружении в трафике пользователя таких объектов Kaspersky Web Traffic Security будет обрабатывать их согласно заданным в правилах параметрам. Это позволяет блокировать опасные объекты до того, как информация о них была добавлена в репутационные базы KSN, а также в локальные базы приложения.

Результат проверки каждого объекта записывается в журнал событий (см. раздел "Журнал событий Kaspersky Web Traffic Security" на стр. 76). Возможны следующие статусы проверки:

- *Не обнаружено* – соответствий в кеше KATA не обнаружено.
- *Обнаружено* – обнаружены угрозы.
- *Не проверен* – проверка не выполнялась согласно параметрам приложения.
- *Ошибка проверки* – проверка завершилась с ошибкой.

Все события, связанные с проверкой трафика на соответствие объектам KATA, записываются в журнал операционной системы по протоколу Syslog (см. раздел "Содержание syslog-сообщений о событиях обработки трафика" на стр. 190).

В этом разделе

Сценарий настройки интеграции с приложением KATA

Настройка интеграции Kaspersky Web Traffic Security с приложением KATA состоит из следующих этапов.

1. **Добавление сервера KATA (на стр. 182)**

   При добавлении сервера KATA требуется сверить отпечатки сертификата, отображаемые в

веб-интерфейсах Kaspersky Web Traffic Security и KATA. Если отпечатки совпадают, администратор подтверждает добавление сервера. После этого Управляющий узел отправляет адрес и сертификат сервера KATA на все узлы кластера, не дожидаясь подтверждения авторизации.

2. **Выбор режима интеграции (на стр. 183)**

   В Kaspersky Web Traffic Security доступно два режима интеграции с приложением KATA. Вы можете отправлять файлы на проверку в KATA (в этом случае Kaspersky Web Traffic Security выступает в качестве внешней системы для приложения KATA) и/или получать информацию об объектах, обнаруженных приложением KATA. Эти режимы работают независимо друг от друга.

3. **Настройка параметров кеша KATA (на стр. 184)**

   При применении правил защиты и политики по умолчанию Kaspersky Web Traffic Security учитывает объекты, информация о которых хранится в кеше KATA. Вы можете настраивать период их хранения в кеше, по истечении которого эти объекты перестают учитываться при обработке трафика.

4. **Авторизация Kaspersky Web Traffic Security в веб-интерфейсе приложения KATA**

   Во время добавления сервера KATA отправляется запрос на авторизацию внешней системы. Администратору KATA требуется подтвердить этот запрос в веб-интерфейсе KATA. Подробнее об обработке запросов от внешних систем см. *Справку Kaspersky Anti Targeted Attack Platform*.

Добавление сервера KATA

Вы можете настроить интеграцию только с одним сервером KATA.

► *Чтобы добавить сервер KATA:*

1. В веб-интерфейсе приложения выберите раздел **Параметры → Внешние службы → Интеграция KATA**.
2. В блоке параметров **Сервер KATA** нажмите на кнопку **Добавить**.

   Откроется окно **Добавление сервера KATA**.
3. В поле **IP-адрес** введите полное доменное имя (FQDN) или IPv4/IPv6-адрес сервера KATA, на котором установлен компонент Central Node.
4. В поле **Порт** введите порт подключения к серверу KATA.

   По умолчанию указано значение 443.
5. Нажмите на кнопку **Далее**.

   Откроется окно **Подтверждение сервера KATA**.
6. Проверьте введенные данные и убедитесь, что отпечаток сертификата, отображаемый в веб-интерфейсе, совпадает с отпечатком сертификата сервера KATA. Если отпечатки совпадают, нажмите на кнопку **Подтвердить**.

Сервер KATA будет добавлен. Информация о сервере отобразится в разделе **Интеграция KATA**, в блоке параметров **Сервер KATA**.

kaspersky

Изменение сервера KATA

В приложении доступна интеграция только с одним сервером KATA. Если вы хотите настроить интеграцию с другим сервером, вы можете изменить сервер KATA.

► *Чтобы изменить сервер KATA:*

1. В веб-интерфейсе приложения выберите раздел **Параметры** → **Внешние службы** → **Интеграция KATA**.
2. В блоке параметров **Сервер KATA** нажмите на кнопку **Заменить**.

   Откроется окно **Изменение сервера KATA**.
3. В поле **IP-адрес** введите полное доменное имя (FQDN) или IPv4/IPv6-адрес нового сервера KATA, на котором установлен компонент Central Node.
4. Нажмите на кнопку **Далее**.

   Откроется окно **Подтверждение сервера KATA**.
5. Проверьте введенные данные и убедитесь, что отпечаток сертификата, отображаемый в веб-интерфейсе, совпадает с отпечатком сертификата сервера KATA. Если отпечатки совпадают, нажмите на кнопку **Подтвердить**.

Сервер KATA будет изменен.

Удаление сервера KATA

► *Чтобы удалить сервер KATA:*

1. В веб-интерфейсе приложения выберите раздел **Параметры** → **Внешние службы** → **Интеграция KATA**.
2. В блоке параметров **Сервер KATA** нажмите на кнопку **Удалить**.
3. В окне подтверждения нажмите на кнопку **Да**.

Сервер KATA будет удален. Информационные панели об интеграции с приложением KATA в разделах **Мониторинг** и **Узлы** перестанут отображаться. Записи об обработанных ранее объектах в журнале событий приложения и в журнале Syslog не будут удалены.

Выбор режима интеграции

Выбор режима интеграции доступен только при добавленном сервере KATA (см. раздел "Добавление сервера KATA" на стр. 182).

► *Чтобы выбрать режим интеграции с приложением KATA:*

1. В веб-интерфейсе приложения выберите раздел **Параметры** → **Внешние службы** → **Интеграция KATA**.
2. В блоке параметров **Режим интеграции KATA** включите нужный режим интеграции с помощью

следующих переключателей:

- **Получать объекты**.

  Kaspersky Web Traffic Security будет получать объекты, обнаруженные приложением KATA, и использовать информацию об этих объектах в правилах защиты и в политике защиты по умолчанию.

- **Отправлять файлы**.

  Kaspersky Web Traffic Security будет авторизован в приложении KATA в качестве внешней системы. Файлы из проверяемого трафика пользователей, удовлетворяющие заданным в приложении критериям, будут отправляться в KATA. Kaspersky Web Traffic Security не будет ожидать результатов проверки отправленных файлов.

Эти режимы работают независимо друг от друга. Вы можете включить один из режимов или оба режима одновременно.

3. Нажмите на кнопку **Сохранить**.

Режим интеграции с приложением KATA будет выбран. В зависимости от выбранного режима в разделе **Узлы** отобразятся информационные панели о состоянии интеграции (см. раздел "Мониторинг интеграции KATA" на стр. 185).

Пересоздание сертификата Kaspersky Web Traffic Security

При компрометации сертификата Kaspersky Web Traffic Security администратор приложения KATA может отменить авторизацию Kaspersky Web Traffic Security как внешней системы. В этом случае вам требуется создать новый сертификат в веб-интерфейсе Kaspersky Web Traffic Security и пройти процедуру авторизации в приложении KATA повторно (см. раздел "Сценарий настройки интеграции с приложением KATA" на стр. 181).

► *Чтобы пересоздать сертификат для авторизации Kaspersky Web Traffic Security в приложении KATA:*

1. В веб-интерфейсе приложения выберите раздел **Параметры → Внешние службы → Интеграция KATA**.
2. В блоке параметров **Учетные данные KWTS** нажмите на кнопку **Создать новый сертификат**.
3. В окне подтверждения нажмите на кнопку **Да**.

Новый сертификат Kaspersky Web Traffic Security будет создан. В блоке параметров **Учетные данные KWTS** отобразятся SensorID и отпечаток нового сертификата.

Настройка параметров кеша KATA

Если включен режим **Получать объекты**, то Kaspersky Web Traffic Security сохраняет информацию об объектах, обнаруженных приложением KATA, на всех узлах кластера в кеше KATA. При применении правил защиты и политики по умолчанию учитываются объекты, информация о которых хранится в кеше KATA.

► *Чтобы настроить параметры кеша KATA:*

1. В веб-интерфейсе приложения выберите раздел **Параметры** → **Внешние службы** → **Интеграция KATA**.
2. В блоке параметров **Кеш KATA** в поле **Срок хранения кеша (часы)** введите время хранения информации об объектах, обнаруженных приложением KATA, в часах.

   Допустимые значения – от 1 до 48. По умолчанию установлено значение 48.
3. Если вы хотите очистить кеш KATA, нажмите на кнопку **Очистить кеш** и в окне подтверждения нажмите на кнопку **Да**.

   Информация об этой операции записывается в журнал событий приложения (см. раздел "Журнал событий Kaspersky Web Traffic Security" на стр. 76), а также в журнал операционной системы по протоколу Syslog (см. раздел "Журнал событий Syslog" на стр. 189).

Параметры кеша KATA будут настроены.

Мониторинг интеграции KATA

► *Чтобы проверить состояние интеграции Kaspersky Web Traffic Security с приложением KATA:*

1. В веб-интерфейсе приложения выберите раздел **Узлы**.

   Откроется страница с информацией об узлах кластера. На странице отображаются следующие информационные панели об интеграции с приложением KATA:

   - **Отправка файлов в KATA**. Количество узлов кластера со статусами отправки файлов на сервер KATA:
     - *Без ошибок*. Все файлы успешно отправлены на сервер KATA.
     - *Отключено*. Режим интеграции **Отправлять файлы** отключен.
     - *С ошибкой*. Во время отправки файлов на сервер KATA за последний час произошли ошибки.
   - **Получение объектов из KATA**. Количество узлов кластера со статусами получения объектов, обнаруженных приложением KATA:
     - *Без ошибок*. Все объекты, обнаруженные приложением KATA, получены успешно.
     - *Отключено*. Режим интеграции **Получать объекты** отключен.
     - *С ошибкой*. Во время получения объектов, обнаруженных приложением KATA, произошли ошибки.
2. Перейдите по ссылке **Подробные сведения** в одной из информационных панелей об интеграции с приложением KATA.

   Откроется страница **Интеграция KATA**.
3. В правом верхнем углу в раскрывающихся списках выберите период отображения данных, а также узлы кластера, статистику о которых вы хотите посмотреть.

На странице **Интеграция KATA** отобразится следующая информация:

- График **Отправка файлов в KATA**.

  > Отображается только при включенном режиме **Отправлять файлы**.

  График показывает, какое количество файлов было отправлено на сервер KATA за выбранный период времени. Линии графиков представляют следующие статусы отправки файлов:

  - *Успешно*.
  - *Не удалось отправить файлы на сервер KATA из-за переполнения буфера*.
  - *Ошибка*.

- Диаграмма **Детальная информация об ошибках**.

  > Отображается только при включенном режиме **Отправлять файлы**.

  Детальная информация о типах ошибок, возникших при отправке файлов на сервер KATA, представлена в виде круговой и столбчатой диаграмм. Круговая диаграмма показывает соотношение количества ошибок определенного типа к общему количеству всех ошибок. Столбчатая диаграмма показывает количество ошибок определенного типа в заданном интервале времени.

  Возможны следующие типы ошибок:

  - Не удалось установить соединение с сервером KATA.
  - SSL-сертификат сервера KATA не совпадает с доверенным.
  - Требуется авторизация на сервере KATA.
  - Превышено время ожидания соединения с сервером KATA.
  - HTTP-код 4xx: ошибка клиента.
  - HTTP-код 5xx: ошибка сервера.
  - Внутренняя ошибка.

- Таблица **Состояние интеграции KATA**.

  В таблице представлена сводная информация об обработанных объектах по узлам кластера. Таблица содержит следующие графы:

  - **IP-адрес:порт**.

    IP-адрес и порт узла кластера, который интегрирован с программой KATA.

  - **Отправка файлов в KATA**.

    Статус отправки файлов из трафика этого узла кластера на сервер KATA. Возможны следующие значения:

    - *ОК*.

- *Ошибка*.
- *Выключено*.

- **Получение объектов из KATA**.

  Статус получения объектов, обнаруженных программой KATA, на этом узле кластера. Возможны следующие значения:

  - *ОК*.
  - *Ошибка*.
  - *Выключено*.

- **Количество объектов в кеше KATA**.

  Количество объектов, обнаруженных программой KATA, которые были сохранены на всех узлах кластера в кеше KATA.

Если включен только один из режимов интеграции KATA, отображаются только графы, относящиеся к этому режиму.

Настройка отправки HTML-файлов в KATA

Действия, описанные в этом разделе, требуется выполнить на каждом узле кластера.

По умолчанию файлы формата HTML не отправляются в KATA. Вы можете настроить фильтр для отправки HTML-файлов в KATA по формату файла или по регулярным выражениям.

► *Чтобы настроить фильтр HTML-файлов, отправляемых в KATA, по формату файла:*

1. В файле с параметрами фильтра KATA /var/opt/kaspersky/kwts/kata-filters.json добавьте в секцию `includeFormats` новую строку следующего формата:

   `{"contentFormat": "<формат файла>", "nameMask": "<маска имени файла>"}`

   Возможные значения ключа `contentFormat`:

   - `GeneralHtml`;
   - `GeneralHtmlStrict`.

   Возможные значения ключа `nameMask`:

   - `*.html`;
   - `*.htm`;
   - `*.xhtml`;
   - `*.xht`;
   - `*.xml`.
   - `*`.

Если вы хотите добавить несколько значений, то для каждого значения требуется добавить отдельную строку.

2. Перезагрузите компьютер с установленным приложением Kaspersky Web Traffic Security.

Изменения, внесенные в конфигурационный файл фильтра KATA, будут применены. Приложение будет отправлять в KATA все HTML-файлы, формат и имя которых соответствуют записям в конфигурационном файле.

► *Чтобы настроить фильтр HTML-файлов, отправляемых в KATA, по регулярным выражениям, выполните следующие действия:*

1. Убедитесь, что в файле с параметрами фильтра KATA /var/opt/kaspersky/kwts/kata-filters.json в секции `includeFormats` отсутствуют записи об HTML-файлах.
2. Переименуйте файл с регулярными выражениями для фильтра KATA, расположенный по пути /var/opt/kaspersky/kwts/kata-html-regex_sample.txt, в kata-html-regex.txt.
3. Перезагрузите компьютер с установленным приложением Kaspersky Web Traffic Security.

Приложение будет отправлять в KATA только те HTML-файлы, которые удовлетворяют регулярным выражениям, указанным в файле kata-html-regex.txt.

kaspersky

Журнал событий Syslog

Вы можете настроить запись событий обработки трафика (см. раздел "Содержание syslog-сообщений о событиях обработки трафика" на стр. 190), системных событий приложения (см. раздел "Содержание syslog-сообщений о системных событиях приложения" на стр. 198) и событий отправки файлов на сервер KATA (см. раздел "Содержание syslog-сообщений о событиях отправки файлов на сервер KATA" на стр. 201) в журнал событий по протоколу Syslog (далее также "журнал событий Syslog").

Информация о событиях записывается в отдельной категории журнала, установленной в параметрах Syslog (см. раздел "Настройка параметров Syslog" на стр. 189). Сведения о каждом событии отправляются как отдельное syslog-сообщение. Текст syslog-сообщения соответствует информации о событии, отображающейся в веб-интерфейсе приложения в разделе **События**.

Для удаленной записи событий по протоколу Syslog рекомендуется использовать протокол TCP. Сетевые порты, используемые сервером Syslog, должны быть открыты.

В этом разделе

Настройка параметров Syslog

При настройке параметров Kaspersky Web Traffic Security рекомендуется учитывать параметры Syslog, установленные в операционной системе.

► *Чтобы настроить параметры Syslog:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Журналы и события** → **Syslog**.
2. В раскрывающемся списке **Категория журнала** выберите категорию журнала, в который будет записываться информация о событиях.

   По умолчанию установлено значение Local1.
3. В раскрывающемся списке **Уровень события** выберите уровень важности событий, которые будут записываться по протоколу Syslog.
   - **Ошибка** – сообщения об ошибках в работе приложения.

     События обработки трафика не будут записаны в журнал Syslog.
   - **Информация** – сообщения об ошибках в работе приложения, а также события обработки трафика.
4. Если специалисты Службы технической поддержки попросили вас включить запись информации об объеме и параметрах потока трафика, обрабатываемого приложением, в журнал событий Syslog,

переведите переключатель **Записывать информацию о профиле трафика** в положение **Включено**.

Включение этой опции увеличивает требования к дисковому пространству сервера с установленным приложением, а также снижает производительность приложения. Не рекомендуется включать эту опцию без запроса специалистов Службы технической поддержки.

Запись событий по протоколу Syslog будет настроена.

Содержание syslog-сообщений о событиях обработки трафика

В каждом syslog-сообщении передаются следующие поля, определяемые параметрами протокола Syslog в операционной системе:

- дата и время события;
- имя хоста, на котором произошло событие;
- название приложения (всегда имеет значение `KWTS`).

Поля syslog-сообщения о событии обработки трафика, определяемые параметрами приложения, представлены в формате `<ключ>="<значение>"`. Если ключ имеет несколько значений, эти значения указываются через запятую. В качестве разделителя между ключами используется двоеточие.

Пример:

```
Oct 9 10:13:06 localhost KWTS: type="Response": method="GET": action="Block":
blocked_by_rule="protection_rules [Workspace1/-/Rule2]":
processing_time="952": scan_result="Malware": workspace="Workspace1":
http_user_name="example@test.local": http_user_agent="curl/7.29.0":
http_user_ip="192.0.2.0": url="http://example.com/eicar.com":
kata-alert="NotDetected": "eicar.com", filesize="69",
kata_upload="SkippedByAction", guid="", rules="access_rules
[Workspace1/Group1/Rule1], protection_rules [Workspace1/-/Rule2]",
av-status="Detected", threats="EICAR-Test-File/Block",
ap-status="NotDetected", mlf-status="NotDetected", encrypted="NotDetected",
macros="NotDetected", kata-alert="NotDetected"
```

Ключи, а также их значения, содержащиеся в сообщении, приведены в таблице ниже.

Таблица 10. Информация о событиях обработки трафика в syslog-сообщении

Ключ	Описание и возможные значения
`type`	Тип HTTP-сообщения. Может принимать значения `Request` (запрос) или `Response` (ответ).
`method`	Метод HTTP-запроса.

Ключ	Описание и возможные значения
`action`	Действие над обнаруженным объектом. Может принимать одно из следующих значений: • `Allow` – Разрешить. • `Block` – Заблокировать. • `Redirect` – Перенаправить.
`blocked_by_rule`	Название правила обработки трафика, по которому веб-ресурс был заблокирован. Отображается в следующем формате: • Для правил обхода: "`[<Название правила>]`". • Для правил защиты и правил доступа: "`[<Название рабочей области>/<Название группы правил>/<Название правила>]`".
`redirected_by_rule`	Название правила обработки трафика, по которому пользователь был перенаправлен на указанный URL-адрес. Отображается в следующем формате: • Для правил обхода: "`[<Название правила>]`". • Для правил доступа: "`[<Название рабочей области>/<Название группы правил>/<Название правила>]`".
`processing_time`	Продолжительность обработки HTTP-сообщения в миллисекундах. Учитывается время с начала обработки заголовка HTTP-сообщения до сохранения записи о выполненной проверке в журнале событий приложения и в журнале событий Syslog.
`scan_result`	Результат проверки HTTP-сообщения. Если обнаружено несколько угроз, отображается название угрозы с наибольшим приоритетом. Если угрозы устранены или не обнаружены, отображается результат проверки с наибольшим приоритетом (*Вылечен*, *Не обнаружено*, *Не проверен*).
`workspace`	Название рабочей области, к которой относится событие обработки трафика. При отсутствии рабочей области отображается прочерк.
`http_user_name`	Имя учетной записи пользователя, инициировавшего HTTP-запрос.
`http_user_agent`	Клиентское приложение, инициировавшее HTTP-запрос.
`http_user_ip`	IP-адрес компьютера, с которого был отправлен HTTP-запрос.
`url`	URL-адрес веб-ресурса, доступ к которому запрашивал пользователь.

Ключ	Описание и возможные значения
kata-alert	Результат проверки URL-адреса на соответствие объектам, обнаруженным приложением KATA. Возможны следующие значения: • NotDetected – URL-адрес проверен, угрозы не обнаружены. • Detected – обнаружено соответствие с объектом в кеше KATA. Указывается ID объекта, критерий совпадения и технология. Например, kata-alert="Detected/128563/Url/Sb". • NotScanned/AccessRuleSettings – проверка не выполнена, так как правило защиты не применяется согласно действию, заданному в правиле доступа. • NotScanned/BypassRuleSettings – проверка не выполнена, так как файл пропущен по правилу обхода без проверки. • NotScanned/ProtectionRuleSettings – проверка не выполнена, так как в правиле защиты для типа объектов **Объекты, обнаруженные KATA** задано действие **Пропустить проверку**. • NotScanned/ApplicationSettings – проверка не выполнена, так как режим получения объектов, обнаруженных KATA или интеграция KATA отключены согласно параметрам приложения. • ScanError/InternalError – проверка завершилась с ошибкой.
Для объекта MIME-типа multipart указывается информация обо всех составных частях. Для каждой составной части используется ключ part с порядковым номером, после которого передаются все атрибуты этой составной части (ключи filename, filesize, part_mimetype, kata_upload, guid, rules, av_status, ap_status, mlf-status, encrypted, macros и kata-alert). Например, part1 "news.html", <атрибуты составной части 1>: part2 <атрибуты составной части 2>.	
filename	Имя проверяемого объекта. Если HTTP-сообщение не содержит объектов, указывается "nofile". В этом случае все последующие поля относятся к проверяемому URL-адресу.

Ключ	Описание и возможные значения
`filesize`	Размер проверяемого объекта. Если HTTP-сообщение не содержит объектов или для применения правил не требуется вычисление размера файла, указывается `"NotApplicable"`.
`part_mimetype`	MIME-тип составной части multipart-объекта. Используется значение заголовка Content-Type. Если HTTP-сообщение не содержит объектов или для применения правил не требуется определение MIME-типа, указывается `"NotApplicable"`.
`kata_upload`	Результат проверки объекта на необходимость отправки на сервер KATA. Возможны следующие значения: • `NotApplicable` – HTTP-сообщение не содержит файлов. • `Scheduled` – отправка файла запланирована. • `DisabledBySettings` – режим отправки файлов на сервер KATA или интеграция KATA отключены в параметрах приложения. • `SkippedByAction` – HTTP-сообщение пропущено по правилу обхода без проверки или к нему применены действия **Заблокировать** или **Перенаправить**. • `RejectedByFilter` – файл не удовлетворяет условиям отправки на сервер KATA. • `Failed/QueueOverflowed` – файл должен быть отправлен на сервер KATA, но запланировать отправку не удалось из-за переполнения очереди. • `Failed/InternalError` – файл должен быть отправлен на сервер KATA, но запланировать отправку не удалось из-за внутренней ошибки приложения.
`guid`	Идентификатор, присвоенный объекту приложением. Идентификатор передается, только если при проверке необходимости отправки на сервер KATA был присвоен один из следующих статусов: • `Scheduled`. • `Failed/QueueOverflowed`. • `Failed/InternalError`. Для других статусов поле `guid` передается с пустым значением.

Ключ	Описание и возможные значения
rules	Названия сработавших правил обработки трафика в следующем формате: "bypass_rule [<Название правила>], access_rules [<Название рабочей области>/<Название группы правил>/<Название правила>], protection_rules [<Название рабочей области>/<Название группы правил>/<Название правила>]". Если правило не относится к рабочей области, вместо названия рабочей области отображается прочерк. Если правило не входит в группу правил, вместо названия группы отображается прочерк. Если не было применено ни одно правило обработки трафика, применяется политика защиты по умолчанию (см. раздел "Настройка политики защиты по умолчанию" на стр. 99). Отображается значение "default_policy [Default Policy]".
av_status	Результаты проверки веб-ресурса модулем Антивирус. Возможны следующие значения: • Detected – в объекте найдены вирусы или другие программы, представляющие угрозу. Через запятую указываются имена обнаруженных угроз и действие приложения над объектом. Например, av-status="Detected", threats="EICAR-Test-File/Block". • ScanError/Timeout – проверка завершилась с ошибкой, так как превышено максимальное время выполнения проверки. • ScanError/InternalError – проверка завершилась с внутренней ошибкой. • ScanError/BasesNotLoaded – проверка завершилась с ошибкой, так как базы модуля Антивирус не загружены. • IncompleteScan/MaxNestingLevelReached – проверка не была выполнена, так как уровень вложенности проверяемого архива превышает максимально допустимый. • IncompleteScan/EncryptedArchive – проверка не была выполнена, так как объект зашифрован. • Disinfected – обнаружены угрозы, все угрозы вылечены. • NotDetected – объект проверен, угрозы не обнаружены. • NotScanned/AccessRuleSettings – к объекту не применялись правила защиты согласно действию, заданному в правиле доступа. • NotScanned/BypassRuleSettings – объект не проходил проверку, так как к нему было применено правило обхода. • NotScanned/ProtectionRuleSettings – объект не проходил проверку согласно действию, заданному в правиле защиты. • NotScanned/ApplicationSettings – объект не проходил проверку согласно заданным параметрам приложения.

Ключ	Описание и возможные значения
ap_status	Результаты проверки веб-ресурса модулем Анти-Фишинг. Возможны следующие значения: • Detected (local bases) – ссылка признана фишинговой на основе записей в локальных базах приложения. • Detected (KSN) – ссылка признана фишинговой на основе проверки репутации в KSN. • Detected (heuristics) – ссылка признана фишинговой на основе данных эвристического анализа. • ScanError/Timeout – проверка завершилась с ошибкой, так как превышено максимальное время выполнения проверки. • ScanError/InternalError – проверка завершилась с внутренней ошибкой. • ScanError/BasesNotLoaded – проверка завершилась с ошибкой, так как базы модуля Анти-Фишинг не загружены. • NotDetected – объект проверен, угрозы не обнаружены. • NotScanned/AccessRuleSettings – к объекту не применялись правила защиты согласно действию, заданному в правиле доступа. • NotScanned/BypassRuleSettings – объект не проходил проверку, так как к нему было применено правило обхода. • NotScanned/ProtectionRuleSettings – объект не проходил проверку согласно действию, заданному в правиле защиты. • NotScanned/ApplicationSettings – объект не проходил проверку согласно заданным параметрам приложения.

Ключ	Описание и возможные значения
mlf-status	Результаты проверки ссылок на наличие вредоносных объектов. Возможны следующие значения: • Detected (local bases) – ссылка признана вредоносной на основе записей в локальных антивирусных базах. • Detected (KSN) – ссылка признана вредоносной на основе проверки репутации в KSN. • ScanError/Timeout – проверка завершилась с ошибкой, так как превышено максимальное время выполнения проверки. • ScanError/InternalError – проверка завершилась с внутренней ошибкой. • ScanError/BasesNotLoaded – проверка завершилась с ошибкой, так как базы модуля Анти-Фишинг не загружены. • NotDetected – ссылка проверена, угрозы не обнаружены. • NotScanned/AccessRuleSettings – к объекту не применялись правила защиты согласно действию, заданному в правиле доступа. • NotScanned/BypassRuleSettings – объект не проходил проверку, так как к нему было применено правило обхода. • NotScanned/ProtectionRuleSettings – объект не проходил проверку согласно действию, заданному в правиле защиты. • NotScanned/ApplicationSettings – объект не проходил проверку согласно заданным параметрам приложения.
encrypted	Информация о шифровании проверяемого объекта. Возможны следующие значения: • Detected – обнаружены угрозы. • ScanError/Timeout – проверка завершилась с ошибкой, так как превышено максимальное время выполнения проверки. • ScanError/InternalError – проверка завершилась с внутренней ошибкой. • ScanError/BasesNotLoaded – проверка завершилась с ошибкой, так как базы модуля Антивирус не загружены. • NotDetected – ссылка проверена, NotScanned/ApplicationSettings – объект не проходил проверку согласно заданным параметрам приложения. Угрозы не обнаружены. • NotScanned/AccessRuleSettings – к объекту не применялись правила защиты согласно действию, заданному в правиле доступа. • NotScanned/BypassRuleSettings – объект не проходил проверку, так как к нему было применено правило обхода. • NotScanned/ProtectionRuleSettings – объект не проходил проверку согласно действию, заданному в правиле защиты. • NotScanned/ApplicationSettings – объект не проходил проверку согласно заданным параметрам приложения.

Ключ	Описание и возможные значения
macros	Информация о наличии макросов в проверяемом объекте. Возможны следующие значения: • Detected – обнаружены макросы. • ScanError/Timeout – проверка завершилась с ошибкой, так как превышено максимальное время выполнения проверки. • ScanError/InternalError – проверка завершилась с внутренней ошибкой. • ScanError/BasesNotLoaded – проверка завершилась с ошибкой, так как базы модуля Антивирус не загружены. • NotDetected – объект проверен, макросы не обнаружены. • NotScanned/AccessRuleSettings – к объекту не применялись правила защиты согласно действию, заданному в правиле доступа. • NotScanned/BypassRuleSettings – объект не проходил проверку, так как к нему было применено правило обхода. • NotScanned/ProtectionRuleSettings – объект не проходил проверку согласно действию, заданному в правиле защиты. • NotScanned/ApplicationSettings – объект не проходил проверку согласно заданным параметрам приложения.
kata-alert	Результат проверки файла, содержащегося в HTTP-сообщении, или составной части (для multipart-объектов) на соответствие объектам, обнаруженным приложением KATA. Возможны следующие значения: • NotDetected – URL-адрес проверен, угрозы не обнаружены. • Detected – обнаружено соответствие с объектом в кеше KATA. Указывается ID объекта, критерий совпадения и технология. Например, kata-alert="Detected/124567/Md5/Yara". • NotScanned/AccessRuleSettings – проверка не выполнена, так как правило защиты не применяется согласно действию, заданному в правиле доступа. • NotScanned/BypassRuleSettings – проверка не выполнена, так как файл пропущен по правилу обхода без проверки. • NotScanned/ProtectionRuleSettings – проверка не выполнена, так как в правиле защиты для типа объектов **Объекты, обнаруженные KATA** задано действие **Пропустить проверку**. • NotScanned/ApplicationSettings – проверка не выполнена, так как режим получения объектов, обнаруженных KATA или интеграция KATA отключены согласно параметрам приложения. • ScanError/InternalError – проверка завершилась с ошибкой.

kaspersky

Содержание syslog-сообщений о системных событиях приложения

Системные события приложения содержат информацию о состоянии узлов кластера, модулей приложения и лицензии.

В каждом syslog-сообщении для всех типов событий передаются следующие поля, определяемые параметрами Syslog в операционной системе:

- дата и время события;
- имя хоста, на котором произошло событие;
- название приложения (всегда имеет значение `KWTS`).

Пример:

```
Jan 5 03:39:01 hostname KWTS: Anti-Phishing bases applied:
publishing-time="2019-01-05T03:08:00"
```

Содержание syslog-сообщений в зависимости от типа системного события приведено в таблице ниже.

Таблица 11. Содержание syslog-сообщений в зависимости от типа системного события

Тип события	Описание события	Сообщение
Запуск / остановка приложения	Приложение запущено	`audit started`
	Приложение остановлено	`audit stopped`
Обновление баз модуля Антивирус	Ошибка загрузки баз	`Anti-Virus bases loading error: <причина ошибки>`
	Ошибка обновления баз	`Anti-Virus bases update error: <причина ошибки>`
	Базы успешно загружены	`Anti-Virus bases applied: publishing-time="<дата и время загрузки>", record-count=<количество записей>`
	Базы успешно обновлены	`Anti-Virus bases updated`
Обновление баз модуля Анти-Фишинг	Ошибка загрузки баз	`Anti-Phishing bases loading error: <причина ошибки>`

Тип события	Описание события	Сообщение
	Ошибка обновления баз	`Anti-Phishing bases update error: <причина ошибки>`
	Базы успешно загружены	`Anti-Phishing bases applied: publishing-time="<дата и время загрузки>", record-count=<количество записей>`
	Базы успешно обновлены	`Anti-Phishing bases updated`
Лицензирование	Срок действия лицензии истек	`license key expired: license-id="<серийный номер лицензионного ключа>" functionalityLevel="Full functionality" expiration-date="<дата и время истечения срока действия лицензии>"`
	Ошибка лицензии	`license error: <описание ошибки>`
	Лицензионный ключ помещен в список запрещенных	`license is blacklisted: license-id="<серийный номер лицензионного ключа>" functionalityLevel="Full functionality"`
	Код активации заблокирован до активации приложения	`activation code cannot be installed as it is blocked`
	Лицензия отсутствует	`no license`
	Код активации успешно добавлен	`license installed: license-id="<серийный номер лицензионного ключа>" functionalityLevel="Full functionality"`

Тип события	Описание события	Сообщение
	Статус лицензионного ключа успешно обновлен	`license updated: license-id="<серийный номер лицензионного ключа>" functionalityLevel="Full functionality"`
	Код активации успешно удален	`license removed: license-id="<серийный номер лицензионного ключа>" functionalityLevel="Full functionality"`
	Срок действия лицензии скоро истекает	`license expires soon: license-id="<серийный номер лицензионного ключа>" functionalityLevel="Full functionality" days-left=<количество оставшихся дней>`
	Действует льготный период действия лицензии	`license grace period: license-id="<серийный номер лицензионного ключа>" functionalityLevel="Full functionality" days-left=<количество оставшихся дней>`
	Лицензия действительна	`license is ok: license-id="<серийный номер лицензионного ключа>" functionalityLevel="Full functionality"`
Процессы	Процесс приложения завершился аварийно (при многократных аварийных остановках указывается количество остановок и период, за который они произошли)	`<имя процесса> crashed [<количество остановок> times during last <количество минут> minutes]`
	Процесс приложения перезапущен (при многократных перезапусках процесса указывается количество перезапусков и период, за который они произошли)	`<имя процесса> restarted [<количество перезапусков> times during last <количество минут> minutes]`

kaspersky

Содержание syslog-сообщений о событиях отправки файлов на сервер KATA

Информация о помещении файла в очередь на отправку в KATA, а также результаты отправки файла в KATA записываются в журнал операционной системы по протоколу Syslog.

В каждом syslog-сообщении передаются следующие поля, определяемые параметрами протокола Syslog в операционной системе:

- дата и время события;
- имя хоста, на котором произошло событие;
- название приложения (всегда имеет значение `KWTS`).

В зависимости от типа события передается поле `KATA upload scheduling` (помещение файла в очередь на отправку) или `KATA uploading` (отправка файла). Поля syslog-сообщения, определяемые параметрами приложения, представлены в формате `<ключ>="<значение>"`. Если ключ имеет несколько значений, эти значения указываются через запятую. В качестве разделителя между ключами используется двоеточие.

Пример:

Oct 2 13:19:27 localhost KWTS: KATA uploading: result="Succeeded": type="Request": http_user_name="example@test.local": http_user_ip="192.0.2.0": url="http://example.com/TEST/test.pdf": guid="A485A9DD-A740-4ED3-9933-63ACAEA964E4": filename="test.pdf": filetype="OfficePdf"

Ключи, а также их значения, содержащиеся в сообщении, приведены в таблице ниже.

Таблица 12. Информация о событиях отправки файлов на сервер KATA в syslog-сообщениях

Ключ	Описание и возможные значения
`result`	Результат помещения файла в очередь на отправку или отправки файла. Возможны следующие значения: • `Succeeded` – операция выполнена успешно. • `Failed/<причина>` – не удалось поместить файл в очередь по указанной причине.
`type`	Тип HTTP-сообщения. Возможны следующие значения: • `Request` – запрос. • `Response` – ответ.
`http_user_name`	Имя учетной записи пользователя, который выполнил операцию с файлом.
`http_user_ip`	IP-адрес компьютера, с которого был отправлен файл.
`url`	URL-адрес веб-ресурса, доступ к которому запрашивал пользователь.
`guid`	Идентификатор, который был присвоен файлу приложением.
`filename`	Имя отправляемого файла.
`filetype`	Тип отправляемого файла.

kaspersky

Работа с приложением по протоколу SNMP

SNMP (Simple Network Management Protocol – простой протокол сетевого управления) – протокол управления сетевыми устройствами.

В Kaspersky Web Traffic Security для работы по протоколу SNMP используется *SNMP-агент*, который отслеживает информацию о работе приложения. Kaspersky Web Traffic Security может отправлять эту информацию в виде *SNMP-ловушек* – уведомлений о событиях работы приложения.

Для работы по протоколу SNMP требуется предварительно настроить службу snmpd в операционной системе (см. раздел «Настройка службы snmpd в операционной системе» на стр. 202).

По протоколу SNMP вы можете получить доступ к следующей информации о приложении:

- общим сведениям;
- статистике работы Kaspersky Web Traffic Security с момента установки приложения;
- данным о событиях, возникающих в ходе работы приложения.

Доступ предоставляется только на чтение информации.

Информация об SNMP-ловушках и статистике, отправляемой по протоколу SNMP, хранится в базе данных MIB (см. раздел "Описание объектов MIB Kaspersky Web Traffic Security" на стр. 213).

В этом разделе

Настройка службы snmpd в операционной системе

Для работы по протоколу SNMP с Kaspersky Web Traffic Security используется служба snmpd из состава операционной системы. Служба snmpd выступает в роли мастер-агента, принимая и обрабатывая запросы от систем мониторинга и других внешних потребителей по протоколу SNMP. Kaspersky Web Traffic Security подключается к службе snmpd в качестве субагента по протоколу AgentX через UNIX™-сокет.

Установка службы snmpd

Проверьте, что в вашей операционной системе установлена служба snmpd. Если службы нет, установите соответствующие пакеты.

► *Чтобы установить службу snmpd и вспомогательные утилиты, выполните команду:*

```
apt install snmp snmpd
```

Создание учетной записи пользователя для доступа к данным

Перед созданием учетной записи остановите службу snmpd.

Для безопасного доступа к данным по протоколу SNMPv3 с аутентификацией и шифрованием нужно создать учетную запись на стороне службы snmpd со следующими данными:

- Имя пользователя (чувствительно к регистру).
- Алгоритм аутентификации (MD5 или SHA, рекомендуется SHA).
- Пароль для аутентификации.
- Алгоритм шифрования (поддерживается только AES).
- Пароль для шифрования.

В целях безопасности рекомендуется использовать отдельные учетные записи на разных узлах кластера Kaspersky Web Traffic Security.

Создать учетную запись можно следующими способами:

- С помощью утилиты net-snmp-create-v3-user, если она есть в операционной системе.
- Вручную, добавив соответствующую директиву в конфигурационный файл службы snmpd.

► *Чтобы создать учетную запись пользователя с помощью утилиты net-snmp-create-v3-user:*

1. Запустите командную оболочку операционной системы для выполнения команд с полномочиями суперпользователя (администратора системы).
2. Выполните команду:

   ```
   net-snmp-create-v3-user -ro -a <алгоритм аутентификации> -x <алгоритм шифрования> <имя пользователя>
   ```

   Пароли для аутентификации и шифрования будут запрошены интерактивно.

Пример:

net-snmp-create-v3-user -ro -a SHA -x AES MonitoringUser

► *Чтобы создать учетную запись пользователя без утилиты:*

1. Запустите командную оболочку операционной системы для выполнения команд с полномочиями суперпользователя (администратора системы).
2. Создайте конфигурационный файл /var/lib/snmp/snmpd.conf с помощью команды:

   ```
   touch /var/lib/snmp/snmpd.conf
   ```

3. Добавьте в конфигурационный файл строку вида:

```
createUser <имя пользователя> <алгоритм аутентификации> "<пароль для аутентификации>" <алгоритм шифрования> "<пароль для шифрования>"
```

Пример:

createUser MonitoringUser SHA "MonitoringAuthSecret" AES "MonitoringPrivSecret"

Создание учетной записи пользователя для приема SNMP-ловушек

Для приема SNMP-ловушек по протоколу SNMPv3 с аутентификацией и шифрованием нужно на стороне системы мониторинга создать учетную запись в контексте соответствующей службы (обычно это служба snmptrapd).

Учетная запись должна содержать следующие данные:

- Имя пользователя.
- Алгоритм аутентификации.
- Пароль для аутентификации.
- Алгоритм шифрования.
- Пароль для шифрования.

В целях безопасности нужно использовать разные учетные записи для доступа к данным и для приема SNMP-ловушек.
Рекомендуется создавать отдельные учетные записи для приема SNMP-ловушек с разных узлов кластера Kaspersky Web Traffic Security.

Инструкцию по созданию учетной записи пользователя для приема SNMP-ловушек см. в документации вашей системы мониторинга.

Настройка службы snmpd

Конфигурация службы snmpd хранится в файле /etc/snmp/snmpd.conf. Вам необходимо создать новый конфигурационный файл и последовательно добавить в него строки, приведенные ниже.

► *Чтобы настроить службу snmpd:*

1. Запустите командную оболочку операционной системы для выполнения команд с полномочиями суперпользователя (администратора системы).
2. Создайте новый конфигурационный файл и задайте права доступа к нему при помощи команд:

```
mv -f /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.backup
touch /etc/snmp/snmpd.conf
chown root:root /etc/snmp/snmpd.conf
chmod 600 /etc/snmp/snmpd.conf
```

3. Укажите протокол, адрес сетевого интерфейса и номер порта, на котором служба snmpd будет

принимать входящие запросы.

- Если вы хотите принимать запросы на всех сетевых интерфейсах, добавьте в конфигурационный файл следующие строки:

  ```
  # Listen for incoming SNMP requests via UDP
  agentAddress udp:161
  ```

- Если вы хотите принимать запросы только на локальном сетевом интерфейсе, например если система мониторинга установлена на этой же машине, добавьте строки:

  ```
  # Listen for incoming SNMP requests via UDP
  agentAddress udp:127.0.0.1:161
  ```

4. Укажите путь и разрешения для UNIX-сокета, на котором служба snmpd будет принимать подключения от субагента по протоколу AgentX. Для этого добавьте в конфигурационный файл следующие строки:

   ```
   # Listen for subagent connections via UNIX socket
   master agentx
   agentXSocket unix:/var/run/agentx-master.socket
   agentXPerms 770 770 kluser klusers
   ```

5. При необходимости вы можете указать описание системы, расположение системы, контактный адрес администратора. Для этого добавьте в конфигурационный файл следующие строки:

   ```
   # Basic system information
   sysDescr <описание системы>
   sysLocation <расположение системы>
   sysContact <контактный адрес администратора>
   sysServices 72
   ```

6. Укажите область OID-дерева, которая будет доступна вашей системе мониторинга по протоколу SNMP. Для доступа к данным приложения Kaspersky Web Traffic Security добавьте в конфигурационный файл следующие строки:

   ```
   # Kaspersky Web Traffic Security SNMP statistics
   view monitoring included .1.3.6.1.4.1.23668.2022
   ```

7. При необходимости дополнительно укажите область OID-дерева с информацией об операционной системе, которую хранит служба snmpd. Эта область будет доступна вашей системе мониторинга.

   Информация об операционной системе включает, например, данные об использовании процессора и оперативной памяти, данные о свободном месте на дисковых разделах, загрузке сетевых интерфейсов, список установленного программного обеспечения, список открытых сетевых соединений, список запущенных процессов. Эта информация может содержать конфиденциальные данные.

   - Если вы хотите разрешить доступ только к общей информации о системе и данным об использовании памяти, процессора, сетевых и дисковых устройств, добавьте в конфигурационный файл следующие строки:

     ```
     # SNMPv2-MIB - Basic system information
     ```

```
view monitoring included .1.3.6.1.2.1.1
# HOST-RESOURCES-MIB - CPU, Memory, Filesystems
view monitoring included .1.3.6.1.2.1.25.1
view monitoring included .1.3.6.1.2.1.25.2
view monitoring included .1.3.6.1.2.1.25.3
view monitoring included .1.3.6.1.2.1.25.5
# UCD-SNMP-MIB - Memory and CPU usage
view monitoring included .1.3.6.1.4.1.2021.4
view monitoring included .1.3.6.1.4.1.2021.10
view monitoring included .1.3.6.1.4.1.2021.11
# UCD-SNMP-DISKIO-MIB - Block devices I/O statistics
view monitoring included .1.3.6.1.4.1.2021.13
# IF-MIB - Network interfaces I/O statistics
view monitoring included .1.3.6.1.2.1.2
view monitoring included .1.3.6.1.2.1.31
```

- Если вы хотите разрешить доступ ко всей системной информации, добавьте в конфигурационный файл следующие строки:

  ```
  # Allow access to the whole OID tree
  view monitoring included .1
  ```

8. Укажите режим доступа и область данных для созданной учетной записи. Для этого добавьте в конфигурационный файл следующие строки:

   ```
   # Access control for SNMPv3 monitoring system user
   rouser <имя пользователя> priv -V monitoring
   ```

9. Для отправки SNMP-ловушек укажите IP-адрес системы мониторинга и учетные данные пользователя для приема ловушек. Для этого добавьте в конфигурационный файл следующие строки:

   ```
   # Send SNMPv3 traps to the monitoring system
   trapsess -Ci -v3 -t0.1 -r1 -l authPriv -u <имя пользователя для приема ловушек> -a <алгоритм аутентификации> -A "<пароль пользователя для приема ловушек>" -x <алгоритм шифрования> -X "<пароль для шифрования>" udp:<IP-адрес>:162
   ```

Служба snmpd будет настроена.

Для интеграции с несколькими системами мониторинга создайте отдельную учетную запись для каждой системы, укажите для учетных записей область доступных данных (директивы view и rouser) и настройте отправку SNMP-ловушек (директива trapsess).

kaspersky

Пример конфигурационного файла службы snmpd:

```
# Listen for incoming SNMP requests via UDP
agentAddress udp:161

# Listen for subagent connections via UNIX socket
master agentx
agentXSocket unix:/var/run/agentx-master.socket
agentXPerms 770 770 kluser klusers

# Basic system information
sysDescr         Example Proxy Server, Node 05
sysLocation      Example Datacenter, Ground floor, B23-U45
sysContact       Proxy Server administrator <admin@example.com>
sysServices 72

# Kaspersky Web Traffic Security SNMP statistics
view monitoring included .1.3.6.1.4.1.23668.2022
# SNMPv2-MIB - Basic system information
view monitoring included .1.3.6.1.2.1.1
# HOST-RESOURCES-MIB - CPU, Memory, Filesystems
view monitoring included .1.3.6.1.2.1.25.1
view monitoring included .1.3.6.1.2.1.25.2
view monitoring included .1.3.6.1.2.1.25.3
view monitoring included .1.3.6.1.2.1.25.5
# UCD-SNMP-MIB - Memory and CPU usage
view monitoring included .1.3.6.1.4.1.2021.4
view monitoring included .1.3.6.1.4.1.2021.10
view monitoring included .1.3.6.1.4.1.2021.11
# UCD-SNMP-DISKIO-MIB - Block devices I/O statistics
view monitoring included .1.3.6.1.4.1.2021.13
```

```
# IF-MIB - Network interfaces I/O statistics

view monitoring included .1.3.6.1.2.1.2

view monitoring included .1.3.6.1.2.1.31


# Access control for SNMPv3 monitoring system user

rouser MonitoringUser priv -V monitoring


# Send SNMPv3 traps to the monitoring system

trapsess -Ci -v3 -t0.1 -r1 -l authPriv -u TrapUser -a SHA -A "TrapAuthSecret" -x AES -X "TrapPrivSecret"
udp:10.16.32.64:162
```

Запуск службы snmpd с новой конфигурацией

► *Чтобы применить новую конфигурацию:*

1. Перезапустите службу snmpd с помощью команды:

   ```
   systemctl restart snmpd
   ```

2. Проверьте статус службы snmpd с помощью команды:

   ```
   systemctl status snmpd
   ```

   Статус должен быть *running*.

3. Разрешите автоматический запуск службы при загрузке операционной системы с помощью команды:

   ```
   systemctl enable snmpd
   ```

4. Если у вас используется сетевой экран в операционной системе или на сетевом оборудовании, добавьте соответствующие правила для пропуска пакетов протокола SNMP.

Служба snmpd будет запущена.

Проверка работоспособности службы snmpd

Для проверки работоспособности службы snmpd настройте использование SNMP в веб-интерфейсе Kaspersky Web Traffic Security (см. раздел "Настройка параметров подключения к SNMP-серверу" на стр. 209) и выполните запрос SNMP-данных с помощью утилиты snmpwalk.

► *Чтобы получить области SNMP-данных, предоставляемых приложением Kaspersky Web Traffic Security, выполните команду:*

```
snmpwalk -v3 -l authPriv -u <имя пользователя> -a <алгоритм аутентификации>
-A "<пароль для аутентификации>" -x <алгоритм шифрования> -X "<пароль для
шифрования>" <IP-адрес> .1.3.6.1.4.1.23668.2022
```

Пример:

snmpwalk -v3 -l authPriv -u MonitoringUser -a SHA -A "MonitoringAuthSecret" -x AES -X "MonitoringPrivSecret" 127.0.0.1 .1.3.6.1.4.1.23668.2022

Включение и отключение использования SNMP в приложении

► *Чтобы включить или отключить использование SNMP в работе приложения:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры → Журналы и события → SNMP**.
2. Выполните одно из следующих действий:
   - Включите переключатель рядом с названием блока параметров **Использовать SNMP**, если вы хотите включить использование SNMP.
   - Выключите переключатель рядом с названием блока параметров **Использовать SNMP**, если вы хотите отключить использование SNMP.
3. Нажмите на кнопку **Сохранить**.

Настройка параметров подключения к SNMP-серверу

► *Чтобы настроить параметры подключения к SNMP-серверу:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры → Журналы и события → SNMP**.
2. Включите переключатель **Использовать SNMP**, если он отключен.
3. В поле **Путь к UNIX-сокету**, укажите путь к файлу сокета.

   По умолчанию указан путь /var/run/agentx-master.socket.

   > Для подключения к SNMP-серверу используется UNIX-сокет. Использование TCP- и UDP-сокетов не поддерживается.

4. В поле **Время ожидания ответа сервера (сек.)** укажите максимальное время ожидания ответа от SNMP-сервера в секундах. Вы можете указать значение в интервале от 1 до 255 секунд.

   Значение по умолчанию: 15 секунд.
5. Нажмите на кнопку **Сохранить**.

Соединение с SNMP-сервером будет настроено.

kaspersky

Включение и отключение отправки SNMP-ловушек

► *Чтобы включить или отключить отправку SNMP-ловушек событий, возникающих в ходе работы приложения:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Журналы и события** → **SNMP**.
2. Включите переключатель рядом с названием блока **Использовать SNMP**, если он выключен.
3. Выполните одно из следующих действий:
   - Установите флажок **Отправлять SNMP-ловушки**, если вы хотите включить отправку SNMP-ловушек.
   - Снимите флажок **Отправлять SNMP-ловушки**, если вы хотите отключить отправку SNMP-ловушек.
4. Нажмите на кнопку **Сохранить**.

Отправка SNMP-ловушек будет настроена.0

Настройка внешней системы мониторинга

Kaspersky Web Traffic Security предоставляет данные по протоколу SNMP отдельно для каждого узла кластера. Для хранения, агрегации и анализа этих данных используется *внешняя система мониторинга* (далее также *система мониторинга*).

Настройка внешней системы мониторинга для работы по протоколу SNMP

► *Чтобы настроить внешнюю систему мониторинга:*

1. Если система мониторинга поддерживает импорт MIB-файлов, импортируйте информацию об объектах MIB приложения Kaspersky Web Traffic Security (см. раздел "Экспорт объектов MIB" на стр. 217).
2. Добавьте в систему мониторинга все узлы кластера Kaspersky Web Traffic Security в качестве наблюдаемых устройств (узлов сети).
3. Для каждого наблюдаемого устройства укажите параметры подключения по протоколу SNMPv3:
   - Адрес подключения.
   - Порт.
   - Протокол.
   - Учетные данные пользователя: имя пользователя, алгоритм аутентификации, пароль для аутентификации, алгоритм шифрования, пароль для шифрования.

     Используйте данные учетной записи, которая была создана при настройке службы snmpd на узле кластера Kaspersky Web Traffic Security.
4. Для каждого наблюдаемого устройства укажите список данных, передаваемых по протоколу SNMP. Используйте символьные имена объектов MIB или их числовые идентификаторы. Для каждого элемента данных задайте его тип (целое число или строка), периодичность опроса, срок хранения.
5. Настройте графики, триггеры и оповещения, используя в качестве основы данные, передаваемые

по протоколу SNMP.

6. Для каждого узла кластера Kaspersky Web Traffic Security создайте учетную запись пользователя для получения ловушек по протоколу SNMPv3.

   Учетные данные пользователей укажите в параметрах службы snmpd на узлах кластера (директива trapsess).

7. Для каждого наблюдаемого устройства укажите список событий, получаемых в виде SNMPv3-ловушек. Используйте символьные имена объектов MIB или их числовые идентификаторы. Для событий, которые вы считаете важными, создайте соответствующие триггеры.

Настройка службы snmptrapd для приема SNMP-ловушек

Некоторые системы мониторинга (например, Zabbix, LibreNMS) используют службу snmptrapd из состава операционной системы в качестве агента для приема SNMP-ловушек. Служба snmptrapd сохраняет информацию о полученных событиях в файл журнала, который в дальнейшем считывается системой мониторинга.

Настройка службы snmptrapd выполняется на компьютере, на котором установлена служба мониторинга.

► *Чтобы настроить службу snmptrapd:*

1. Проверьте, что в операционной системе установлены служба snmptrapd и базовые MIB-файлы.

   Если служба snmptrapd отсутствует, установите соответствующие пакеты:

   - В операционных системах РЕД ОС, Red Hat® Enterprise Linux®, CentOS, Rocky Linux™ выполните команду:

     ```
     yum install net-snmp net-snmp-utils
     ```

   - В операционных системах Debian, Ubuntu, Astra Linux Special Edition выполните команду:

     ```
     apt install snmp snmptrapd
     ```

   Чтобы установить базовые MIB-файлы:

   - В операционных системах РЕД ОС, Red Hat Enterprise Linux, CentOS, Rocky Linux выполните команду:

     ```
     yum install net-snmp-libs
     ```

   - В операционных системах Debian, Ubuntu выполните команду:

     ```
     apt install snmp-mibs-downloader
     ```

   - В операционной системе Astra Linux Special Edition следуйте инструкциям в документации Astra Linux.

2. Скопируйте MIB-файлы Kaspersky Web Traffic Security в каталог с MIB-файлами, например в папку /usr/share/snmp/mibs/kwts.

3. Для подключения MIB-файлов приложения добавьте в конфигурационный файл /etc/snmp/snmp.conf следующие строки:

   ```
   mibdirs +/usr/share/snmp/mibs/kwts
   mibs all
   ```

4. Конфигурация службы snmptrapd хранится в файле /etc/snmp/snmptrapd.conf. Вы можете добавить нужные данные в существующий конфигурационный файл или создать новый конфигурационный файл и последовательно добавить в него строки параметров.

   Если вы создали новый конфигурационный файл, убедитесь, что доступ к нему имеет только суперпользователь. При необходимости задайте нужные разрешения при помощи команд:

   ```
   chown root:root /etc/snmp/snmptrapd.conf
   chmod 600 /etc/snmp/snmptrapd.conf
   ```

5. Укажите протокол, адрес сетевого интерфейса и номер порта, на котором служба snmptrapd будет принимать SNMP-ловушки. Чтобы принимать запросы на всех сетевых интерфейсах, добавьте в конфигурационный файл следующую строку:

   ```
   snmpTrapdAddr udp:162
   ```

6. Для приема SNMP-ловушек по протоколу SNMPv3 с аутентификацией и шифрованием необходимо на стороне службы snmptrapd добавить учетные записи пользователей со следующими данными:

   - имя пользователя (чувствительно к регистру);
   - алгоритм аутентификации (MD5 или SHA, рекомендуется SHA);
   - пароль для аутентификации;
   - алгоритм шифрования (поддерживается только AES);
   - пароль для шифрования.

   > В целях безопасности рекомендуется создавать разные учетные записи пользователей для приема SNMP-ловушек с разных узлов кластера Kaspersky Web Traffic Security.

7. Для каждой созданной учетной записи пользователя добавьте в конфигурационный файл следующие строки:

   ```
   createUser <имя пользователя> <алгоритм аутентификации> "<пароль для аутентификации>" <алгоритм шифрования> "<пароль для шифрования>"
   authUser log <имя пользователя> priv
   ```

   Пример конфигурационного файла:

   ```
   snmpTrapdAddr udp:162
   createUser TrapUser SHA "TrapAuthSecret" AES "TrapPrivSecret"
   authUser log TrapUser priv
   createUser TrapUser2 SHA "TrapAuthSecret2" AES "TrapPrivSecret2"
   authUser log TrapUser2 priv
   ```

8. Для проверки работоспособности службы snmptrapd выполните следующие действия:

   a. Настройте службу snmpd на узле кластера Kaspersky Web Traffic Security на отправку SNMP-ловушек на адрес системы мониторинга.

   b. Настройте отправку SNMP-ловушек в веб-интерфейсе Kaspersky Web Traffic Security.

   c. Запустите службу snmptrapd в отладочном режиме и ожидайте получения SNMP-ловушек.

      Для запуска службы snmptrapd в отладочном режиме выполните команду:

      ```
      snmptrapd -f -Lo
      ```

   Если все настроено правильно, в течение 5-10 минут вы получите SNMP-ловушку с событием о

состоянии KSN в приложении:

```
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (4504) 0:00:45.04
SNMPv2-MIB::snmpTrapOID.0 = OID: Kaspersky Web Traffic
Security-EVENTS-MIB::ksnConnectionStatusEvent
KWTS-EVENTS-MIB::sourceNode = STRING: kwts01.example.com
KWTS-EVENTS-MIB::status = STRING: KsnDisabled
```

9. Настройте интеграцию службы snmptrapd с системой мониторинга.

   Для этого следуйте инструкциям документации вашей системы мониторинга.

Служба snmptrapd будет настроена.

Описание объектов MIB Kaspersky Web Traffic Security

В таблицах ниже приведена информация об объектах MIB Kaspersky Web Traffic Security.

События управления кластером

Таблица 13. События управления кластером

Идентификатор (OID)	Символьное имя	Описание	Параметры
.1.3.6.1.4.1.23668.2022.1.1600	clusterConsistencyErrorEvent	Ошибка состояния серверов. Например, нет ни одного сервера с ролью Управляющий узел.	• Имя Управляющего узла. • Сообщение об ошибке.
.1.3.6.1.4.1.23668.2022.1.1610	clusterEmergencyStateEvent	Приложение перешло в аварийный режим.	• Имя Управляющего узла. • Сообщение об ошибке.
.1.3.6.1.4.1.23668.2022.1.1620	settingsSynchronizationErrorEvent	Ошибка синхронизации параметров между Управляющим и Подчиненными узлами.	• Имя Управляющего узла. • Сообщение об ошибке.

События обработки трафика

Таблица 14. События обработки трафика

Идентификатор (OID)	Символьное имя	Описание	Параметры
.1.3.6.1.4.1.23668.2022.1.420	productStartEvent	Приложение запущено. Это событие возникает после того, как запускаются все службы, необходимые для работы Kaspersky Web Traffic Security.	Нет параметров.
.1.3.6.1.4.1.23668.2022.1.400	taskCrashEvent	Процесс приложения завершился аварийно.	Полный путь к бинарному файлу.
.1.3.6.1.4.1.23668.2022.1.410	taskRestartEvent	Процесс приложения перезапущен.	Полный путь к бинарному файлу.
.1.3.6.1.4.1.23668.2022.1.300	licenseInstalledEvent	Код активации добавлен.	Серийный номер лицензионного ключа.
.1.3.6.1.4.1.23668.2022.1.360	licenseUpdatedEvent	Статус лицензионного ключа изменен.	• Серийный номер лицензионного ключа. • Тип лицензии. • Дата окончания срока действия лицензии.
.1.3.6.1.4.1.23668.2022.1.310	licenseRevokedEvent	Код активации удален.	Серийный номер лицензионного ключа.
.1.3.6.1.4.1.23668.2022.1.330	licenseExpiredEvent	Истек срок действия лицензии.	• Серийный номер лицензионного ключа. • Дата окончания срока действия лицензии.

Идентификатор (OID)	Символьное имя	Описание	Параметры
.1.3.6.1.4.1.23668.2022.1.320	licenseExpiresSoonEvent	Срок действия лицензии скоро истечет.	• Серийный номер лицензионного ключа. • Дата окончания срока действия лицензии.
.1.3.6.1.4.1.23668.2022.1.340	licenseTrialPeriodIsOverEvent	Истек срок действия пробной лицензии.	• Серийный номер лицензионного ключа. • Дата окончания срока действия лицензии.
.1.3.6.1.4.1.23668.2022.1.380	gracePeriodEvent	Начался льготный период действия лицензии.	• Серийный номер лицензионного ключа. • Количество дней до завершения льготного периода.
.1.3.6.1.4.1.23668.2022.1.10	updateErrorEvent	Обновление баз приложения завершилось ошибкой.	Причина ошибки.
.1.3.6.1.4.1.23668.2022.1.100	avBasesOutdatedEvent	Базы модуля Антивирус устарели.	Нет параметров.
.1.3.6.1.4.1.23668.2022.1.120	avBasesObsoletedEvent	Базы модуля Антивирус сильно устарели.	Нет параметров.
.1.3.6.1.4.1.23668.2022.1.150	apBasesOutdatedEvent	Базы модуля Анти-Фишинг устарели.	Нет параметров.
.1.3.6.1.4.1.23668.2022.1.160	apBasesObsoletedEvent	Базы модуля Анти-Фишинг сильно устарели.	Нет параметров.

Другие события приложения

Таблица 15. Другие события приложения

Идентификатор (OID)	Символьное имя	Описание	Параметры
.1.3.6.1.4.1.23668.2022.1.700	KsnConnectionStatusEvent	Изменение состояния подключения к службам KSN.	Новое состояние подключения: • `Ok`. • `Error`. • `KsnDisabled`. • `KsnRestrictedLicense`.
.1.3.6.1.4.1.23668.2022.1.910	LdapCacheUpdateEvent	Запуск синхронизации данных с Active Directory.	• Статус синхронизации LDAP-кеша. • Статус синхронизации данных для автозаполнения учетных записей.

Статистика приложения

Таблица 16. Статистика приложения

Идентификатор (OID)	Символьное имя	Описание
.1.3.6.1.4.1.23668.2022.2.8.1	productName	Название приложения.
.1.3.6.1.4.1.23668.2022.2.8.2	productVersion	Версия приложения.
.1.3.6.1.4.1.23668.2022.2.8.3	installDate	Дата установки приложения.
.1.3.6.1.4.1.23668.2022.2.8.4	licenseExpireDate	Дата окончания срока действия лицензии.
.1.3.6.1.4.1.23668.2022.2.8.5	licenseStatus	Состояние кода активации.

Статистика модуля Антивирус

Таблица 17. Статистика модуля Антивирус

Идентификатор (OID)	Символьное имя	Описание
.1.3.6.1.4.1.23668.2022.2.8.5	cleanObjects	Количество объектов, в которых не обнаружены угрозы.
.1.3.6.1.4.1.23668.2022.2.2.2	infectedObjects	Количество зараженных объектов.
.1.3.6.1.4.1.23668.2022.2.2.3	passwordProtectedObjects	Количество объектов, защищенных паролем.
.1.3.6.1.4.1.23668.2022.2.2.4	docsWithMacro	Количество документов, содержащих макросы.
.1.3.6.1.4.1.23668.2022.2.2.5	scanErrors	Количество ошибок, связанных с превышением максимального допустимого времени проверки.

Идентификатор (OID)	Символьное имя	Описание
.1.3.6.1.4.1.23668.2022.2.2.6	notScannedSettingsObjects	Количество объектов, не проверенных в соответствии с параметрами правила обработки трафика.
.1.3.6.1.4.1.23668.2022.2.2.7	notScannedDueToNestingLevel	Количество объектов, не проверенных из-за превышения допустимой глубины проверки архивов.

Экспорт объектов MIB

Файлы, содержащие информацию об объектах MIB Kaspersky Web Traffic Security, расположены в директории /opt/kaspersky/kwts/share/snmp-mibs. Вы можете скопировать эти файлы с любого узла кластера и импортировать их в свою систему мониторинга.

Директория /opt/kaspersky/kwts/share/snmp-mibs содержит следующие файлы:

- KASPERSKY-MIB.txt
- KWTS-ANTIVIRUS-STATISTICS.txt
- KWTS-CONTROL-EVENTS-MIB.txt
- KWTS-EVENTS-MIB.txt
- KWTS-MIB.txt
- KWTS-PRODUCTINFO-STATISTICS.txt
- KWTS-STATISTICS-MIB.txt

Перед использованием MIB-файлов Kaspersky Web Traffic Security убедитесь, что в вашей системе установлены следующие базовые объекты MIB:

- SNMPv2-SMI
- SNMPv2-CONF
- SNMPv2-TC
- SNMP-FRAMEWORK-MIB

kaspersky

Аутентификация с помощью технологии единого входа

При включении технологии единого входа пользователям не требуется вводить учетные данные для подключения к веб-интерфейсу. Аутентификация осуществляется с помощью доменной учетной записи пользователя.

Рекомендуется использовать Kerberos-аутентификацию, так как данный механизм является более надежным. При NTLM-аутентификации злоумышленники могут получить доступ к хешам паролей пользователей, перехватив сетевой трафик.

В этом разделе

Создание keytab-файла

Вы можете использовать одну учетную запись для аутентификации на всех узлах кластера. Для этого требуется создать keytab-файл, содержащий *имена субъекта-службы (далее также "SPN")* для каждого из этих узлов. При создании keytab-файла потребуется использовать атрибут для генерации *соли* (salt, модификатор входа хеш-функции).

Сгенерированную соль необходимо сохранить любым удобным способом для дальнейшего добавления новых SPN в keytab-файл.

Вы также можете создать отдельную учетную запись Active Directory для каждого узла кластера, для которого вы хотите настроить Kerberos-аутентификацию.

Действия перед созданием keytab-файла

Перед созданием keytab-файла следует для каждого SPN убедиться, что он не зарегистрирован в Active Directory. Сделать это можно с помощью команды `setspn -Q <SPN>`, где `<SPN>` имеет следующий вид: `HTTP/<полное доменное имя (FQDN) узла кластера>`.

Команда должна вернуть ответ "`No such SPN found`", что означает, что этот SPN не зарегистрирован. Если SPN уже зарегистрирован, перед созданием keytab-файла нужно удалить привязку SPN к учетной записи или удалить саму учетную запись в Active Directory, к которой был привязан этот SPN.

Пример проверки SPN для одного Управляющего и двух Подчиненных узлов:

setspn -Q HTTP/control-01.test.local

setspn -Q HTTP/secondary-01.test.local

setspn -Q HTTP/secondary-02.test.local

Создание keytab-файла

Keytab-файл создается на сервере контроллера домена или на компьютере под управлением Windows Server, входящем в домен, под учетной записью с правами доменного администратора.

► *Чтобы создать keytab-файл, используя одну учетную запись:*

1. В оснастке **Active Directory Users and Computers** создайте учетную запись пользователя (например, с именем `control-user`).
2. Чтобы использовать алгоритм шифрования AES256-SHA1, в оснастке **Active Directory Users and Computers** выполните следующие действия:
   a. Откройте свойства созданной учетной записи.
   b. На закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.
3. Создайте keytab-файл для пользователя `control-user` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) Управляющего узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out <путь к файлу>\<имя файла>.keytab
   ```

   Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

   В созданный keytab-файл будет добавлено SPN Управляющего узла. На экране отобразится сгенерированная соль: `Hashing password with salt "<хеш-значение>".`
4. Для каждого узла кластера добавьте в keytab-файл запись SPN. Для этого выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <путь и имя ранее созданного файла>.keytab -out <путь и новое имя>.keytab -setupn -setpass -rawsalt "<хеш-значение соли, полученное при создании keytab-файла на шаге 3>"
   ```

   Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

Keytab-файл будет создан. Этот файл будет содержать все добавленные SPN узлов кластера.

Пример:

Например, вам нужно создать keytab-файл, содержащий SPN-имена 3 узлов: `control-01.test.local`, `secondary-01.test.local` и `secondary-02.test.local`.

Чтобы создать в папке C:\keytabs\ файл под названием `filename1.keytab`, содержащий SPN Управляющего узла, требуется выполнить команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL
-mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL
-pass * +dumpsalt -out C:\keytabs\filename1.keytab
```

Допустим, вы получили соль `"TEST.LOCALHTTPcontrol-01.test.local"`.

Для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ
HTTP/secondary-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL
-crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in
C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab -setupn
-setpass -rawsalt "TEST.LOCALHTTPcontrol-01.test.local"
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ
HTTP/secondary-02.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL
-crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in
C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab -setupn
-setpass -rawsalt "TEST.LOCALHTTPcontrol-01.test.local"
```

В результате будет создан файл с именем `filename3.keytab`, содержащий все три добавленные SPN.

► *Чтобы создать keytab-файл, используя отдельную учетную запись для каждого узла:*

1. В оснастке **Active Directory Users and Computers** создайте отдельную учетную запись пользователя для каждого узла кластера (например, учетные записи с именами `control-user`, `secondary1-user`, `secondary2-user` и т.д.).
2. Чтобы использовать алгоритм шифрования AES256-SHA1, в оснастке **Active Directory Users and Computers** выполните следующие действия:
   a. Откройте свойства созданной учетной записи.
   b. На закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.
3. Создайте keytab-файл для пользователя `control-user` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN)
   Управляющего узла>@<realm имя домена Active Directory в верхнем регистре>
   -mapuser control-user@<realm имя домена Active Directory в верхнем
   регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out <путь
   к файлу>\<имя файла>.keytab
   ```

Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

В созданный keytab-файл будет добавлено SPN Управляющего узла.

4. Для каждого узла кластера добавьте в keytab-файл запись SPN. Для этого выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser secondary1-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <путь и имя ранее созданного файла>.keytab -out <путь и новое имя>.keytab
   ```

   Утилита запросит пароль пользователя `secondary1-user` в процессе выполнения команды.

Keytab-файл будет создан. Этот файл будет содержать все добавленные SPN узлов кластера.

Пример:

Например, вам нужно создать keytab-файл, содержащий SPN-имена 3 узлов: `control-01.test.local`, `secondary-01.test.local` и `secondary-02.test.local`.

Чтобы создать в папке C:\keytabs\ файл под названием `filename1.keytab`, содержащий SPN Управляющего узла, требуется выполнить команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out C:\keytabs\filename1.keytab
```

Для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-01.test.local@TEST.LOCAL -mapuser secondary1-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-02.test.local@TEST.LOCAL -mapuser secondary2-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab
```

В результате будет создан файл с именем `filename3.keytab`, содержащий все три добавленные SPN.

Действия после создания keytab-файла

После создания keytab-файла следует для каждого SPN убедиться. что он зарегистрирован и привязан к соответствующей учетной записи. Сделать это можно с помощью команды `setspn -Q <SPN>`, где `<SPN>` имеет следующий вид: `HTTP/<полное доменное имя (FQDN) узла кластера>@<realm имя домена Active Directory в верхнем регистре>`.

Команда должна вернуть ответ "`Existing SPN found`" и учетную запись, к которой привязан SPN.

Дополнительно после создания keytab-файла можно проверить список SPN, который привязан к соответствующей учетной записи. Сделать это можно с помощью команды `setspn -L <account>`, где

<account> имеет следующий вид: <имя пользователя>@<realm имя домена Active Directory в верхнем регистре>.

Если keytab-файл создан с одной учетной записью, команда должна вернуть список всех SPN, для которых создавался keytab-файл. Если keytab-файл создан с отдельными учетными записями для каждого узла, то команда должна вернуть один SPN, который привязан к конкретной учетной записи.

Пример команды для одной учетной записи:

setspn -L control-user@TEST.LOCAL

Пример команды для отдельных учетных записей для каждого узла:

setspn -L control-user@TEST.LOCAL

setspn -L secondary1-user@TEST.LOCAL

setspn -L secondary2-user@TEST.LOCAL

Настройка Kerberos-аутентификации

Для использования Kerberos-аутентификации необходимо убедиться, что в системе DNS в зонах обратного просмотра присутствует PTR-запись для полного доменного имени (FQDN) и URL (если URL отличается от FQDN) каждого узла кластера.

Если вы настраиваете аутентификацию с доменом, в названии которого содержится корневой домен .local, то для корректной работы Kerberos-аутентификации требуется выполнить предварительные действия в операционной системе.

1. Проверьте состояние службы avahi-daemon. Для этого выполните команду:

   ```
   systemctl status avahi-daemon
   ```

2. Если служба запущена, остановите ее. Для этого выполните команду:

   ```
   systemctl stop avahi-daemon
   ```

3. Отключите автоматический запуск службы. Для этого выполните команду:

   ```
   systemctl disable avahi-daemon
   ```

► *Чтобы настроить Kerberos-аутентификацию:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Доступ к программе** → **Вход с помощью службы единого входа**.
2. В блоке параметров **Kerberos-аутентификация** переведите переключатель **Использовать Kerberos** в положение **Включено**.
3. Нажмите на кнопку **Загрузить**, чтобы загрузить ранее созданный keytab-файл (см. раздел "Создание keytab-файла" на стр. 218).

   Keytab-файл должен содержать SPN Управляющего узла и Подчиненных узлов.

   Откроется окно выбора файла.

4. Выберите keytab-файл и нажмите на кнопку **Открыть**.
5. Нажмите на кнопку **Сохранить**.

   Если в keytab-файле не найдено SPN Управляющего узла или SPN какого-либо из Подчиненных узлов, то для этого узла в разделе **Узлы** отображается статус *Отсутствует SPN-идентификатор для службы единого входа Kerberos*. Если в keytab-файле не найдено SPN ни одного из узлов, кнопка **Сохранить** недоступна.

Kerberos-аутентификация будет настроена. Пользователи, прошедшие аутентификацию в Active Directory, смогут подключаться к веб-интерфейсу приложения с помощью технологии единого входа. Доступ к функциональности приложения будет определяться правами учетной записи приложения.

При отключении Kerberos-аутентификации ранее загруженный keytab-файл удаляется.

Настройка NTLM-аутентификации

► *Чтобы настроить NTLM-аутентификацию:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Доступ к программе** → **Вход с помощью службы единого входа**.
2. В блоке параметров **NTLM-аутентификация** переведите переключатель **Использовать NTLM** в положение **Включено**.
3. В поле **IP-адрес/доменное имя контроллера домена** укажите IP-адрес или доменное имя доменного контроллера, с помощью которого будет осуществляться аутентификация.

   Вы можете указать два доменных контроллера. Для добавления второго контроллера необходимо нажать на кнопку  .
4. В поле **Порт** укажите порт для подключения к доменному контроллеру.

   По умолчанию используется порт 445.
5. Нажмите на кнопку **Сохранить**.

NTLM-аутентификация будет настроена. Пользователи, прошедшие аутентификацию в Active Directory, смогут подключаться к веб-интерфейсу приложения с помощью технологии единого входа. Доступ к функциональности приложения будет определяться правами учетной записи приложения.

При подключении с компьютеров, не входящих в домен, пользователю потребуется указать данные своей доменной учетной записи.

kaspersky

Публикация событий приложения в SIEM-систему

Kaspersky Web Traffic Security может публиковать события, происходящие во время работы приложения, в *SIEM-систему*, которая уже используется в вашей организации, по протоколу Syslog.

Информация о каждом событии приложения передается как отдельное syslog-сообщение формата CEF (см. раздел "Содержание и свойства syslog-сообщений в формате CEF" на стр. 226) (далее также "CEF-сообщение").

CEF-сообщение с информацией о событии передается сразу после появления события.

По умолчанию экспорт CEF-сообщений в приложении отключен. Вы можете настроить публикацию событий в SIEM-систему (см. раздел "Настройка публикации событий приложения в SIEM-систему" на стр. 224) и затем включить экспорт событий (см. раздел "Настройка экспорта событий в формате CEF" на стр. 225).

В этом разделе

Настройка публикации событий приложения в SIEM-систему

Выполните инструкцию ниже на каждом узле кластера, события с которого вы хотите публиковать в SIEM-систему. Только после настройки публикации событий следует включать экспорт событий в формате CEF (см. раздел "Настройка экспорта событий в формате CEF" на стр. 225).

В операционной системе Astra Linux Special Edition события передаются во внешнюю SIEM-систему с помощью системной службы ведения журналов syslog-ng.

► *Чтобы настроить публикацию событий приложения в SIEM-систему:*

1. Запустите командную оболочку операционной системы для выполнения команд с полномочиями суперпользователя (администратора системы).
2. Убедитесь, что служба syslog-ng установлена и запущена, с помощью команды:

   ```
   systemctl status syslog-ng
   ```

   Статус службы должен быть *running*.

   Если служба syslog-ng не запущена или отсутствует, установите и активируйте службу syslog-ng согласно документации операционной системы.
3. Создайте файл /etc/syslog-ng/conf.d/kwts-cef-messages.conf и добавьте в него следующую строку:

   ```
   filter f_kwtscef { facility(local5); };
   ```
4. В зависимости от протокола передачи данных добавьте в файл одну из следующих строк:

- Если вы хотите передавать события в SIEM-систему по протоколу UDP:

  ```
  destination d_kwtscef_forward { network("<IP-адрес SIEM-системы>"
  transport("udp") port(<порт, на котором SIEM-система принимает сообщения
  от Syslog по протоколу UDP>)); };
  ```

- Если вы хотите передавать события в SIEM-систему по протоколу TCP:

  ```
  destination d_kwtscef_forward { network("<IP-адрес SIEM-системы>"
  transport("tcp") port(<порт, на котором SIEM-система принимает сообщения
  от Syslog по протоколу TCP>)); };
  ```

5. Добавьте в конец файла строку:

   ```
   log { source(s_src); filter(f_kwtscef); destination(d_kwtscef_forward); };
   ```

   Пример конфигурационного файла для экспорта по протоколу UDP:

   filter f_kwtscef { facility(local5); };

   destination d_kwtscef_forward { network("10.16.32.64" transport("udp") port(514)); };

   log { source(s_src); filter(f_kwtscef); destination(d_kwtscef_forward); };

   Пример конфигурационного файла для экспорта по протоколу TCP:

   filter f_kwtscef { facility(local5); };

   destination d_kwtscef_forward { network("10.16.32.64" transport("tcp") port(514)); };

   log { source(s_src); filter(f_kwtscef); destination(d_kwtscef_forward); };

6. Перезапустите службу syslog-ng. Для этого выполните команду:

   ```
   systemctl restart syslog-ng
   ```

7. Проверьте статус службы syslog-ng с помощью команды:

   ```
   systemctl status syslog-ng
   ```

   Статус службы должен быть *running*.

8. Отправьте тестовое сообщение в SIEM-систему при помощи команды:

   ```
   logger -p local5.info Test message
   ```

Публикация событий приложения в SIEM-систему будет настроена.

Настройка экспорта событий в формате CEF

Для включения экспорта событий требуется предварительно настроить публикацию событий приложения в SIEM-систему (см. раздел "Настройка публикации событий приложения в SIEM-систему" на стр. 224).

Выполните инструкцию ниже на каждом узле кластера, события с которого вы хотите экспортировать в формате CEF.

► *Чтобы настроить экспорт событий в формате CEF:*

1. Запустите командную оболочку операционной системы для выполнения команд с полномочиями суперпользователя (администратора системы).
2. Перейдите в каталог /opt/kaspersky/kwts/share/templates/core_settings и создайте резервную копию файла event_logger.json.template с помощью команды:

   ```
   cp -p event_logger.json.template event_logger.json.template.backup
   ```

3. Откройте файл event_logger.json.template на редактирование и, соблюдая синтаксис и структуру JSON-файла, в секции `siemSettings` укажите следующие значения параметров:

   ```
   "enabled": true,
   "facility": "Local5",
   "logLevel": "Info",
   ```

4. В веб-интерфейсе приложения в разделе **Параметры** → **Журналы и события** внесите изменение в значение любого параметра и нажмите на кнопку **Сохранить**.

   Это необходимо для синхронизации параметров между узлами кластера и применения изменений, внесенных в конфигурационный файл. После этого вы можете вернуть исходное значение измененного параметра.

5. Убедитесь, что изменения применены, с помощью команды:

   ```
   /opt/kaspersky/kwts/bin/kwts-control --get-settings 20 --format json | grep -A 4 siemSettings
   ```

   Ответ должен содержать параметры со значениями, указанными в п. 3.

Экспорт событий в формате CEF будет настроен.

Если вы хотите отключить экспорт событий в формате CEF, выполните шаги инструкции выше и в п. 3 установите значение параметра `"enabled": false`.

Содержание и свойства syslog-сообщений в формате CEF

Информация о каждом обнаруженном событии передается сразу после появления события и представляет собой отдельное syslog-сообщение формата CEF в кодировке UTF-8.

Сообщение в формате CEF состоит из *тела сообщения* и *заголовка*.

Заголовок CEF-сообщения состоит из следующих частей:

- Syslog-префикс: `<дата и время события> <имя хоста, на котором произошло событие>.`
- Последовательность полей, разделенных между собой символами "|" и отделенных от syslog-префикса пробелом. Все поля обязательны.
  - Версия формата. В текущий момент номер версии – 0, соответственно поле имеет вид "CEF:0".
  - Производитель. Поле заполняется значением `AO Kaspersky Lab`.
  - Название приложения. Поле заполняется значением `Kaspersky Web Traffic Security`.

- Версия продукта. Поле заполняется номером текущей версии продукта (`6.2.0.xxxx`).
- Класс события.
- Имя события.
- Уровень критичности. Может принимать значения `Low` (низкий), `Medium` (средний) или `High` (высокий).

Пример:

```
Oct 30, 2021 10:34:23

host.domain.com CEF:0|AO Kaspersky Lab|Kaspersky Web Traffic
Security|6.2.0.1234|LMS_EV_SETTINGS_CHANGED|task settings changed|Low|…
```

Поля syslog-сообщения о событии, определяемые параметрами приложения, представлены в формате `<ключ>="<значение>"`. Если ключ имеет несколько значений, эти значения указываются через запятую. В качестве разделителя между ключами используется двоеточие.

Ключи, а также их значения, содержащиеся в сообщении, зависят от класса события.

Максимальный размер syslog-сообщения об обнаруженном событии зависит от значений параметров syslog на сервере, на котором установлен Kaspersky Web Traffic Security. Вы можете настроить пересылку syslog-сообщений только на один внешний syslog-сервер единовременно.

Правила кодирования символов в CEF-сообщениях:

- Пробелы не требуют экранирования.
- В заголовке символ вертикальной черты ("|") используется как разделитель. Если вам нужно использовать этот символ в одном из полей заголовка, его следует экранировать символом обратной косой черты ("\|"). В теле сообщения символ "|" не нужно экранировать.
- В заголовке и теле сообщения не допускается одиночный символ обратной косой черты. Если нужно его использовать в поле заголовка, символ следует дублировать ("\\").
- В теле сообщения символ "=" используется как разделитель пары "ключ-значение". Если нужно использовать этот символ в поле тела сообщения, его следует экранировать символом обратной косой черты ("\="). В заголовке символ "=" не требует экранирования.
- Многострочные значения допустимы только для значения в паре "ключ-значение". Для обозначения перехода на следующую строку следует использовать символы "\n" или "\r".

В этом разделе

Классы событий группы Settings

В теле CEF-сообщений классов событий группы Settings допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 18. Допустимые значения полей классов событий группы Settings

Ключ	Значение
cn1	Номер задачи.
cn1Label	Всегда имеет значение `TaskId`.
cs1	Имя задачи.
cs1Label	Всегда имеет значение `TaskName`.
act	Действие, выполненное с настройками. Всегда имеет значение `changed`.

В каждом классе событий группы Settings допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 19. Релевантные ключи для классов событий группы Settings

Класс событий	Релевантные ключи
LMS_EV_SETTINGS_CHANGED	cn1, cn1Label, cs1, cs1Label, act

Классы событий группы Tasks

В теле CEF-сообщений классов событий группы Tasks допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 20. Допустимые значения полей классов событий группы Tasks

Ключ	Значение
deviceProcessName	Имя задачи.
cnt	Количество ошибок за последние 5 минут.
cs1	Режим работы приложения (`real time scan` / `configuration mode`).
cs1Label	Всегда имеет значение `Mode`.

В каждом классе событий группы Tasks допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 21. Релевантные ключи для классов событий группы Tasks

Класс событий	Релевантные ключи
LMS_EV_PROCESS_CRASHED	deviceProcessName, cnt
LMS_EV_RESTARTED	deviceProcessName, cnt
LMS_EV_PRODUCT_STARTED	cs1, cs1Label

Классы событий группы License

В теле CEF-сообщений классов событий группы License допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 22. Допустимые значения полей классов событий группы License

Ключ	Значение
cs1	Серийный номер лицензионного ключа.
cs1Label	Всегда имеет значение `LicenseID`.
cs2	Режим работы Kaspersky Web Traffic Security в соответствии с лицензией.
cs2Label	Всегда имеет значение `FunctionalityLevel`.
cs3	Тип лицензии.
cs3Label	Всегда имеет значение `KeyType`.
cn1	Количество дней до истечения срока действия лицензии.
cn1Label	Всегда имеет значение `DaysLeft`.
reason	Описание ошибки.
deviceCustomDate1	Дата истечения срока действия лицензии.
deviceCustomDate1Label	Всегда имеет значение `ExpirationDate`.

В каждом классе событий группы License допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 23. Релевантные ключи для классов событий группы License

Класс событий	Релевантные ключи
LMS_EV_LICENSE_OK	cs1, cs1Label, cs2, cs2Label
LMS_EV_LICENSE_INVALID	cs1, cs1Label, reason
LMS_EV_NO_LICENSE	Нет значения
LMS_EV_LICENSE_BLACKLISTED	cs1, cs1Label
LMS_EV_LICENSE_TRIAL_EXPIRED	cs1, cs1Label, deviceCustomDate1, deviceCustomDate1Label
LMS_EV_LICENSE_EXPIRED	cs1, cs1Label, deviceCustomDate1, deviceCustomDate1Label
LMS_EV_LICENSE_ERROR	reason
LMS_EV_LICENSE_INSTALLED	cs1, cs1Label, cs2, cs2Label, cs3, cs3Label
LMS_EV_LICENSE_UPDATED	cs1, cs1Label, cs2, cs2Label, cs3, cs3Label, deviceCustomDate1, deviceCustomDate1Label
LMS_EV_GRACE_PERIOD	cs1, cs1Label, cn1, cn1Label
LMS_EV_LICENSE_REVOKED	cs1, cs1Label
LMS_EV_LICENSE_EXPIRES_SOON	cs1, cs1Label, cn1, cn1Label

Классы событий группы Update

В теле CEF-сообщений классов событий группы Update допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 24. Допустимые значения полей классов событий группы Update

Ключ	Значение
reason	Причина возникновения события.
cn1	Количество дней.
cn1Label	Всегда имеет значение `Days`.
cnt	Количество записей в базах.
deviceCustomDate1	Дата публикации баз.
deviceCustomDate1Label	Всегда имеет значение `PublishingTime`.
deviceCustomDate2	Дата публикации индекса.
deviceCustomDate2Label	Всегда имеет значение `IndexPublishingTime`.

В каждом классе событий группы Update допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 25. Релевантные ключи для классов событий группы Update

Класс событий	Релевантные ключи
LMS_EV_ANTIVIRUS_BASES_UPDATED	Нет значения
LMS_EV_ANTIPHISHING_BASES_UPDATED	Нет значения
LMS_EV_BASES_NOTHING_TO_UPDATE	Нет значения
LMS_EV_ANTIVIRUS_BASES_UP_TO_DATE	Нет значения
LMS_EV_ANTIPHISHING_BASES_UP_TO_DATE	Нет значения
LMS_EV_ANTIVIRUS_BASES_OUT_OF_DATE	cn1, cn1Label
LMS_EV_ANTIPHISHING_BASES_OUT_OF_DATE	cn1, cn1Label
LMS_EV_ANTIVIRUS_BASES_OBSOLETED	cn1, cn1Label
LMS_EV_ANTIPHISHING_BASES_OBSOLETED	cn1, cn1Label
LMS_EV_ANTIVIRUS_BASES_APPLIED	deviceCustomDate2, deviceCustomDate2Label, cnt, deviceCustomDate1, deviceCustomDate1Label
LMS_EV_ANTIPHISHING_BASES_APPLIED	deviceCustomDate1, deviceCustomDate1Label
LMS_EV_BASES_UPDATE_ERROR	reason

Классы событий группы ICAP

В теле CEF-сообщений классов событий группы ICAP допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 26. Допустимые значения полей классов событий группы ICAP

Ключ	Значение
cs1	Имя пользователя.
cs1Label	Всегда имеет значение `UserNname`.
cs2	Название рабочей области.
cs2Label	Всегда имеет значение `Workspace`.
cs3	Имя правила обработки трафика. Может быть несколько имен.
cs3Label	Всегда имеет значение `RulesNames`.
request	URL запроса.
src	IP-адрес пользователя.

Ключ	Значение
requestClientApplication	Название браузера или программы, обрабатывающей трафик (User agent).
act	Действие из списка: `Allow`, `Block`, `Redirect`.

В каждом классе событий группы ICAP допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 27. Релевантные ключи для классов событий группы ICAP

Класс событий	Релевантные ключи
LMS_EV_ICAP_MESSAGE_PROCESSED	cs1, cs1Label, cs2, cs2Label,cs3, cs3Label, src, request, requestClientApplication, act

kaspersky

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Web Traffic Security (см. раздел "Источники информации о приложении" на стр. 238), рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Web Traffic Security.

Kaspersky предоставляет поддержку Kaspersky Web Traffic Security в течение жизненного цикла (см. страницу жизненного цикла приложений (https://support.kaspersky.com/corporate/lifecycle)). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules/ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки (https://support.kaspersky.ru/b2b);
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

kaspersky

Получение информации для Службы технической поддержки

После того как вы проинформируете специалистов Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас предоставить отладочную информацию, которая содержит в себе файлы трассировки и дополнительную информацию об операционной системе, запущенных процессах на сервере и другую диагностическую информацию. Файлы трассировки позволяют отследить процесс пошагового выполнения команд приложения и обнаружить, на каком этапе работы приложения возникает ошибка. Вы можете выбрать, какие события будут записаны в файлы трассировки (ошибки или информационные сообщения). Все файлы трассировки и дополнительная отладочная информация помещаются в архив, который вы сможете передать в Службу технической поддержки.

Файлы трассировки могут содержать данные о вашей организации, которые вы считаете конфиденциальными. Необходимо согласовать состав отправляемого архива со Службой безопасности вашей организации. Перед отправкой журнала трассировки удалите из него все данные, которые вы считаете конфиденциальными.

Отладочная информация о работе приложения записывается в соответствии с заданным уровнем трассировки (см. раздел "Изменение уровня трассировки" на стр. 236) и хранится в папке /var/log/kaspersky/kwts.

Если веб-интерфейс приложения недоступен, вы можете получить информацию для Службы технической поддержки с помощью утилиты collect_diag_info.py (см. раздел "Получение информации с помощью утилиты collect_diag_info.py" на стр. 237).

В этом разделе

Запуск трассировки

► *Чтобы запустить трассировку:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. По кнопке  откройте меню раздела **Узлы**.
3. Выберите пункт **Запустить трассировку**.

   Откроется окно **Выбор узлов для запуска трассировки**.
4. В таблице серверов установите флажки напротив тех серверов, для которых вы хотите

сформировать файлы трассировки.

5. Нажмите на кнопку **Запустить**.

   Откроется окно **Журналы трассировки для Службы технической поддержки** с результатом запуска трассировки. Созданный журнал трассировки содержит отдельный файл для каждого сервера.

Изменение уровня трассировки

Изменение уровня трассировки сохраняется в конфигурации приложения и не влияет на уже созданные файлы трассировки.

► *Чтобы выбрать уровень трассировки:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. По кнопке  откройте меню раздела **Узлы**.
3. Выберите пункт **Изменить уровень трассировки**.

   Откроется окно **Уровень трассировки**.
4. Выберите один из следующих вариантов:
   - **Уровень ошибки**.
   - **Уровень отладки**.

     Этот уровень трассировки значительно повышает требования к подсистеме хранения данных и снижает производительность приложения. Используйте уровень отладки только если Служба технической поддержки "Лаборатории Касперского" просит предоставить файлы трассировки такого типа.

   По умолчанию установлено значение **Уровень ошибки**.
5. Нажмите на кнопку **Сохранить**.

   Прокси-сервер будет перезагружен. До завершения перезагрузки обработка трафика будет приостановлена.

Трассировка будет производиться в соответствии с выбранным уровнем трассировки.

Просмотр журналов трассировки

► *Чтобы просмотреть журналы трассировки:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. По кнопке  откройте меню раздела **Узлы**.

3. Выберите пункт **Просмотреть журналы трассировки**.

   Откроется страница **Журналы трассировки для Службы технической поддержки** со списком ранее созданных журналов трассировки.

4. Если вы хотите посмотреть, информация о каких серверах содержится в журнале трассировки, нажмите на кнопку  в выбранной строке.

Сохранение файла трассировки на компьютере

► *Чтобы сохранить файл трассировки на компьютере:*

1. В окне веб-интерфейса приложения выберите раздел **Узлы**.
2. По кнопке  откройте меню раздела **Узлы**.
3. Выберите пункт **Просмотреть журналы трассировки**.

   Откроется страница **Журналы трассировки для Службы технической поддержки** со списком ранее созданных журналов трассировки.

4. Нажмите на кнопку  напротив названия журнала трассировки, файлы которого вы хотите загрузить.
5. В строке с нужным файлом нажмите на значок  .

Файл трассировки будет сохранен на компьютере в папке загрузки браузера.

Получение информации с помощью утилиты collect_diag_info.py

Утилиту следует запускать от имени пользователя root.

Утилита расположена в директории /opt/kaspersky/kwts/bin.

► *Чтобы получить информацию для Службы технической поддержки, выполните следующую команду:*

```
/opt/kaspersky/kwts/bin/collect_diag_info.py <полный путь к архиву с диагностической информацией> 2> <полный путь к файлу журнала утилиты>
```

Пример:

/opt/kaspersky/kwts/bin/collect_diag_info.py /tmp/diaginfo.tar.gz 2> /tmp/log.file

В результате работы утилиты будет создан архив с диагностической информацией и файл журнала утилиты. Эти файлы необходимо передать сотрудникам Службы технической поддержки.

Устранение уязвимостей и установка критических обновлений в приложении

"Лаборатория Касперского" может выпускать обновления приложения, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте (https://support.kaspersky.ru/general/certificates) и рассылаются по адресам электронной почты, указанным при заказе приложения, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: http://support.kaspersky.ru/subscribe).

Порядок получения критических обновлений изложен в формуляре.

Допускается устанавливать только обновления модулей приложения, прошедшие процедуру сертификации, и критические обновления. Включение автоматического обновления модулей приводит к выходу приложения из сертифицированного состояния.

Лицо, ответственное за эксплуатацию приложения, должно периодически (не реже одного раза в три месяца) проверять отсутствие обнаруженных уязвимостей в приложении, используя веб-сайт "Лаборатории Касперского" (https://support.kaspersky.ru/vulnerability), банк данных угроз безопасности информации ФСТЭК России (http://www.bdu.fstec.ru) и иные общедоступные источники.

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях приложения следующими способами:

- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского" (https://community.kaspersky.com/).

Действия после сбоя или неустранимой ошибки в работе приложения

Приложение автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда приложение не может восстановить свою работу, вам требуется переустановить приложение или его компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. 233).

kaspersky

Приложение 1. MIME-типы объектов

Наиболее часто используются следующие MIME-типы объектов:

- application/font-woff;
- application/javascript;
- application/json;
- application/ocsp-response;
- application/octet-stream;
- application/x-javascript;
- audio/mp4;
- audio/mpeg;
- image/gif;
- image/jpeg;
- image/png;
- image/svg+xml;
- image/vnd.microsoft.icon;
- image/x-icon;
- text/css;
- text/html;
- text/javascript;
- text/plain;
- video/mpeg.

kaspersky

Приложение 2. Нормализация URL-адресов

Kaspersky Web Traffic Security поддерживает импорт URL-адресов, состоящих из четырех частей и представленных в следующем формате:

<протокол>://<домен>:<порт>/<путь>

Указание домена является обязательным. Остальные части URL-адреса могут быть опущены.

Пример:

`https://example.com:8080/path`

Здесь `https` – протокол, `example.com` – домен, `8080` – порт, `path` – путь.

Если в процессе нормализации URL-адреса произошла ошибка и адрес не был принят приложением, рекомендуется выполнить следующие действия.

1. Определите, с какой частью URL-адреса возникла проблема. Для этого добавляйте части адреса последовательно по следующему алгоритму:
   a. <домен>.
   b. <протокол>://<домен>.
   c. <протокол>://<домен>:<порт>.
   d. <протокол>://<домен>:<порт>/<путь>.
2. Проверьте, соответствует ли значение части URL-адреса, с которой возникла проблема, требованиям, приведенным в таблице ниже.

Таблица 28. Требования к URL-адресу для успешного выполнения нормализации

Часть URL-адреса	Требования
Протокол	• Должен начинаться с буквы латинского алфавита (ASCII A–Z, a–z). • Может содержать в себе буквы латинского алфавита (ASCII A–Z, a–z), цифры от 0 до 9, а также знаки плюса, минуса и точку.
Домен	• Допускается указывать IPv4-, IPv6-адреса (в квадратных скобках), а также полное доменное имя (FQDN). • Допускается использование символов . _ ~ ! $ & ' ( ) * + , =
Порт	Допускается использовать цифровое значение в диапазоне от 1 до 65535.
Путь	• Допускается использование одного или нескольких сегментов, разделенных символом /. • В каждом сегменте допускается использование латинских букв (ASCII a-z), цифр (0-9), символов в кодировке UTF, %-encoded символов, а также символов - . _ ~ : @ ! $ & ' ( ) * , =

3. Если указанный URL-адрес содержит точку с запятой, укажите его без пути. Вы сможете указать путь позже в списке добавленных URL-адресов.

Приложение 3. Категории сайтов

По ссылке вы можете ознакомиться с описанием категорий веб-сайтов https://support.kaspersky.com/help/Legal/WebCategories/ru-RU/206917.htm.

kaspersky

Приложение 4. Значения параметров программы в сертифицированном режиме

Этот раздел содержит перечень параметров программы, влияющих на сертифицированный режим работы программы. В таблице ниже приведены значения этих параметров в сертифицированном режиме работы программы.

Если вы меняете какие-либо из перечисленных значений параметров с их значений в сертифицированном режиме работы программы на другие значения, вы выводите программу из сертифицированного режима работы.

Таблица 29. Параметры и их значения при работе программы в сертифицированном режиме

Раздел / подраздел	Название параметра	Значение параметра в сертифицированном режиме работы программы
KSN/KPSN	Использование KSN / KPSN	• **Не использовать KSN/KPSN** • **KPSN**
Защита: **Антивирус**	**Использовать эвристический анализ**	**Включено**
	Обнаруживать некоторые легальные программы	**Включено**
	Максимальная длительность проверки (сек.)	**120**
	Максимальная глубина проверки архивов	**32**
Защита: **Анти-Фишинг**	**Использовать эвристический анализ**	**Включено**
	Максимальная длительность проверки (сек.)	**120**

kaspersky

Приложение 5. Настройка балансировки ICAP с помощью HAProxy

Балансировка ICAP-соединений с помощью балансировщика нагрузки HAProxy позволяет подключить один внешний прокси-сервер одновременно к нескольким узлам кластера Kaspersky Web Traffic Security и распределить нагрузку обработки трафика между ними.

По умолчанию ICAP-трафик не шифруется. Администратору приложения необходимо самостоятельно обеспечить безопасное сетевое соединение между балансировщиком и Kaspersky Web Traffic Security, а также между внешним прокси-сервером и балансировщиком с помощью туннелирования трафика или средствами iptables.

В этом разделе

Настройка ICAP-сервера на прием внешних соединений

► *Чтобы разрешить прием внешних соединений ICAP-сервером:*

1. В главном окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **ICAP-сервер**.
2. В поле **Адрес ICAP-сервера** измените значение с `127.0.0.1` на `0.0.0.0`.

   Если вы используете IP-адрес в формате IPv6, то вам требуется изменить значение с `::1` на `::`.
3. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

IP-адрес, на который ICAP-сервер принимает трафик, будет изменен.

Установка и настройка HAProxy

Балансировщик HAProxy должен быть установлен на отдельном сервере с целью обеспечения отказоустойчивости. Вы можете использовать любую операционную систему Linux, в которых есть возможность установить пакет HAProxy из официального репозитория операционной системы.

► *Чтобы установить и настроить HAProxy:*

1. Если на сервере используется межсетевой экран, откройте доступ к порту 1344.
2. Установите пакет haproxy из репозитория при помощи пакетного менеджера операционной системы.
3. В конфигурационный файл /etc/haproxy/haproxy.cfg добавьте следующие блоки параметров:

```
frontend ICAP
  bind 0.0.0.0:1344
  mode tcp
  default_backend icap_pool

backend icap_pool
  balance <схема балансировки, рекомендуется использовать roundrobin>
  mode tcp
  server <имя ICAP-сервера 1> <IP-адрес узла кластера>:<порт ICAP-сервера>
check
  server <имя ICAP-сервера 2> <IP-адрес узла кластера>:<порт ICAP-сервера>
check
  server <имя ICAP-сервера 3> <IP-адрес узла кластера>:<порт ICAP-сервера>
check
```

4. Перезапустите службу haproxy с помощью команды:

```
systemctl restart haproxy
```

Балансировщик нагрузки HAProxy будет настроен.

Настройка внешнего прокси-сервера для работы через HAProxy

► *Чтобы настроить внешний прокси-сервер для работы по протоколу ICAP через балансировщик:*

1. Укажите следующий адрес для REQMOD-сервиса:

```
icap://<IP-адрес сервера с HAProxy>:1344/av/reqmod
```

2. Укажите следующий адрес для RESPMOD-сервиса:

```
icap://<IP-адрес сервера с HAProxy>:1344/av/respmod
```

Настройка внешнего прокси-сервера для работы через балансировщик будет выполнена.

kaspersky

Приложение 6. HTTPS-запросы для управления правилами Kaspersky Web Traffic Security

Для управления параметрами правил Kaspersky Web Traffic Security внешняя программа должна выполнять HTTPS-запросы к Kaspersky Web Traffic Security. Ниже запросы описаны на примере программы curl. Вы можете выполнить их из командной строки терминала.

► *Чтобы управлять параметрами правил с помощью внешней программы:*

1. Получите токен для работы с Kaspersky Web Traffic Security. Для этого выполните следующий запрос:

   ```
   HOSTNAME=$(hostname); \
   curl -q --silent --show-error --max-time 5 --noproxy '*' \
     --cacert /var/opt/kaspersky/kwts/certs/webapi.crt \
     --cookie-jar ./cookies.dat \
     https://${HOSTNAME}/web/api/get-auth-info
   ```

   Вы получите XSRF-токен, который будет сохранен в файле cookies.dat, и в консоли отобразятся данные в формате JSON. Пример

2. Создайте файл login_data.json следующего содержания:

   ```
   {
     "username":"<имя пользователя Kaspersky Web Traffic Security>",
     "password":"<пароль пользователя Kaspersky Web Traffic Security>"
   }
   ```

3. Для авторизации в Kaspersky Web Traffic Security выполните запрос:

   ```
   XSRF_TOKEN=$(grep XSRF-TOKEN ./cookies.dat | awk '{print $NF}'); \
   HOSTNAME=$(hostname); \
   curl -q --silent --show-error --fail --max-time 5 --noproxy '*' \
     --cacert /var/opt/kaspersky/kwts/certs/webapi.crt \
     -H "KWTS-XSRF-TOKEN:$XSRF_TOKEN" \
     -X POST -H 'Content-Type: application/json' \
     --data "$(cat ./login_data.json)" \
     --cookie ./cookies.dat --cookie-jar ./cookies.dat \
     https://${HOSTNAME}/web/api/user-login
   ```

   В консоли отобразится информация о пользователе.

Пример:


```
{
  "data": {
      "cert_digest": "<Дайджест сертификата SHA256>",
    "cluster_state": "normal",
    "ip": "<IP-адрес узла>",
    "kata_alert_enabled": false,
    "kata_upload_enabled": false,
    "ksn_regions": [],
    "node_role": "master",
    "port": <node port>,
    "suggest_ksn": true,
    "user_info": {
      "capabilities": [
        "delete_global_role",
        "delete_global_rule",
        "delete_workspace",
        "diagnostic",
        "get_node_info",
        "integrity_check",
        "manage_global_dashboard",
        "manage_global_role",
        "manage_global_rule",
        "manage_node",
        "manage_settings",
        "manage_workspace",
        "reset_user_password",
        "show_audit_log",
        "show_global_dashboard",
        "show_global_roles",
        "show_global_rules",
        "show_global_traffic_events",
        "show_settings",
        "show_system_events",
        "show_workspaces",
        "ssh_access"
      ],
      "is_local": true,
      "session_remaining_seconds": 600,
      "user_id": 1,
      "username": "<Имя пользователя>",
      "workspaces": []
    }
  }
}
```


Время действия авторизации составляет 10 минут. В случае неактивности более 10 минут необходимо повторить шаг авторизации.

4. Для получения списка правил из раздела **Защита** выполните запрос:

```
XSRF_TOKEN=$(grep XSRF-TOKEN ./cookies.dat | awk '{print $NF}'); \
HOSTNAME=$(hostname); \
curl -q --silent --show-error --fail --max-time 5 --noproxy '*' \
  --cacert /var/opt/kaspersky/kwts/certs/webapi.crt \
  -H " KWTS-XSRF-TOKEN:$XSRF_TOKEN" \
```

```
-X GET -H "Content-Type: application/json" \
--cookie ./cookies.dat --output ./protection_rules.json \
https://${HOSTNAME}/web/api/show-rules?section=protection
```

В текущей папке будет сохранен файл protection_rules.json, содержащий информацию обо всех правилах защиты.

Пример:


```
{
  "data": {
    "rules": [
      {
        "node_type": "rule",
        "rule_exclusions": [],
        "rule_general": {
          "rule_actions": {
            "doc_with_macro_action": "Block",
            "encrypted_action": "Block",
            "malicious_link_action": "Block",
            "malware_action": "Cure",
            "phishing_action": "Block"
          },
          "rule_blocking_template_text": "",
          "rule_comment": null,
          "rule_destinations": {},
          "rule_is_enabled": true,
          "rule_name": "Test 1",
          "rule_sources": {}
        },
        "rule_group_id": null,
        "rule_id": 11,
        "rule_time_restrictions": {
          "enable_revoke_at": false,
          "enable_schedule": false,
          "revoke_at": 1750663620,
          "schedule": {
            "days": {
              "Fri": true,
              "Mon": true,
              "Sat": true,
              "Sun": true,
              "Thu": true,
              "Tue": true,
              "Wed": true
            },
            "from": {
              "hour": 10,
              "minute": 27
            },
            "to": {
              "hour": 10,
```

```
                },
                "from": {
                    "hour": 10,
                    "minute": 27
                },
                "to": {
                    "hour": 10,
                    "minute": 27
                }
            }
        },
        "rule_version": 0,
        "section": "protection",
        "workspace_id": null
    },
    {
        "node_id": 3,
        "node_type": "workspace_placeholder",
        "section": "protection"
    }
  ]
 }
}
```


5. Если вы хотите получить детальную информацию о конкретном правиле, выполните запрос:

```
XSRF_TOKEN=$(grep XSRF-TOKEN ./cookies.dat | awk '{print $NF}'); \
HOSTNAME=$(hostname); \
curl -q --silent --show-error --fail --max-time 5 --noproxy '*' \
  --cacert /var/opt/kaspersky/kwts/certs/webapi.crt \
  -H "KWTS-XSRF-TOKEN:$XSRF_TOKEN" \
  -X GET -H "Content-Type: application/json" \
  --cookie ./cookies.dat --output ./protection_rule.json \
  https://${HOSTNAME}/web/api/get-rule-info?rule_id=<ID правила из файла
protection_rules.json, полученного на шаге 4>
```

Информация о правиле будет сохранена в файл protection_rule.json.

Пример:


```
{
    "data": {
        "node_type": "rule",
        "rule_exclusions": [],
        "rule_general": {
            "rule_actions": {
                "doc_with_macro_action": "Block",
                "encrypted_action": "Block",
                "malicious_link_action": "Block",
                "malware_action": "Cure",
                "phishing_action": "Block"
            },
            "rule_blocking_template_text": "",
            "rule_comment": null,
            "rule_destinations": {},
            "rule_is_enabled": true,
```

```
            "rule_destinations": {},
            "rule_is_enabled": true,
            "rule_name": "Rule_1",
            "rule_sources": {
                "operation": "any_of",
                "sources": [
                    {
                        "type": "useragent",
                        "values": [
                            "Firefox"
                        ]
                    },
                    {
                        "type": "ip",
                        "values": [
                            "10.0.0.0"
                        ]
                    }
                ]
            }
        },
        "rule_group_id": null,
        "rule_id": 5,
        "rule_time_restrictions": {
            "enable_revoke_at": false,
            "enable_schedule": false,
            "revoke_at": 1750942260,
            "schedule": {
                "days": {
                    "Fri": true,
                    "Mon": true,
                    "Sat": true,
                    "Sun": true,
                    "Thu": true,
                    "Tue": true,
                    "Wed": true
                },
                "from": {
                    "hour": 15,
                    "minute": 51
                },
                "to": {
                    "hour": 15,
                    "minute": 51
                }
            }
        },
        "rule_version": 0,
        "section": "protection",
        "workspace_id": null
    }
}
```


6. Если вы хотите изменить правило, выполните следующие действия:

   a. В файле protection_rule.json удалите объект `"data"`.

      В примере ниже показаны только удаляемые строки:

Пример:

```
        "data": {
  }
```

b. В файле protection_rule.json измените параметры правила. Вы можете изменить следующие параметры:

- `rule actions` – настройка действий для правил:
  - `malware_action` – действия при обнаружении вредоносной программы. Возможные значения: `Cure` – заблокировать, по возможности вылечить, `Block` – заблокировать, `Allow` – пропустить проверку.
  - `phishing_action` – действия при обнаружении фишинга. Возможные значения: `Block` – заблокировать, `Allow` – пропустить проверку.
  - `malicious_link_action` – действия при обнаружении вредоносной ссылки. Возможные значения: `Block` – заблокировать, `Allow` – пропустить проверку.
  - `encrypted_action` – действия при обнаружении зашифрованного объекта. Возможные значения: `Block` – заблокировать, `Allow` – пропустить проверку.
  - `doc_with_macro_action` – действия при обнаружении документа с макросом. Возможные значения: `Block` – заблокировать, `Allow` – пропустить проверку.
- `rule_name` – название правила.
- `rule_is_enabled` – статус правила. Возможные значения: `true` – включено, `false` – выключено.
- `rule_sources` – инициатор, массив значений:
  - `type` – тип инициатора. Возможные значения: `useragent` – браузер, `ip` – IP-адрес.
  - `values` – значения инициатора.
  - `operation` – логический оператор. Возможные значения: `any_of` – любой из, `all_of` – все из.

Пример измененного файла:

```
{
        "node_type": "rule",
        "rule_exclusions": [],
        "rule_general": {
            "rule_actions": {
                "doc_with_macro_action": "Block",
                "encrypted_action": "Block",
                "malicious_link_action": "Block",
                "malware_action": "Cure",
                "phishing_action": "Block"
            },
            "rule_blocking_template_text": "",
            "rule_comment": null,
            "rule_destinations": {},
            "rule_is_enabled": true,
```

```
            "rule_name": "Rule_1",
            "rule_sources": {
                "operation": "any_of",
                "sources": [
                    {
                        "type": "useragent",
                        "values": [
                            "Firefox"
                        ]
                    },
                    {
                        "type": "ip",
                        "values": [
                            "10.0.0.0"
                        ]
                    }
                ]
            }
        },
        "rule_group_id": null,
        "rule_id": 5,
        "rule_time_restrictions": {
            "enable_revoke_at": false,
            "enable_schedule": false,
            "revoke_at": 1750942260,
            "schedule": {
                "days": {
                    "Fri": true,
                    "Mon": true,
                    "Sat": true,
                    "Sun": true,
                    "Thu": true,
                    "Tue": true,
                    "Wed": true
                },
                "from": {
                    "hour": 15,
                    "minute": 51
                },
                "to": {
                    "hour": 15,
                    "minute": 51
                }
            }
        },
        "rule_version": 0,
        "section": "protection",
        "workspace_id": null
    }
```


c. Выполните запрос:

```
XSRF_TOKEN=$(grep XSRF-TOKEN ./cookies.dat | awk '{print $NF}');
HOSTNAME=$(hostname); curl -H "Expect:" -q --silent --show-error --fail
--max-time 5 --noproxy '*'   --cacert
/var/opt/kaspersky/kwts/certs/webapi.crt   -H
"KWTS-XSRF-TOKEN:$XSRF_TOKEN"   -X POST -H 'Content-Type:
```

```
application/json'   --data "$(cat ./protection_rule.json)"
--cookie ./cookies.dat   https://${HOSTNAME}/web/api/edit-rule
```

В консоли отобразится ответ:

```
{"data":"success"}
```

7. Если вы хотите удалить правило, выполните следующие действия:

   a. Создайте файл delete_protection_rule_id.json следующего содержания:

   ```
   {
     "rule_id":<ID удаляемого правила>,
     "section":"protection"
   }
   ```

   b. Выполните запрос:

   ```
   XSRF_TOKEN=$(grep XSRF-TOKEN ./cookies.dat | awk '{print $NF}'); \
   HOSTNAME=$(hostname); \
   curl -q --silent --show-error --fail --max-time 5 --noproxy '*' \
     --cacert /var/opt/kaspersky/kwts/certs/webapi.crt \
     -H " KWTS-XSRF-TOKEN:$XSRF_TOKEN" \
     -X POST -H 'Content-Type: application/json' \
     --data "$(cat ./delete_protection_rule_id.json)" \
     --cookie ./cookies.dat \
     https://${HOSTNAME}/web/api/delete-rule
   ```

   В консоли отобразится ответ:

   ```
   {"data":"success"}
   ```

kaspersky

Приложение 7. Установка и настройка сервиса Squid

Если вы используете отдельный прокси-сервер, по умолчанию Kaspersky Web Traffic Security не обеспечивает шифрование ICAP-трафика и аутентификацию ICAP-клиентов. Администратору приложения необходимо самостоятельно обеспечить безопасное сетевое соединение между вашим прокси-сервером и Kaspersky Web Traffic Security с помощью туннелирования трафика или средствами iptables.

Вы можете не использовать отдельный прокси-сервер и вместо него установить сервис Squid на каждый узел кластера Kaspersky Web Traffic Security.

Установка и настройка сервиса Squid включает следующие этапы.

1. **Установка сервиса Squid (на стр. 255)**
2. **Настройка сервиса Squid (на стр. 255)**
3. **Настройка SSL Bumping в сервисе Squid (на стр. 256)**

   Рекомендуется настроить SSL Bumping в сервисе Squid для обработки шифрованных соединений. Если SSL Bumping не настроен, то прокси-сервер не может вмешаться в процесс установки шифрованного соединения. В этом случае модули защиты Kaspersky Web Traffic Security (Антивирус и Анти-Фишинг) не могут проверить данные, передаваемые внутри шифрованного канала связи. Это снижает уровень защиты IT-инфраструктуры организации.
4. **Добавление исключений для SSL Bumping (на стр. 258)**

   Применение SSL Bumping может привести к неработоспособности некоторых программ или сервисов, использующих прокси-сервер. Для корректной работы требуется добавить их в исключения SSL Bumping.
5. **Дополнительная настройка при высокой нагрузке (на стр. 259)**

   Для обработки большого количества сетевых соединений необходимо выполнить настройку параметров производительности сервиса Squid и сетевого стека операционной системы.

В этом разделе

kaspersky

Установка сервиса Squid

► *Чтобы установить сервис Squid:*

1. Установите пакет сервиса Squid с помощью следующей команды:

   ```
   apt install squid-openssl
   ```

2. Добавьте сервис Squid в автозагрузку. Для этого выполните команду:

   ```
   systemctl enable squid
   ```

3. Запустите сервис Squid. Для этого выполните команду:

   ```
   systemctl start squid
   ```

4. Проверьте статус сервиса Squid. Для этого выполните команду:

   ```
   systemctl status squid
   ```

   Параметр **Active** должен содержать значение **active (running)**.

Сервис Squid будет установлен.

Настройка сервиса Squid

► *Чтобы настроить сервис Squid:*

1. Измените параметры сервиса Squid. Для этого в конец конфигурационного файла /etc/squid/squid.conf добавьте следующие строки:

   ```
   icap_enable on
   adaptation_send_username on
   adaptation_send_client_ip on
   icap_service kwts_req reqmod_precache icap://127.0.0.1:1344/av/reqmod
   icap_service kwts_res respmod_precache icap://127.0.0.1:1344/av/respmod
   icap_service_failure_limit -1
   adaptation_access kwts_req allow all
   adaptation_access kwts_res allow all
   ```

2. В том же конфигурационном файле к директиве http_port добавьте опцию tcpkeepalive:

   ```
   http_port 3128 tcpkeepalive=60,30,3
   ```

3. Перезагрузите сервис Squid. Для этого выполните команду:

   ```
   systemctl restart squid
   ```

Настройка сервиса Squid будет завершена.

kaspersky

Настройка SSL Bumping в сервисе Squid

Рекомендуется настроить SSL Bumping в сервисе Squid для обработки шифрованных соединений. Если SSL Bumping не настроен, то прокси-сервер не может вмешаться в процесс установки шифрованного соединения. В этом случае модули защиты Kaspersky Web Traffic Security (Антивирус и Анти-Фишинг) не могут проверить данные, передаваемые внутри шифрованного канала связи. Это снижает уровень защиты IT-инфраструктуры организации.

Для работы SSL Bumping требуется SSL-сертификат и приватный ключ в формате PEM. Вы можете создать новый самоподписанный SSL-сертификат (см. раздел "Создание самоподписанного SSL-сертификата" на стр. 257) или использовать готовый (например, SSL-сертификат, выданный центром сертификации организации).

Если приватный ключ защищен паролем, его нужно предварительно расшифровать.

► *Чтобы настроить SSL Bumping в сервисе Squid:*

1. Убедитесь, что используемый сервис Squid поддерживает необходимые опции. Для этого выполните команду:

   ```
   squid -v
   ```

   Параметр `configure options` должен содержать значения `--enable-ssl-crtd` и `--with-openssl`.

2. Скопируйте SSL-сертификат в формате PEM в файл /etc/squid/bump.crt.
3. Скопируйте приватный ключ в формате PEM в файл /etc/squid/bump.key.
4. Сгенерируйте файл параметров для алгоритма Diffie-Hellman. Для этого выполните команду:

   ```
   openssl dhparam -outform PEM -out /etc/squid/bump_dhparam.pem 2048
   ```

5. Настройте права на использование файла SSL-сертификата с помощью следующих команд:

   ```
   chown proxy:proxy /etc/squid/bump*
   chmod 400 /etc/squid/bump*
   ```

6. Определите версию сервиса Squid, используемую на вашем сервере. Для этого выполните команду:

   ```
   squid -v
   ```

   Информация об используемой версии отобразится в формате `Squid Cache: Version <версия>`.

7. Остановите сервис Squid, если он запущен. Для этого выполните команду:

   ```
   systemctl stop squid
   ```

8. Создайте каталог для базы данных сертификатов и инициализируйте базу данных с помощью команд:

   ```
   mkdir -p /var/lib/squid
   rm -rf /var/lib/squid/ssl_db
   /usr/lib/squid/security_file_certgen -c -s /var/lib/squid/ssl_db -M 20MB
   ```

```
chown -R proxy:proxy /var/lib/squid
```

9. В конфигурационном файле /etc/squid/squid.conf выполните следующие изменения:
   a. Добавьте в начало файла или перед первой директивой http_access следующие директивы:

      ```
      acl intermediate_fetching transaction_initiator certificate-fetching
      http_access allow intermediate_fetching
      ```

   b. Добавьте в конец файла следующие директивы:

      ```
      sslcrtd_program /usr/lib/squid/security_file_certgen -s
      /var/lib/squid/ssl_db -M 20MB
      sslproxy_cert_error allow all
      ssl_bump stare all
      ```

   c. Замените директиву http_port на одну из следующих, в зависимости от версии Squid:
      - Squid версии 4.x или 5.x:

        ```
        http_port 3128 tcpkeepalive=60,30,3 ssl-bump
        generate-host-certificates=on dynamic_cert_mem_cache_size=20MB
        tls-cert=/etc/squid/bump.crt tls-key=/etc/squid/bump.key
        cipher=HIGH:MEDIUM:!LOW:!RC4:!SEED:!IDEA:!3DES:!MD5:!EXP:!PSK:!DSS
        options=NO_TLSv1,NO_SSLv3,SINGLE_DH_USE,SINGLE_ECDH_USE
        tls-dh=prime256v1:/etc/squid/bump_dhparam.pem
        ```

      - Squid версии 6.x и выше:

        ```
        http_port 3128 tcpkeepalive=60,30,3 ssl-bump
        generate-host-certificates=on dynamic_cert_mem_cache_size=20MB
        tls-cert=/etc/squid/bump.crt tls-key=/etc/squid/bump.key
        cipher=HIGH:MEDIUM:!LOW:!RC4:!SEED:!IDEA:!3DES:!MD5:!EXP:!PSK:!DSS
        options=NO_TLSv1,NO_SSLv3 tls-dh=/etc/squid/bump_dhparam.pem
        ```

10. Перезагрузите сервис Squid. Для этого выполните команду:

    ```
    systemctl restart squid
    ```

Настройка SSL Bumping в сервисе Squid будет завершена.

Создание самоподписанного SSL-сертификата

► *Чтобы создать самоподписанный SSL-сертификат:*

1. Перейдите в директорию сервиса Squid. Для этого выполните команду:

   ```
   cd /etc/squid
   ```

2. Создайте самоподписанный SSL-сертификат. Для этого выполните команду:

   ```
   openssl req -new -newkey rsa:2048 -days <количество дней действия
   сертификата> -nodes -x509 -keyout bump.key -out bump.crt
   ```

   Отобразится предложение заполнить поля самоподписанного SSL-сертификата.

3. Заполните поля самоподписанного SSL-сертификата.

Будут созданы файлы сертификата bump.crt и приватного ключа bump.key в формате PEM.

> Во избежание несанкционированного доступа к трафику файл приватного ключа необходимо хранить в защищенном месте.

4. Преобразуйте файл сертификата в доверенный сертификат формата DER для импорта в браузер. Для этого выполните команду:

   ```
   openssl x509 -in bump.crt -outform DER -out bump.der
   ```

5. Импортируйте файл bump.der в список доверенных корневых центров сертификации на компьютерах пользователей.

   При использовании некоторых браузеров (например, Mozilla Firefox) требуется также добавить сертификат в хранилище браузера.

Самоподписанный SSL-сертификат будет создан.

Добавление исключений для SSL Bumping

Добавление исключений для SSL Bumping может потребоваться в следующих случаях:

- Программное обеспечение использует протокол, отличный от HTTPS (например, SSH, RDP, VPN).
- Программное обеспечение или веб-ресурс использует протокол WebSockets или HTTP/2.0.
- Для доступа к веб-ресурс используются национальные алгоритмы шифрования (GOST, SM2).
- Программное обеспечение использует привязку серверного сертификата (pinning).
- Программное обеспечение или веб-ресурс требует авторизации по клиентскому SSL-сертификату.

► *Чтобы добавить исключения для SSL Bumping:*

1. Создайте файл /etc/squid/donotbump.list со списком доменных имен веб-ресурсов и хостов, которые вы хотите добавить в исключения.

   Каждое доменное имя должно располагаться на новой строке.

   > Чтобы добавить в исключения домен со всеми поддоменами, укажите точку в начале значения (например, `.domain.com`).

2. Добавьте в конфигурационный файл /etc/squid/squid.conf следующие директивы:

   ```
   acl do_not_bump dstdomain "/etc/squid/donotbump.list"
   ssl_bump splice do_not_bump
   ```

   Эти строки должны располагаться перед финальной директивой ssl_bump stare all.

3. Перезагрузите сервис Squid. Для этого выполните команду:

   ```
   systemctl restart squid
   ```

Исключения для SSL Bumping будут добавлены.

kaspersky

Дополнительная настройка при высокой нагрузке

Для обработки большого количества сетевых соединений необходимо выполнить настройку параметров производительности сервиса Squid и сетевого стека операционной системы.

► *Чтобы выполнить дополнительную настройку:*

1. Создайте конфигурационный файл /etc/sysctl.d/90-net-tcp.conf следующего содержания:

   ```
   net.core.somaxconn = 1024
   net.core.netdev_max_backlog = 2048
   net.ipv4.ip_local_port_range = 1024 65535
   net.ipv4.tcp_max_syn_backlog = 2048
   net.ipv4.tcp_fin_timeout = 20
   net.ipv4.tcp_syncookies = 1
   net.ipv4.tcp_timestamps = 1
   net.ipv4.tcp_tw_reuse = 1
   net.ipv4.tcp_rfc1337 = 1
   ```

2. Примените внесенные изменения. Для этого выполните команду:

   ```
   sysctl -p /etc/sysctl.d/90-net-tcp.conf
   ```

3. Настройте параметры производительности сервиса Squid. Для этого в конец конфигурационного файла /etc/squid/squid.conf добавьте строку:

   ```
   workers <количество физических ядер всех процессоров сервера>
   ```

4. Перезагрузите сервис Squid. Для этого выполните команду:

   ```
   systemctl restart squid
   ```

Дополнительная настройка будет выполнена.

kaspersky

Приложение 8. Настройка интеграции сервиса Squid с Active Directory

Интеграция с Active Directory позволяет добавлять пользователей из Active Directory в качестве инициатора срабатывания правила обработки трафика (см. раздел "Настройка инициатора срабатывания правила" на стр. 87);

Вы можете использовать следующие механизмы аутентификации:

- Kerberos-аутентификация.
- NTLM-аутентификация.
- Basic-аутентификация.

Рекомендуется использовать Kerberos-аутентификацию, так как данный механизм является самым надежным. При NTLM- и Basic-аутентификации злоумышленники могут получить доступ к паролям пользователей, перехватив сетевой трафик.

В этом разделе

Настройка Kerberos-аутентификации

Для использования Kerberos-аутентификации необходимо убедиться, что в системе DNS присутствует PTR-запись для каждого контроллера домена.

Выполняйте действия по настройке Kerberos-аутентификации на сервере с сервисом Squid.

Для настройки аутентификации учетная запись администратора сервера должна обладать правами суперпользователя.

В этом разделе

Настройка синхронизации времени

► *Чтобы настроить синхронизацию времени с NTP-серверами, выполните следующие действия:*

1. Установите пакет chrony с помощью команды:

   ```
   apt-get install chrony
   ```

2. Включите автозапуск сервиса chronyd с помощью команды:

   ```
   systemctl enable chrony
   ```

   Откройте на редактирование файл /etc/chrony/chrony.conf.

3. Добавьте строки с IP-адресами тех NTP-серверов, с которыми вы хотите настроить синхронизацию времени. Например:

   ```
   server <IP-адрес NTP-сервера> iburst
   ```

4. Закомментируйте (добавьте символ # в начало строки) строки, начинающиеся со слова pool или server, с IP-адресами тех NTP-серверов, которые вы не хотите использовать для синхронизации времени.

5. Если для синхронизации времени вы используете контроллер домена Windows®, добавьте строку:

   ```
   maxdistance 16.0
   ```

6. Сохраните и закройте файл chrony.conf.

7. Перезапустите сервис chronyd с помощью команды:

   ```
   systemctl restart chrony
   ```

8. Проверьте синхронизацию времени. Для этого выполните команду:

   ```
   chronyc sources -v
   ```

   Если отобразившиеся IP-адреса совпадают с адресами NTP-серверов, которые вы указали в файле chrony.conf, то синхронизация настроена верно.

Синхронизация времени сервера Squid и NTP-серверов будет настроена.

Настройка DNS

► *Чтобы настроить параметры DNS:*

1. Укажите IP-адрес DNS-сервера (серверов), который используется для работы с Active Directory, на сервере с сервисом Squid.

   Подробнее о способах настройки DNS в различных операционных системах см. в документации к этим операционным системам.

2. Убедитесь, что DNS-зона Active Directory доступна. Для этого выполните команду:

   ```
   host -t a <домен Active Directory>
   ```

> Для использования утилиты host может потребоваться предварительная установка пакета bind-utils или bind9-host.

Отобразятся A-записи контроллеров домена Active Directory.

3. Убедитесь, что для каждого контроллера домена присутствует PTR-запись. Для этого выполните команду:

   ```
   host <IP-адрес контроллера домена>
   ```

   Отобразится PTR-запись контроллера домена Active Directory.

4. Добавьте A- и PTR-записи на DNS-сервере Active Directory для сервера с сервисом Squid. Имя сервера должно быть уникальным и содержать не более 15 символов.

   > Для создания PTR-записи вам может потребоваться добавить обратную DNS-зону.

5. Укажите имя сервера с сервисом Squid. Для этого выполните команду:

   ```
   hostnamectl set-hostname <имя сервера с сервисом Squid>
   ```

   Имя сервера с сервисом Squid должно совпадать с именем этого сервера на DNS-сервере.

6. Убедитесь, что контроллер домена Active Directory доступен с сервера с сервисом Squid. Для этого выполните команду:

   ```
   ping <имя контроллера домена Active Directory>
   ```

   Если контроллер домена Active Directory доступен, отобразится успешный обмен пакетами.

7. Убедитесь, что сервер с сервисом Squid доступен с контроллера домена Active Directory. Для этого выполните команду:

   ```
   ping <имя сервера с сервисом Squid>
   ```

   Если сервер с сервисом Squid доступен, отобразится успешный обмен пакетами.

Параметры DNS будут настроены.

Создание keytab-файла для сервиса Squid

Вы можете использовать одну учетную запись для аутентификации на всех узлах кластера. Для этого требуется создать keytab-файл, содержащий *имена субъекта-службы (далее также "SPN")* для каждого из этих узлов. При создании keytab-файла потребуется использовать атрибут для генерации *соли* (salt, модификатор входа хеш-функции).

> Сгенерированную соль необходимо сохранить любым удобным способом для дальнейшего добавления новых SPN в keytab-файл.

Вы также можете создать отдельную учетную запись Active Directory для каждого узла кластера, для которого вы хотите настроить Kerberos-аутентификацию.

Keytab-файл создается на сервере контроллера домена или на компьютере под управлением Windows Server, входящем в домен, под учетной записью с правами доменного администратора.

► *Чтобы создать keytab-файл для сервиса Squid, используя одну учетную запись:*

1. В оснастке **Active Directory Users and Computers** создайте учетную запись пользователя с именем `squid-user`.
2. Чтобы использовать алгоритм шифрования AES256-SHA1, в оснастке **Active Directory Users and Computers** выполните следующие действия:
   a. Откройте свойства созданной учетной записи.
   b. На вкладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.
3. Создайте keytab-файл для пользователя `squid-user` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<имя сервера с сервисом Squid>@<realm имя домена Active Directory в верхнем регистре> -mapuser squid-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out <путь к файлу>\<имя файла>.keytab
   ```

   Имя сервера с сервисом Squid требуется указывать в нижнем регистре (например, `proxy.company.com`).

   Утилита запросит пароль пользователя `squid-user` в процессе выполнения команды.

   В созданный keytab-файл будет добавлена запись SPN Управляющего узла. На экране отобразится сгенерированная соль: `Hashing password with salt "<хеш-значение>"`.
4. Для каждого узла кластера добавьте в keytab-файл запись SPN. Для этого выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser squid-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <путь и имя ранее созданного файла>.keytab -out <путь и новое имя>.keytab -setupn -setpass -rawsalt "<хеш-значение соли, полученное при создании keytab-файла на шаге 3>"
   ```

   Утилита запросит пароль пользователя `squid-user` в процессе выполнения команды.

Keytab-файл для сервиса Squid будет создан. Этот файл будет содержать все добавленные SPN узлов кластера.

Пример:

Например, вам нужно создать keytab-файл, содержащий SPN-имена 3 узлов: `control-01.test.local`, `secondary-01.test.local` и `secondary-02.test.local`.

Чтобы создать в папке C:\keytabs\ файл под названием `filename1.keytab`, содержащий SPN Управляющего узла, требуется выполнить команду:

```
C:\Windows\system32\ktpass.exe -princ
HTTP/control-01.test.local@TEST.LOCAL -mapuser squid-user@TEST.LOCAL
-crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out
C:\keytabs\filename1.keytab
```

Допустим, вы получили соль `"TEST.LOCALHTTPcontrol-01.test.local"`.

Для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ
HTTP/secondary-01.test.local@TEST.LOCAL -mapuser squid-user@TEST.LOCAL
-crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in
C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab -setupn
-setpass -rawsalt "TEST.LOCALHTTPcontrol-01.test.local"
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ
HTTP/secondary-02.test.local@TEST.LOCAL -mapuser squid-user@TEST.LOCAL
-crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in
C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab -setupn
-setpass -rawsalt "TEST.LOCALHTTPcontrol-01.test.local"
```

В результате будет создан файл с именем `filename3.keytab`, содержащий все три добавленные SPN.

► *Чтобы создать keytab-файл для сервиса Squid, используя отдельную учетную запись для каждого узла:*

1. В оснастке **Active Directory Users and Computers** создайте отдельную учетную запись пользователя для каждого узла кластера (например, учетные записи с именами `squid-user`, `squid-user2`, `squid-user3` и т.д.).
2. Чтобы использовать алгоритм шифрования AES256-SHA1, в оснастке **Active Directory Users and Computers** выполните следующие действия:
   a. Откройте свойства созданной учетной записи.
   b. На вкладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.
3. Создайте keytab-файл для пользователя `squid-user` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<имя сервера с сервисом Squid
   в нижнем регистре>@<realm имя домена Active Directory в верхнем регистре>
   -mapuser squid-user@<realm имя домена Active Directory в верхнем регистре>
   -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out <путь к
   файлу>\<имя файла>.keytab
   ```

> Имя сервера с сервисом Squid требуется указывать в нижнем регистре (например, `proxy.company.com`).

Утилита запросит пароль пользователя `squid-user` в процессе выполнения команды.

В созданный keytab-файл будет добавлена запись SPN Управляющего узла.

4. Для каждого узла кластера добавьте в keytab-файл запись SPN. Для этого выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser squid-user2@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <путь и имя ранее созданного файла>.keytab -out <путь и новое имя>.keytab
   ```

   Утилита запросит пароль пользователя `squid-user2` в процессе выполнения команды.

Keytab-файл для сервиса Squid будет создан. Этот файл будет содержать все добавленные SPN узлов кластера.

Пример:

Например, вам нужно создать keytab-файл, содержащий SPN-имена 3 узлов: `control-01.test.local`, `secondary-01.test.local` и `secondary-02.test.local`.

Чтобы создать в папке C:\keytabs\ файл под названием `filename1.keytab`, содержащий SPN Управляющего узла, требуется выполнить команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser squid-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out C:\keytabs\filename1.keytab
```

Для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-01.test.local@TEST.LOCAL -mapuser squid-user2@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-02.test.local@TEST.LOCAL -mapuser squid-user3@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab
```

В результате будет создан файл с именем `filename3.keytab`, содержащий все три добавленные SPN.

kaspersky

Настройка сервиса Squid для Kerberos-аутентификации

Если вы настраиваете аутентификацию с доменом, в названии которого содержится корневой домен `.local`, то для корректной работы Kerberos-аутентификации требуется выполнить предварительные действия в операционной системе.

1. Проверьте состояние службы avahi-daemon. Для этого выполните команду:

   ```
   systemctl status avahi-daemon
   ```

2. Если служба запущена, остановите ее. Для этого выполните команду:

   ```
   systemctl stop avahi-daemon
   ```

3. Отключите автоматический запуск службы. Для этого выполните команду:

   ```
   systemctl disable avahi-daemon
   ```

► *Чтобы настроить сервис Squid для Kerberos-аутентификации:*

1. Скопируйте файл squid.keytab в директорию /etc/squid/.
2. Настройте доступ к keytab-файлу с помощью команды:

   ```
   chown proxy:proxy /etc/squid/squid.keytab
   ```

   ```
   chmod 400 /etc/squid/squid.keytab
   ```

   По умолчанию владельцем файла krb5.keytab является суперпользователь.
3. Добавьте в начало файла /etc/squid/squid.conf следующие параметры:

   ```
   auth_param negotiate program /usr/lib/squid/negotiate_kerberos_auth -k
   /etc/squid/squid.keytab -s HTTP/<имя сервера с сервисом Squid>@<realm имя
   домена Active Directory в верхнем регистре>
   ```

   ```
   auth_param negotiate children 100 startup=0 idle=10
   ```

   ```
   auth_param negotiate keep_alive on
   ```

   ```
   acl authenticated_user proxy_auth REQUIRED
   ```

   ```
   http_access deny !authenticated_user
   ```

4. Если вы хотите включить запись событий в журнал в режиме отладки, в файле /etc/squid/squid.conf добавьте параметр `-d` в первую строку:

   ```
   auth_param negotiate program /usr/lib/squid/negotiate_kerberos_auth -d -k
   /etc/squid/squid.keytab -s HTTP/<имя сервера с сервисом Squid>@<realm имя
   домена Active Directory>
   ```

   Отладочные события будут записаны в файл /var/log/squid/cache.log.
5. Если вы хотите отключить Replay cache, выполните следующие действия:
   a. Создайте файл /etc/systemd/system/squid.service.d/override.conf следующего содержания:

      ```
      [Service]
      ```

      ```
      Environment=KRB5RCACHETYPE=none
      ```

   b. Выполните команду:

      ```
      systemctl daemon-reload
      ```

По умолчанию Replay cache включен.

> Replay cache обеспечивает более надежную защиту, но может снижать производительность приложения.

6. Перезагрузите сервис Squid. Для этого выполните команду:

   ```
   systemctl restart squid
   ```

7. На компьютерах локальной сети организации в параметрах браузера укажите полное доменное имя (FQDN) сервера с сервисом Squid в качестве прокси-сервера.

Сервис Squid будет настроен для использования Kerberos-аутентификации.

Настройка NTLM-аутентификации

> Рекомендуется использовать Kerberos-аутентификацию для обеспечения безопасности передачи данных. Используйте NTLM-аутентификацию, только если невозможно использовать Kerberos-аутентификацию. Если вы используете NTLM-аутентификацию, необходимо включить протокол Samba версии 2.

Выполняйте действия по настройке NTLM-аутентификации на сервере с сервисом Squid.

Для настройки аутентификации учетная запись администратора сервера должна обладать правами суперпользователя.

В этом разделе

Установка сервиса Samba

► *Чтобы установить сервис Samba и пакеты, необходимые для работы сервиса Samba, выполните команду:*

```
apt-get install samba winbind
```

Настройка синхронизации времени

► *Чтобы настроить синхронизацию времени с NTP-серверами, выполните следующие действия:*

1. Установите пакет chrony с помощью команды:

   ```
   apt-get install chrony
   ```

2. Включите автозапуск сервиса chronyd с помощью команды:

   ```
   systemctl enable chrony
   ```

   Откройте на редактирование файл /etc/chrony/chrony.conf.

3. Добавьте строки с IP-адресами тех NTP-серверов, с которыми вы хотите настроить синхронизацию времени. Например:

   ```
   server <IP-адрес NTP-сервера> iburst
   ```

4. Закомментируйте (добавьте символ # в начало строки) строки, начинающиеся со слова pool или server, с IP-адресами тех NTP-серверов, которые вы не хотите использовать для синхронизации времени.

5. Если для синхронизации времени вы используете контроллер домена Windows, добавьте строку:

   ```
   maxdistance 16.0
   ```

6. Сохраните и закройте файл chrony.conf.

7. Перезапустите сервис chronyd с помощью команды:

   ```
   systemctl restart chrony
   ```

8. Проверьте синхронизацию времени. Для этого выполните команду:

   ```
   chronyc sources -v
   ```

   Если отобразившиеся IP-адреса совпадают с адресами NTP-серверов, которые вы указали в файле chrony.conf, то синхронизация настроена верно.

Синхронизация времени сервера Squid и NTP-серверов будет настроена.

Настройка DNS

► *Чтобы настроить параметры DNS:*

1. Укажите IP-адрес DNS-сервера (серверов), который используется для работы с Active Directory, на сервере с сервисом Squid.

   Подробнее о способах настройки DNS в различных операционных системах см. в документации к этим операционным системам.

2. Убедитесь, что DNS-зона Active Directory доступна с сервера с сервисом Squid. Для этого выполните команду:

   ```
   host -t a <домен Active Directory>
   ```

> Для использования утилиты host может потребоваться предварительная установка пакета bind-utils или bind9-host.

Отобразятся A-записи контроллеров домена Active Directory.

3. Укажите имя сервера с сервисом Squid. Для этого выполните команду:

   ```
   hostnamectl set-hostname <имя сервера с сервисом Squid>
   ```

4. Добавьте A- и PTR-записи на DNS-сервере Active Directory для сервера с сервисом Squid. Имя сервера должно быть уникальным и содержать не менее 15 символов.

   > Для создания PTR-записи вам может потребоваться добавить обратную зону.

5. Убедитесь, что имя сервера с сервисом Squid совпадает с именем этого сервера на DNS-сервере Active Directory.
6. Убедитесь, что контроллер домена Active Directory доступен с сервера с сервисом Squid. Для этого выполните команду:

   ```
   ping <имя контроллера домена Active Directory>
   ```

   Если контроллер домена Active Directory доступен, отобразится успешный обмен пакетами.
7. Убедитесь, что сервер с сервисом Squid доступен с контроллера домена Active Directory. Для этого выполните команду:

   ```
   ping <имя сервера с сервисом Squid>
   ```

   Если сервер с сервисом Squid доступен, отобразится успешный обмен пакетами.

Параметры DNS будут настроены.

Настройка Samba на сервере с сервисом Squid

► *Чтобы настроить сервис Samba:*

1. Запустите сервисы Samba и добавьте их в автозагрузку с помощью команд:

   ```
   systemctl start smbd
   systemctl enable smbd
   systemctl start nmbd
   systemctl enable nmbd
   ```

2. Добавьте в файл /etc/samba/smb.conf следующие параметры:

   ```
   [global]
     netbios name = <NetBIOS-имя (хостнейм) сервера>
     workgroup = <NetBIOS-имя домена Active Directory>
     password server = <DNS-имя контроллера домена Active Directory>
     realm = <имя домена Active Directory в верхнем регистре>
   ```

```
security = ads
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind use default domain = no
winbind request timeout = 300
```

Если доменное имя (хостнейм) сервера превышает 15 символов, в параметре `netbios name` следует указывать укороченное имя (псевдоним), не превышающее 15 символов.

3. Добавьте сервер с сервисом Squid в домен Active Directory. Для этого выполните команду:

   ```
   net ads join -U <администратор домена>
   ```

   Отобразится предложение ввести пароль администратора домена или пользователя с правами администратора домена.

4. Введите пароль администратора и нажмите на клавишу **ENTER**.

   Сервер с сервисом Squid будет добавлен в домен Active Directory.

5. Проверьте добавление сервера с сервисом Squid в домен Active Directory. Для этого выполните команду:

   ```
   net ads testjoin
   ```

   Если сервер с сервисом Squid добавлен в домен Active Directory, в консоли отобразится `Join is OK`.

6. Перезапустите сервисы Samba с помощью команд

   ```
   systemctl restart smbd
   systemctl restart nmbd
   ```

   Если возникла ошибка "ERROR: failed to setup guest info", требуется настроить сопоставление для гостевой группы. Для этого выполните команду:
   `net groupmap add sid=S-1-5-32-546 unixgroup=nobody type=builtin`

7. Запустите службу winbind. Для этого выполните команду:

   ```
   systemctl start winbind
   ```

8. Добавьте службу winbind в автозагрузку. Для этого выполните команду:

   ```
   systemctl enable winbind
   ```

9. Если вы используете операционную систему Ubuntu или Debian, вам требуется добавить пользователя proxy в группу winbindd_priv. Для этого выполните команду:

   ```
   usermod -a -G winbindd_priv proxy
   ```

Настройка Samba будет завершена. Перейдите к проверке параметров Samba.

kaspersky

Проверка параметров Samba на сервере с сервисом Squid

► *Чтобы проверить параметры сервиса Samba:*

1. Проверьте получение сервером списка доменных групп. Для этого выполните команду:

   ```
   wbinfo -g
   ```

   Отобразится список доменных групп сервера.

2. Проверьте получение сервером списка пользователей. Для этого выполните команду:

   ```
   wbinfo -u
   ```

   Отобразится список пользователей сервера.

Если авторизация выполнена успешно, параметры сервиса Samba на сервере с сервисом Squid настроены верно.

Настройка сервиса Squid

► *Чтобы настроить сервис Squid:*

1. Добавьте в начало файла /etc/squid/squid.conf следующие строки:

   ```
   auth_param ntlm program /usr/bin/ntlm_auth
   --helper-protocol=squid-2.5-ntlmssp --domain=<NetBIOS-имя домена Active
   Directory>

   auth_param ntlm children 100 startup=0 idle=10

   auth_param ntlm keep_alive off

   acl authenticated_user proxy_auth REQUIRED

   http_access deny !authenticated_user
   ```

2. Если вы хотите включить запись событий в журнал в режиме отладки, в файле /etc/squid/squid.conf добавьте параметр `-d 10` в следующей строке:

   ```
   auth_param ntlm program /usr/bin/ntlm_auth -d 10
   --helper-protocol=squid-2.5-ntlmssp --domain=<NetBIOS-имя домена Active
   Directory>
   ```

   События отладки будут записаны в файл /var/log/squid/cache.log.

3. Перезагрузите сервис Squid. Для этого выполните команду:

   ```
   systemctl restart squid
   ```

Настройка сервиса Squid завершится.

Настройка клиентской части NTLM-аутентификации

► *Чтобы настроить клиентскую часть NTLM-аутентификации:*

1. На сервере с сервисом Squid убедитесь, что в файле /etc/resolv.conf первый параметр `nameserver`

содержит IP-адрес DNS-сервера с зоной Active Directory. Для этого выполните команду:

```
cat /etc/resolv.conf
```

2. На DNS-сервере Active Directory добавьте A- и PTR-записи для сервера с сервисом Squid.

   > Для создания PTR-записи вам может потребоваться добавить обратную зону.

3. Убедитесь, что контроллер домена Active Directory доступен с сервера с сервисом Squid. Для этого выполните команды:

   ```
   ping <имя контроллера домена Active Directory>
   ```

   Если контроллер домена Active Directory доступен, отобразится успешный обмен пакетами.

   ```
   telnet <имя контроллера домена Active Directory> 445
   ```

   Если контроллер домена Active Directory доступен, соединение будет успешно установлено.

   Для закрытия соединения нажмите **CTRL-]**, затем введите `quit` и нажмите на клавишу **ENTER**.

4. Убедитесь, что сервер с сервисом Squid доступен с контроллера домена Active Directory. Для этого выполните команду:

   ```
   ping <имя сервера с сервисом Squid>
   ```

   Если сервер с сервисом Squid доступен, отобразится успешный обмен пакетами.

5. На компьютерах локальной сети организации в параметрах браузера укажите FQDN-адрес сервера с сервисом Squid в качестве прокси-сервера.

Клиентская часть NTLM-аутентификации будет настроена.

Настройка NTLM-аутентификации хоста, не входящего в домен

► *Чтобы настроить NTLM-аутентификацию хоста, не входящего в домен Active Directory:*

1. На компьютерах локальной сети организации в параметрах браузера укажите полное доменное имя (FQDN) сервера с сервисом Squid в качестве прокси-сервера.
2. Если вы хотите сохранить учетные данные в операционной системе, чтобы не вводить их при каждом запуске браузера, откройте Диспетчер учетных данных Windows (**Пуск** → **Панель управления** → **Диспетчер учетных данных**).
3. Нажмите на ссылку **Добавить учетные данные Windows**.
4. В открывшемся окне укажите полное доменное имя (FQDN) сервера с сервисом Squid, а также доменную учетную запись пользователя.
5. Нажмите на кнопку **OK**.

NTLM-аутентификация будет настроена.

Настройка Basic-аутентификации

Выполняйте действия по настройке Basic-аутентификации на сервере с сервисом Squid.

Для настройки аутентификации учетная запись администратора сервера должна обладать правами

суперпользователя.

► *Чтобы настроить Basic-аутентификацию:*

1. Добавьте в начало файла /etc/squid/squid.conf следующие строки:

```
auth_param basic program /usr/lib/squid/basic_ldap_auth -R -b
"<LDAP-объект (домен, группа или организационная единица) в формате DN
(например, "ou=ou_name,dc=test,dc=local" или
"dc=domain,dc=example,dc=com")>" -D "<имя пользователя>@<домен Active
Directory>" -w "<пароль пользователя>" -f "sAMAccountName=%s" <IP-адрес
контроллера домена Active Directory>

auth_param basic children 10

auth_param basic realm Squid proxy-caching web server

auth_param basic casesensitive off

auth_param basic credentialsttl 1 minute

acl authenticated_user proxy_auth REQUIRED

http_access deny !authenticated_user
```

2. Если вы хотите включить запись событий в журнал в режиме отладки, в файле /etc/squid/squid.conf добавьте параметр `-d` в первую строку:

```
auth_param basic program /usr/lib/squid/basic_ldap_auth -R -d -b
"<LDAP-объект (домен, группа или организационная единица) в формате DN
(например, "ou=ou_name,dc=test,dc=local" или
"dc=domain,dc=example,dc=com")>" -D "<имя пользователя>@<домен Active
Directory>" -w "<пароль пользователя>" -f "sAMAccountName=%s" <IP-адрес
контроллера домена Active Directory>
```

   События отладки будут записаны в файл /var/log/squid/cache.log.

3. Перезагрузите сервис Squid. Для этого выполните команду:

```
systemctl restart squid
```

Basic-аутентификация будет настроена.

kaspersky

Глоссарий

I

ICAP-сервер

Сервер, реализующий ICAP-протокол. Этот протокол позволяет фильтровать и изменять данные HTTP-запросов и HTTP-ответов. Например, производить антивирусную проверку данных, блокировать спам, запрещать доступ к персональным ресурсам. В качестве ICAP-клиента обычно выступает прокси-сервер, который взаимодействует с ICAP-сервером по ICAP-протоколу. Kaspersky Web Traffic Security получает данные с прокси-сервера организации, выступая в роли ICAP-сервера.

K

Kaspersky Private Security Network

Решение, позволяющее пользователям антивирусных приложений "Лаборатории Касперского" получать доступ к данным Kaspersky Security Network, не отправляя информацию на серверы Kaspersky Security Network "Лаборатории Касперского" со своей стороны.

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Kerberos-аутентификация

Механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, позволяющий передавать данные через незащищенные сети. Механизм основан на использовании билета (ticket), который выдается пользователю доверенным центром аутентификации.

Keytab-файл

Файл, содержащий пары уникальных имен (principals) для клиентов, которым разрешается Kerberos-аутентификация, и зашифрованные ключи, полученные из пароля пользователя. Keytab-файлы используются в системах, поддерживающих Kerberos, для аутентификации пользователей без ввода пароля.

L

LDAP

Lightweight Directory Access Protocol – облегченный клиент-серверный протокол доступа к службам каталогов.

M

MIB (Management Information Base)

Виртуальная база данных, используемая для управления объектами, которые передаются по протоколу SNMP.

N

NTLM-аутентификация

Механизм аутентификации, который работает посредством вопросов/ответов между сервером и клиентом без передачи пароля пользователя через сеть в открытом виде. Для шифрования запроса и ответа используются хеши пароля пользователя, которые передаются по сети. При захвате сетевого трафика злоумышленники могут получить доступ к хешам пароля, что делает этот механизм менее надежным, чем Kerberos-аутентификация.

P

PTR-запись

DNS-запись, связывающая IP-адрес компьютера с его доменным именем.

R

Replay cache

Кеш, используемый в технологии Kerberos для хранения записей о запросах пользователей на аутентификацию. Этот механизм помогает защитить инфраструктуру от атак повторного воспроизведения. Во время таких атак злоумышленники записывают трафик пользователя, чтобы воспроизвести ранее отправленные им сообщения и успешно пройти аутентификацию на прокси-сервере. При использовании replay cache сервер аутентификации обнаруживает дубликат запроса и отправляет в ответ сообщение об ошибке.

S

SIEM-система

SIEM-система (Security Information and Event Management) – решение для управления информацией и событиями в системе безопасности организации.

SNI (Server Name Indication)

Расширение протокола TLS, передающее имя веб-сайта, с которым требуется установить соединение. SNI необходим в случаях, когда несколько сервисов, работающих по протоколу HTTPS, расположены на одном физическом сервере и используют один IP-адрес, но при этом у каждого сервиса есть свой сертификат безопасности.

SNMP-агент

Программный модуль сетевого управления Kaspersky Web Traffic Security, отслеживает информацию о работе приложения.

SNMP-ловушка

Уведомление о событиях работы приложения, отправляемое SNMP-агентом.

Squid

Программный пакет, выполняющий функцию кеширующего прокси-сервера для протоколов HTTP(S) и FTP. Сервис Squid использует списки контроля доступа для распределения доступа к ресурсам.

SRV-запись

Стандарт в DNS, определяющий местоположение, то есть имя хоста и номер порта серверов для определенных служб.

SSL Bumping

Режим работы сервиса Squid, используемый для перехвата содержимого зашифрованных HTTPS-сеансов.

Syslog

Стандарт отправки и записи сообщений о происходящих в системе событиях, используемый на платформах UNIX™ и GNU/Linux.

T

TLS-шифрование

Шифрование соединения между двумя серверами, обеспечивающее защищенную передачу данных между серверами сети Интернет.

B

Вирус

Программа, которая заражает другие программы – добавляет в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – заражение.

Вредоносные ссылки

Веб-адреса, которые ведут на вредоносные ресурсы, то есть ресурсы, занимающиеся распространением вредоносного программного обеспечения.

kaspersky

З

Замкнутая программная среда

Механизм контроля целостности (неизменности) файлов для повышения безопасности в Astra Linux Special Edition. Применение замкнутой программной среды позволяет определить перечень программного обеспечения, разрешенного для использования.

И

Имя субъекта-службы (SPN)

Уникальный идентификатор службы в сети для проверки подлинности по протоколу Kerberos.

Источник обновлений

Ресурс, содержащий обновления антивирусных баз приложения Kaspersky Web Traffic Security. Источником обновлений антивирусных баз могут служить серверы обновлений "Лаборатории Касперского", а также HTTP-, FTP-сервер, локальная или сетевая папка.

К

Кластер

Группа серверов с установленным приложением Kaspersky Web Traffic Security, объединенных для централизованного управления через веб-интерфейс приложения.

Н

Нормализация

Процесс, в результате которого текстовое представление адреса веб-ресурса изменяется по определенными правилами (например, исключение из текстового представления адреса веб-ресурса имени пользователя, пароля и порта соединения, понижение верхнего регистра символов адреса веб-ресурса до нижнего регистра).

О

Отпечаток сертификата

Информация, по которой можно проверить подлинность сертификата сервера. Отпечаток создается путем применения криптографической хеш-функции к содержанию сертификата сервера.

П

Подчиненный узел

Компонент приложения, который проверяет сетевой трафик пользователей согласно правилам обработки трафика. Подчиненный узел получает заданные администратором параметры от Управляющего узла.

Правило доступа

Список разрешений и запретов доступа пользователей к указанным веб-ресурсам и направлению трафика.

Правило защиты

Список проверок трафика на вирусы, фишинг, некоторые легальные программы (см. раздел "О защите трафика от некоторых легальных программ" на стр. 149), которые могут быть использованы злоумышленниками, и другие программы, представляющие угрозу, проводимых при выполнении заданных условий.

Правило обработки трафика

Набор действий, которые приложение выполняет над веб-ресурсом, удовлетворяющим заданным условиям.

Правило обхода

Набор критериев фильтрации трафика, согласно которым пользователям разрешается или запрещается доступ к веб-ресурсам без выполнения проверок по правилам доступа и правилам защиты.

P

Рабочая область

Набор параметров и прав доступа, применимых к выделенной группе пользователей.

Репутационная фильтрация

Облачная служба, использующая технологии определения репутации сообщений. Информация о появлении новых видов спама в облачной службе появляется раньше, чем в базах модуля Анти-Спам, что дает возможность повысить скорость и точность обнаружения признаков спама в сообщении.

C

Серийный номер лицензии

Уникальное сочетание букв и цифр, использующееся для однозначной идентификации приобретателя лицензии на приложение.

Служба каталогов

Программный комплекс, позволяющий хранить в одном месте информацию о сетевых ресурсах (например, о пользователях) и обеспечивающий централизованное управление ими.

Схема расположения графиков

Вид окна веб-интерфейса приложения в разделе **Мониторинг**. Вы можете добавлять, удалять и перемещать графики на схеме расположения графиков, а также настраивать масштаб некоторых графиков.

kaspersky

Т

Трассировка

Запись отладочной информации о работе приложения.

У

Управляющий узел

Компонент приложения, который позволяет администратору управлять параметрами приложения через веб-интерфейс. Управляющий сервер следит за состоянием обрабатывающих серверов, передает им заданные параметры и установленные лицензионные ключи.

Ф

Фишинг

Вид интернет-мошенничества, целью которого является получение неправомерного доступа к конфиденциальным данным пользователей.

Э

Эвристический анализ

Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса.

kaspersky

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке /opt/kaspersky/kwts/share/doc.

Для проверки электронной цифровой подписи используется программная библиотека защиты информации Крипто-Си версии 2.0, (C) ООО "КриптоЭкс" http://www.cryptoex.ru.

kaspersky

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Apache является либо зарегистрированным товарным знаком, либо товарным знаком Apache Software Foundation.

Ubuntu является зарегистрированным товарным знаком Canonical Ltd.

Google Chrome – товарный знак Google LLC.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Windows и Windows Server являются товарными знаками группы компаний Microsoft.

Mozilla и Firefox являются товарными знаками Mozilla Foundation в США и других странах.

OpenSSL является товарным знаком правообладателя OpenSSL Software Foundation.

CentOS, Red Hat, Red Hat Enterprise Linux – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Rocky Linux является товарным знаком The Rocky Enterprise Software Foundation.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

Zabbix – зарегистрированный товарный знак Zabbix SIA.