Dr.WEB

Gateway Security Suite (Unix)

Руководство администратора

© «Доктор Веб», 2025. Все права защищены

Настоящий документ носит информационный и справочный характер в отношении указанного в нем программного обеспечения семейства Dr.Web. Настоящий документ не является основанием для исчерпывающих выводов о наличии или отсутствии в программном обеспечении семейства Dr.Web каких-либо функциональных и/или технических параметров и не может быть использован при определении соответствия программного обеспечения семейства Dr.Web каким-либо требованиям, техническим заданиям и/или параметрам, а также иным документам третьих лиц.

Материалы, приведенные в данном документе, являются собственностью ООО «Доктор Веб» и могут быть использованы исключительно для личных целей приобретателя продукта. Никакая часть данного документа не может быть скопирована, размещена на сетевом ресурсе или передана по каналам связи и в средствах массовой информации или использована любым другим образом кроме использования для личных целей без ссылки на источник.

Товарные знаки

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk, KATANA и логотип Dr.WEB являются зарегистрированными товарными знаками ООО «Доктор Веб» в России и/или других странах. Иные зарегистрированные товарные знаки, логотипы и наименования компаний, упомянутые в данном документе, являются собственностью их владельцев.

Ограничение ответственности

Ни при каких обстоятельствах ООО «Доктор Веб» и его поставщики не несут ответственности за ошибки и/или упущения, допущенные в данном документе, и понесенные в связи с ними убытки приобретателя продукта (прямые или косвенные, включая упущенную выгоду).

Dr.Web Gateway Security Suite (Unix)
Версия 11.1
Руководство администратора
29.05.2025

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Москва, ул. 3-я Ямского Поля, д. 2, корп. 12А

Сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

Информацию о региональных представительствах и офисах вы можете найти на официальном сайте компании.

ООО «Доктор Веб»

Компания «Доктор Веб» — российский разработчик средств информационной безопасности.

Компания «Доктор Веб» предлагает эффективные антивирусные и антиспам-решения как для государственных организаций и крупных компаний, так и для частных пользователей.

Антивирусные решения семейства Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности.

Сертификаты и награды, а также обширная география пользователей свидетельствуют об исключительном доверии к продуктам компании.

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

1. Введение 8

2. Условные обозначения и сокращения 9

3. О продукте 10

3.1. Основные функции Dr.Web Gateway Security Suite 10

3.2. Структура Dr.Web Gateway Security Suite 13

3.3. Помещение в карантин 21

3.4. Полномочия для работы с файлами 22

3.5. Режимы работы 23

4. Системные требования и совместимость 28

5. Лицензирование 33

6. Установка и удаление 34

6.1. Установка Dr.Web Gateway Security Suite 35

6.1.1. Установка универсального пакета 36

6.1.1.1. Установка в режиме командной строки 38

6.1.2. Установка из репозитория 39

6.2. Обновление Dr.Web Gateway Security Suite 43

6.2.1. Получение текущих обновлений 43

6.2.2. Переход на новую версию продукта 44

6.2.3. Обновление без подключения к интернету 48

6.3. Удаление Dr.Web Gateway Security Suite 49

6.3.1. Удаление универсального пакета 49

6.3.1.1. Удаление в режиме командной строки 50

6.3.2. Удаление Dr.Web Gateway Security Suite, установленного из репозитория 50

6.4. Дополнительно 53

6.4.1. Пакеты и файлы Dr.Web Gateway Security Suite 53

6.4.2. Выборочные установка и удаление компонентов 56

6.5. Настройка подсистем безопасности 62

6.5.1. Настройка политик безопасности SELinux 62

7. Начало работы 67

7.1. Регистрация и активация 67

7.1.1. Ключевой файл 70

7.2. Проверка работоспособности 71

7.3. Интеграция с прокси-сервером Squid 73

7.4. Защита локального веб-сервера **77**
7.5. Использование SpIDer Gate в режиме прокси **80**
8. Краткие инструкции **83**
9. Компоненты Dr.Web Gateway Security Suite **88**
9.1. Dr.Web ConfigD **88**
9.1.1. Принципы работы 88
9.1.2. Аргументы командной строки 90
9.1.3. Параметры конфигурации 91
9.2. Dr.Web Ctl **95**
9.2.1. Формат вызова из командной строки 96
9.2.2. Примеры использования 130
9.2.3. Параметры конфигурации 134
9.3. Веб-интерфейс управления Dr.Web **135**
9.3.1. Управление компонентами 137
9.3.2. Управление угрозами 138
9.3.3. Управление настройками 140
9.3.3.1. Управление централизованной защитой 146
9.3.4. Проверка локальных файлов 148
9.4. Dr.Web ICAPD **152**
9.4.1. Принципы работы 152
9.4.2. Аргументы командной строки 155
9.4.3. Параметры конфигурации 156
9.4.4. Обработка HTTP-сообщений на Lua 174
9.5. SpIDer Gate **193**
9.5.1. Принципы работы 195
9.5.2. Аргументы командной строки 196
9.5.3. Параметры конфигурации 196
9.6. Dr.Web Firewall для Linux **199**
9.6.1. Принципы работы 199
9.6.2. Аргументы командной строки 205
9.6.3. Параметры конфигурации 206
9.6.4. Обработка соединений на Lua 236
9.7. Dr.Web ClamD **246**
9.7.1. Принципы работы 246
9.7.2. Аргументы командной строки 247
9.7.3. Параметры конфигурации 248

9.7.4. Интеграция с внешними приложениями 254
9.8. Dr.Web File Checker 256
9.8.1. Принципы работы 256
9.8.2. Аргументы командной строки 257
9.8.3. Параметры конфигурации 258
9.9. Dr.Web Network Checker 261
9.9.1. Принципы работы 261
9.9.2. Аргументы командной строки 263
9.9.3. Параметры конфигурации 264
9.9.4. Организация сканирующего кластера 270
9.10. Dr.Web Scanning Engine 274
9.10.1. Принципы работы 274
9.10.2. Аргументы командной строки 276
9.10.3. Параметры конфигурации 279
9.11. Dr.Web Updater 282
9.11.1. Принципы работы 282
9.11.2. Аргументы командной строки 283
9.11.3. Параметры конфигурации 284
9.12. Dr.Web ES Agent 291
9.12.1. Принципы работы 291
9.12.2. Аргументы командной строки 292
9.12.3. Параметры конфигурации 293
9.13. Dr.Web HTTPD 296
9.13.1. Принципы работы 296
9.13.2. Аргументы командной строки 297
9.13.3. Параметры конфигурации 298
9.13.4. Описание HTTP API 302
9.14. Dr.Web SNMPD 326
9.14.1. Принципы работы 326
9.14.2. Аргументы командной строки 328
9.14.3. Параметры конфигурации 329
9.14.4. Интеграция с системами мониторинга 332
9.14.5. Dr.Web SNMP MIB 342
9.15. Dr.Web MeshD 368
9.15.1. Принципы работы 368
9.15.2. Аргументы командной строки 372

9.15.3. Параметры конфигурации 373
9.16. Dr.Web URL Checker 377
9.16.1. Принципы работы 377
9.16.2. Аргументы командной строки 377
9.16.3. Параметры конфигурации 378
9.17. Dr.Web CloudD 380
9.17.1. Принципы работы 380
9.17.2. Аргументы командной строки 381
9.17.3. Параметры конфигурации 382
9.18. Dr.Web LookupD 384
9.18.1. Принципы работы 384
9.18.2. Аргументы командной строки 386
9.18.3. Параметры конфигурации 387
9.19. Dr.Web StatD 403
9.19.1. Принципы работы 403
9.19.2. Аргументы командной строки 403
9.19.3. Параметры конфигурации 404
10. Приложения 406
10.1. Приложение А. Виды компьютерных угроз 406
10.2. Приложение Б. Устранение компьютерных угроз 412
10.3. Приложение В. Техническая поддержка 415
10.4. Приложение Г. Конфигурационный файл Dr.Web Gateway Security Suite 417
10.4.1. Структура файла 418
10.4.2. Типы параметров 419
10.4.3. Правила проверки трафика 422
10.5. Приложение Д. Генерация сертификатов SSL 445
10.6. Приложение Е. Описание известных ошибок 448
10.7. Приложение Ж. Список сокращений 504

1. Введение

Благодарим вас за приобретение решения Dr.Web Gateway Security Suite. Оно позволит вам обеспечить надежную защиту вашего сервера от распространения компьютерных угроз всех возможных типов, используя наиболее современные технологии обнаружения и обезвреживания угроз. Это повысит качество услуг, предоставляемых сервером.

Данное руководство предназначено для помощи администраторам серверов, работающих под управлением Unix-подобных ОС, таких как ОС семейства GNU/Linux и FreeBSD (далее в документе будет использовано обозначение Unix), в установке и использовании Dr.Web Gateway Security Suite.

Если у вас уже установлен Dr.Web Gateway Security Suite предыдущей версии, и вы желаете обновить его до актуальной версии, выполните на нее переход (см. раздел Переход на новую версию продукта).

2. Условные обозначения и сокращения

В данном руководстве используются следующие условные обозначения:

Обозначение	Комментарий
	Важное замечание или указание.
	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание.
Антивирусная сеть	Новый термин или акцент на термине в описаниях.
<IP-address>	Поля для замены функциональных названий фактическими значениями.
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
`/home/user`	Наименования файлов и каталогов, фрагменты программного кода.
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

Команды, которые требуется ввести с клавиатуры в командную строку операционной системы (в терминале или эмуляторе терминала), в руководстве предваряются символом приглашения к вводу `$` или `#`, определяющим, какие полномочия пользователя необходимы для исполнения указанной команды. Стандартным для Unix-систем образом подразумевается, что:

`$` — для исполнения команды достаточно обычных прав пользователя.

`#` — для исполнения команды требуются права суперпользователя (обычно — *root*). Для повышения прав можно использовать команды `su` и `sudo`.

Перечень сокращений приведен в разделе Приложение Ж. Список сокращений.

3. О продукте

Назначение

Dr.Web Gateway Security Suite создан для защиты интернет-шлюзов и/или прокси, работающих под управлением Unix-подобных ОС (GNU/Linux и FreeBSD) от вирусов и всех прочих видов вредоносного программного обеспечения, а также для предотвращения распространения через них угроз для различных платформ.

Основные компоненты (антивирусное ядро и вирусные базы) являются не только крайне эффективными и нетребовательными к системным ресурсам, но и кросс-платформенными, что позволяет специалистам компании «Доктор Веб» создавать надежные антивирусные решения, обеспечивающие защиту компьютеров и мобильных устройств, работающих под управлением распространенных операционных систем, от угроз, предназначенных для различных платформ. В настоящее время, наряду с Dr.Web Gateway Security Suite, в компании «Доктор Веб» разработаны также и другие антивирусные решения для Unix-подобных операционных систем (GNU/Linux и FreeBSD), macOS и Windows. Кроме того, разработаны антивирусные решения, обеспечивающие защиту мобильных устройств, работающих под управлением ОС Android, «Аврора».

Компоненты Dr.Web Gateway Security Suite постоянно обновляются, а вирусные базы и базы категорий веб-ресурсов регулярно дополняются новыми сигнатурами угроз, что обеспечивает актуальный уровень защищенности серверов, рабочих станций и мобильных устройств пользователей, а также используемых ими программ и данных. Для дополнительной защиты от неизвестного вредоносного программного обеспечения используются методы эвристического анализа, реализованные в антивирусном ядре, и обращение к облачному сервису Dr.Web Cloud, хранящему информацию о новейших угрозах, сигнатуры которых еще отсутствуют в базах.

Дополнительно:

- Основные функции Dr.Web Gateway Security Suite
- Структура Dr.Web Gateway Security Suite
- Помещение в карантин
- Полномочия для работы с файлами
- Режимы работы

3.1. Основные функции Dr.Web Gateway Security Suite

1. **Поиск и обезвреживание угроз.** Производится поиск как непосредственно вредоносных программ всех возможных типов (различных вирусов, включая вирусы, инфицирующие почтовые файлы и загрузочные записи дисков, а также троянских программ, почтовых червей и т. п.), так и нежелательных программ (рекламных

программ, программ-шуток, программ автоматического дозвона). Подробнее о видах угроз см. Приложение А. Виды компьютерных угроз.

Для обнаружения угроз используются:

- *сигнатурный анализ* — метод проверки, позволяющий обнаружить уже известные угрозы, информация о которых содержится в вирусных базах;
- *эвристический анализ* — набор методов проверки, позволяющих обнаруживать угрозы, которые еще неизвестны;
- *облачные технологии обнаружения угроз* — производится обращение к сервису Dr.Web Cloud, собирающему свежую информацию об актуальных угрозах, рассылаемую различными антивирусными продуктами Dr.Web.

Эвристический анализатор может ложно реагировать на программное обеспечение, не являющегося вредоносным. Поэтому объекты, содержащие обнаруженные им угрозы, получают специальный статус «подозрительные». Рекомендуется помещать такие файлы в карантин, а также передавать на анализ в антивирусную лабораторию «Доктор Веб». Подробнее о методах обезвреживания угроз см. Приложение Б. Устранение компьютерных угроз.

При проверке файловой системы по запросу пользователя имеется возможность как полной проверки всех объектов файловой системы, доступных пользователю, так и выборочной проверки только указанных объектов (отдельных каталогов или файлов, соответствующих указанным критериям). Кроме того, доступна возможность отдельной проверки загрузочных записей томов и исполняемых файлов, из которых запущены процессы, активные в системе в данный момент. В последнем случае при обнаружении угрозы выполняется не только обезвреживание вредоносного исполняемого файла, но и принудительное завершение работы всех процессов, запущенных из него. В системах, реализующих мандатную модель доступа к файлами с набором различных уровней доступа, сканирование файлов, недоступных на текущем уровне доступа, может производиться в специальном режиме автономного экземпляра.

Все объекты с угрозами, обнаруженные в файловой системе, регистрируются в постоянно хранимом реестре угроз, за исключением тех угроз, которые были обнаружены в режиме автономного экземпляра.

Утилита управления из командной строки Dr.Web Ctl, входящая в состав Dr.Web Gateway Security Suite, позволяет также выполнять проверку на наличие угроз файловых систем удаленных узлов сети, предоставляющих удаленный терминальный доступ через SSH или Telnet.

Вы можете использовать удаленное сканирование только для обнаружения вредоносных или подозрительных файлов на удаленном узле. Для устранения обнаруженных угроз на удаленном узле необходимо воспользоваться средствами управления, предоставляемыми непосредственно этим узлом. Например, на роутерах и прочих «умных» устройствах вы можете воспользоваться механизмом обновления прошивки, а на вычислительных машинах — подключитесь к ним (в том числе в удаленном терминальном режиме) и произведите соответствующие операции в их файловой системе (удаление или перемещение файлов и т. п.) или запустите антивирусное программное обеспечение (ПО), установленное на них.

2. **Анализ данных, передаваемых в интернет**. Отслеживаются и проверяются как запросы пользователей (т. е. попытки подключиться к веб-серверу и загрузить на него некоторый файл), так и непосредственно данные, направляемые веб-серверами в ответ на запросы пользователей. Для анализа запросов и возвращаемых данных, Dr.Web Gateway Security Suite подключается по протоколу ICAP как внешний фильтр к прокси-серверу, обрабатывающему HTTP-соединения пользователей локальной сети. Кроме того, при помощи компонента SpIDer Gate можно реализовать функции барьера, предотвращающего прием и передачу инфицированных файлов публичным веб-сервером организации (*данная возможность доступна только в ОС* GNU/Linux). Для ограничения доступа к нежелательным сайтам используются как автоматически обновляемая база данных, содержащая перечень веб-ресурсов, разбитых на категории, поставляемая вместе с Dr.Web Gateway Security Suite, так и черные и белые списки, ведущиеся системным администратором вручную. Также производится обращение к сервису Dr.Web Cloud для проверки наличия информации, не отмечен ли веб-ресурс, к которому пытается обратиться пользователь, как вредоносный, другими антивирусными продуктами Dr.Web.
3. **Надежная изоляция инфицированных или подозрительных объектов**, обнаруженных в файловой системе сервера, в специальном хранилище — карантине, чтобы они не могли нанести ущерба системе. При перемещении объектов в карантин они специальным образом переименовываются и могут быть восстановлены в исходное место (в случае необходимости) только по команде пользователя.

   Угрозы, обнаруженные компонентом Dr.Web ICAPD в сообщениях протокола HTTP, не перемещаются в карантин на интернет-шлюзе. Вместо этого блокируется их загрузка и передача получателю, о чем он информируется путем отправки ему специальной HTML-страницы с сообщением о блокировке.
4. **Автоматическое обновление** антивирусного ядра, содержимого вирусных баз, базы категорий веб-ресурсов для поддержания высокого уровня надежности защиты от вредоносных программ.
5. **Сбор статистики** проверок и инцидентов, связанных с вредоносным ПО. Ведение журнала обнаруженных угроз. Отправка уведомлений об обнаруженных угрозах по SNMP внешним системам мониторинга и серверу централизованной защиты, если Dr.Web Gateway Security Suite работает в режиме централизованной защиты, а также облачному сервису Dr.Web Cloud.
6. **Обеспечение работы под управлением сервера централизованной защиты** для применения на сервере единых политик безопасности, принятых в некоторой сети, в

состав которой он входит. Это может быть как сеть некоторого предприятия (корпоративная сеть) или частная сеть VPN, так и сеть, организованная провайдером каких-либо услуг, например, доступа к интернету.

3.2. Структура Dr.Web Gateway Security Suite

Dr.Web Gateway Security Suite представляет собой программный комплекс, состоящий из набора компонентов, каждый из которых выполняет свой набор функций. В соответствии с задачами, решаемыми компонентами, они разделены на категории:

- Базовые антивирусные компоненты, образующие ядро продукта Dr.Web Gateway Security Suite. При отсутствии компонентов этой категории продукт не может выполнять сканирование файлов (и иных данных) на предмет наличия вирусов и иных угроз.
- Компоненты поиска угроз. Данные компоненты используются для решения базовых задач Dr.Web Gateway Security Suite — поиска вредоносных и потенциально опасных объектов. В своей работе компоненты этой категории используют базовые антивирусные компоненты.
- Сервисные компоненты, решающие вспомогательные задачи для поддержки антивирусной защиты (обновление вирусных баз, подключение к серверам централизованной защиты, общая координация работы компонентов Dr.Web Gateway Security Suite и т. д.).
- Интерфейсные компоненты, предоставляющие (пользователю или сторонним приложениям) интерфейс для управления работой Dr.Web Gateway Security Suite.

Перечень компонентов, входящих в состав Dr.Web Gateway Security Suite, перечислен в таблицах ниже.

1. Базовые антивирусные компоненты

Компонент	Описание
Dr.Web Virus-Finding Engine	Антивирусное ядро. Реализует алгоритмы поиска и распознавания вирусов и прочих вредоносных программ (используя сигнатурный и эвристический анализ). Работает под управлением компонента Dr.Web Scanning Engine Файл библиотеки: `drweb32.dll`. Внутреннее наименование, выводимое в журнал: `CoreEngine`
Dr.Web Scanning Engine	Сканирующее ядро. Компонент, отвечающий за загрузку антивирусного ядра Dr.Web Virus-Finding Engine и вирусных баз. • Передает антивирусному ядру на проверку содержимое файлов и загрузочных записей дисковых устройств. • Организует очередь файлов, ожидающих проверки.

Компонент	Описание
	• Выполняет лечение тех угроз, для которых данное действие применимо. Может работать как под управлением демона Dr.Web ConfigD, так и в автономном режиме. Используется компонентами Dr.Web File Checker и Dr.Web Network Checker. Также может использоваться компонентом Dr.Web MeshD (в некоторых режимах работы) и внешними (по отношению к Dr.Web Gateway Security Suite) приложениями, использующими непосредственно API Dr.Web Scanning Engine Исполняемый файл компонента: `drweb-se`. Внутреннее наименование, выводимое в журнал: `ScanEngine`
Вирусные базы	Автоматически обновляемая база данных сигнатур вирусов и прочих угроз, а также алгоритмов распознавания и нейтрализации вредоносного программного обеспечения. Используется антивирусным ядром Dr.Web Virus-Finding Engine и поставляется совместно с ним
Базы категорий веб-ресурсов	Автоматически обновляемая база данных, содержащая перечень веб-ресурсов, разбитых на категории, и используемая для идентификации нежелательных сайтов. Используется компонентами, проверяющими сетевую активность пользователей и приложений, такими как SpIDer Gate, Dr.Web ICAPD
Dr.Web File Checker	Компонент проверки объектов файловой системы и менеджер карантина. • Принимает от компонента поиска угроз задания на проверку файлов, находящихся в локальной (по отношению к Dr.Web Scanning Engine) файловой системе. • Обходит каталоги файловой системы согласно заданию, передает файлы на проверку сканирующему ядру Dr.Web Scanning Engine и оповещает компоненты-клиенты о ходе проверки. • Выполняет удаление инфицированных файлов, перемещение их в карантин и восстановление из карантина, управляет каталогами карантина. • Организует и содержит в актуальном состоянии кеш, хранящий информацию о ранее проверенных файлах для уменьшения частоты повторных проверок файлов. Используется компонентами, проверяющими объекты файловой системы Исполняемый файл компонента: `drweb-filecheck`. Внутреннее наименование, выводимое в журнал: `FileCheck`
Dr.Web Network Checker	Агент сетевой проверки данных.

Компонент	Описание
	• Используется для передачи на проверку в сканирующее ядро данных, отправленных компонентами программного комплекса через сеть (это такие компоненты, как Dr.Web ClamD, SpIDer Gate, Dr.Web ICAPD). • Позволяет Dr.Web Gateway Security Suite организовывать распределенную проверку данных: принимать на проверку данные с удаленных узлов сети и передавать локальные данные на проверку на удаленные узлы сети. Для приема и передачи данных на удаленных узлах также должен функционировать антивирусный продукт Dr.Web для операционных систем семейства Unix. В режиме распределенной проверки позволяет автоматически распределять интенсивность антивирусного сканирования по доступным узлам, снижая нагрузку на узлы с большим объемом проверки (например, выполняющих роль почтовых серверов и интернет-шлюзов). При наличии в сети узлов-партнеров, способных принимать данные на проверку, компоненты, использующие Dr.Web Network Checker для проверки, могут не использовать мощности локального сканирующего ядра Dr.Web Scanning Engine. Таким образом, локальное сканирующее ядро Dr.Web Scanning Engine, Dr.Web Virus-Finding Engine и вирусные базы могут отсутствовать. Для обеспечения безопасности при передаче файлов по сети использует SSL Исполняемый файл компонента: `drweb-netcheck`. Внутреннее наименование, выводимое в журнал: `NetCheck`
Dr.Web URL Checker	Компонент для анализа URL на предмет принадлежности к нежелательным или потенциально опасным категориям Исполняемый файл компонента: `drweb-urlcheck`. Внутреннее наименование, выводимое в журнал: `UrlCheck`
Dr.Web MeshD	Компонент, осуществляющий подключение продукта Dr.Web Gateway Security Suite к локальному облаку, позволяющему продуктам Dr.Web для Unix обмениваться обновлениями, результатами проверки файлов, передавать друг другу на проверку файлы, а также предоставлять услуги сканирующего ядра напрямую. При наличии этого компонента в составе продукта и при наличии в составе локального облака, к которому он подключен, узлов, предоставляющих услуги сканирующего ядра, локальное сканирующее ядро Dr.Web Scanning Engine, Dr.Web Virus-Finding Engine и вирусные базы могут отсутствовать Исполняемый файл компонента: `drweb-meshd`. Внутреннее наименование, выводимое в журнал: `MeshD`

2. Компоненты поиска угроз

Компонент	Описание
Dr.Web ICAPD	ICAP-сервер, выполняющий анализ запросов и трафика, проходящего через прокси-серверы HTTP, поддерживающие ICAP (такие как Squid). Предотвращает передачу инфицированных файлов и доступ к узлам сети, относящимся к нежелательным категориям веб-ресурсов или внесенным в черные списки, формируемые системным администратором. При запрете доступа к внешним серверам и при обнаружении угроз в передаваемых данных формирует специальную веб-страницу, содержащую сообщение о невозможности доступа к запрошенному ресурсу или загрузки инфицированного файла, которую прокси-сервер возвращает клиенту. Для проверки данных, получаемых от прокси-сервера, использует компонент Dr.Web Network Checker Исполняемый файл компонента: `drweb-icapd`. Внутреннее наименование, выводимое в журнал: `ICAPD`
SpIDer Gate	Компонент проверки сетевого трафика и URL. Предназначен для проверки данных, загружаемых на локальный узел из сети и передаваемых с него во внешнюю сеть, на наличие угроз, и предотвращения соединения с узлами сети, внесенными как в нежелательные категории веб-ресурсов, так и в черные списки, формируемые системным администратором. Для проверки получаемых данных использует компонент Dr.Web Network Checker. При наличии соответствующего разрешения от пользователя посылает запрашиваемые им URL на проверку в сервис Dr.Web Cloud. Поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux. Исполняемый файл компонента: `drweb-gated`. Внутреннее наименование, выводимое в журнал: `GateD`
Dr.Web Firewall для Linux	Менеджер сетевых соединений. Используется SpIDer Gate и обеспечивает прохождение через него соединений, устанавливаемых приложениями, работающими на узле, для проверки передаваемого через них трафика.

Компонент	Описание
	Поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux. Исполняемый файл компонента: `drweb-firewall`. Внутреннее наименование, выводимое в журнал: `LinuxFirewall`

3. Сервисные компоненты

Компонент	Описание
Dr.Web CloudD	Компонент взаимодействия с облаком Dr.Web Cloud. Отправляет URL, посещаемые пользователем, а также сведения о проверяемых файлах, в облачный сервис Dr.Web Cloud для их проверки на наличие угроз, информация о которых пока отсутствует в вирусных базах Исполняемый файл компонента: `drweb-cloudd`. Внутреннее наименование, выводимое в журнал: `CloudD`
Dr.Web ConfigD	Демон управления конфигурацией комплекса Dr.Web Gateway Security Suite. • Управляет активностью (запуск и остановка) других компонентов программного комплекса в зависимости от настроек. • Перезапускает компоненты, завершившие работу в результате сбоя, запускает одни компоненты комплекса по требованию других, информирует компоненты продукта об изменении состава запущенных компонентов. • Хранит и предоставляет всем компонентам информацию об имеющихся лицензионных ключах и настройках. Получает измененные настройки и ключи от уполномоченных компонентов Dr.Web Gateway Security Suite и оповещает все компоненты об изменении лицензионных ключей и настроек Исполняемый файл компонента: `drweb-configd`. Внутреннее наименование, выводимое в журнал: `ConfigD`
Dr.Web ES Agent	Агент централизованной защиты. Обеспечивает работу программного комплекса в централизованном и мобильном режимах. • Организует связь с сервером централизованной защиты, получает от него лицензионный ключевой файл, обновления вирусных баз и антивирусного ядра.

Компонент	Описание
	• Передает на сервер информацию о составе и состоянии компонентов Dr.Web Gateway Security Suite и накопленную статистику инцидентов, связанных с вредоносным ПО Исполняемый файл компонента: `drweb-esagent`. Внутреннее наименование, выводимое в журнал: `ESAgent`
Dr.Web LookupD	Компонент получения внешних данных. Осуществляет выборку данных из внешних хранилищ данных (служб каталогов, файлов, реляционных баз данных и т. п.), для использования их в правилах проверки сетевого трафика пользователей Исполняемый файл компонента: `drweb-lookupd`. Внутреннее наименование, выводимое в журнал: `LookupD`
Dr.Web StatD	Компонент для хранения статистики событий компонентов Dr.Web Gateway Security Suite. Получает и организует хранение событий, поступающих от компонентов программного комплекса, таких как неожиданное завершение работы, обнаружение угрозы и др. Исполняемый файл компонента: `drweb-statd`. Внутреннее наименование, выводимое в журнал: `StatD`
Dr.Web Updater	Компонент обновления. Отвечает за загрузку с серверов обновлений компании «Доктор Веб» обновлений для вирусных баз и баз категорий веб-ресурсов, антивирусного ядра. Обновления могут загружаться как автоматически, по расписанию, так и непосредственно по команде пользователя (через утилиту Dr.Web Ctl или через веб-интерфейс управления) Исполняемый файл компонента: `drweb-update`. Внутреннее наименование, выводимое в журнал: `Update`

4. Интерфейсные компоненты

Компонент	Описание
Dr.Web HTTPD	Веб-сервер управления компонентами Dr.Web Gateway Security Suite. Предоставляет специализированный HTTP API для управления компонентами Dr.Web Gateway Security Suite. Указанный API используется веб-интерфейсом управления.

Компонент	Описание
	Для обеспечения безопасности при подключении к веб-интерфейсу управления использует протокол HTTPS. Для передачи данных на проверку в Dr.Web Scanning Engine использует Dr.Web Network Checker Исполняемый файл компонента: `drweb-httpd`. Внутреннее наименование, выводимое в журнал: `HTTPD`
Веб-интерфейс управления Dr.Web	Веб-интерфейс управления. Может быть открыт в любом браузере на локальном или удаленном узле сети. Наличие веб-интерфейса управления позволяет продукту не использовать сторонние веб-серверы (такие, например, как Apache HTTP Server) и утилиты удаленного администрирования наподобие Webmin. Работоспособность обеспечивается веб-сервером Dr.Web HTTPD
Dr.Web Ctl	Утилита, обеспечивающая интерфейс управления Dr.Web Gateway Security Suite из командной строки. Позволяет осуществлять запуск проверки файлов, просматривать содержимое карантина и управлять им, запускать обновление вирусных баз, подключать Dr.Web Gateway Security Suite к серверу централизованной защиты и отключаться от него, просматривать и изменять значения параметров конфигурации программного комплекса Исполняемый файл компонента: `drweb-ctl`. Внутреннее наименование, выводимое в журнал: `Ctl`
Dr.Web SNMPD	Представляет собой SNMP-агент. Предназначен для интеграции Dr.Web Gateway Security Suite с внешними системами мониторинга посредством протокола SNMP. Такая интеграция позволяет отслеживать состояние работы компонентов комплекса, а также собирать статистику обнаружения и нейтрализации угроз. Поддерживает протоколы SNMP v2c и v3 Исполняемый файл компонента: `drweb-snmpd`. Внутреннее наименование, выводимое в журнал: `SNMPD`
Dr.Web ClamD	Компонент, эмулирующий интерфейс антивирусного демона `clamd` (компонент антивирусного продукта ClamAV®). Позволяет прозрачно использовать Dr.Web Gateway Security Suite для антивирусной проверки любым приложениям, которые могут использовать антивирусный продукт ClamAV®. Для передачи данных на проверку в Dr.Web Scanning Engine, в зависимости от режима, использует Dr.Web File Checker или Dr.Web Network Checker

Компонент	Описание
	Исполняемый файл компонента: `drweb-clamd`. Внутреннее наименование, выводимое в журнал: `ClamD`

На рисунке ниже показана структура Dr.Web Gateway Security Suite и его взаимодействия с внешними приложениями.

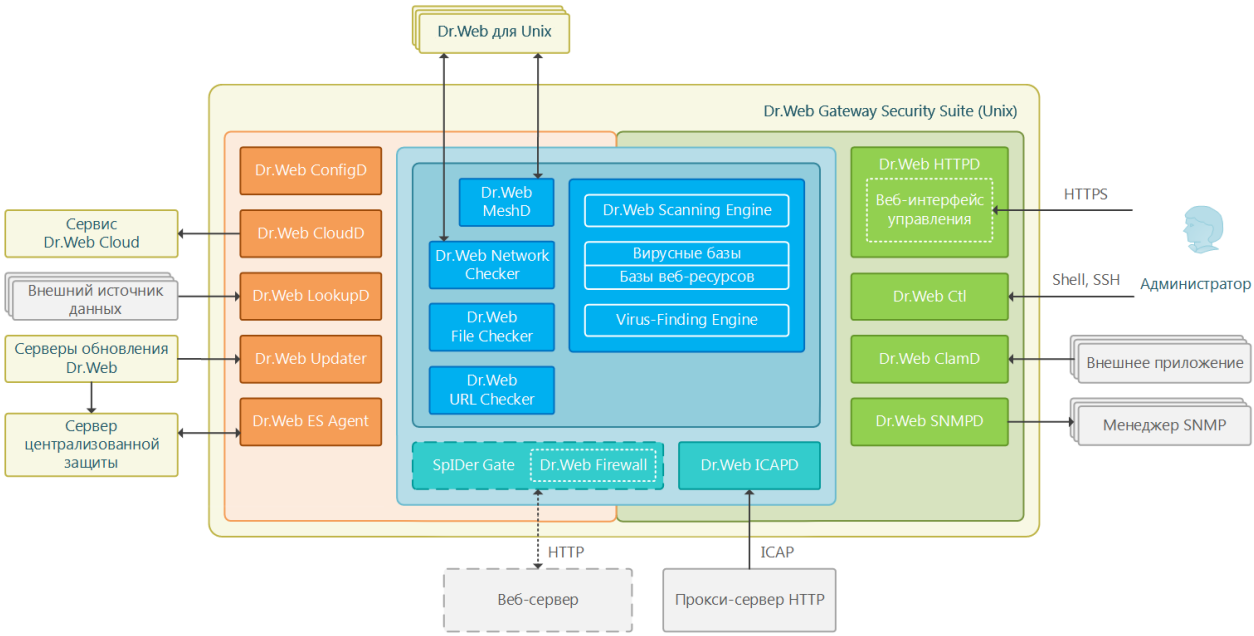

Рисунок 1. Структура Dr.Web Gateway Security Suite

На приведенном рисунке использованы следующие обозначения:

	Dr.Web Gateway Security Suite в целом и внешние по отношению к нему программные продукты Dr.Web, не входящие непосредственно в его состав
	Внешние по отношению к Dr.Web Gateway Security Suite программы и программные комплексы, с которыми он интегрируется
	Сервисные компоненты, решающие конкретные задачи в рамках антивирусной защиты (обновление вирусных баз, подключение к серверам централизованной защиты, общая координация работы и т. д.)
	Компоненты, предоставляющие (пользователю или сторонним приложениям) интерфейс для управления работой Dr.Web Gateway Security Suite
	Компоненты, используемые для антивирусной проверки
	Базовые антивирусные компоненты, образующие ядро Dr.Web Gateway Security Suite. Используются компонентами, осуществляющими проверку файлов и данных

Компоненты, обозначенные пунктирной границей, могут отсутствовать, в зависимости от поставки или сценария использования Dr.Web Gateway Security Suite.

Более подробно компоненты Dr.Web Gateway Security Suite описаны в разделе Компоненты Dr.Web Gateway Security Suite.

3.3. Помещение в карантин

Карантин Dr.Web Gateway Security Suite представляет собой систему каталогов, предназначенных для надежной изоляции файлов, содержащих выявленные угрозы, которые в данный момент не могут быть обезврежены по каким-либо причинам. Например, обнаруженная угроза может быть неизлечимой, потому что еще неизвестна Dr.Web Gateway Security Suite (например, она была обнаружена эвристическим анализатором, а в вирусных базах ее сигнатура, а следовательно, и метод лечения, отсутствует), или при попытке ее лечения возникают ошибки. Кроме того, файл может быть перемещен в карантин непосредственно по желанию пользователя, если он выбрал соответствующее действие в списке обнаруженных угроз или указал его как реакцию на угрозы определенного типа.

Когда файл, содержащий угрозу, перемещается в карантин, он специальным образом переименовывается, чтобы предотвратить возможность его идентификации пользователями и программами, и затруднить доступ к нему, минуя инструменты работы с карантином, реализованные в Dr.Web Gateway Security Suite. Кроме того, при перемещении файла в карантин у него всегда сбрасывается бит исполнения для предотвращения запуска.

Каталоги карантина размещаются:

- *в домашнем каталоге пользователя* (если на данном компьютере имеется несколько учетных записей разных пользователей, то в домашнем каталоге каждого из этих пользователей может быть создан свой собственный каталог карантина);
- *в корневом каталоге каждого логического тома,* смонтированного в файловой системе.

Каталоги карантина Dr.Web Gateway Security Suite всегда имеют имя `.com.drweb.quarantine` и создаются по мере необходимости в тот момент, когда к какой-либо угрозе применяется действие «**В карантин**» (`QUARANTINE`), другими словами, до тех пор, пока угроз не обнаружено, каталоги карантина не создаются. При этом всегда создается только тот каталог карантина, который требуется для изоляции файла. Для определения, в какой из каталогов требуется изолировать файл, используется имя владельца файла. Если при движении к корню файловой системы `/` от каталога, содержащего файл, достигается домашний каталог владельца, файл изолируется в каталог карантина, находящийся в нем. В противном случае файл будет изолирован в каталог карантина, созданный в корне тома, содержащего файл (корневой каталог тома необязательно совпадет с корнем файловой системы). Таким образом, любой инфицированный файл, помещаемый в карантин, всегда остается на том томе, на котором он был обнаружен. Это обеспечивает корректную работу карантина при наличии в системе съемных накопителей и других томов, которые могут монтироваться в файловой системе периодически и в различные точки.

Пользователь может управлять содержимым карантина из командной строки, используя утилиту Dr.Web Ctl или через веб-интерфейс управления. При этом всегда обрабатывается консолидированный карантин, объединяющий в себе все каталоги с изолированными объектами, доступные в данный момент. С точки зрения пользователя, просматривающего содержимое консолидированного карантина, каталог карантина, располагающийся в его домашнем каталоге, называется *Пользовательским* карантином, а все остальные каталоги карантина считаются *Системным* карантином.

Работа с карантином возможна даже тогда, когда отсутствует активная лицензия, но в этом случае становится невозможным лечение изолированных объектов.

Не все антивирусные компоненты Dr.Web Gateway Security Suite используют карантин для изоляции угроз. Например, его не используют компоненты Dr.Web ClamD и Dr.Web ICAPD.

3.4. Полномочия для работы с файлами

При сканировании объектов файловой системы и нейтрализации угроз Dr.Web Gateway Security Suite (точнее, пользователь, от имени которого он запущен) должен обладать следующими полномочиями:

Действие	**Требуемые полномочия**
Вывод всех обнаруженных угроз	Без ограничений. Специальных полномочий не требуется.
Вывод содержимого контейнера (архива, почтового файла и т. п.) (Отображение только элементов, которые содержат ошибку или угрозу)	Без ограничений. Специальных полномочий не требуется.
Перемещение в карантин	Без ограничений. Пользователь может отправлять в карантин все инфицированные файлы, независимо от наличия у него прав на чтение и запись для перемещаемого файла.
Удаление угроз	Пользователь должен иметь права на запись в удаляемый файл. Если угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т. п.), вместо удаления выполняется перемещение контейнера в карантин.

Действие	Требуемые полномочия
Лечение файлов	Без ограничений. После выполнения лечения остается вылеченный файл с исходными правами доступа и владельцем. Файл может быть удален, если удаление является методом лечения обнаруженной в нем угрозы.
Восстановление файла из карантина	Пользователь должен иметь разрешение на чтение восстанавливаемого файла и иметь разрешение выполнять запись в каталог восстановления.
Удаление файла из карантина	Пользователь должен иметь разрешение на запись в исходный файл, который был перемещен в карантин.

Для запуска утилиты управления из командной строки Dr.Web Ctl с правами суперпользователя (обычно *root*) вы можете воспользоваться командой смены пользователя `su` или командой выполнения от имени другого пользователя `sudo`.

3.5. Режимы работы

В этом разделе

- Принципы централизованной защиты
- Подключение к серверу централизованной защиты
- Отключение от сервера централизованной защиты

Dr.Web Gateway Security Suite может работать как в автономном режиме, так и в составе корпоративной или частной *антивирусной сети,* управляемой каким-либо *сервером централизованной защиты.* Такой режим работы называется *режимом централизованной защиты.* Использование этого режима не требует установки дополнительного программного обеспечения, переустановки или удаления Dr.Web Gateway Security Suite.

- В *автономном режиме* защищаемый компьютер не включен в антивирусную сеть и управляется локально. В этом режиме конфигурационный и лицензионный ключевой файлы находятся на локальных дисках, а Dr.Web Gateway Security Suite полностью управляется с защищаемого компьютера. Обновления вирусных баз получаются с серверов обновлений компании «Доктор Веб».
- В *режиме централизованной защиты* защитой компьютера управляет сервер централизованной защиты. В этом режиме некоторые функции и настройки Dr.Web Gateway Security Suite могут быть изменены или заблокированы в соответствии с общей (корпоративной) стратегией антивирусной защиты, принятой в антивирусной сети. В этом режиме на компьютере используется особый лицензионный ключевой файл, полученный от выбранного сервера централизованной защиты, к которому

подключен Dr.Web Gateway Security Suite. Лицензионный или демонстрационный ключевой файл пользователя, если он имеется на локальном компьютере, не используется. На сервер централизованной защиты отсылается статистика работы Dr.Web Gateway Security Suite, включая статистику инцидентов, связанных с вредоносным ПО. Обновление вирусных баз также выполняется с сервера централизованной защиты.

- В *мобильном режиме* Dr.Web Gateway Security Suite получает обновления вирусных баз с серверов обновлений компании «Доктор Веб», но использует локально хранящиеся настройки и особый лицензионный ключевой файл, полученные от сервера централизованной защиты.

Возможность настройки монитора файловой системы SpIDer Guard, а также его включения и выключения при работе Dr.Web Gateway Security Suite под управлением сервера централизованной защиты зависит от разрешений, заданных на сервере.

Принципы централизованной защиты

Решения компании «Доктор Веб» по организации централизованной антивирусной защиты имеют клиент-серверную архитектуру (см. иллюстрацию ниже).

Компьютеры компании или пользователей поставщика IT-услуг защищаются от угроз *локальными антивирусными компонентами* (в данном случае продуктом Dr.Web Gateway Security Suite), которые обеспечивают антивирусную защиту и поддерживают соединение с сервером централизованной защиты.

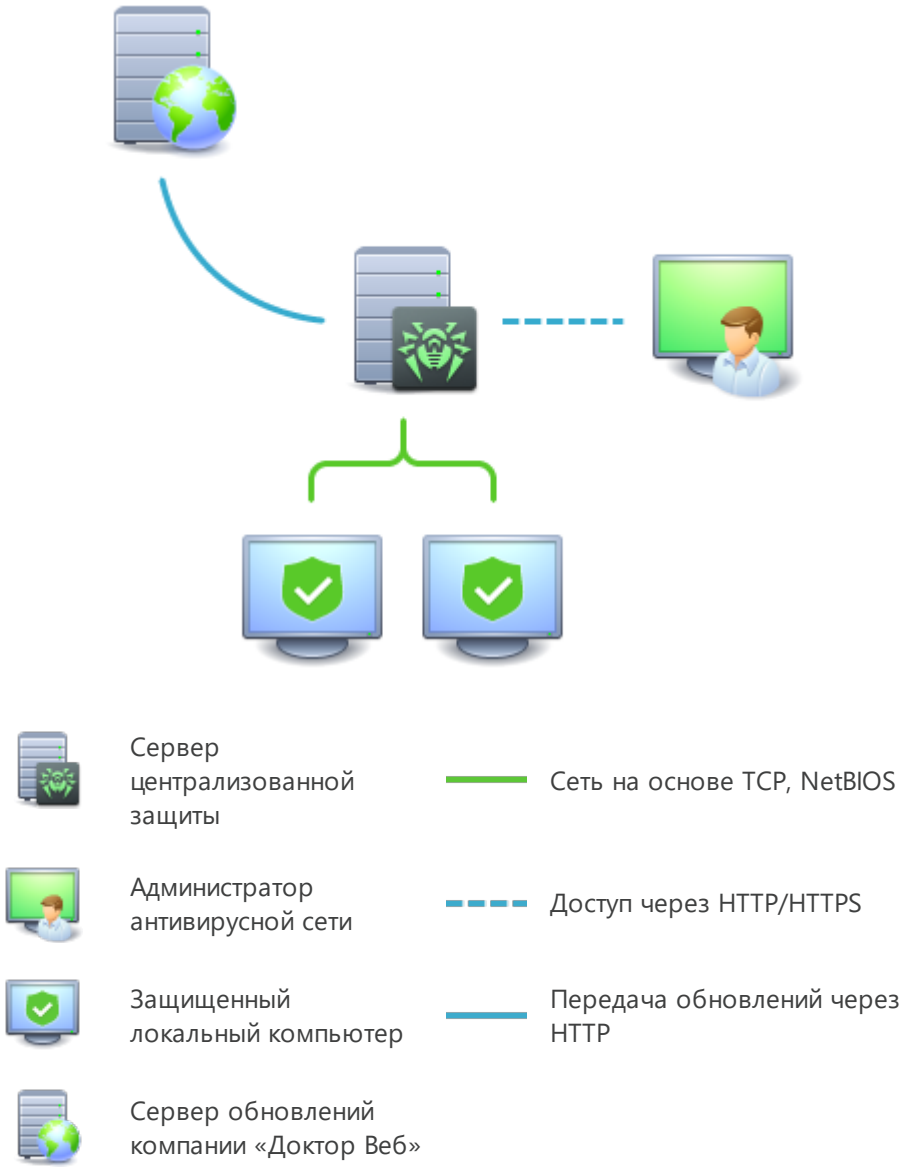

Рисунок 2. Логическая структура антивирусной сети

Обновление и конфигурация локальных компонентов производится через *сервер централизованной защиты*. Весь поток команд, данных и статистической информации в антивирусной сети также проходит через сервер централизованной защиты. Объем трафика между защищенными компьютерами и сервером централизованной защиты может быть весьма значительным, поэтому предусматривается возможность его сжатия. Использование шифрования при передаче данных позволяет избежать разглашения ценных сведений и подмены программного обеспечения, загружаемого на защищенные компьютеры.

Все необходимые обновления загружаются на сервер централизованной защиты с серверов обновлений компании «Доктор Веб».

Изменения в конфигурации локальных антивирусных компонентов и передача команд осуществляется сервером централизованной защиты по указанию администраторов

антивирусной сети. Администраторы управляют конфигурацией сервера централизованной защиты и формированием антивирусной сети (в частности, подтверждают правомерность подключения локальной станции к сети), а также, при необходимости, задают настройки работы конкретных локальных антивирусных компонентов.

Локальные антивирусные компоненты несовместимы с антивирусным программным обеспечением как других компаний, так и антивирусными решениями Dr.Web, не поддерживающими режим централизованной защиты (например, антивирус Dr.Web версии 5.0). Установка двух антивирусных программ на одном компьютере может привести к отказу системы или потере важных данных.

В режиме централизованной защиты возможен экспорт и сохранение отчетов о функционировании Dr.Web Gateway Security Suite с помощью сервера централизованной защиты. Поддерживается экспорт и сохранение отчетов в форматах HTML, CSV, PDF и XML.

Подключение к серверу централизованной защиты

Dr.Web Gateway Security Suite может быть подключен к серверу централизованной защиты антивирусной сети при помощи команды `esconnect` утилиты управления из командной строки `drweb-ctl`.

Для верификации сервера централизованной защиты используется сертификат, соответствующий уникальному открытому ключу шифрования, используемому сервером. По умолчанию агент централизованной защиты Dr.Web ES Agent не позволит произвести подключение к серверу, если вы не укажете файл сертификата сервера, к которому производится подключение. Файл сертификата необходимо предварительно получить у администратора антивирусной сети, обслуживаемой сервером, к которому вы хотите подключить Dr.Web Gateway Security Suite.

Если Dr.Web Gateway Security Suite подключен к серверу централизованной защиты, то имеется возможность перевести его в мобильный режим и вернуть назад в режим централизованной защиты. Включение и выключение мобильного режима регулируется параметром конфигурации `MobileMode` компонента Dr.Web ES Agent.

Возможность перехода Dr.Web Gateway Security Suite в мобильный режим работы зависит от разрешений, заданных на используемом сервере централизованной защиты.

Отключение от сервера централизованной защиты

Dr.Web Gateway Security Suite может быть отключен от сервера централизованной защиты антивирусной сети при помощи команды `esdisconnect` утилиты управления из командной строки `drweb-ctl`.

4. Системные требования и совместимость

В этом разделе

- Системные требования
- Перечень поддерживаемых версий ОС
  - GNU/Linux
  - FreeBSD
- Дополнительные пакеты и компоненты
- Ограничения совместимости
- Поддерживаемые прокси-серверы HTTP
- Совместимость с подсистемами безопасности

Системные требования

Использование Dr.Web Gateway Security Suite возможно на компьютере, удовлетворяющем следующим требованиям:

Параметр	Требования
Платформа	Поддерживаются процессоры следующих архитектур и систем команд: • Intel/AMD: 32-бит (*IA-32*, *x86*); 64-бит (*x86-64*, *x64*, *amd64*); • ARM64; • E2K (*Эльбрус*); • IBM POWER9, Power10 (*ppc64el*)
Оперативная память	Не менее 500 МБ свободной оперативной памяти (рекомендуется 1 ГБ и более)
Место на жестком диске	Не менее 2 ГБ свободного дискового пространства на томе, на котором размещаются каталоги устанавливаемого продукта
Операционная система	GNU/Linux (на основе ядра версии 2.6.37 или более поздней, использующая библиотеку `glibc` версии 2.13 или более поздней, систему инициализации `systemd` версии 209 или более позднюю), FreeBSD. Перечень поддерживаемых версий операционных систем приведен ниже. Операционная система должна поддерживать механизм аутентификации PAM
Прочее	Наличие сетевого подключения: • подключение к интернету для обновления вирусных баз и компонентов антивирусного продукта; • при работе в режиме централизованной защиты достаточно только подключения к используемому серверу в рамках локальной сети, доступ в интернет не требуется

Для корректной работы компонента Dr.Web Firewall для Linux ядро ОС должно быть собрано со включением следующих опций:

- *CONFIG_NETLINK_DIAG, CONFIG_INET_TCP_DIAG;*
- *CONFIG_NF_CONNTRACK_IPV4, CONFIG_NF_CONNTRACK_IPV6, CONFIG_NF_CONNTRACK_EVENTS;*
- *CONFIG_NETFILTER_NETLINK_QUEUE, CONFIG_NETFILTER_NETLINK_QUEUE_CT, CONFIG_NETFILTER_XT_MARK.*

Конкретный набор требуемых опций из указанного перечня может зависеть от используемой версии ОС.

Для обеспечения правильной работы Dr.Web Gateway Security Suite должны быть открыты следующие порты:

Назначение	Направление	Номера портов
Для получения обновлений	исходящий	80
Для соединения с облачным сервисом Dr.Web Cloud	исходящий	2075 (в том числе для UDP), 3010 (TCP), 3020 (TCP), 3030 (TCP), 3040 (TCP)

Перечень поддерживаемых версий операционных систем

GNU/Linux

Платформа	Поддерживаемые версии GNU/Linux
x86_64	• Astra Linux Common Edition (Орел) 2.12; • Astra Linux Special Edition 1.6 (с кумулятивным патчем 20200722SE16), 1.7, 1.8; • CentOS 7, 8; • Debian 9, 10, 11, 12; • Fedora 37, 38; • Red Hat Enterprise Linux 7, 8; • SUSE Linux Enterprise Server 12 SP3; • Ubuntu 18.04, 20.04, 22.04, 24.04; • Альт 8 СП; • Альт Рабочая станция 9, 10; • Альт Сервер 9, 10; • Гослинукс IC6;

Платформа	Поддерживаемые версии GNU/Linux
	• РЕД ОС 7.2 МУРОМ, РЕД ОС 7.3 МУРОМ, РЕД ОС 8
x86	• CentOS 7; • Debian 10; • Альт 8 СП; • Альт Рабочая станция 9, 10
ARM64	• Astra Linux Special Edition (Новороссийск) 4.7; • CentOS 7, 8; • Debian 11, 12; • Ubuntu 18.04; • Альт 8 СП; • Альт Рабочая станция 9, 10; • Альт Сервер 9, 10
E2K	• Astra Linux Special Edition (Ленинград) 8.1 (с кумулятивным патчем 20200429SE81); • Альт 8 СП; • Альт Рабочая станция 10; • Альт Сервер 10; • ОПО ВК Эльбрус-8.32 ТВГИ.00311-28; • Эльбрус-Д МЦСТ 1.4
ppc64el	• CentOS 8; • Ubuntu 20.04

В ОС Альт 8 СП, Эльбрус-Д МЦСТ 1.4 и Гослинукс IC6 работа с мандатными уровнями доступа не поддерживается.

Для прочих версий GNU/Linux, соответствующих описанным требованиям, полная совместимость с Dr.Web Gateway Security Suite не гарантируется. При возникновении проблем с совместимостью с вашим дистрибутивом обратитесь в техническую поддержку.

FreeBSD

Платформа	Поддерживаемые версии FreeBSD
x86	11, 12, 13, 14
x86_64	11, 12, 13, 14

Для ОС FreeBSD установка Dr.Web Gateway Security Suite возможна только из универсального пакета.

Для корректной работы Dr.Web Gateway Security Suite в ОС FreeBSD 13 и 14 необходимо установить пакет совместимости `compat12x`.

Дополнительные пакеты и компоненты

Dr.Web Gateway Security Suite не требует установки дополнительных пакетов и компонентов ОС (кроме программного обеспечения защищаемого серверного решения, см. ниже).

Для удобной работы с Dr.Web Gateway Security Suite из командной строки рекомендуется включить автодополнение команд в используемой командной оболочке, если оно не включено.

В случае возникновения проблем с установкой требуемых дополнительных пакетов и компонентов обратитесь к справочным руководствам используемой вами версии операционной системы.

Ограничения совместимости

- Компонент SpIDer Gate *может конфликтовать* с другими брандмауэрами, установленными в вашей ОС (такими, как Shorewall и SuseFirewall2 в ОС SUSE Linux Enterprise Server и FirewallD в ОС Fedora, CentOS, Red Hat Enterprise Linux). Признаком наличия конфликта является сообщение об ошибке SpIDer Gate с кодом x109 или сообщение об ошибке Dr.Web Firewall для Linux с кодом x102. Способы устранения конфликта описаны в разделе Приложение Е. Описание известных ошибок, см. ошибки x109 и x102.
- Если в состав ОС включен NetFilter версии младше 1.4.15, в работе компонента SpIDer Gate возможно возникновение следующей проблемы, связанной с внутренней ошибкой в реализации NetFilter: при выключении SpIDer Gate нарушается работа сети. Рекомендуется обновить ОС до версии, включающей NetFilter версии 1.4.15 или более поздней. Руководство по устранению указанной проблемы приведено в разделе Приложение Е. Описание известных ошибок.

Поддерживаемые прокси-серверы HTTP

Для интеграции с прокси-сервером HTTP требуется установленный и настроенный прокси-сервер HTTP Squid версии не ниже 3.0. Squid должен быть собран с поддержкой ICAP (скомпилирован с опцией `--enable-icap-client`).

В режиме интернет-барьера и прозрачного прокси никаких требований к веб-серверам и прокси-серверам HTTP не предъявляется.

Режимы интернет-барьера и прозрачного прокси работают только в ОС GNU/Linux.

Совместимость с подсистемами безопасности

При настройках по умолчанию Dr.Web Gateway Security Suite не совместим с подсистемой безопасности SELinux. Кроме того, по умолчанию Dr.Web Gateway Security Suite работает в режиме ограниченной функциональности в системах GNU/Linux, использующих мандатные модели доступа (например, в системах, оснащенных подсистемой мандатного доступа PARSEC, основанной на присвоении пользователям и файлам различных уровней привилегий, называемых мандатными уровнями).

В случае необходимости установки Dr.Web Gateway Security Suite в системы с SELinux (а также в системы, использующие мандатные модели доступа) необходимо выполнить дополнительные настройки подсистемы безопасности для снятия ограничений в функционировании Dr.Web Gateway Security Suite. Подробнее см. в разделе Настройка подсистем безопасности.

5. Лицензирование

Права пользователя на использование копии Dr.Web Gateway Security Suite подтверждаются и регулируются лицензией, приобретенной пользователем у компании «Доктор Веб» или ее партнеров. Параметры лицензии, регулирующие права пользователя, установлены в соответствии с Лицензионным соглашением (см. https://license.drweb.com/agreement/), условия которого принимаются пользователем при установке Dr.Web Gateway Security Suite на свой компьютер. В лицензии фиксируется информация о пользователе и продавце, а также параметры использования приобретенной копии продукта, в частности:

- перечень компонентов, которые разрешено использовать данному пользователю;
- период, в течение которого разрешено использование Dr.Web Gateway Security Suite;
- другие ограничения (в частности, количество компьютеров, на которых разрешено использовать приобретенную копию Dr.Web Gateway Security Suite).

Каждой лицензии на использование программных продуктов компании «Доктор Веб» сопоставлен уникальный серийный номер, а на локальном компьютере с лицензией связывается специальный файл, регулирующий работу компонентов Dr.Web Gateway Security Suite в соответствии с параметрами лицензии. Он называется *лицензионным ключевым файлом*.

Для предварительного ознакомления с возможностями продукта вы можете активировать *демонстрационный период*. При активации демонстрационного периода вы получаете право на полноценное использование установленной копии Dr.Web Gateway Security Suite в течение всего этого периода, если не нарушены условия его активации. При этом также автоматически формируется специальный ключевой файл, называемый *демонстрационным*.

При отсутствии действующей лицензии или активированного демонстрационного периода (в том числе, если срок действия ранее приобретенной лицензии или демонстрационный период истек), антивирусные функции Dr.Web Gateway Security Suite блокируются, кроме того, сервис регулярных обновлений вирусных баз Dr.Web с серверов обновлений компании «Доктор Веб» становится недоступным. Однако имеется возможность активировать Dr.Web Gateway Security Suite, подключив его к серверу централизованной защиты антивирусной сети предприятия или антивирусной сети, организованной интернет-провайдером. В этом случае управление антивирусными функциями и обновлениями копии продукта, установленной на компьютере в составе антивирусной сети, возлагается на сервер централизованной защиты.

6. Установка и удаление

В этом разделе описываются процедуры установки и удаления Dr.Web Gateway Security Suite, а также процедура получения текущих обновлений и процедура перехода на новую версию, если на вашем компьютере уже установлен Dr.Web Gateway Security Suite более ранней версии.

Кроме этого, в этом разделе описана процедура выборочной установки и удаления компонентов Dr.Web Gateway Security Suite (например, для устранения ошибок, возникших в процессе эксплуатации Dr.Web Gateway Security Suite, или для установки продукта с ограниченным набором функций) и настройка расширенных подсистем безопасности (таких как SELinux), что может потребоваться при установке или в процессе эксплуатации Dr.Web Gateway Security Suite.

Для осуществления этих операций необходимы права суперпользователя (обычно пользователя *root*). Для получения прав суперпользователя воспользуйтесь командой смены пользователя `su` или командой выполнения от имени другого пользователя `sudo`.

Не гарантируется совместимость Dr.Web Gateway Security Suite с антивирусными программами других производителей. Так как установка двух антивирусов на один компьютер может привести к ошибкам в работе операционной системы и потере важных данных, перед установкой Dr.Web Gateway Security Suite настоятельно рекомендуется удалить с компьютера антивирусные программы других производителей.

Если на вашем компьютере уже имеется другой антивирусный продукт Dr.Web, установленный из универсального пакета (`.run`), и вы желаете установить еще один антивирусный продукт Dr.Web (например, у вас из универсального пакета установлен продукт Dr.Web Desktop Security Suite, и вы хотите в дополнение к нему установить Dr.Web Gateway Security Suite), то предварительно убедитесь, что версия уже установленного продукта совпадает с версией Dr.Web Gateway Security Suite, которую вы планируете установить. Если версия, которую вы собираетесь установить, новее, чем версия продукта, который уже установлен на вашем компьютере, перед началом установки дополнительного продукта обновите уже установленный продукт до версии Dr.Web Gateway Security Suite, которую вы хотите установить дополнительно.

Для ОС FreeBSD установка Dr.Web Gateway Security Suite возможна только из универсального пакета.

Дополнительно:

- Установка Dr.Web Gateway Security Suite
- Обновление Dr.Web Gateway Security Suite
- Удаление Dr.Web Gateway Security Suite
- Настройка подсистем безопасности

- Пакеты и файлы Dr.Web Gateway Security Suite
- Выборочные установка и удаление компонентов

6.1. Установка Dr.Web Gateway Security Suite

Вы можете установить Dr.Web Gateway Security Suite одним из двух способов:

1. Загрузив с сайта компании «Доктор Веб» установочный файл, представляющий собой универсальный пакет для Unix-систем, снабженный программой установки в режиме командной строки. Для ее работы в режиме графического рабочего стола необходимо наличие эмулятора терминала.
2. Выполнив установку Dr.Web Gateway Security Suite в виде набора нативных пакетов (для этого потребуется подключиться к соответствующему репозиторию пакетов компании «Доктор Веб»).

Для ОС FreeBSD установка Dr.Web Gateway Security Suite возможна только из универсального пакета.

В Альт 8 СП и других ОС, использующих устаревшие версии пакетного менеджера, рекомендуется устанавливать Dr.Web Gateway Security Suite из универсального пакета.

После установки Dr.Web Gateway Security Suite подсистема IMA/EVM ОС Альт 8 СП 11100-01 может выдавать предупреждение о возможном нарушении целостности. Чтобы избежать этого предупреждения, после установки Dr.Web Gateway Security Suite необходимо выполнить следующую команду:

```
# integalert fix
```

ОС Альт 8 СП 11100-02 и ОС Альт 8 СП 11100-03 не подвержены этой проблеме.

После установки Dr.Web Gateway Security Suite любым из указанных в этом руководстве способов в начале работы вам потребуется активировать лицензию или установить ключевой файл. Кроме того, вы можете подключить Dr.Web Gateway Security Suite к серверу централизованной защиты (подробнее см. раздел Лицензирование). До тех пор, пока вы этого не сделаете, *функции антивирусной защиты будут отключены*. Кроме того, в ряде случаев необходимо выполнить основную настройку базовой функциональности Dr.Web Gateway Security Suite, как описано в разделе Начало работы.

В процессе работы программы установки (как из универсального пакета `.run`, так и из нативных пакетов при помощи пакетного менеджера), на локальный почтовый адрес `root@localhost` отправляются сообщения электронной почты, содержащие результаты установки Dr.Web Gateway Security Suite.

Dr.Web Gateway Security Suite, установленный любым из рассмотренных в этом разделе способов, вы можете впоследствии удалить или обновить при наличии исправлений для

входящих в него компонентов или выходе новой версии Dr.Web Gateway Security Suite. При необходимости выполните также настройку подсистем безопасности GNU/Linux для корректной работы Dr.Web Gateway Security Suite. При возникновении проблем с функционированием отдельных компонентов вы можете выполнить их выборочную установку и удаление, не удаляя Dr.Web Gateway Security Suite целиком.

6.1.1. Установка универсального пакета

Универсальный пакет Dr.Web Gateway Security Suite распространяется в виде установочного файла с именем `drweb-<версия>-av-igw-<ОС>-<платформа>.run`, где <*ОС*> — Unix-подобная операционная система, а <*платформа*> — строка, указывающая тип платформы, для которой предназначен Dr.Web Gateway Security Suite (для 32-битных платформ — `x86`, для 64-битных платформ — `amd64`, `arm64`, `e2s` и `ppc64el`), например:

```
drweb-11.1.0-av-igw-linux-amd64.run
```

Далее в данном разделе руководства имя установочного файла, соответствующее формату, указанному выше, обозначается как <*имя файла .run*>, а путь к этому файлу — как <*путь к файлу .run*>.

Версия Dr.Web Gateway Security Suite определяется первыми двумя числами, разделенными точкой, в имени универсального пакета.

Чтобы установить компоненты Dr.Web Gateway Security Suite

1. Если у вас отсутствует установочный файл (универсальный пакет), загрузите его с официального сайта компании «Доктор Веб»: https://download.drweb.com/.
2. Сохраните установочный файл на жесткий диск компьютера в любой доступный для записи каталог (например, `/home/`<*username*>, где <*username*> — имя текущего пользователя).
3. Разрешите исполнение файла, например, командой:

   ```
   # chmod +x <путь к файлу .run>
   ```

4. Запустите его на исполнение командой:

   ```
   # <путь к файлу .run>
   ```

   или воспользуйтесь стандартным файловым менеджером вашей графической оболочки как для изменения свойств файла (прав доступа), так и для его запуска.

   При этом будет проверена целостность архива, затем файлы, содержащиеся в архиве, будут распакованы во временный каталог и автоматически запустится программа установки. Если запуск был осуществлен не с правами суперпользователя, то

программа установки автоматически попытается повысить свои права, запросив пароль (используется утилита `sudo`). Если попытка повышения прав окончится неудачей, установка будет отменена.

Если раздел файловой системы, содержащий временный каталог, не имеет достаточного количества свободного места для распаковки дистрибутива, процесс установки будет завершен после выдачи соответствующего сообщения. В этом случае повторите распаковку, изменив значение системной переменной окружения `TMPDIR` таким образом, чтобы она указывала на каталог в разделе файловой системы, имеющем достаточное количество свободного места. Также вы можете воспользоваться ключом распаковки в указанный каталог `--target` (см. раздел Выборочные установка и удаление компонентов).

После этого запустится программа установки для режима командной строки (для ее работы в режиме графического рабочего стола необходимо наличие эмулятора терминала).

5. Следуйте инструкциям программы установки.

Имеется возможность запустить программу установки в полностью автоматическом режиме, выполнив команду:

```
# <путь к файлу .run> -- --non-interactive
```

В этом случае программа установки будет запущена в полностью автоматическом режиме, без показа диалогов программы установки для режима командной строки.

Использование этой опции означает, что вы соглашаетесь с условиями Лицензионного соглашения Dr.Web. Ознакомиться с текстом Лицензионного соглашения после установки Dr.Web Gateway Security Suite вы можете, прочитав файл `/opt/drweb.com/share/doc/LICENSE` для GNU/Linux или `/usr/local/libexec/drweb.com/share/doc/LICENSE` для FreeBSD. Расширение файла указывает язык, на котором написан текст Лицензионного соглашения. Файл `LICENSE` (без расширения) хранит текст Лицензионного соглашения Dr.Web на английском языке. Если вы не согласны с условиями Лицензионного соглашения, вам следует удалить Dr.Web Gateway Security Suite после установки.

Запуск программы установки в полностью автоматическом режиме требует наличия прав суперпользователя (обычно пользователя *root*). Для повышения прав вы можете использовать команду `su` или `sudo`.

Если ваш дистрибутив GNU/Linux оснащен подсистемой безопасности SELinux, то возможно возникновение ситуации, когда работа программы установки будет прервана подсистемой безопасности. В этом случае вам необходимо временно перевести SELinux в *разрешающий (Permissive)* режим, для чего выполните команду:

```
# setenforce 0
```

После этого перезапустите программу установки. Также в этом случае по окончании процесса установки необходимо выполнить настройку политик безопасности SELinux, чтобы в дальнейшем антивирусные компоненты работали корректно.

Все установочные файлы, извлеченные из архива, будут автоматически удалены по окончании установки.

Рекомендуется сохранить файл `.run`, из которого производилась установка, для возможной переустановки Dr.Web Gateway Security Suite или его компонентов в последующем, без обновления его версии.

6.1.1.1. Установка в режиме командной строки

После запуска программы установки, работающей в режиме командной строки, на экране появится текст приглашения к установке.

1. Для начала установки ответьте `Yes` или `Y` на запрос «Вы хотите продолжить?». Чтобы отказаться от установки, введите `No` или `N`. В этом случае работа программы установки будет завершена.
2. Далее перед началом установки вам необходимо ознакомиться с текстом Лицензионного соглашения компании «Доктор Веб», который будет выведен на экран. Для перелистывания текста соглашения пользуйтесь клавишами ENTER (перелистывание текста на одну строчку вниз) и ПРОБЕЛ (перелистывание текста вниз на экран).

Перелистывание текста Лицензионного соглашения назад (вверх) не предусмотрено.

3. После прочтения Лицензионного соглашения вам будет предложено принять его условия. Введите `Yes` или `Y`, если вы принимаете условия, и `No` или `N`, если вы не согласны с условиями Лицензионного соглашения. В случае отказа от принятия условий Лицензионного соглашения работа программы установки будет завершена.
4. После принятия условий Лицензионного соглашения автоматически будет запущен процесс установки на компьютер компонентов Dr.Web Gateway Security Suite. При этом на экран будет выводиться информация о ходе установки (журнал установки), включающая в себя перечень устанавливаемых компонентов.

5. В случае успешного окончания процесса установки на экране появится информационное сообщение, содержащее инструкции по способам управления работой Dr.Web Gateway Security Suite.

В случае возникновения ошибки на экран будет выведено соответствующее сообщение с описанием ошибки, после чего работа программы установки будет завершена. Если установка была прервана из-за ошибки, устраните проблемы, вызвавшие ошибку установки, и повторите процесс установки заново.

6.1.2. Установка из репозитория

Нативные пакеты Dr.Web Gateway Security Suite находятся в официальном репозитории Dr.Web https://repo.drweb.com/. После добавления репозитория Dr.Web в список репозиториев, используемых менеджером пакетов вашей операционной системы, вы сможете устанавливать его в виде нативных пакетов для операционной системы так же, как и любые другие программы из репозиториев вашей операционной системы. Необходимые зависимости будут разрешаться автоматически. Кроме того, при установке Dr.Web Gateway Security Suite из подключенного репозитория пакетный менеджер ОС обнаруживает обновления всех компонентов Dr.Web и предлагает их установку.

Для доступа к репозиторию Dr.Web требуется подключение к интернету.

Все нижеприведенные команды для подключения репозиториев, импортирования ключей, установки и удаления пакетов должны быть выполнены с правами суперпользователя (обычно пользователя *root*). Для получения соответствующих прав используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

Для ОС FreeBSD установка Dr.Web Gateway Security Suite возможна только из универсального пакета.

Ниже приведены процедуры для следующих ОС (менеджеров пакетов):

- Astra Linux, Debian, Mint, Ubuntu (apt);
- Альт (apt-rpm);
- Mageia, OpenMandriva Lx (urpmi);
- Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf);
- SUSE Linux (zypper).

Astra Linux, Debian, Mint, Ubuntu (apt)

1. Репозиторий для этих ОС защищен цифровой подписью «Доктор Веб». Для доступа к репозиторию импортируйте и добавьте в хранилище пакетного менеджера ключ цифровой подписи, выполнив команду:

```
# wget https://repo.drweb.com/drweb/drweb.gpg -
O /etc/apt/trusted.gpg.d/drweb.gpg
```

Ключ цифровой подписи «Доктор Веб» ранее устанавливался с помощью утилиты `apt-key`, которая признана устаревшей и не рекомендуется для использования. Кроме того, теперь для хранения ключей подписи разработчики ОС рекомендуют использовать каталог `/etc/apt/trusted.gpg.d` вместо файла `/etc/apt/trusted.gpg`. Ввиду этого при выполнении установки Dr.Web Gateway Security Suite из репозитория, если ключ подписи установлен в каталог `/etc/apt/trusted.gpg`, команда `apt-get update` (см. ниже) выдаст следующее предупреждение: `Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details`. Установка Dr.Web Gateway Security Suite при этом продолжится в обычном режиме, а функциональность продукта не пострадает. Чтобы предупреждение больше не выводилось при установке или переустановке продуктов «Доктор Веб», установите ключ подписи как указано выше.

2. Чтобы подключить репозиторий, выполните команду:

```
# echo "deb https://repo.drweb.com/drweb/debian 11.1 non-free"
> /etc/apt/sources.list.d/drweb.list
```

Вы можете выполнить пункты 1 и 2, загрузив специальный DEB-пакет по ссылке https://repo.drweb.com/drweb/drweb-repo11.1.deb и установив его.

3. Для установки Dr.Web Gateway Security Suite из репозитория выполните команды:

```
# apt-get update
# apt-get install drweb-internet-gateways
```

Установка также может осуществляться с помощью альтернативных менеджеров (например, Synaptic или aptitude). Кроме того, альтернативные менеджеры, такие как aptitude, рекомендуется использовать для разрешения конфликта пакетов, если он возникнет.

Альт (apt-rpm)

1. Чтобы подключить репозиторий, добавьте следующую строку в файл `/etc/apt/sources.list.d/drweb-apt-rpm-<arch>.list`:

```
rpm http://repo.drweb.com/drweb/altlinux 11.1/<arch> drweb
```

где <*arch*> — обозначение используемой архитектуры пакетов:

- для 32-разрядной версии: `i386`;
- для архитектуры AMD64: `x86_64`;
- для архитектуры ARM64: `aarch64`;
- для архитектуры E2K: `e2s`;
- для архитектуры IBM POWER (ppc64el): `ppc64le`.

2. Перед установкой Dr.Web Gateway Security Suite на компьютере архитектуры E2K под управлением ОС Альт добавьте в файл `/etc/rpmrc` следующие строки:

```
arch_compat: e2kv4: e2s
arch_compat: e2k: e2s
arch_compat: e2s: noarch
```

3. Чтобы установить Dr.Web Gateway Security Suite из репозитория, выполните команды:

```
# apt-get update
# apt-get install drweb-internet-gateways
```

Установка также может осуществляться с помощью альтернативных менеджеров (например, Synaptic или aptitude).

Mageia, OpenMandriva Lx (urpmi)

1. Подключите репозиторий с помощью команды:

```
# urpmi.addmedia drweb https://repo.drweb.com/drweb/linux/11.1/<arch>/
```

где <*arch*> — обозначение используемой архитектуры пакетов:

- для 32-разрядной версии: `i386`;
- для 64-разрядной версии: `x86_64`.

2. Для установки Dr.Web Gateway Security Suite из репозитория выполните команду:

```
# urpmi drweb-internet-gateways
```

Установка также может осуществляться с помощью альтернативных менеджеров (например, rpmdrake).

Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf)

1. Добавьте файл `drweb.repo` со следующим содержимым в каталог `/etc/yum.repos.d`:

```
[drweb]
name=DrWeb - 11.1
baseurl=https://repo.drweb.com/drweb/linux/11.1/$basearch/
gpgcheck=1
enabled=1
gpgkey=https://repo.drweb.com/drweb/drweb.key
```

Если планируется записать вышеуказанное содержимое в файл при помощи команды типа `echo` с перенаправлением вывода, символ `$` следует экранировать: `\$`.

Вы можете выполнить пункт 1, загрузив специальный RPM-пакет по ссылке https://repo.drweb.com/drweb/drweb-repo11.1.rpm и установив его.

2. Для установки Dr.Web Gateway Security Suite из репозитория выполните команду:

```
# yum install drweb-internet-gateways
```

В ОС Fedora, начиная с версии 22, рекомендуется вместо менеджера `yum` использовать менеджер `dnf`, например:

```
# dnf install drweb-internet-gateways
```

Установка также может осуществляться с помощью альтернативных менеджеров (например, PackageKit или Yumex).

SUSE Linux (zypper)

1. Чтобы подключить репозиторий, выполните команду:

```
# zypper ar https://repo.drweb.com/drweb/linux/11.1/\$basearch/ drweb
```

2. Для установки Dr.Web Gateway Security Suite из репозитория выполните команды:

```
# zypper refresh
# zypper install drweb-internet-gateways
```

Установка также может осуществляться с помощью альтернативных менеджеров (например, YaST).

6.2. Обновление Dr.Web Gateway Security Suite

Предусмотрено два режима обновления Dr.Web Gateway Security Suite.

1. Получение обновлений пакетов и компонентов, выпущенных в рамках эксплуатации текущей версии Dr.Web Gateway Security Suite (как правило, такие обновления содержат исправления ошибок и мелкие улучшения в функционировании компонентов).
2. Переход на новую версию Dr.Web Gateway Security Suite. Этот способ обновления используется, если компания «Доктор Веб» выпустила новую версию Dr.Web Gateway Security Suite, отличающуюся новыми возможностями.

Dr.Web Gateway Security Suite позволяет обновлять вирусные базы и антивирусное ядро даже при отсутствии доступа в интернет на защищаемом сервере.

6.2.1. Получение текущих обновлений

После установки Dr.Web Gateway Security Suite любым из способов, описанных в соответствующем разделе, происходит автоматическое подключение менеджера пакетов к репозиторию пакетов Dr.Web:

- Если установка производилась из универсального пакета (файл `.run`), а в системе используются пакеты в формате DEB (например, ОС Astra Linux, Debian, Mint, Ubuntu), или в системе не имеется менеджера пакетов (FreeBSD), для работы с пакетами Dr.Web используется отдельная версия менеджера пакетов `zypper`, автоматически установленная в рамках установки Dr.Web Gateway Security Suite.

  Чтобы получить и установить обновленные пакеты Dr.Web этим менеджером, перейдите в каталог `/opt/drweb.com/bin` для GNU/Linux или `/usr/local/libexec/drweb.com/bin` для FreeBSD и выполните команды:

```
# ./zypper refresh
# ./zypper update
```

В ОС FreeBSD версии 11.x для платформы `amd64` при обновлении с использованием менеджера `zypper` может возникнуть ошибка обновления репозитория. В этом случае установите пакет совместимости `compat10x-amd64` и повторите попытку обновления.

Для установки пакета используйте команду:

```
# pkg install compat10x-amd64
```

- Во всех остальных случаях используйте команды обновления пакетного менеджера, используемого в вашей ОС, например:
  - в Red Hat Enterprise Linux и CentOS используйте команду `yum`;
  - в Fedora используйте команду `yum` или `dnf`;
  - в SUSE Linux используйте команду `zypper`;
  - в Mageia и OpenMandriva Lx используйте команду `urpmi`;
  - в Альт, Astra Linux, Debian, Mint, Ubuntu используйте команду `apt-get`.

Вы также можете использовать альтернативные менеджеры пакетов, разработанные для вашей операционной системы. При необходимости обратитесь к справочному руководству по используемому вами менеджеру пакетов.

В случае выпуска новой версии Dr.Web Gateway Security Suite, пакеты, содержащие его компоненты, помещаются в раздел репозитория Dr.Web, соответствующий новой версии. В этом случае для обновления необходимо переключить менеджер пакетов на новый раздел репозитория Dr.Web (см. раздел Переход на новую версию продукта).

6.2.2. Переход на новую версию продукта

В этом разделе

- Предварительные замечания
- Обновление установкой универсального пакета
- Обновление из репозитория
  - Пакеты RPM (yum, dnf)
  - Пакеты DEB (apt-get)
- Перенос ключевого файла
- Повторное подключение к серверу централизованной защиты

Предварительные замечания

Перед тем, как выполнить переход на новую версию, убедитесь, что ваш сервер отвечает системным требованиям новой версии, в том числе, что на нем установлены необходимые дополнительные программы.

Переход на новую версию Dr.Web Gateway Security Suite следует выполнять тем же способом, каким была установлена версия Dr.Web Gateway Security Suite, подлежащая обновлению.

- Если версия Dr.Web Gateway Security Suite, подлежащая обновлению, была установлена из репозитория, то переход на новую версию следует выполнять обновлением из репозитория.

- Если версия Dr.Web Gateway Security Suite, подлежащая обновлению, была установлена из универсального пакета, то переход на новую версию следует производить установкой из универсального пакета, содержащего новую версию Dr.Web Gateway Security Suite.

Чтобы уточнить способ, которым была установлена версия Dr.Web Gateway Security Suite, подлежащая обновлению, проверьте наличие в каталоге исполняемых файлов Dr.Web Gateway Security Suite скрипта программы удаления `uninst.sh`. Если этот файл присутствует, текущая версия Dr.Web Gateway Security Suite была установлена из универсального пакета, а в противном случае — из репозитория.

Для ОС FreeBSD установка Dr.Web Gateway Security Suite возможна только из универсального пакета.

Если вы не имеете возможности обновить Dr.Web Gateway Security Suite тем же способом, каким он был установлен изначально, вам следует предварительно удалить текущую версию, а потом выполнить установку новой версии Dr.Web Gateway Security Suite доступным для вас способом. Способы установки и удаления предыдущих версий Dr.Web Gateway Security Suite аналогичны способам установки и удаления, рассмотренным в данном руководстве. Для дополнительной информации обратитесь к Руководству администратора для установленной у вас версии Dr.Web Gateway Security Suite.

Если версия Dr.Web Gateway Security Suite, подлежащая обновлению, работает под управлением сервера централизованной защиты, то перед началом обновления рекомендуется сохранить адрес сервера централизованной защиты, к которому подключен Dr.Web Gateway Security Suite. Например, для получения адреса сервера централизованной защиты, к которому подключен Dr.Web Gateway Security Suite с версией новее 6.0.2, вы можете воспользоваться командой:

```
$ drweb-ctl appinfo
```

Из присутствующей в выводе команды строчки вида:

```
ESAgent; <PID>; RUNNING 1; Connected <адрес>, on-line
```

сохраните часть *<адрес>* (может выглядеть как строка вида `tcp://<IP-адрес>:<порт>`, например: `tcp://10.20.30.40:1234`). Кроме того, рекомендуется сохранить файл сертификата сервера.

В случае возникновения затруднений с получением параметров текущего подключения обратитесь к Руководству администратора для установленной версии Dr.Web Gateway Security Suite, а также к администратору вашей антивирусной сети.

Обновление через установку универсального пакета

Выполните установку Dr.Web Gateway Security Suite новой версии из универсального пакета. Если автоматическое обновление невозможно, то в процессе установки новой версии программа установки предложит вам автоматически удалить имеющиеся компоненты старой версии Dr.Web Gateway Security Suite.

Если в процессе обновления вам необходимо выполнить удаление имеющейся версии Dr.Web Gateway Security Suite и на вашем сервере одновременно установлено несколько серверных продуктов Dr.Web (например, Dr.Web Server Security Suite, Dr.Web Mail Security Suite и Dr.Web Gateway Security Suite), то для сохранения работоспособности продуктов, не подлежащих обновлению (Dr.Web Server Security Suite и Dr.Web Mail Security Suite), следует отметить для удаления только следующие пакеты:

- `drweb-internet-gateways-doc`,
- `drweb-icapd`.

Обновление из репозитория

Вы не сможете обновить Dr.Web для интернет-шлюзов UNIX версии 6.0.2 до новой версии из репозитория, если на вашем сервере установлено одновременно несколько серверных продуктов Dr.Web версии 6.0.2 (например, для файловых серверов, для почтовых серверов и интернет-шлюзов). В этом случае вам следует установить новую версию Dr.Web Gateway Security Suite на отдельную машину.

Чтобы обновить текущую версию Dr.Web Gateway Security Suite, установленную из репозитория компании «Доктор Веб»

В зависимости от типа используемых пакетов, вам необходимо выполнить следующие действия:

• Пакеты RPM (yum, dnf)

1. Смените используемый репозиторий (с репозитория пакетов текущей версии на репозиторий пакетов новой версии).

Имя репозитория, хранящего пакеты новой версии, см. в разделе Установка из репозитория. Для уточнения способа смены репозиториев обратитесь к справочным руководствам дистрибутива вашей операционной системы.

2. Установите новую версию Dr.Web Gateway Security Suite из репозитория, выполнив команду:

```
# yum update
```

или, если используется менеджер `dnf` (как, например, в ОС Fedora версии 22 и более поздних):

```
# dnf update
```

Если в процессе обновления пакетов возникнет ошибка, то выполните удаление и последующую установку Dr.Web Gateway Security Suite. При необходимости см. разделы Удаление Dr.Web Gateway Security Suite, установленного из репозитория и Установка из репозитория (пункты, соответствующие используемой вами ОС и менеджеру пакетов).

- **Пакеты DEB (apt-get)**

1. Смените используемый репозиторий (с репозитория пакетов текущей версии на репозиторий пакетов новой версии).
2. Обновите пакеты Dr.Web Gateway Security Suite, выполнив команды:

```
# apt-get update
# apt-get dist-upgrade
```

Перенос ключевого файла

При любом способе обновления Dr.Web Gateway Security Suite уже имеющийся у вас ключевой файл будет автоматически установлен в надлежащее место для использования новой версией.

В случае возникновения проблем с автоматической установкой лицензионного ключевого файла, вы можете выполнить его установку вручную.

В случае утраты действующего лицензионного ключевого файла обратитесь в службу технической поддержки.

Повторное подключение к серверу централизованной защиты

Если это возможно, то после обновления (если обновляемая версия Dr.Web Gateway Security Suite была подключена к серверу централизованной защиты) подключение будет восстановлено автоматически. Если подключение не восстановилось автоматически, для подключения обновленной версии Dr.Web Gateway Security Suite к антивирусной сети используйте команду:

```
$ drweb-ctl esconnect <адрес> --Certificate <путь к файлу сертификата>
```

В случае возникновения затруднений с подключением обратитесь к администратору вашей антивирусной сети.

6.2.3. Обновление без подключения к интернету

В условиях повышенных требований к безопасности, когда подключение к интернету отсутствует или ограничено, обновление вирусных баз и антивирусного ядра можно выполнять без подключения к интернету. В этом случае обновления загружаются на компьютер, подключенный к интернету, копируются на USB-накопитель или сетевой диск, после чего устанавливаются на другой, не подключенный к интернету компьютер. Процедура обновления выполняется через командную строку.

Чтобы получить обновления

1. На компьютере, подключенном к интернету, выполните команду:

   ```
   $ drweb-ctl update --Path <путь к каталогу для загрузки обновлений>
   ```

2. Скопируйте полученные обновления на USB-накопитель или сетевой диск.
3. Примонтируйте сетевой диск или накопитель на компьютере, на который требуется установить обновления. Если вы получаете обновления с USB-накопителя, для этого потребуется выполнить команды:

   ```
   # mkdir /mnt/usb
   # mount <путь к устройству> /mnt/usb
   ```

4. Установите обновления с помощью команды:

   ```
   $ drweb-ctl update --From /mnt/usb
   ```

6.3. Удаление Dr.Web Gateway Security Suite

В зависимости от способа установки, вы можете удалить Dr.Web Gateway Security Suite одним из двух способов:

- запустив программу удаления универсального пакета для режима командной строки;
- удалив пакеты, установленные из репозитория компании «Доктор Веб», используя системный менеджер пакетов.

6.3.1. Удаление универсального пакета

Удаление Dr.Web Gateway Security Suite, установленного из универсального пакета, можно выполнить при помощи командной строки (в графическом режиме необходимо наличие эмулятора терминала).

Программа удаления удалит не только Dr.Web Gateway Security Suite, но и все другие продукты Dr.Web, установленные на вашем компьютере.

Если на вашем компьютере, кроме Dr.Web Gateway Security Suite, установлены и другие продукты Dr.Web, для удаления только Dr.Web Gateway Security Suite вместо запуска программы удаления воспользуйтесь процедурой выборочной установки или удаления компонентов.

Удаление Dr.Web Gateway Security Suite из командной строки

Для запуска программы удаления запустите файл скрипта `uninst.sh`, который расположен в каталоге `/opt/drweb.com/bin` для GNU/Linux или `/usr/local/libexec/drweb.com/bin` для FreeBSD. Процедура удаления Dr.Web Gateway Security Suite рассмотрена в разделе Удаление в режиме командной строки.

Имеется возможность запустить программу удаления в полностью автоматическом режиме, запустив скрипт с помощью команды:

```
# env DRWEB_NON_INTERACTIVE=yes /opt/drweb.com/bin/uninst.sh
```

В этом случае программа удаления будет запущена в полностью автоматическом режиме, без показа интерфейса пользователя (включая диалоги программы удаления для режима командной строки).

Запуск программы удаления в полностью автоматическом режиме требует наличия прав суперпользователя. Для повышения прав вы можете использовать команды `su` и `sudo`.

В Альт 8 СП и других ОС, использующих устаревшие версии пакетного менеджера, во время удаления универсального пакета на консоль могут выводиться сообщения вида:

```
/etc/init.d/drweb-configd: Нет такого файла или каталога
```

На работу системы эти сообщения никак не влияют. Процедура удаления выполняется корректно.

6.3.1.1. Удаление в режиме командной строки

После запуска программы удаления, работающей в режиме командной строки, на экране появится текст приглашения к удалению.

1. Для начала удаления ответьте `Yes` или `Y` на запрос «Вы хотите продолжить?». Чтобы отказаться от удаления продуктов Dr.Web с вашего компьютера, введите `No` или `N`. В этом случае работа программы удаления будет завершена.
2. После подтверждения удаления запустится процедура удаления всех установленных пакетов Dr.Web. При этом на экран будут выдаваться записи, фиксируемые в журнал и отражающие ход процесса удаления.
3. По окончании процесса программа удаления завершит свою работу автоматически.

6.3.2. Удаление Dr.Web Gateway Security Suite, установленного из репозитория

Ниже приведены процедуры для следующих ОС (менеджеров пакетов):

- Astra Linux, Debian, Mint, Ubuntu (apt);
- Альт (apt-rpm);
- Mageia, OpenMandriva Lx (urpmi);
- Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf);
- SUSE Linux (zypper).

Все нижеприведенные команды для удаления пакетов должны быть выполнены с правами суперпользователя (обычно пользователя *root*). Для этого используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

Astra Linux, Debian, Mint, Ubuntu (apt)

Чтобы удалить корневой метапакет Dr.Web Gateway Security Suite, выполните команду:

```
# apt-get remove drweb-internet-gateways
```

При этом остальные пакеты, которые были автоматически установлены при установке корневого метапакета для удовлетворения его зависимостей, останутся в системе.

Чтобы удалить корневой метапакет вместе со всеми зависимостями, выполните команду:

```
# apt-get remove drweb-internet-gateways --autoremove
```

При этом будут удалены все более не требуемые пакеты (а не только пакеты Dr.Web Gateway Security Suite), которые были автоматически установлены для удовлетворения зависимостей других пакетов.

Если корневой метапакет уже был удален, то чтобы автоматически удалить из системы все более не используемые пакеты, выполните команду:

```
# apt-get autoremove
```

Вы также можете удалить пакеты Dr.Web Gateway Security Suite с помощью альтернативных менеджеров (например, Synaptic или aptitude).

Альт (apt-rpm)

Удаление Dr.Web Gateway Security Suite в данном случае выполняется так же, как в ОС Debian и Ubuntu (см. выше).

Вы также можете удалить пакеты Dr.Web Gateway Security Suite с помощью альтернативных менеджеров (например, Synaptic или aptitude).

В ОС Альт 8 СП во время удаления на консоль могут выводиться сообщения вида:

```
/etc/init.d/drweb-configd: Нет такого файла или каталога
```

На работу системы эти сообщения никак не влияют. Процедура удаления выполняется корректно.

Mageia, OpenMandriva Lx (urpme)

Чтобы удалить корневой метапакет Dr.Web Gateway Security Suite, выполните команду:

```
# urpme drweb-internet-gateways
```

При этом остальные пакеты, которые были автоматически установлены при установке корневого метапакета для удовлетворения его зависимостей, останутся в системе.

Чтобы удалить корневой метапакет вместе со всеми зависимостями, выполните команду:

```
# urpme --auto-orphans drweb-internet-gateways
```

При этом будут удалены все более не требуемые пакеты (а не только пакеты Dr.Web Gateway Security Suite), которые были автоматически установлены для удовлетворения зависимостей других пакетов.

Вы также можете удалить пакеты Dr.Web Gateway Security Suite с помощью альтернативных менеджеров (например, `rpmdrake`).

Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf)

Чтобы удалить все установленные пакеты Dr.Web, выполните команду (в некоторых системах символ `*` требуется экранировать: `\*`):

```
# yum remove drweb*
```

В ОС Fedora, начиная с версии 22, вместо менеджера `yum` рекомендуется использовать менеджер `dnf`, например:

```
# dnf remove drweb*
```

Эти команды удалят из системы все пакеты, название которых начинается на `drweb` (стандартное наименование для пакетов программных продуктов Dr.Web). Будут удалены все пакеты с таким именем, а не только пакеты Dr.Web Gateway Security Suite.

Вы также можете удалить пакеты Dr.Web Gateway Security Suite с помощью альтернативных менеджеров (например, PackageKit или Yumex).

SUSE Linux (zypper)

Чтобы удалить корневой метапакет Dr.Web Gateway Security Suite, выполните команду:

```
# zypper remove drweb-internet-gateways
```

При этом остальные пакеты, которые были автоматически установлены при установке корневого метапакета для удовлетворения его зависимостей, останутся в системе.

Чтобы удалить все установленные пакеты Dr.Web, выполните команду (в некоторых системах символ `*` требуется экранировать: `\*`):

```
# zypper remove drweb*
```

Эта команда удалит из системы все пакеты, название которых начинается на `drweb` (стандартное наименование для пакетов программных продуктов Dr.Web). Будут удалены все пакеты с таким именем, а не только пакеты Dr.Web Gateway Security Suite.

Вы также можете удалить пакеты Dr.Web Gateway Security Suite с помощью альтернативных менеджеров (например, YaST).

6.4. Дополнительно

6.4.1. Пакеты и файлы Dr.Web Gateway Security Suite

В этом разделе

- Пакеты
- Файлы

Пакеты

Dr.Web Gateway Security Suite состоит из следующих пакетов:

Пакет	Содержимое
`drweb-bases`	Файлы вирусных баз
`drweb-boost`	Библиотеки Boost
`drweb-clamd`	Файлы компонента Dr.Web ClamD

Пакет	Содержимое
drweb-cloudd	Файлы компонента Dr.Web CloudD
drweb-common	Основной конфигурационный файл drweb.ini, основные библиотеки, документация и структура каталогов Dr.Web Gateway Security Suite, утилита сбора данных о конфигурации продукта и системном окружении. В процессе установки данного пакета также будут созданы пользователь drweb и группа drweb
drweb-configd	Файлы компонента Dr.Web ConfigD
drweb-ctl	Файлы компонента Dr.Web Ctl
drweb-documentation	Файлы документации в формате HTML по продуктам Dr.Web для Unix
drweb-dws	Файлы базы данных категорий веб-ресурсов
drweb-engine	Файлы антивирусного ядра Dr.Web Virus-Finding Engine
drweb-esagent	Файлы компонента Dr.Web ES Agent
drweb-filecheck	Файлы компонента Dr.Web File Checker
drweb-internet-gateways-doc	Документация в формате PDF
drweb-internet-gateways	Корневой метапакет Dr.Web Gateway Security Suite
drweb-gated	Файлы компонента SpIDer Gate
drweb-firewall	Файлы компонента Dr.Web Firewall для Linux
drweb-httpd	Файлы компонента Dr.Web HTTPD и веб-интерфейса управления (метапакет)
drweb-httpd-bin	Файлы компонента Dr.Web HTTPD
drweb-httpd-webconsole	Файлы веб-интерфейса управления
drweb-icu	Библиотеки поддержки интернационализации и Unicode
drweb-icapd	Файлы компонента Dr.Web ICAPD
drweb-libs	Файлы основных библиотек
drweb-lookupd	Файлы компонента Dr.Web LookupD

Пакет	Содержимое
drweb-lua	Файлы интерпретатора Lua, используемого компонентами Dr.Web Gateway Security Suite, предназначенными для проверки сетевых соединений
drweb-netcheck	Файлы компонента Dr.Web Network Checker
drweb-openssl	Библиотеки OpenSSL
drweb-protobuf	Библиотеки Google Protobuf
drweb-se	Файлы компонента Dr.Web Scanning Engine
drweb-snmpd	Файлы компонента Dr.Web SNMPD
drweb-update	Файлы компонента Dr.Web Updater

В разделе Выборочные установка и удаление компонентов приведены типовые наборы компонентов для выборочной установки, обеспечивающие решение типовых задач Dr.Web Gateway Security Suite.

Файлы

Файлы Dr.Web Gateway Security Suite размещаются в каталогах /opt, /etc и /var дерева файловой системы.

Структура используемых каталогов:

Каталог	Содержимое
• Для GNU/Linux: /etc/init.d/ • Для FreeBSD: /usr/local/etc/rc.d/	Управляющий скрипт drweb-configd для демона управления конфигурацией Dr.Web ConfigD
• Для GNU/Linux: /etc/opt/drweb.com/ • Для FreeBSD: /usr/local/etc/drweb.com/	Общий конфигурационный файл drweb.ini и ключевой файл drweb32.key. Кроме этого, содержит:
certs/	– файлы используемых сертификатов.
• Для GNU/Linux: /opt/drweb.com/	Основной каталог Dr.Web Gateway Security Suite. Содержит в себе:

Каталог	Содержимое
• Для FreeBSD: `/usr/local/libexec/drweb.com/`	
`bin/`	– исполняемые файлы всех компонентов (за исключением Dr.Web Virus-Finding Engine);
`include/`	– заголовочные файлы используемых библиотек;
`lib/`	– используемые библиотеки;
`man/`	– файлы системной справки `man`;
`share/`	– вспомогательные файлы, в том числе:
`doc/`	▫ документация Dr.Web Gateway Security Suite (текст Лицензионного соглашения и руководства администратора, если пакеты с документацией установлены),
`drweb-bases/`	▫ файлы вирусных баз Dr.Web (исходные образы, поставляемые при установке),
`scripts/`	▫ файлы вспомогательных скриптов.
• Для GNU/Linux: `/var/opt/drweb.com/` • Для FreeBSD: `/var/drweb.com/`	Вспомогательные и временные файлы, в том числе:
`bases/`	– файлы вирусных баз Dr.Web (актуальная обновленная версия);
`cache/`	– кеш обновлений;
`drl/`	– списки используемых серверов обновлений;
`dws/`	– файлы базы категорий веб-ресурсов;
`lib/`	– антивирусное ядро Dr.Web Virus-Finding Engine в виде динамически загружаемой библиотеки `drweb32.dll` и настройки режима работы с сервером централизованной защиты;
`update/`	– каталог для временного хранения обновлений в процессе их получения.

6.4.2. Выборочные установка и удаление компонентов

В этом разделе

- Типовые комплекты компонентов для выборочной установки

- Установка и удаление компонентов Dr.Web Gateway Security Suite, установленного из репозитория
- Установка и удаление компонентов Dr.Web Gateway Security Suite, установленного из универсального пакета
  - Распаковка установочного файла
  - Выборочная установка компонентов
  - Выборочное удаление компонентов

В случае необходимости вы можете выполнить выборочную установку и удаление отдельных компонентов Dr.Web Gateway Security Suite, установив или удалив соответствующие пакеты. Выборочную установку и удаление следует производить тем же способом, каким был установлен Dr.Web Gateway Security Suite.

Для переустановки какого-либо компонента вы можете сначала удалить его, а потом установить заново.

Типовые комплекты компонентов для выборочной установки

Если требуется установить Dr.Web Gateway Security Suite с ограниченной функциональностью, вместо установки корневого метапакета из репозитория или из универсального пакета, вы можете установить только пакеты компонентов, обеспечивающих необходимую функциональность. Пакеты, требуемые для разрешения зависимостей, будут установлены автоматически. В таблице ниже приведены комплекты компонентов, предназначенные для решения типовых задач Dr.Web Gateway Security Suite. В столбце **Пакеты для установки** перечислены пакеты, которые необходимо установить для получения указанного комплекта компонентов.

Выборочный комплект компонентов	**Пакеты для установки**	**Будут установлены**
Минимальный комплект для консольного сканирования	• `drweb-filecheck`, • `drweb-se`	• Dr.Web ConfigD, • Dr.Web Ctl, • Dr.Web File Checker, • Dr.Web Scanning Engine, • Dr.Web Updater, • Вирусные базы
Комплект для эмуляции ClamAV (`clamd`)	• `drweb-clamd`, • `drweb-se`	• Dr.Web ClamD, • Dr.Web ConfigD, • Dr.Web Ctl, • Dr.Web File Checker, • Dr.Web Network Checker, • Dr.Web Scanning Engine, • Dr.Web Updater,

Выборочный комплект компонентов	Пакеты для установки	Будут установлены
		• Вирусные базы
Комплект для проверки доступа к сайтам через прокси-сервер по протоколу ICAP (без антивирусной проверки трафика)	• drweb-icapd	• Dr.Web ConfigD, • Dr.Web Ctl, • Dr.Web ICAPD, • Dr.Web Updater, • Dr.Web URL Checker, • База категорий веб-ресурсов
Комплект для проверки доступа к сайтам через прокси-сервер по протоколу ICAP (с антивирусной проверкой трафика) Пакет drweb-se можно не устанавливать, если антивирусная проверка будет производиться на другом сервере, на который данные для проверки будут передаваться через Dr.Web Network Checker.	• drweb-icapd, • drweb-netcheck, • drweb-se	• Dr.Web ConfigD, • Dr.Web Ctl, • Dr.Web ICAPD, • Dr.Web Network Checker, • Dr.Web Scanning Engine, * • Dr.Web Updater, • Dr.Web URL Checker, • База категорий веб-ресурсов, • Вирусные базы *
Комплект для локальной проверки HTTP-соединений Если антивирусная проверка соединений не требуется, пакеты drweb-netcheck и drweb-se можно не устанавливать. Пакет drweb-se можно не устанавливать, если антивирусная проверка будет производиться на другом сервере, на который данные для проверки будут передаваться через	• drweb-dws, • drweb-gated, • drweb-firewall, • drweb-netcheck, • drweb-se	• Dr.Web ConfigD, • Dr.Web Ctl, • Dr.Web Firewall для Linux, • Dr.Web Network Checker, • Dr.Web Scanning Engine, * • Dr.Web Updater, *** • Dr.Web URL Checker, • SpIDer Gate, • База категорий веб-ресурсов, ** • Вирусные базы *

Выборочный комплект компонентов	Пакеты для установки	Будут установлены
Dr.Web Network Checker. Пакет `drweb-dws` можно не устанавливать, если не требуется проверка URL на принадлежность к категории нежелательных веб-ресурсов.		

* Компонент не будет установлен, если не устанавливать пакет `drweb-se`.
** Компонент не будет установлен, если не устанавливать пакет `drweb-dws`.
*** Компонент Dr.Web Updater будет установлен, только если будут установлены вирусные базы, база категорий веб-ресурсов или спам-фильтр.

Установка и удаление компонентов Dr.Web Gateway Security Suite, установленного из репозитория

Если Dr.Web Gateway Security Suite был установлен из репозитория, для установки или удаления отдельного компонента воспользуйтесь соответствующей командой менеджера пакетов, используемого в вашей ОС, например:

1. Чтобы удалить компонент Dr.Web Network Checker (пакет `drweb-netcheck`) из состава Dr.Web Gateway Security Suite, установленного в ОС CentOS, используйте команду:

   ```
   # yum remove drweb-netcheck
   ```

2. Чтобы добавить компонент Dr.Web Network Checker (пакет `drweb-netcheck`) в состав Dr.Web Gateway Security Suite, установленного в ОС Ubuntu, используйте команду:

   ```
   # apt-get install drweb-netcheck
   ```

При необходимости воспользуйтесь справкой по менеджеру пакетов, используемому в вашей ОС.

Установка и удаление компонентов Dr.Web Gateway Security Suite, установленного из универсального пакета

Если Dr.Web Gateway Security Suite был установлен из универсального пакета, и вы хотите дополнительно установить или переустановить пакет какого-либо компонента, вам

понадобится установочный файл (с расширением `.run`), из которого был установлен Dr.Web Gateway Security Suite. Если вы не сохранили этот файл, загрузите его с сайта компании «Доктор Веб».

Распаковка установочного файла

При запуске файла `.run` вы можете воспользоваться следующими параметрами командной строки:

`--noexec` — распаковать установочные файлы Dr.Web Gateway Security Suite вместо запуска процесса установки;

`--keep` — не удалять установочные файлы Dr.Web Gateway Security Suite и журнал установки по окончании установки;

`--target` <*каталог*> — распаковать установочные файлы Dr.Web Gateway Security Suite в указанный каталог <*каталог*>.

С полным перечнем параметров командной строки, которые могут быть использованы для установочного файла, можно ознакомиться, выполнив команду:

```
$ ./<имя файла .run> --help
```

Для выборочной установки компонентов Dr.Web Gateway Security Suite предварительно распакуйте содержимое установочного файла. Для этого выполните команду:

```
$ ./<имя файла .run> --noexec --target <каталог>
```

Выборочная установка компонентов

Установочный файл `.run` содержит пакеты всех компонентов, из которых состоит Dr.Web Gateway Security Suite (в формате RPM), а также вспомогательные файлы. Файлы пакетов каждого компонента имеют вид:

```
<имя_компонента>_<версия>~linux_<платформа>.rpm
```

где <*версия*> — это строка, включающая в себя версию и дату выпуска пакета, а <*платформа*> — строка, указывающая тип платформы, для которой предназначен Dr.Web Gateway Security Suite. Имена всех пакетов, содержащих компоненты Dr.Web Gateway Security Suite, начинаются с префикса `drweb`.

Для установки пакетов в состав установочного комплекта включен менеджер пакетов `zypper`. Для выборочной установки используйте служебный скрипт `installpkg.sh`. Для этого предварительно распакуйте содержимое установочного файла в любой каталог, доступный для записи.

Для установки пакетов необходимы права суперпользователя (обычно пользователя *root*). Для получения прав суперпользователя воспользуйтесь командой смены пользователя `su` или командой выполнения от имени другого пользователя `sudo`.

Чтобы выполнить установку пакета компонента, перейдите в каталог, содержащий распакованный установочный файл, и выполните в командной строке или эмуляторе терминала команду:

```
# ./scripts/installpkg.sh <имя_пакета>
```

Например:

```
# ./scripts/installpkg.sh drweb-netcheck
```

Если требуется установить Dr.Web Gateway Security Suite целиком, запустите скрипт установки, выполнив команду:

```
$ ./install.sh
```

Кроме этого, вы можете установить все пакеты Dr.Web Gateway Security Suite (в том числе, чтобы установить недостающие компоненты, или компоненты, удаленные по ошибке), запустив установку корневого метапакета:

```
# ./scripts/installpkg.sh drweb-internet-gateways
```

Выборочное удаление компонентов

Если в вашей ОС используется формат пакетов RPM, для выборочного удаления пакета какого-либо компонента используйте соответствующую команду удаления менеджера пакетов вашей операционной системы:

- в Red Hat Enterprise Linux и CentOS используйте команду `yum remove` <*имя_пакета*>;
- в Fedora используйте команду `yum remove` <*имя_пакета*> или `dnf remove` <*имя_пакета*>;
- в SUSE Linux используйте команду `zypper remove` <*имя_пакета*>;
- в Mageia, OpenMandriva Lx используйте команду `urpme` <*имя_пакета*>;
- в Альт используйте команду `apt-get remove` <*имя_пакета*>.

Например, для Red Hat Enterprise Linux:

```
# yum remove drweb-netcheck
```

Если ваша ОС использует пакеты формата DEB, либо если в составе системы не имеется менеджера пакетов (FreeBSD), для выборочного удаления воспользуйтесь менеджером пакетов `zypper`, поставляемым с Dr.Web Gateway Security Suite. Для этого перейдите в каталог `/opt/drweb.com/bin` для GNU/Linux
или `/usr/local/libexec/drweb.com/bin` для FreeBSD и выполните команду:

```
# ./zypper remove <имя_пакета>
```

Например:

```
# ./zypper remove drweb-netcheck
```

Если вы хотите удалить Dr.Web Gateway Security Suite целиком, запустите скрипт удаления, выполнив команду:

```
# ./uninst.sh
```

Для переустановки какого-либо компонента вы можете сначала удалить его, а потом установить, запустив выборочную или полную установку.

6.5. Настройка подсистем безопасности

Наличие в составе ОС подсистемы обеспечения дополнительной безопасности SELinux (а также использование систем мандатного управления доступом (в отличие от классической дискреционной модели Unix), таких как PARSEC) приводит к проблемам в функционировании Dr.Web Gateway Security Suite при настройках по умолчанию. Для обеспечения корректной работы Dr.Web Gateway Security Suite в этом случае необходимо внести дополнительные изменения в настройки подсистемы безопасности и/или Dr.Web Gateway Security Suite.

См. далее описание настройки политик безопасности SELinux.

6.5.1. Настройка политик безопасности SELinux

В этом разделе

- Проблемы при установке универсального пакета
- Проблемы функционирования Dr.Web Gateway Security Suite

Если используемый вами дистрибутив GNU/Linux оснащен подсистемой безопасности SELinux (*Security-Enhanced Linux — Linux с улучшенной безопасностью*), то, чтобы

служебные компоненты Dr.Web Gateway Security Suite (такие как сканирующее ядро) работали корректно после установки компонентов, вам, возможно, потребуется внести изменения в политики безопасности, используемые SELinux.

Проблемы при установке универсального пакета

При включенном SELinux установка Dr.Web Gateway Security Suite в виде универсального пакета из установочного файла (`.run`) может окончиться неудачей, поскольку будет заблокирована попытка создания в системе специального пользователя *drweb*, с полномочиями которого работают компоненты Dr.Web Gateway Security Suite.

Если попытка установки Dr.Web Gateway Security Suite из установочного файла (`.run`) была прервана из-за невозможности создания пользователя *drweb*, проверьте режим работы SELinux, для чего выполните команду `getenforce`. Эта команда выводит на экран текущий режим защиты:

- `Enforcing` — защита активна, используется запрещающая стратегия: действия, нарушающие политики безопасности, регистрируются в журнале аудита и блокируются;
- `Permissive` — защита активна, но используется разрешающая стратегия: действия, нарушающие политики безопасности, не запрещаются, а только фиксируются в журнале аудита;
- `Disabled` — SELinux установлен, но неактивен.

Если SELinux работает в режиме *Enforcing*, временно (на период установки Dr.Web Gateway Security Suite) переведите ее в режим *Permissive*. Для этого выполните команду:

```
# setenforce 0
```

Указанная команда временно (до первой перезагрузки системы) переведет SELinux в режим *Permissive*.

Какой бы режим защиты вы ни установили при помощи команды `setenforce`, после перезагрузки операционной системы SELinux вернется в режим защиты, заданный в ее настройках (обычно файл настроек SELinux находится в каталоге `/etc/selinux`).

После успешной установки Dr.Web Gateway Security Suite из установочного файла, но до его запуска и активации верните режим *Enforcing*, для чего выполните команду:

```
# setenforce 1
```

Проблемы функционирования Dr.Web Gateway Security Suite

В некоторых случаях при работающем SELinux отдельные компоненты Dr.Web Gateway Security Suite (такие как `drweb-se` и `drweb-filecheck`) не смогут запуститься, вследствие чего сканирование объектов и мониторинг файловой системы станут невозможны. Признаком того, что эти компоненты не могут быть запущены, является появление сообщений об ошибках 119 и 120 в системном журнале, который ведет служба `syslog` (обычно этот журнал расположен в каталоге `/var/log/`).

В случае срабатывания системы безопасности SELinux информация об отказах фиксируется также в системном журнале аудита. В общем случае, при использовании в системе демона audit, журнал аудита хранится в файле `/var/log/audit/audit.log`. В противном случае сообщения о запрете операции записываются в общий файл журнала (`/var/log/messages` или `/var/log/syslog`).

Если установлено, что компоненты сканирования не функционируют из-за того, что они блокируются SELinux, скомпилируйте для них специальные *политики безопасности*.

В некоторых дистрибутивах GNU/Linux указанные ниже утилиты могут быть по умолчанию не установлены. В этом случае вам, возможно, потребуется установить их дополнительно.

Чтобы настроить политики безопасности SELinux

1. Создайте новый файл с исходным кодом политики SELinux (файл с расширением `.te`). Данный файл определяет ограничения, относящиеся к описываемому модулю. Исходный файл политики может быть создан двумя способами:
   1) С помощью утилиты `audit2allow`. Это наиболее простой способ, поскольку данная утилита генерирует разрешающие правила на основе сообщений об отказе в доступе в файлах системных журналов. Возможно задать автоматический поиск сообщений в файлах журналов или указать путь к файлу журнала вручную.

Этот способ можно использовать только в том случае, когда в системном журнале аудита уже зарегистрированы инциденты нарушения политик безопасности SELinux компонентами Dr.Web Gateway Security Suite. Если это не так, дождитесь таких инцидентов в процессе работы Dr.Web Gateway Security Suite или создайте разрешающие политики принудительно, воспользовавшись утилитой `policygentool` (см. ниже).

Утилита `audit2allow` находится в пакете `policycoreutils-python` или `policycoreutils-devel` (для ОС Red Hat Enterprise Linux, CentOS, Fedora, в зависимости от версии) или в пакете `python-sepolgen` (для ОС Debian, Ubuntu).

Пример использования `audit2allow`:

```
# grep drweb-se.real /var/log/audit/audit.log | audit2allow -M drweb-se
```

В данном примере утилита `audit2allow` производит поиск в файле `/var/log/audit/audit.log` сообщений об отказе в доступе для компонента `drweb-se`.

В результате работы утилиты создаются два файла: исходный файл политики `drweb-se.te` и готовый к установке модуль политики `drweb-se.pp`.

Если подходящих инцидентов в системном журнале не обнаружено, утилита вернет сообщение об ошибке.

В большинстве случаев вам не потребуется вносить изменения в файл политики, созданный утилитой `audit2allow`, поэтому рекомендуется сразу переходить к пункту 4 для установки полученного модуля политики `drweb-se.pp`.

По умолчанию утилита `audit2allow` в качестве результата своей работы выводит на экран готовый вызов команды `semodule`. Скопировав его в командную строку и выполнив, вы выполните пункт 4. Перейдите к пункту 2, только если вы хотите внести изменения в политики, автоматически сформированные для компонентов Dr.Web Gateway Security Suite.

2) С помощью утилиты `policygentool`. Для этого укажите в качестве параметров имя компонента, работу с которым вы хотите настроить, и полный путь к его исполняемому файлу.

Утилита `policygentool`, входящая в состав пакета `selinux-policy` для ОС Red Hat Enterprise Linux и CentOS, может работать некорректно. В таком случае воспользуйтесь утилитой `audit2allow`.

Пример создания политик при помощи `policygentool`:

- для компонента `drweb-se`:

```
# policygentool drweb-se /opt/drweb.com/bin/drweb-se.real
```

- для компонента `drweb-filecheck`:

```
# policygentool drweb-filecheck /opt/drweb.com/bin/drweb-filecheck.real
```

Вам будет предложено указать несколько общих характеристик домена, после чего для каждого компонента будут созданы три файла, определяющих политику:

<module_name>`.te`, *<module_name>*`.fc` и *<module_name>*`.if`.

2. При необходимости отредактируйте сгенерированный исходный файл политики *<module_name>.te*, а затем, используя утилиту `checkmodule`, создайте бинарное представление (файл с расширением `.mod`) исходного файла локальной политики.

Для успешной работы этой команды в системе должен быть установлен пакет `checkpolicy`.

Пример использования:

```
# checkmodule -M -m -o drweb-se.mod drweb-se.te
```

3. Создайте устанавливаемый модуль политики (файл с расширением `.pp`) с помощью утилиты `semodule_package`.

   Пример:

   ```
   # semodule_package -o drweb-se.pp -m drweb-se.mod
   ```

4. Для установки созданного модуля политики воспользуйтесь утилитой `semodule`.

   Пример:

   ```
   # semodule -i drweb-se.pp
   ```

Для получения дополнительной информации о принципах работы и настройки SELinux обратитесь к документации по используемому вами дистрибутиву GNU/Linux.

7. Начало работы

1. Для начала работы с установленным Dr.Web Gateway Security Suite выполните его активацию, получив и установив ключевой файл.
2. Далее рекомендуется выполнить проверку работоспособности Dr.Web Gateway Security Suite.
3. Интегрируйте Dr.Web Gateway Security Suite с используемым вами прокси-сервером HTTP (см. инструкцию для прокси-сервера Squid).
4. Для защиты локального веб-сервера от угроз из внешней сети внесите изменения в настройки монитора SpIDer Gate.
5. Если вы не используете сторонний прокси-сервер, настройте для монитора SpIDer Gate режим прокси.
6. Проверьте состав запущенных компонентов и при необходимости включите дополнительные компоненты, которые по умолчанию отключены, если они необходимы для защиты вашего сервера (например, Dr.Web ClamD или Dr.Web SNMPD).

Для корректной работы дополнительных компонентов может оказаться недостаточно только их включения. Возможно также потребуется внести изменения в их настройки, заданные по умолчанию.

Для просмотра перечня установленных и запущенных компонентов, а также их настройки, вы можете воспользоваться:

- утилитой управления из командной строки Dr.Web Ctl (используйте команды `drweb-ctl appinfo`, `drweb-ctl cfshow` и `drweb-ctl cfset`);
- веб-интерфейсом управления Dr.Web Gateway Security Suite (по умолчанию доступ через браузер осуществляется по адресу `https://127.0.0.1:4443`).

7.1. Регистрация и активация

В этом разделе

- Приобретение и регистрация лицензии
- Активация Dr.Web Gateway Security Suite
  - Запрос демонстрационного периода
  - Установка ключевого файла
- Повторная регистрация

Приобретение и регистрация лицензии

При приобретении лицензии клиент получает возможность в течение всего срока ее действия получать обновления с серверов обновлений компании «Доктор Веб», а также получать стандартную техническую поддержку компании «Доктор Веб» и ее партнеров.

Приобрести любой антивирусный продукт Dr.Web или серийный номер для него вы можете у наших партнеров или через интернет-магазин. Дополнительную информацию о возможных вариантах лицензий можно найти на официальном сайте компании «Доктор Веб» по адресу https://license.drweb.com/license_manager.

Регистрация лицензии подтверждает, что вы являетесь полноправным пользователем Dr.Web Gateway Security Suite, и активирует его функции, включая функции обновления вирусных баз. Рекомендуется выполнять регистрацию и активацию лицензии сразу после установки.

Активация Dr.Web Gateway Security Suite

Приобретенная лицензия может быть активирована непосредственно на сайте компании «Доктор Веб» по адресу https://products.drweb.com/register/v4.

При активации или продлении лицензии требуется указать серийный номер. Этот номер может поставляться вместе с Dr.Web Gateway Security Suite или по электронной почте, при покупке или продлении лицензии онлайн.

Запрос демонстрационного периода

Вы можете воспользоваться командой `license` утилиты командной строки Dr.Web Ctl (`drweb-ctl`), которая позволяет автоматически получить демонстрационный ключевой файл или лицензионный ключевой файл для серийного номера зарегистрированной лицензии. Для получения демонстрационного периода на использование Dr.Web Gateway Security Suite следует обратиться к мастеру запроса демо на сайте компании «Доктор Веб» по адресу https://download.drweb.com/demoreq/biz/v2/. После выбора продукта и заполнения анкеты вы получите по электронной почте серийный номер или ключевой файл для активации демонстрационного периода.

Демонстрационный период использования Dr.Web Gateway Security Suite может быть выдан повторно для того же компьютера только по истечении определенного периода времени.

Установка ключевого файла

Если уже имеется ключевой файл, соответствующий действующей лицензии на этот продукт (например, он был получен от продавца по электронной почте после регистрации или Dr.Web Gateway Security Suite переносится на другой сервер), имеется возможность активировать Dr.Web Gateway Security Suite, просто указав путь к имеющемуся ключевому файлу. Это можно сделать следующим образом:

- Вручную, для этого:
  1. Распакуйте ключевой файл, если он был вами получен в архиве.
  2. Далее выполните любое из указанных ниже действий.
     - Скопируйте его в каталог `/etc/opt/drweb.com` для GNU/Linux или `/usr/local/etc/drweb.com` для FreeBSD и переименуйте в `drweb32.key`.
     - В файле конфигурации Dr.Web Gateway Security Suite установите значение параметра `KeyPath` таким образом, чтобы он указывал на ключевой файл. В этом случае название ключа может отличаться от `drweb32.key`.
  3. Перезагрузите конфигурацию Dr.Web Gateway Security Suite, выполнив команду:

```
# drweb-ctl reload
```

  для применения внесенных изменений.

Вы также можете воспользоваться командой:

```
# drweb-ctl cfset Root.KeyPath <путь к ключевому файлу>
```

В последнем случае дополнительно перезагружать конфигурацию Dr.Web Gateway Security Suite не требуется. Ключевой файл не будет скопирован в каталог `/etc/opt/drweb.com` для GNU/Linux или `/usr/local/etc/drweb.com` для FreeBSD, а останется в исходном каталоге.

Если ключевой файл не скопирован в каталог `/etc/opt/drweb.com` для GNU/Linux или `/usr/local/etc/drweb.com` для FreeBSD, пользователь сам несет ответственность за его сохранность. Такой способ установки ключевого файла не рекомендуется из-за возможности его случайного удаления (например, если он был размещен в каталоге, подвергающемся автоматической очистке системой). Помните, что в случае утраты вы можете запросить ключевой файл повторно, но количество запросов на его получение ограничено.

Повторная регистрация

Повторная регистрация может потребоваться в случае утраты лицензионного ключевого файла при наличии активной лицензии. При повторной регистрации укажите

те же персональные данные, которые вы ввели при первой регистрации лицензии. Допускается использовать другой адрес электронной почты — в таком случае лицензионный ключевой файл будет выслан по новому адресу.

Получить лицензионный ключевой файл с помощью команды управления лицензией можно ограниченное количество раз. Если это число превышено, то ключевой файл можно получить, подтвердив регистрацию своего серийного номера на сайте https://products.drweb.com/register/. Ключевой файл будет выслан на адрес электронной почты, который был указан при первой регистрации.

После получения ключевого файла по электронной почте вам необходимо выполнить процедуру его установки.

7.1.1. Ключевой файл

Ключевой файл — это специальный файл, который хранится на локальном компьютере и соответствует приобретенной лицензии или активированному демонстрационному периоду для Dr.Web Gateway Security Suite. В ключевом файле фиксируются параметры использования продукта в соответствии с приобретенной лицензией или активированным демонстрационным периодом.

Ключевой файл имеет расширение `.key` и является действительным при одновременном выполнении следующих условий:

- Срок действия лицензии или демонстрационного периода, которым он соответствует, не истек.
- Разрешение, определяемое лицензией или активным демонстрационным периодом, распространяется на все используемые модули.
- Целостность файла не нарушена.

При нарушении любого из этих условий ключевой файл становится недействительным.

При работе Dr.Web Gateway Security Suite ключевой файл по умолчанию должен находиться в каталоге `/etc/opt/drweb.com` для GNU/Linux или `/usr/local/etc/drweb.com` для FreeBSD и называться `drweb32.key`.

Компоненты Dr.Web Gateway Security Suite регулярно проверяют наличие и корректность ключевого файла. Его содержимое защищено от редактирования при помощи механизма электронной цифровой подписи, поэтому редактирование делает ключевой файл недействительным. Не рекомендуется открывать ключевой файл в текстовых редакторах во избежание случайной порчи его содержимого.

При отсутствии действительного ключевого файла (лицензионного или демонстрационного), а также по истечении срока его действия, антивирусные функции всех компонентов блокируются до установки действующего ключевого файла.

Рекомендуется сохранять имеющийся лицензионный ключевой файл до истечения срока его действия. В этом случае при переустановке Dr.Web Gateway Security Suite или переносе его на другой сервер повторная регистрация серийного номера лицензии не потребуется, и вы сможете использовать лицензионный ключевой файл, полученный при первом прохождении процедуры регистрации.

По электронной почте ключевые файлы Dr.Web обычно передаются запакованными в архивы `.zip`. Архив, содержащий ключевой файл для активации Dr.Web Gateway Security Suite, обычно имеет имя `agent.zip`. Если в сообщении электронной почты содержится *несколько* архивов, то нужно использовать именно архив `agent.zip`. Перед установкой ключевого файла вы должны распаковать архив любым удобным для вас способом и извлечь из него ключевой файл, сохранив его в любой доступный каталог (например, в домашний каталог или на съемный носитель USB flash).

7.2. Проверка работоспособности

Для проверки работоспособности антивирусных программ, использующих сигнатурные методы обнаружения угроз, используется тест *EICAR (European Institute for Computer Anti-Virus Research)*, разработанный одноименной организацией. Этот тест разработан для того, чтобы пользователь, не подвергая свой компьютер опасности, мог посмотреть, как установленный антивирус будет сигнализировать об обнаружении угрозы.

Программа, используемая для теста *EICAR*, не является вредоносной, но специально определяется большинством антивирусных программ как вирус. Антивирусные продукты Dr.Web называют этот «вирус» следующим образом: *EICAR Test File (NOT a Virus!)*. Примерно так его называют и другие антивирусные программы. Тестовая программа EICAR представляет собой последовательность из 68 байт, образующую тело исполняемого файла `.com` для ОС MS-DOS/Windows, в результате исполнения которого в консоль или на экран эмулятора терминала выводится текстовое сообщение:

```
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
```

Тело тестовой программы состоит только из текстовых символов, которые формируют следующую строку:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Если вы создадите текстовый файл, состоящий из приведенной выше строки, то в результате получится программа, которая и будет описанным «вирусом».

В случае корректной работы Dr.Web Gateway Security Suite этот файл должен обнаруживаться при проверке объектов файловой системы любым доступным способом, с уведомлением об обнаружении угрозы EICAR Test File (NOT a Virus!).

Пример команды для проверки работоспособности Dr.Web Gateway Security Suite при помощи тестовой программы EICAR:

```
$ echo 'X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*' > testfile && drweb-ctl rawscan testfile && rm testfile
```

Данная команда записывает строку, представляющую собой тело тестовой программы EICAR, в файл `testfile` в текущий каталог, выполняет проверку полученного файла, после чего удаляет созданный файл.

Для успешного проведения вышеуказанного теста вы должны иметь права записи в текущий каталог. Кроме того, убедитесь, что в нем отсутствует файл с именем `testfile` (при необходимости измените имя файла в команде).

В случае успешного обнаружения тестового «вируса» на экран будет выдано следующее сообщение:

```
<путь к текущему каталогу>/testfile - infected with EICAR Test File (NOT a
Virus!)
```

Если при проверке будет получено сообщение об ошибке, обратитесь к описанию известных ошибок.

Проверку входящего HTTP-трафика на наличие угроз можно выполнить двумя способами.

Через браузер

1. Открыть браузер и перейти к настройке прокси-сервера.
2. Ввести соответствующие параметры прокси-сервера для ICAP.
3. Зайти на страницу https://www.eicar.org/download/eicar.com — в окне браузера появится уведомление о зараженном файле.

Через консоль

Выполнить запрос:

```
$ curl -x 127.0.0.1:3128 https://www.eicar.org/download/eicar.com
```

В ответ на запрос в консоли появится уведомление о блокировке запрошенного ресурса.

7.3. Интеграция с прокси-сервером Squid

В этом разделе

- Настройка параметров Dr.Web ICAPD
- Настройка параметров Squid
  - Для Squid 3.2 и более поздних версий
  - Для Squid версии 3.1
  - Для Squid версии 3.0
- Дополнительные настройки Squid: ограничение размера данных

Настройка параметров Dr.Web ICAPD

Для интеграции Dr.Web ICAPD с прокси-сервером HTTP Squid нужно проверить и при необходимости изменить значения ряда параметров в секции настроек Dr.Web ICAPD (секция `[ICAPD]`):

- В параметре `ListenAddress` укажите путь к сетевому сокету (<*IP-адрес*>:<*порт*>), который Dr.Web ICAPD будет прослушивать в ожидании подключений от прокси-сервера (по умолчанию используется сокет `127.0.0.1:1344`).
- В параметрах `Block*` включите или отключите категории сайтов и типы угроз, которые должен блокировать или разрешать Dr.Web ICAPD.
- При необходимости укажите пути доменов доступ к которым должен блокироваться при любых условиях, в параметре `BlackList`. В параметре `WhiteList` вы можете указать пути к доменам, доступ к которым никогда не должен блокироваться.

Параметр `BlackList` имеет приоритет над параметром `WhiteList`. Если один и тот же домен указан в значениях обоих параметров, он будет заблокирован.

- Для более детальной настройки доступа к сайтам (в зависимости от условий) отредактируйте правила проверки трафика.

Значения параметров `UsePreview`, `Use204` и `AllowEarlyResponse` в секции настроек Dr.Web ICAPD, заданные по умолчанию, разрешают использование компонентом соответствующих возможностей протокола ICAP (использование режима *ICAP preview*, возврат кода 204 не только в режиме *ICAP preview* и «раннее» начало отправки ответа клиенту, не дожидаясь окончания приема запроса, поступившего от прокси-сервера). Значения этих параметров рекомендуется оставить заданными по умолчанию, изменяя их только в случае возникновения проблем в обработке HTTP-запросов.

После внесения изменений в настройки перезагрузите конфигурацию Dr.Web Gateway Security Suite, выполнив команду:

```
# drweb-ctl reload
```

Вы также можете перезапустить Dr.Web Gateway Security Suite, перезапустив демон управления конфигурацией Dr.Web ConfigD с помощью команды:

```
# service drweb-configd restart
```

Настройка параметров Squid

Для обеспечения взаимодействия между Squid и Dr.Web ICAPD требуется указать в конфигурационном файле `squid.conf` (обычно он находится в каталоге `/etc/squid3/`) настройки для активации протокола ICAP. Для интеграции ICAP с Dr.Web Gateway Security Suite необходимо:

1. Активировать протокол ICAP в настройках Squid.
2. Зарегистрировать Dr.Web ICAPD в качестве службы ICAP для Squid.
3. Активировать режим *ICAP preview* (опционально).
4. Разрешить передачу данных клиентов (IP-адреса и аутентифицированного на прокси-сервере имени пользователя) для использования в правилах Dr.Web ICAPD (опционально).
5. Активировать поддержку постоянных соединений между Dr.Web ICAPD и Squid (опционально; использование постоянных соединений необязательно, но повышает производительность связки Squid + Dr.Web ICAPD).

- Чтобы Squid проверял HTTP-запросы (*REQMOD*) и HTTP-ответы (*RESPMOD*) через ICAP, требуется добавить две службы ICAP соответствующего типа.
- Чтобы Squid использовал Dr.Web ICAPD в качестве службы ICAP, адрес и порт, указанные в `icap_service`, должны совпадать с адресом и портом, указанными в параметре `ListenAddress` настроек Dr.Web ICAPD.
- Dr.Web ICAPD не будет работать со Squid, если значение `icap_preview_size` не равно `0`.
- Значения «IP-адрес клиента» и «Имя пользователя» Squid формирует самостоятельно и передает их Dr.Web ICAPD в ICAP-запросе в заголовках `X-Client-Username` и `X-Client-IP`. Значения этих заголовков должны быть закодированы с при помощи методов, используемых Squid. Настройки Squid, которые влияют на способ кодирования этих заголовков (`icap_client_username_encode` и `icap_client_username_header`) изменять не следует.

Для интеграции с Dr.Web Gateway Security Suite Squid должен быть собран с поддержкой ICAP (т. е. скомпилирован с опцией `--enable-icap-client`). В противном случае подключение Squid к Dr.Web ICAPD невозможно.

Для работы по протоколу HTTPS Squid должен быть собран с поддержкой SSL-сертификатов (скомпилирован с опциями `--with-openssl` и `--enable-ssl-crtd`). В настройках Squid должен обязательно быть активирован SSL Bumping.

Настройки для разных версий Squid могут различаться. В этом разделе приведены три варианта настройки для следующих версий Squid: 3.2 и более ранних, 3.1, и 3.0. Откорректируйте ваш конфигурационный файл в соответствии с примерами.
Если строки из примеров ниже в вашем конфигурационном файле закомментированы, раскомментируйте их. Если строки из примеров отсутствуют в вашем конфигурационном файле, просто добавьте их.

Для настройки взаимодействия между Dr.Web ICAPD и Squid обязательны только параметры из секций №1 и №2. Параметры из секций №3 и №4 являются факультативными.

Для Squid 3.2 и более поздних версий

```
#1
icap_enable on

#2
icap_service i_req reqmod_precache bypass=0 icap://127.0.0.1:1344/reqmod
icap_service i_res respmod_precache bypass=0 icap://127.0.0.1:1344/respmod

adaptation_access i_req allow all
adaptation_access i_res allow all

#3
icap_preview_enable on
icap_preview_size 0

#4 (в версии Squid 3.2 параметры icap_send_client_ip и
icap_send_client_username были переименованы)
adaptation_send_client_ip on
adaptation_send_username on

#5
icap_persistent_connections on
```

Для Squid версии 3.1

```
#1
icap_enable on
```

```
#2 (в версии Squid 3.1 формат определения сервиса был изменен, а параметр
icap_access был переименован)
icap_service i_req reqmod_precache bypass=0 icap://127.0.0.1:1344/reqmod
icap_service i_res respmod_precache bypass=0 icap://127.0.0.1:1344/respmod

adaptation_access i_req allow all
adaptation_access i_res allow all

#3
icap_preview_enable on
icap_preview_size 0

#4
icap_send_client_ip on
icap_send_client_username on

#5
icap_persistent_connections on
```

Для Squid версии 3.0

```
#1
icap_enable on

#2
icap_service i_req reqmod_precache 0 icap://127.0.0.1:1344/reqmod
icap_service i_res respmod_precache 0 icap://127.0.0.1:1344/respmod

icap_class icapd_class_req i_req
icap_class icapd_class_resp i_res

icap_access icapd_class_req allow all
icap_access icapd_class_resp allow all

#3
icap_preview_enable on
icap_preview_size 0

#4
icap_send_client_ip on
icap_send_client_username on

#5
icap_persistent_connections on
```

После редактирования конфигурационного файла и сохранения изменений нужно перезапустить Squid.

Дополнительные настройки Squid: ограничение размера данных

При необходимости вы можете ограничить размер данных, которые Squid будет передавать на проверку по протоколу ICAP. Для этого в конфигурационном файле укажите в значении заголовка `Content-Length` конкретный размер данных в байтах или регулярное выражение, например:

```
acl <name> rep_header Content-Length ^[0-9]{7,}$
```

В этом примере условие <*name*> будет выполняться, если значение заголовка `Content-Length` превышает 999999.

Условие из примера выше можно использовать для разрешения (`allow`) или запрета (`deny`) проверки ответа от сервера по протоколу ICAP (в параметрах подключения Squid к внешнему ICAP-серверу `all` потребуется заменить на имя условия <*name*>).
Ниже приводится пример настроек для *запрета* проверки ответов, для которых условие <*name*> выполняется:

```
#версия Squid 3.1 и более поздняя
adaptation_access i_res deny <name>

#версия Squid 3.0 и более поздняя
icap_access icapd_class_resp deny <name>
```

Заголовок `Content-Length` может отсутствовать в ответе веб-сервера. В этом случае описанные выше настройки не будут действовать.

Подробные инструкции по настройке ограничения проверки веб-трафика для Squid приведены в официальной документации на английском языке.

Чтобы измененные настройки вступили в силу, необходимо перезапустить Squid.

7.4. Защита локального веб-сервера

В этом разделе

- Настройки перенаправления соединений
- Настройка параметров проверки

Данная возможность доступна только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux.

Для защиты веб-сервера, работающего на том же узле, на котором установлен Dr.Web Gateway Security Suite, необходимо активировать проверку всех поступающих на веб-сервер данных Dr.Web Firewall для Linux в мониторе SpIDer Gate.

Настройки перенаправления соединений

Чтобы настроить защиту веб-сервера, установите в конфигурационном файле для параметров в секции `[LinuxFirewall]` следующие значения:

Параметр	Требуемое значение
`InspectHttp`	`On`
`AutoconfigureIptables`	`Yes`
`AutoconfigureRouting`	`Yes`
`LocalDeliveryMark`	`Auto`
`ClientPacketsMark`	`Auto`
`ServerPacketsMark`	`Auto`
`TproxyListenAddress`	`127.0.0.1:0` Если для работы Dr.Web Firewall для Linux используется особый IP-адрес или порт, укажите их здесь
`InputDivertEnable`	`Yes`
`InputDivertNfqueueNumber`	`Auto`
`InputDivertConnectTransparently`	`Yes`

Чтобы просмотреть или изменить настройки Dr.Web Firewall для Linux, используйте:

- Утилиту управления из командной строки Dr.Web Ctl (используйте команды `drweb-ctl cfshow` и `drweb-ctl cfset`).

  Например, команда:

  ```
  # drweb-ctl cfset LinuxFirewall.InputDivertEnable Yes
  ```

  настроит Dr.Web Firewall для Linux таким образом, чтобы все входящие данные проходили проверку в мониторе SpIDer Gate, если используется протокол HTTP и если значение параметра `InspectHttp` установлено в `On`.

- Веб-интерфейс управления Dr.Web Gateway Security Suite (по умолчанию доступ через браузер осуществляется по адресу `https://127.0.0.1:4443`).

Чтобы обеспечить проверку данных, передаваемых с использованием безопасного протокола HTTPS, дополнительно:

- Включите проверку трафика, передаваемого через SSL/TLS, с помощью команды:

  ```
  # drweb-ctl cfset LinuxFirewall.UnwrapSsl Yes
  ```

  Рекомендуется использовать команду `cfset` утилиты `drweb-ctl` или веб-интерфейс управления, т. к. в этом случае также будут автоматически изменены правила проверки, зависящие от данного параметра.
- Экспортируйте сертификат, который Dr.Web Gateway Security Suite будет использовать для встраивания в защищенные каналы SSL/TLS, выполнив команду:

  ```
  $ drweb-ctl certificate > <cert_name>.pem
  ```

  Необходимо указать имя файла, в который будет сохранен сертификат в формате PEM.
- Добавьте полученный сертификат в системный перечень доверенных сертификатов и пропишите его в качестве доверенного у веб-клиентов (браузеров) и веб-сервера (подробнее см. в разделе Приложение Д. Генерация сертификатов SSL).

Настройка параметров проверки

В конфигурационном файле в секции настроек Dr.Web Firewall для Linux (секция `[LinuxFirewall]`) установите значения следующих параметров:

1. Параметры сканирования передаваемых данных (`ScanTimeout`, `HeuristicAnalysis`, `PackerMaxLevel`, `ArchiveMaxLevel`, `MailMaxLevel`, `ContainerMaxLevel`, `MaxCompressionRatio`), ограничивающие длительность и ресурсоемкость их проверки. Если детальная настройка не требуется, сохраните значения по умолчанию.
2. Параметры `Block*`, предназначенные для блокировки нежелательных URL и нежелательного содержимого.
3. Параметр `BlockUnchecked` для определения действий со стороны SpIDer Gate в случае, когда проверка полученных данных невозможна.

Для более детальной настройки правил фильтрации сообщений HTTP (в зависимости от условий) отредактируйте Lua-процедуру либо правила `RuleSet`.

После внесения изменений в настройки перезагрузите конфигурацию Dr.Web Gateway Security Suite, выполнив команду:

```
# drweb-ctl reload
```

Вы также можете перезапустить Dr.Web Gateway Security Suite, перезапустив демон управления конфигурацией Dr.Web ConfigD с помощью команды:

```
# service drweb-configd restart
```

7.5. Использование SplDer Gate в режиме прокси

В этом разделе

- Настройки режима прокси
- Настройка параметров проверки

Данная возможность доступна только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux.

Если на интернет-шлюзе отсутствует прокси-сервер HTTP, который мог бы быть сопряжен с Dr.Web Gateway Security Suite посредством протоколов ICAP или ClamAV (используя непосредственно компонент Dr.Web ClamD), для защиты локальной сети от угроз, распространяемых через интернет, необходимо настроить Dr.Web Firewall для Linux таким образом, чтобы данные, поступающие на интернет-шлюз, на котором установлен Dr.Web Gateway Security Suite, проходили проверку в мониторе SplDer Gate (режим «прозрачного» прокси).

Настройки режима прокси

Чтобы настроить защиту веб-сервера, установите в конфигурационном файле для параметров в секции `[LinuxFirewall]` следующие значения:

Параметр	Требуемое значение
`InspectHttp`	`On`
`AutoconfigureIptables`	`Yes`
`AutoconfigureRouting`	`Yes`
`LocalDeliveryMark`	`Auto`
`ClientPacketsMark`	`Auto`
`ServerPacketsMark`	`Auto`
`TproxyListenAddress`	`127.0.0.1:0` Если для работы Dr.Web Firewall для Linux используется особый IP-адрес или порт, укажите их здесь

Параметр	Требуемое значение
`ForwardDivertEnable`	`Yes`
`ForwardDivertNfqueueNumber`	`Auto`
`ForwardDivertConnectTransparently`	`Yes`

Для просмотра и изменения настроек Dr.Web Firewall для Linux вы можете воспользоваться:

- Утилитой управления из командной строки Dr.Web Ctl (используйте команды `drweb-ctl cfshow` и `drweb-ctl cfset`).

  Например, команда:

  ```
  # drweb-ctl cfset LinuxFirewall.ForwardDivertEnable Yes
  ```

  настроит Dr.Web Firewall для Linux таким образом, чтобы данные, следующие через узел, проходили проверку в мониторе SpIDer Gate, если используется протокол HTTP и если параметр `InspectHttp` имеет значение `On`.
- Веб-интерфейсом управления Dr.Web Gateway Security Suite (по умолчанию доступ через браузер осуществляется по адресу `https://127.0.0.1:4443`).

Чтобы обеспечить проверку данных, передаваемых с использованием протокола HTTPS:

- Включите проверку трафика, передаваемого через SSL/TLS:

  ```
  # drweb-ctl cfset LinuxFirewall.UnwrapSsl Yes
  ```

  Рекомендуется использовать команду `cfset` утилиты `drweb-ctl` или веб-интерфейс управления, поскольку в этом случае также будут автоматически изменены правила проверки, зависящие от данного параметра.
- Экспортируйте сертификат, который Dr.Web Gateway Security Suite будет использовать для встраивания в защищенные каналы SSL/TLS, выполнив команду:

  ```
  $ drweb-ctl certificate > <cert_name>.pem
  ```

  Необходимо указать имя файла, в который будет сохранен сертификат в формате PEM.
- Добавьте полученный сертификат в системный перечень доверенных сертификатов и пропишите его в качестве доверенного у веб-клиентов (браузеров) и веб-сервера (подробнее см. раздел Приложение Д. Генерация сертификатов SSL).

Настройка параметров проверки

В конфигурационном файле, в секции настроек Dr.Web Firewall для Linux (секция `[LinuxFirewall]`) установите значения следующих параметров:

1. Параметры сканирования передаваемых данных (`ScanTimeout`, `HeuristicAnalysis`, `PackerMaxLevel`, `ArchiveMaxLevel`, `MailMaxLevel`, `ContainerMaxLevel`, `MaxCompressionRatio`), ограничивающие длительность и ресурсоемкость их проверки. Если детальная настройка не требуется, оставьте значения по умолчанию.
2. Параметры `Block*`, предназначенные для блокировки нежелательных URL и нежелательного содержимого.
3. Параметр `BlockUnchecked` для определения действий со стороны SpIDer Gate в случае, когда проверка полученных данных невозможна.

Для более детальной настройки правил фильтрации сообщений HTTP (в зависимости от условий) отредактируйте Lua-процедуру либо правила `RuleSet`.

После внесения изменений в настройки перезагрузите конфигурацию Dr.Web Gateway Security Suite, выполнив команду:

```
# drweb-ctl reload
```

Вы также можете перезапустить Dr.Web Gateway Security Suite, перезапустив демон управления конфигурацией Dr.Web ConfigD с помощью команды:

```
# service drweb-configd restart
```

8. Краткие инструкции

В этом разделе

- Работа с прокси-серверами HTTP и веб-серверами:
  - Как подключить Dr.Web Gateway Security Suite к Squid
  - Как защитить веб-сервер
  - Как настроить режим прокси для SplDer Gate
- Общие вопросы по управлению Dr.Web Gateway Security Suite:
  - Как перезапустить Dr.Web Gateway Security Suite
  - Как подключиться к серверу централизованной защиты
  - Как отключиться от сервера централизованной защиты
  - Как активировать Dr.Web Gateway Security Suite
  - Как обновить версию Dr.Web Gateway Security Suite
  - Как добавить или удалить компонент Dr.Web Gateway Security Suite
  - Как управлять работой компонентов Dr.Web Gateway Security Suite
  - Как просмотреть журнал Dr.Web Gateway Security Suite

Как подключить Dr.Web Gateway Security Suite к Squid

Следуйте инструкции, представленной в разделе Интеграция с прокси-сервером Squid.

Как защитить веб-сервер

Следуйте инструкции, представленной в разделе Защита локального веб-сервера.

Как настроить режим прокси для SplDer Gate

Следуйте инструкции, представленной в разделе Использование SplDer Gate в режиме прокси.

Как перезапустить Dr.Web Gateway Security Suite

Для перезапуска уже работающего Dr.Web Gateway Security Suite вы можете использовать управляющий скрипт демона управления конфигурацией Dr.Web ConfigD. Запуск, останов и перезапуск этого демона приводит, соответственно, к запуску, останову и перезапуску всех компонентов Dr.Web Gateway Security Suite.

Скрипт для управления Dr.Web ConfigD располагается в стандартном для ОС каталоге (`/etc/init.d/` для GNU/Linux или `/usr/local/etc/rc.d/` для FreeBSD) и называется `drweb-configd`. Скрипт имеет следующие управляющие параметры:

Параметр	Описание
`start`	Запустить Dr.Web ConfigD, если он еще не запущен. При запуске Dr.Web ConfigD запустит все необходимые компоненты Dr.Web Gateway Security Suite.
`stop`	Завершить работу Dr.Web ConfigD, если он запущен. При завершении работы Dr.Web ConfigD завершит работу всех компонентов Dr.Web Gateway Security Suite.
`restart`	Перезапустить (завершить и запустить) Dr.Web ConfigD, который завершит и запустит все компоненты Dr.Web Gateway Security Suite. Если Dr.Web ConfigD не был запущен, равносильно `start`.
`condrestart`	Перезапустить Dr.Web ConfigD только в том случае, если он был запущен.
`reload`	Послать Dr.Web ConfigD сигнал HUP, если он запущен. Dr.Web ConfigD перешлет этот сигнал всем компонентам Dr.Web Gateway Security Suite. Используется для инициации процесса перечитывания конфигурации всеми компонентами Dr.Web Gateway Security Suite.
`status`	Вывести на консоль текущее состояние Dr.Web ConfigD.

Например, для перезапуска Dr.Web Gateway Security Suite (или запуска, если он не был запущен) в ОС семейства GNU/Linux используйте команду:

```
# /etc/init.d/drweb-configd restart
```

Как подключиться к серверу централизованной защиты

1. Получите от администратора антивирусной сети адрес сервера централизованной защиты и файл его сертификата, а также, при необходимости, дополнительные параметры, такие как идентификатор станции и пароль, или идентификаторы основной и тарифной группы.
2. Воспользуйтесь командой `esconnect` утилиты управления Dr.Web Gateway Security Suite из командной строки Dr.Web Ctl.

   Для подключения обязательно используйте параметр `--Certificate`, указав путь к файлу сертификата сервера. Дополнительно вы можете указать идентификатор узла («станции», с точки зрения сервера централизованной защиты) и пароль для аутентификации на сервере, если они вам известны, используя параметры `--Login` и `--Password`. Если эти параметры заданы, то подключение к серверу будет успешным только при указании правильной пары идентификатор/пароль. Если эти параметры не указаны, то подключение к серверу будет успешным только в случае его одобрения на сервере (автоматически или администратором антивирусной сети, в зависимости от настроек сервера).

Кроме того, вы можете использовать параметр `--Newbie` (подключиться как «новичок»). Если этот режим подключения разрешен на сервере, то, после одобрения подключения, сервер автоматически сгенерирует для хоста уникальную пару идентификатор/пароль, которая в дальнейшем будет использоваться для его подключения к этому серверу.

При подключении как «новичок», новая учетная запись для хоста будет сгенерирована сервером централизованной защиты даже в том случае, если ранее он уже имел учетную запись на этом сервере.

Типовой пример команды подключения Dr.Web Gateway Security Suite к серверу централизованной защиты:

```
# drweb-ctl esconnect <адрес сервера> --Certificate
<путь к файлу сертификата сервера>
```

После успешного подключения к серверу централизованной защиты Dr.Web Gateway Security Suite будет работать в режиме централизованной защиты или в мобильном режиме, в зависимости от разрешений, установленных на сервере и значения параметра конфигурации `MobileMode` компонента Dr.Web ES Agent. Для принудительного использования мобильного режима установите этот параметр в значение `On`. Для работы в режиме централизованной защиты установите параметр в значение `Off`.

Типовой пример команды перевода Dr.Web Gateway Security Suite, подключенного к серверу централизованной защиты, в мобильный режим:

```
# drweb-ctl cfset ESAgent.MobileMode On
```

Если используемый сервер централизованной защиты не поддерживает или запрещает мобильный режим работы, то изменение значения параметра конфигурации `MobileMode` не переведет Dr.Web Gateway Security Suite в мобильный режим.

Как отключиться от сервера централизованной защиты

Для отключения Dr.Web Gateway Security Suite от сервера централизованной защиты и перевода его в автономный режим используйте команду `esdisconnect` утилиты управления Dr.Web Gateway Security Suite из командной строки Dr.Web Ctl:

```
# drweb-ctl esdisconnect
```

Для успешной работы Dr.Web Gateway Security Suite в автономном режиме необходимо иметь действующий лицензионный ключевой файл. В противном случае антивирусные функции Dr.Web Gateway Security Suite после перехода в автономный режим *будут заблокированы*.

Как активировать Dr.Web Gateway Security Suite

1. Пройдите регистрацию на сайте компании «Доктор Веб» по адресу https://products.drweb.com/register/v4.
2. Получите на указанный при регистрации адрес электронной почты (или загрузите непосредственно с сайта после окончания регистрации) архив, содержащий действительный лицензионный ключевой файл.
3. Выполните процедуру установки ключевого файла.

Как обновить версию Dr.Web Gateway Security Suite

Обновите версии компонентов или выполните переход на новую версию.

Вам может быть предложено удалить текущую версию Dr.Web Gateway Security Suite.

Как добавить или удалить компонент Dr.Web Gateway Security Suite

Воспользуйтесь процедурой выборочной установки и удаления компонентов.

При установке или удалении компонента для удовлетворения зависимостей могут быть дополнительно установлены или удалены другие компоненты Dr.Web Gateway Security Suite.

Как управлять работой компонентов Dr.Web Gateway Security Suite

Для просмотра состояния компонентов Dr.Web Gateway Security Suite и управления их работой используйте:

- Утилиту управления из командной строки Dr.Web Ctl. Используйте команды `drweb-ctl appinfo`, `drweb-ctl cfshow` и `drweb-ctl cfset`. Чтобы просмотреть перечень доступных команд управления, используйте команду `drweb-ctl --help`.
- Веб-интерфейс управления Dr.Web Gateway Security Suite. По умолчанию доступ через браузер осуществляется по адресу `https://127.0.0.1:4443`.

Как просмотреть журнал Dr.Web Gateway Security Suite

При настройках по умолчанию общий журнал всех компонентов Dr.Web Gateway Security Suite выводится в `syslog` (файл, в который записывает сообщения системный

компонент `syslog`, зависит от системы и находится в каталоге `/var/log`). Общие настройки ведения журнала задаются в конфигурационном файле в секции `[Root]` (параметры `Log` и `DefaultLogLevel`). Для каждого из компонентов в его секции настроек доступны параметры `Log` и `LogLevel`, задающие место хранения журнала и уровень подробности сообщений, выводимых компонентом в журнал.

Также вы можете использовать команду `drweb-ctl log`.

Чтобы изменить настройки ведения журнала, используйте утилиту управления из командной строки Dr.Web Ctl или веб-интерфейс управления Dr.Web Gateway Security Suite.

Чтобы облегчить идентификацию ошибок, настройте вывод общего журнала всех компонентов в отдельный файл и разрешите вывод расширенной отладочной информации. Для этого выполните команды:

```
# drweb-ctl cfset Root.Log <путь к файлу журнала>
# drweb-ctl cfset Root.DefaultLogLevel DEBUG
```

Чтобы вернуть настройки ведения общего журнала всех компонентов по умолчанию, выполните команды:

```
# drweb-ctl cfset Root.Log -r
# drweb-ctl cfset Root.DefaultLogLevel -r
```

9. Компоненты Dr.Web Gateway Security Suite

В разделе перечислены компоненты, входящие в состав Dr.Web Gateway Security Suite. Для каждого компонента указаны его назначение, принципы функционирования, а также параметры, которые он хранит в файле конфигурации.

9.1. Dr.Web ConfigD

Демон управления конфигурацией Dr.Web ConfigD — это центральный управляющий компонент Dr.Web Gateway Security Suite. Он обеспечивает централизованное хранение настроек для всех компонентов Dr.Web Gateway Security Suite, управляет активностью всех компонентов и организует доверительный обмен данными между ними.

Dr.Web ConfigD выполняет следующие функции:

- запуск и остановка компонентов Dr.Web Gateway Security Suite в зависимости от настроек;
- автоматический перезапуск компонентов в случае сбоев;
- запуск компонентов по запросу от других компонентов;
- оповещение компонентов об изменении настроек;
- предоставление возможности централизованного управления конфигурационными параметрами;
- предоставление компонентам информации из используемого ключевого файла;
- получение лицензионной информации от компонентов;
- получение новой лицензионной информации от специализированных компонентов;
- оповещение запущенных компонентов об изменении лицензионной информации.

9.1.1. Принципы работы

Демон управления конфигурацией Dr.Web ConfigD всегда запускается с правами суперпользователя (*root*). Он запускает остальные компоненты Dr.Web Gateway Security Suite и связывается с ними через предварительно открытый сокет. Демон управления конфигурацией принимает подключения от прочих компонентов Dr.Web Gateway Security Suite через информационный сокет (доступен публично) и административный сокет (доступен только компонентам, запущенным с правами суперпользователя). Демон загружает параметры конфигурации и лицензионные данные из файлов или обеспечивает их получение от используемого сервера централизованной защиты через агент Dr.Web ES Agent, а также подстановку корректных значений по умолчанию для параметров конфигурации. К моменту старта любого компонента или отсылки ему сигнала SIGHUP демон управления конфигурацией всегда имеет целостный непротиворечивый набор настроек всех компонентов Dr.Web Gateway Security Suite.

При получении сигнала SIGHUP Dr.Web ConfigD перечитывает параметры конфигурации и данные из лицензионного ключевого файла. В случае необходимости демон также рассылает компонентам уведомления, чтобы они перечитали собственные параметры конфигурации.

При получении сигнала SIGTERM Dr.Web ConfigD сначала завершает работу всех компонентов, а потом сам завершает работу. Dr.Web ConfigD обеспечивает удаление всех временных файлов компонентов после того, как они завершат работу.

Принципы взаимодействия с другими компонентами

1. При запуске все компоненты получают от Dr.Web ConfigD параметры конфигурации и лицензионную информацию. В дальнейшей работе компоненты используют только эти полученные настройки.
2. Dr.Web ConfigD обеспечивает сбор сообщений от всех запущенных под его управлением компонентов в единый журнал. Dr.Web ConfigD собирает все сообщения, выводимые компонентами в *stderr*, и помещает в общий журнал Dr.Web Gateway Security Suite с отметкой, у какого компонента и в какой момент произошла ошибка.
3. Все управляемые компоненты завершают работу с определенным кодом. Если код завершения отличен от `101`, `102` и `103`, компонент будет перезапущен, а соответствующее сообщение из *stderr* будет зафиксировано в журнале Dr.Web Gateway Security Suite.
   - Завершение работы с кодом 101 означает, что компонент не может функционировать с предоставленной лицензией. Компонент будет перезапущен только при изменении параметров лицензии.
   - Завершение работы с кодом 102 означает, что он не может функционировать с текущими параметрами конфигурации. Dr.Web ConfigD предпримет попытку перезапустить компонент, когда будет изменены какие-либо параметры конфигурации.
   - Завершение работы с кодом `103` происходит в результате длительного отсутствия обращений к компонентам, запускаемым Dr.Web ConfigD по требованию (Dr.Web Scanning Engine и Dr.Web File Checker). Период, по истечении которого компонент завершает работу с кодом `103`, указывается в настройках соответствующего компонента (параметр `IdleTimeLimit`).
   - Если новые значения параметров конфигурации, полученные компонентом от Dr.Web ConfigD, не могут быть применены «на лету», компонент завершает работу с кодом `0`, чтобы Dr.Web ConfigD перезапустил его.
   - Если компонент не может подключиться к Dr.Web ConfigD или происходит ошибка протокола взаимодействия, компонент отправляет соответствующее сообщение в *stderr* и завершает работу с кодом `1`.

4. Организован обмен сигналами.
   - Чтобы компонент применил измененные параметры конфигурации, Dr.Web ConfigD отправляет ему сигнал SIGHUP.
   - Чтобы компонент завершил работу, Dr.Web ConfigD отправляет ему сигнал SIGTERM. Компонент должен завершить работу в течение 30 секунд после получения сигнала.
   - Если компонент не завершает работу в течение положенных 30 секунд, Dr.Web ConfigD отправляет ему сигнал SIGKILL для принудительного завершения работы.

9.1.2. Аргументы командной строки

Для запуска демона управления конфигурацией Dr.Web ConfigD из командной строки используется следующая команда:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-configd [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-configd [<параметры>]
```

Dr.Web ConfigD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет
`--config`	Назначение: Использовать при работе указанный конфигурационный файл. Краткий вариант: `-c` Аргументы: <*путь к файлу*> — путь к используемому конфигурационному файлу.
`--daemonize`	Назначение: Запустить компонент в режиме демона, т. е. без доступа к терминалу. Краткий вариант: `-d` Аргументы: Нет
`--pid-file`	Назначение: Использовать при работе указанный PID-файл. Краткий вариант: `-p` Аргументы: <*путь к файлу*> — путь к файлу, в котором следует сохранить идентификатор процесса (PID).

Пример:

```
$ /opt/drweb.com/bin/drweb-configd -d -c /etc/opt/drweb.com/drweb.ini
```

Приведенная команда запустит Dr.Web ConfigD в режиме демона, заставив его использовать конфигурационный файл `/etc/opt/drweb.com/drweb.ini`.

Замечания о запуске

Для обеспечения работоспособности Dr.Web Gateway Security Suite компонент должен быть запущен в режиме демона. В штатном режиме Dr.Web ConfigD запускается при старте операционной системы, для чего он оснащен скриптом управления с именем `drweb-configd`, размещенным в системном каталоге (`/etc/init.d` для GNU/Linux или `/usr/local/etc/rc.d` для FreeBSD). Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Gateway Security Suite из командной строки (запускается командой `drweb-ctl`).

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-configd`.

9.1.3. Параметры конфигурации

Демон управления конфигурацией Dr.Web ConfigD использует параметры, указанные в секции `[Root]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента Dr.Web ConfigD. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала демона управления конфигурацией, а также метод ведения журнала для тех компонентов, у которых не указан свой собственный метод ведения журнала.

Параметр	Описание
	 При начальной загрузке, пока конфигурационный файл еще не прочитан, демон управления конфигурацией будет использовать следующие значения этого параметра: • в режиме демона (если был запущен с параметром `-d`) — `SYSLOG:Daemon`; • в ином случае — `Stderr`. Если компонент работает в фоновом режиме (запущен с параметром командной строки `-d`), значение `Stderr` *не может* быть использовано для данного параметра. Значение по умолчанию: `SYSLOG:Daemon`
`PublicSocketPath` *{путь к файлу}*	Путь к сокету, используемому для взаимодействия всех компонентов Dr.Web Gateway Security Suite. Значение по умолчанию: `/var/run/.com.drweb.public`
`AdminSocketPath` *{путь к файлу}*	Путь к сокету, используемому для взаимодействия компонентов Dr.Web Gateway Security Suite, обладающих повышенными (административными) привилегиями. Значение по умолчанию: `/var/run/.com.drweb.admin`
`DebugIpc` *{логический}*	Включать или не включать в журнал на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения IPC (взаимодействие демона управления конфигурацией с другими компонентами). Значение по умолчанию: `No`
`UseCloud` *{логический}*	Использовать или не использовать сервис Dr.Web Cloud для получения сведений о вредоносности файлов и URL. Значение по умолчанию: `No`
`UseVxcube` *{логический}*	Использовать или не использовать Dr.Web vxCube при проверке почтовых вложений в режиме внешнего фильтра, подключенного к MTA. Значение по умолчанию: `No`
`KeyPath` *{путь к файлу}*	Путь к ключевому файлу (лицензионному или демонстрационному). Значение по умолчанию: • для GNU/Linux: `/etc/opt/drweb.com/drweb32.key` • для FreeBSD: `/usr/local/etc/drweb.com/drweb32.key`
`CoreEnginePath` *{путь к файлу}*	Путь к динамической библиотеке антивирусного ядра Dr.Web Virus-Finding Engine. Значение по умолчанию:

Параметр	Описание
	• для GNU/Linux: `/var/opt/drweb.com/lib/drweb32.dll` • для FreeBSD: `/var/drweb.com/lib/drweb32.dll`
`VirusBaseDir` *{путь к каталогу}*	Путь к каталогу, в котором хранятся файлы вирусных баз. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/bases` • для FreeBSD: `/var/drweb.com/bases`
`DwsDir` *{путь к каталогу}*	Путь к каталогу, в котором хранятся файлы автоматически обновляемой базы данных категорий веб-ресурсов. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/dws` • для FreeBSD: `/var/drweb.com/dws`
`VersionDir` *{путь к каталогу}*	Путь к каталогу, в котором хранится информация о текущих версиях используемых компонентов Dr.Web Gateway Security Suite. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/version` • для FreeBSD: `/var/drweb.com/version`
`CacheDir` *{путь к каталогу}*	Путь к каталогу кеша (используется как для кеша обновлений, так и для кеша проверенных файлов). Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/cache` • для FreeBSD: `/var/drweb.com/cache`
`TempDir` *{путь к каталогу}*	Путь к каталогу для хранения временных файлов. Значение по умолчанию: *Путь, извлеченный из системной переменной окружения* `TMPDIR`, `TMP`, `TEMP` или `TEMPDIR` (переменные перебираются в указанном порядке). Если ни одна из них не обнаружена, то используется `/tmp`.
`RunDir` *{путь к каталогу}*	Путь к каталогу, в котором находятся PID-файлы запущенных компонентов и сокеты, используемые для взаимодействия компонентов Dr.Web Gateway Security Suite. Значение по умолчанию: `/var/run`
`VarLibDir` *{путь к каталогу}*	Путь к каталогу библиотек, используемых компонентами Dr.Web Gateway Security Suite. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/lib` • для FreeBSD: `/var/drweb.com/lib`

Параметр	Описание
`AdminGroup` *{имя группы | GID}*	Группа пользователей, обладающих административными правами в рамках Dr.Web Gateway Security Suite. Данные пользователи, наряду с суперпользователем (пользователем *root*), могут повышать привилегии компонентов Dr.Web Gateway Security Suite до привилегий суперпользователя. Значение по умолчанию: *Определяется автоматически* в момент установки Dr.Web Gateway Security Suite
`TrustedGroup` *{имя группы | GID}*	Группа пользователей, являющихся доверенными. Параметр используется в работе компонента проверки сетевого трафика SpIDer Gate. Сетевой трафик таких пользователей пропускается SpIDer Gate без проверки. Значение по умолчанию: `drweb`
`VersionNotification` *{логический}*	Уведомлять или не уведомлять пользователя о наличии обновлений для текущей установленной версии Dr.Web Gateway Security Suite. Значение по умолчанию: `Yes`
`DefaultLogLevel` *{уровень подробности}*	Уровень подробности ведения журнала *для всех компонентов* Dr.Web Gateway Security Suite по умолчанию. Используется, если в конфигурации какого-либо из компонентов не указан свой уровень подробности ведения журнала. Значение по умолчанию: `Notice`
`VxcubeApiAddress` *{строка}*	Доменное имя (FQDN) или IP-адрес узла, на котором находится сервер API Dr.Web vxCube. Значение по умолчанию: *(не задано)*
`VxcubeApiKey` *{строка}*	Ключ API Dr.Web vxCube. Значение по умолчанию: *(не задано)*
`VxcubeProxyUrl` *{адрес подключения}*	Адрес прокси-сервера, который используется для подключения к Dr.Web vxCube. Поддерживаются только HTTP-прокси без авторизации. Возможные значения: <*адрес подключения*> — параметры подключения к прокси-серверу в формате `http://`<*хост*>`:`<*порт*>, где: • <*хост*> — адрес узла, на котором работает прокси-сервер (IP-адрес или имя домена, т. е. FQDN); • <*порт*> — используемый порт. Значение по умолчанию: *(не задано)*

9.2. Dr.Web Ctl

В этом разделе

- Общие сведения
- Удаленная проверка узлов

Общие сведения

Имеется возможность управлять работой Dr.Web Gateway Security Suite из командной строки. Для этого в его состав входит специальная утилита Dr.Web Ctl (`drweb-ctl`). С ее помощью вы можете выполнять из командной строки следующие действия:

- запуск проверки файлов, загрузочных записей дисков и исполняемых файлов активных процессов;
- запуск проверки файлов на удаленных узлах сети (см. примечание ниже);
- запуск обновления антивирусных компонентов (вирусных баз, антивирусного ядра, и прочих, в зависимости от поставки);
- просмотр и изменение параметров конфигурации Dr.Web Gateway Security Suite;
- просмотр состояния компонентов Dr.Web Gateway Security Suite и статистики обнаруженных угроз;
- просмотр карантина и управление его содержимым (через компонент Dr.Web File Checker);
- подключение к серверу централизованной защиты или отключение от него.

Чтобы команды управления, вводимые пользователем, имели эффект, должен быть запущен демон управления конфигурацией Dr.Web ConfigD (по умолчанию он автоматически запускается при старте операционной системы).

Для выполнения некоторых управляющих команд требуются полномочия суперпользователя.

Для получения полномочий суперпользователя используйте команду смены пользователя `su` или команду выполнения от имени другого пользователя `sudo`.

Утилита `drweb-ctl` поддерживает стандартное автодополнение команд управления Dr.Web Gateway Security Suite, если функция автодополнения включена в используемой вами командной оболочке. В случае если командная оболочка не поддерживает автодополнение, вы можете настроить ее при необходимости. Для этого обратитесь к справочному руководству по используемому вами дистрибутиву операционной системы.

При завершении работы утилита возвращает код выхода в соответствии с соглашением для POSIX-совместимых систем: 0 (нуль) — если операция выполнена успешно, и не нуль — в противном случае.

Ненулевой код выхода утилита возвращает только в том случае, когда произошла внутренняя ошибка (например: утилита не смогла подключиться к некоторому компоненту, запрошенная операция не может быть выполнена и т. п.). Если утилита обнаруживает (и, возможно) нейтрализует некоторую угрозу, она возвращает код выхода 0, так как запрошенная операция (такая как `scan` и т. п.) выполнена успешно. Если необходимо установить перечень обнаруженных угроз и примененных к ним действий, то проанализируйте сообщения, которые утилита выводит на консоль.

Коды всех имеющихся ошибок приведены в разделе Приложение Е. Описание известных ошибок.

Удаленная проверка узлов

Dr.Web Gateway Security Suite позволяет проверять на наличие угроз файлы, находящиеся на удаленных узлах сети. В качестве таких узлов могут выступать не только полноценные вычислительные машины (рабочие станции и серверы), но и роутеры, ТВ-приставки и прочие «умные» устройства, образующие так называемый «интернет вещей». Для выполнения удаленной проверки требуется, чтобы удаленный узел предоставлял возможность удаленного доступа к нему через *SSH* (*Secure Shell*) или *Telnet*. Для доступа к устройству вы должны знать его IP-адрес или доменное имя, имя и пароль пользователя, который может совершить удаленный доступ к системе через *SSH* или *Telnet*. Указанный пользователь должен иметь права доступа к проверяемым файлам (как минимум — право на их чтение).

Данная функция может быть использована только для обнаружения вредоносных или подозрительных файлов на удаленном узле. Устранение угроз (то есть изоляция их в карантин, удаление или лечение вредоносных объектов) средствами удаленной проверки невозможно. Для устранения обнаруженных угроз на удаленном узле воспользуйтесь средствами управления, предоставляемыми непосредственно этим узлом. Например, для роутеров и прочих «умных» устройств вы можете обновить прошивку, а для вычислительных машин — подключиться к ним (в том числе в удаленном терминальном режиме) и произвести соответствующие операции в их файловой системе (удаление или перемещение файлов и т. п.) или запустить установленное на них антивирусное ПО.

Удаленная проверка реализуется только через утилиту управления из командной строки `drweb-ctl` (используется команда `remotescan`).

9.2.1. Формат вызова из командной строки

В этом разделе

- Формат вызова утилиты управления из командной строки

- Общие опции
- Команды
  - Команды антивирусной проверки
  - Команды управления обновлением и работой в режиме централизованной защиты
  - Команды управления конфигурацией
  - Команды управления угрозами и карантином
  - Информационные команды

1. Формат вызова утилиты управления из командной строки

Утилита управления работой Dr.Web Gateway Security Suite имеет следующий формат вызова:

```
$ drweb-ctl [<общие опции> | <команда> [<аргумент>] [<опции команды>]]
```

где:

- *<общие опции>* — опции, которые могут быть использованы при запуске без указания команды или для любой из команды. Не являются обязательными для запуска.
- *<команда>* — команда, которая должна быть выполнена Dr.Web Gateway Security Suite (например, запустить проверку файлов, вывести содержимое карантина и т. п.).
- *<аргумент>* — аргумент команды. Зависит от указанной команды. У некоторых команд аргументы отсутствуют.
- *<опции команды>* — опции, управляющие работой указанной команды. Зависят от команды. У некоторых команд опции отсутствуют.

2. Общие опции

Доступны следующие общие опции:

Опция	Описание
`-h, --help`	Вывести на экран краткую общую справку и завершить работу. Для вывода справки по любой команде используйте вызов: `$ drweb-ctl <команда> -h`
`-v, --version`	Вывести на экран версию модуля и завершить работу
`-d, --debug`	Предписывает выводить на экран расширенные диагностические сообщения во время выполнения указанной команды. Не имеет смысла без указания команды. Используйте вызов:

Опция	Описание
	`$ drweb-ctl <команда> -d`

3. Команды

Команды управления Dr.Web Gateway Security Suite разделены на следующие группы:

- команды антивирусной проверки;
- команды управления обновлением и работой в режиме централизованной защиты;
- команды управления конфигурацией;
- команды управления угрозами и карантином;
- информационные команды.

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-ctl`.

3.1. Команды антивирусной проверки

Доступны следующие команды антивирусной проверки файловой системы:

Команда	Описание
`scan <путь>`	**Назначение**: Инициировать проверку компонентом проверки файлов Dr.Web File Checker указанного файла или каталога. **Аргументы** *<путь>* — путь к файлу или каталогу, который нужно проверить (может быть относительным). Этот аргумент может быть опущен в случае использования опции `--stdin` или `--stdin0`. Для проверки перечня файлов, выбираемых по некоторому условию, рекомендуется использовать утилиту `find` (см. Примеры использования) и опцию `--stdin` или `--stdin0`. **Опции** `-a [--Autonomous]` — запустить автономные экземпляры Dr.Web Scanning Engine и Dr.Web File Checker для выполнения заданной проверки, завершив их работу после окончания проверки.

Команда	Описание
	Угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже), также о них не будет сообщено серверу централизованной защиты, если Dr.Web Gateway Security Suite работает под его управлением. `--Report` <*тип*> — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--FollowSymlinks` — автоматически разрешать символические ссылки. `--PackerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ArchiveMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MailMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться.

Команда	Описание
	Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ContainerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MaxCompressionRatio` <*степень*> — максимально допустимая степень сжатия проверяемых объектов. Значение должно быть не менее `2`. Значение по умолчанию: `3000`. `--MaxSizeToExtract` <*число*> — ограничение на размер файлов в архиве. Файлы, размер которых превышает значение этого параметра, будут пропущены при проверке. Размер указывается как число с суффиксом (*b, kb, mb, gb*). Если никакого суффикса не указано, число интерпретируется как размер в байтах. Значение по умолчанию: *(не задано)*. `--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`. `--Exclude` <*путь*> — путь, исключаемый из проверки. Может быть относительным и включать в себя файловую маску (содержащую символы `?` и `*`, а также символьные классы `[ ]`, `[! ]`, `[^ ]`). Необязательная опция; может быть указана более одного раза. `--OnKnownVirus` <*действие*> — действие, которое нужно выполнить, если методами сигнатурного анализа обнаружена известная угроза. Возможные действия: `REPORT`, `CURE`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnIncurable` <*действие*> — действие, которое нужно выполнить, если лечение (`CURE`) обнаруженной угрозы окончилось неудачей или оно невозможно. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnSuspicious` <*действие*> — действие, которое нужно выполнить, если эвристический анализ обнаружит подозрительный объект. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnAdware` <*действие*> — действие, которое нужно выполнить, если обнаружена рекламная программа. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`.

Команда	Описание
	Значение по умолчанию: `REPORT`. `--OnDialers` <*действие*> — действие, которое нужно выполнить, если обнаружена программа дозвона. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnJokes` <*действие*> — действие, которое нужно выполнить, если обнаружена программа-шутка. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnRiskware` <*действие*> — действие, которое нужно выполнить, если обнаружена потенциально опасная программа. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnHacktools` <*действие*> — действие, которое нужно выполнить, если обнаружена программа взлома. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. Если угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т. п.), вместо удаления (`DELETE`) выполняется перемещение контейнера в карантин (`QUARANTINE`). `--stdin` — получить список путей для проверки из стандартного потока ввода (*stdin*). Пути в списке должны быть разделены символом новой строки (`\n`). `--stdin0` — получить список путей для проверки из стандартного потока ввода (*stdin*). Пути в списке должны быть разделены нулевым символом NUL (`\0`). При использовании опций `--stdin` и `--stdin0` пути в списке не должны содержать шаблонов. Предпочтительное использование опций `--stdin` и `--stdin0` — обработка в команде `scan` списка путей, сформированного внешней программой, например, `find` (см. Примеры использования).
`bootscan` <*устройство*> `| ALL`	**Назначение**: Инициировать проверку компонентом проверки файлов Dr.Web File Checker загрузочной записи на указанных дисковых устройствах. Проверяются как записи MBR, так и записи VBR.

Команда	Описание
	Аргументы <*устройство*> — путь к блочному файлу дискового устройства, загрузочная запись на котором подлежит проверке. Может быть указано несколько дисковых устройств через пробел. Обязательный аргумент. Если вместо файла устройства указано `ALL`, будут проверены все загрузочные записи на всех доступных дисковых устройствах. **Опции** `-a [--Autonomous]` — запустить автономные экземпляры Dr.Web Scanning Engine и Dr.Web File Checker для выполнения заданной проверки, завершив их работу после окончания проверки. ⚠ Угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже), также о них не будет сообщено серверу централизованной защиты, если Dr.Web Gateway Security Suite работает под его управлением. `--Report` <*тип*> — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`. `--Cure` <*Yes*|*No*> — требуется ли делать попытки лечения обнаруженных угроз. Если указано `No`, то производится только информирование об обнаруженной угрозе. Значение по умолчанию: `No`. `--ShellTrace` — включить вывод дополнительной отладочной информации при проверке загрузочной записи
`procscan`	**Назначение**: Инициировать проверку компонентом проверки файлов Dr.Web File Checker содержимого исполняемых файлов, содержащих код процессов, запущенных в системе. При обнаружении угрозы выполняется не только обезвреживание вредоносного исполняемого

Команда	Описание
	файла, но и принудительное завершение работы всех процессов, запущенных из него. **Аргументы**: Нет. Эта команда предназначена только для дистрибутивов Dr.Web Gateway Security Suite, работающих под управлением ОС семейства GNU/Linux. **Опции** `-a [--Autonomous]` — запустить автономные экземпляры Dr.Web Scanning Engine и Dr.Web File Checker для выполнения заданной проверки, завершив их работу после окончания проверки. Угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже), также о них не будет сообщено серверу централизованной защиты, если Dr.Web Gateway Security Suite работает под его управлением. `--Report` <*тип*> — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--PackerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке.

Команда	Описание
	Значение по умолчанию: `On`. `--ContainerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--Exclude` <*путь*> — путь, исключаемый из проверки. Может включать в себя файловую маску (содержащую символы `?` и `*`, а также символьные классы `[ ]`, `[! ]`, `[^ ]`). Путь (в том числе содержащий маску) должен быть абсолютным. Необязательная опция; может быть указана более одного раза. `--OnKnownVirus` <*действие*> — действие, которое нужно выполнить, если методами сигнатурного анализа обнаружена известная угроза. Возможные действия: `REPORT`, `CURE`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnIncurable` <*действие*> — действие, которое нужно выполнить, если лечение (`CURE`) обнаруженной угрозы окончилось неудачей или оно невозможно. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnSuspicious` <*действие*> — действие, которое нужно выполнить, если эвристический анализ обнаружит подозрительный объект. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnAdware` <*действие*> — действие, которое нужно выполнить, если обнаружена рекламная программа. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnDialers` <*действие*> — действие, которое нужно выполнить, если обнаружена программа дозвона. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnJokes` <*действие*> — действие, которое нужно выполнить, если обнаружена программа-шутка. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnRiskware` <*действие*> — действие, которое нужно выполнить, если обнаружена потенциально опасная программа. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`.

Команда	Описание
	Значение по умолчанию: `REPORT`. `--OnHacktools` <*действие*> — действие, которое нужно выполнить, если обнаружена программа взлома. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. При обнаружении угроз в исполняемом файле все запущенные из него процессы принудительно завершаются Dr.Web Gateway Security Suite.
`netscan [`<*путь*>`]`	**Назначение**: Инициировать распределенную проверку указанного файла или каталога через агент сетевой проверки данных Dr.Web Network Checker. Если настроенные соединения с другими узлами, на которых имеется продукт Dr.Web для Unix, поддерживающий функцию распределенной проверки, отсутствуют, то будет произведена проверка с использованием сканирующего ядра, доступного локально (аналогично команде `scan`). **Аргументы** <*путь*> — путь к файлу или каталогу, который нужно проверить. Если этот аргумент опущен, то производится сканирование данных, поступающих через входной поток stdin. **Опции** `--Report` <*тип*> — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--PackerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены.

Команда	Описание
	Значение по умолчанию: `8`. `--ArchiveMaxLevel <число>` — максимальный уровень вложенности объектов при проверке архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MailMaxLevel <число>` — максимальный уровень вложенности объектов при проверке файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ContainerMaxLevel <число>` — максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MaxCompressionRatio <степень>` — максимально допустимая степень сжатия проверяемых объектов. Значение должно быть не менее `2`. Значение по умолчанию: `3000`. `--MaxSizeToExtract <число>` — ограничение на размер файлов в архиве. Файлы, размер которых превышает значение этого параметра, будут пропущены при проверке. Размер указывается как число с суффиксом (*b, kb, mb, gb*). Если никакого суффикса не указано, число интерпретируется как размер в байтах. Значение по умолчанию: *(не задано)*. `--HeuristicAnalysis <On|Off>` — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`. `--Cure <Yes|No>` — требуется ли делать попытки лечения обнаруженных угроз. Если указано `No`, то производится только информирование об обнаруженной угрозе. Значение по умолчанию: `No`

Команда	Описание
`flowscan <путь>`	**Назначение**: Инициировать проверку компонентом проверки файлов Dr.Web File Checker указанного файла или каталога с использованием метода проверки «flow». ⚠ Для проверки файлов и каталогов рекомендуется использовать команду `scan`. **Аргументы** *<путь>* — путь к файлу или каталогу, который нужно проверить. **Опции** `--ScanTimeout` *<интервал времени>* — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--PackerMaxLevel` *<число>* — максимальный уровень вложенности объектов при проверке запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ArchiveMaxLevel` *<число>* — максимальный уровень вложенности объектов при проверке архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MailMaxLevel` *<число>* — максимальный уровень вложенности объектов при проверке файлов почтовых программ (`.pst`, `.tbb` и т. п.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. п. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ContainerMaxLevel` *<число>* — максимальный уровень вложенности объектов при проверке других типов объектов с

Команда	Описание
	вложениями (страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MaxCompressionRatio` <*степень*> — максимально допустимая степень сжатия проверяемых объектов. Должна быть не менее `2`. Значение по умолчанию: `3000`. `--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`. `--OnKnownVirus` <*действие*> — действие, которое нужно выполнить, если методами сигнатурного анализа обнаружена известная угроза. Возможные действия: `REPORT`, `CURE`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnIncurable` <*действие*> — действие, которое нужно выполнить, если лечение (`CURE`) обнаруженной угрозы окончилось неудачей или оно невозможно. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnSuspicious` <*действие*> — действие, которое нужно выполнить, если эвристический анализ обнаружит подозрительный объект. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnAdware` <*действие*> — действие, которое нужно выполнить, если обнаружена рекламная программа. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnDialers` <*действие*> — действие, которое нужно выполнить, если обнаружена программа дозвона. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnJokes` <*действие*> — действие, которое нужно выполнить, если обнаружена программа-шутка. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. `--OnRiskware` <*действие*> — действие, которое нужно выполнить, если обнаружена потенциально опасная программа. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`.

Команда	Описание
	Значение по умолчанию: `REPORT`. `--OnHacktools` <*действие*> — действие, которое нужно выполнить, если обнаружена программа взлома. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`. Если угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т. п.), вместо удаления (`DELETE`) выполняется перемещение контейнера в карантин (`QUARANTINE`).
`rawscan` <*путь*>	**Назначение**: Инициировать «сырую» проверку указанного файла или каталога с использованием сканирующего ядра Dr.Web Scanning Engine напрямую, без использования компонента проверки файлов Dr.Web File Checker. Угрозы, обнаруженные при «сыром» сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже). Рекомендуется использовать эту команду только для отладки функционирования Dr.Web Scanning Engine. Команда имеет следующую особенность: она выводит заключение «cured» (вылечен), если нейтрализована, по меньшей мере, *одна* из угроз, обнаруженных в файле (не обязательно *все* из них). Таким образом, *не рекомендуется* использовать эту команду, если требуется надежное сканирование файлов. Вместо этого для проверки файлов и каталогов рекомендуется использовать команду `scan`. **Аргументы** <*путь*> — путь к файлу или каталогу, который нужно проверить. **Опции** `--ScanEngine` <*путь*> — путь к Unix-сокету сканирующего ядра Dr.Web Scanning Engine. Если не указан, то для проверки будет запущен автономный экземпляр сканирующего ядра (будет завершен после окончания проверки). `--Report` <*тип*> — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON.

Команда	Описание
	Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--PackerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ArchiveMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MailMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ContainerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MaxCompressionRatio` <*степень*> — максимально допустимая степень сжатия проверяемых объектов. Должна быть не менее `2`. Значение по умолчанию: `3000`.

Команда	Описание
	`--MaxSizeToExtract` <*число*> — ограничение на размер файлов в архиве. Файлы, размер которых превышает значение этого параметра, будут пропущены при проверке. Размер указывается как число с суффиксом (*b, kb, mb, gb*). Если никакого суффикса не указано, число интерпретируется как размер в байтах. Значение по умолчанию: *(не задано)*. `--HeuristicAnalysis` <*On*|*Off*> — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`. `--Cure` <*Yes*|*No*> — требуется ли делать попытки лечения обнаруженных угроз. Если указано `No`, то производится только информирование об обнаруженной угрозе. Значение по умолчанию: `No`. `--ListCleanItem` — включить вывод списка чистых файлов при проверке контейнера. `--ShellTrace` — включить вывод дополнительной отладочной информации при проверке файла. `--Output` <*путь к файлу*> — дублировать вывод команды в указанный файл
`remotescan` <*узел*> <*путь*>	**Назначение**: Инициировать проверку указанного файла или каталога на указанном удаленном узле, подключившись к нему через *SSH* или *Telnet*. Угрозы, обнаруженные при удаленном сканировании, не будут нейтрализованы, более того, они не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже). Вы можете использовать эту команду только для обнаружения вредоносных или подозрительных файлов на удаленном узле. Для устранения обнаруженных угроз на удаленном узле необходимо воспользоваться средствами управления, предоставляемыми непосредственно этим узлом. Например, для роутеров, ТВ-приставок и прочих «умных» устройств вы можете воспользоваться механизмом обновления прошивки, а для вычислительных машин — выполнив подключение к ним (в том числе — в удаленном терминальном режиме) и произведя соответствующие операции в их файловой системе (удаление или перемещение файлов и т. п.) или запустив антивирусное ПО, установленное на них.

Команда	Описание
	Аргументы • <*узел*> — IP-адрес или доменное имя узла, к которому необходимо подключиться для проверки. • <*путь*> — путь к файлу или каталогу, который нужно проверить (должен быть абсолютным). **Опции** `-l [--Login]` <*имя*> — логин (имя пользователя) для авторизации на удаленном узле через выбранный протокол. Если имя пользователя не указано, будет произведена попытка подключиться к удаленному узлу от имени пользователя, запустившего команду. `-i [--Identity]` <*путь к файлу*> — файл закрытого ключа для аутентификации указанного пользователя через выбранный протокол. `-m [--Method]` <*SSH|Telnet*> — метод (протокол) подключения к удаленному узлу. Если метод не указан, будет использован SSH. `-p [--Port]` <*число*> — номер порта на удаленном узле для подключения через выбранный протокол. Значение по умолчанию: Порт по умолчанию для выбранного протокола (`22` — для SSH, `23` — для Telnet). `--UseChannels` <*число*> — число каналов передачи данных. Значение по умолчанию: `5`. `--Password` <*пароль*> — пароль для аутентификации указанного пользователя через выбранный протокол. Пароль передается в открытом виде. `--Report` <*тип*> — тип отчета о проверке. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. Значение по умолчанию: `BRIEF`. `--ScanTimeout` <*интервал времени*> — тайм-аут на проверку одного файла в миллисекундах. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0`. `--PackerMaxLevel` <*число*> — максимальный уровень вложенности объектов при проверке запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи

Команда	Описание
	специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ArchiveMaxLevel <число>` — максимальный уровень вложенности объектов при проверке архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MailMaxLevel <число>` — максимальный уровень вложенности объектов при проверке файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--ContainerMaxLevel <число>` — максимальный уровень вложенности объектов при проверке других типов объектов с вложениями (страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8`. `--MaxCompressionRatio <степень>` — максимально допустимая степень сжатия проверяемых объектов. Должна быть не менее `2`. Значение по умолчанию: `3000`. `--MaxSizeToExtract <число>` — ограничение на размер файлов в архиве. Файлы, размер которых превышает значение этого параметра, будут пропущены при проверке. Размер указывается как число с суффиксом (*b, kb, mb, gb*). Если никакого суффикса не указано, число интерпретируется как размер в байтах. Значение по умолчанию: *(не задано)*. `--HeuristicAnalysis <On|Off>` — использовать ли эвристический анализ при проверке. Значение по умолчанию: `On`.

Команда	Описание
	`--Exclude` <*путь*> — путь, исключаемый из проверки. Может включать в себя файловую маску (содержащую символы `?` и `*`, а также символьные классы `[ ]`, `[! ]`, `[^ ]`). Путь (в том числе содержащий маску) должен быть абсолютным. Необязательная опция; может быть указана более одного раза. `--TransferListenAddress` <*адрес*> — адрес, прослушиваемый для приема файлов, передаваемых на проверку удаленным устройством. Необязательная опция. Если не указана, используется произвольный адрес. `--TransferListenPort` <*порт*> — порт, прослушиваемый для приема файлов, передаваемых на проверку удаленным устройством. Необязательная опция. Если не указана, используется случайный порт. `--TransferExternalAddress` <*адрес*> — адрес для передачи файлов на проверку, сообщаемый удаленному устройству. Необязательная опция. Если не указана, используется значение опции `--TransferListenAddress`, либо исходящий адрес уже установленной сессии. `--TransferExternalPort` <*порт*> — порт для передачи файлов на проверку, сообщаемый удаленному устройству. Необязательная опция. Если не указана, используется порт, определенный автоматически. `--ForceInteractive` — использовать интерактивную сессию SSH (только для метода подключения SSH). *Необязательная опция.*

3.2. Команды управления обновлением и работой в режиме централизованной защиты

Доступны следующие команды управления обновлением и работой в режиме централизованной защиты:

Команда	Описание
`update`	**Назначение**: Инициировать процесс обновления антивирусных компонентов (вирусных баз, антивирусного ядра и прочих, в зависимости от поставки) с серверов обновлений компании «Доктор Веб» или из локального облака, через Dr.Web MeshD, прервать уже запущенный процесс обновления или откатить результаты последнего обновления, восстановив предыдущие версии обновленных файлов. Команда не имеет эффекта, если Dr.Web Gateway Security Suite работает под управлением сервера централизованной защиты.

Команда	Описание
	Аргументы: Нет. **Опции** `--Stop` — прервать уже идущий процесс обновления. `--Rollback` — откатить последнее обновление и восстановить последние сохраненные копии обновленных файлов. `--From` <*путь*> — выполнить обновление из указанного каталога без подключения к интернету. `--Path` <*путь*> — сохранить в указанный каталог файлы, которые будут использоваться для обновления без подключения к интернету. Если в этот каталог уже были загружены файлы, то они будут обновлены.
`esconnect` <*сервер*>`[:`<*порт*>`]`	**Назначение**: Подключить Dr.Web Gateway Security Suite к указанному серверу централизованной защиты. О режимах работы см. в разделе Режимы работы. **Аргументы** • <*сервер*> — IP-адрес или имя узла в сети, на котором располагается сервер централизованной защиты. Обязательный аргумент. • <*порт*> — номер порта, используемого сервером централизованной защиты. Необязательный аргумент, указывается только в случае, если сервер централизованной защиты использует нестандартный порт. **Опции** `--Certificate` <*путь*> — путь к файлу сертификата сервера централизованной защиты, к которому производится подключение. `--Login` <*ID*> — логин (идентификатор рабочей станции) для подключения к серверу централизованной защиты. `--Password` <*пароль*> — пароль для подключения к серверу централизованной защиты. `--Compress` <*On*|*Off*> — принудительно инициировать сжатие передаваемых данных (`On`) или запретить его (`Off`). Если опция не указана, использование сжатия определяется сервером. `--Encrypt` <*On*|*Off*> — принудительно инициировать шифрование передаваемых данных (`On`) или запретить его (`Off`). Если опция не указана, использование шифрования определяется сервером. `--Newbie` — подключиться как «новичок» (получить новую учетную запись на сервере). `--Group` <*ID*> — идентификатор группы на сервере, в которую следует поместить рабочую станцию при подключении. `--Rate` <*ID*> — идентификатор тарифной группы, которую следует применить к рабочей станции при ее включении в группу на сервере централизованной защиты (может быть указана только совместно с опцией `--Group`).

Команда	Описание
	`--CfgFile` <*путь*> — подключиться к серверу централизованной защиты, используя конфигурационный файл с настройками соединения. Для выполнения этой команды требуется, чтобы `drweb-ctl` была запущена от имени суперпользователя (пользователя *root*). При необходимости используйте команды `su` или `sudo`.
`esdisconnect`	**Назначение**: Отключить Dr.Web Gateway Security Suite от сервера централизованной защиты и перевести его в автономный режим работы. Команда не имеет эффекта, если Dr.Web Gateway Security Suite уже работает в автономном режиме. **Аргументы**: Нет. **Опции**: Нет. Для выполнения этой команды требуется, чтобы `drweb-ctl` была запущена от имени суперпользователя (пользователя *root*). При необходимости используйте команды `su` или `sudo`.

3.3. Команды управления конфигурацией

Доступны следующие команды управления конфигурацией:

Команда	Описание
`cfset` <*секция*>`.`<*параметр*> <*значение*>	**Назначение**: Изменить активное значение указанного параметра текущей конфигурации Dr.Web Gateway Security Suite. **Аргументы** • <*секция*> — имя секции конфигурационного файла, в которой находится изменяемый параметр. Обязательный аргумент. • <*параметр*> — имя изменяемого параметра. Обязательный аргумент. • <*значение*> — новое значение параметра. Обязательный аргумент.

Команда	Описание
	Для задания значения параметров всегда используется формат `<секция>.<параметр> <значение>`, знак присваивания = не используется. Если вы хотите задать несколько значений параметра, то нужно повторить вызов команды `cfset` столько раз, сколько значений параметра вы хотите добавить. При этом для добавления нового значения в список значений параметра необходимо использовать опцию `-a` (см. ниже). Нельзя указывать в качестве аргумента последовательность `<параметр> <значение 1>, <значение 2>`, так как строка "`<значение 1>, <значение 2>`" будет считаться единым значением параметра `<параметр>`. Описание конфигурационного файла доступно в разделе Приложение Г. Конфигурационный файл Dr.Web Gateway Security Suite, а также в документации `man 5 drweb.ini`. **Опции** `-a [--Add]` — не заменять текущее значение параметра, а добавить указанное значение в список значений параметра (допустимо только для параметров, которые могут иметь список значений). Также эту опцию необходимо использовать для добавления новых групп параметров с тегом. `-e [--Erase]` — не заменять текущее значение параметра, а удалить указанное значение из его списка (допустимо только для параметров, которые имеют список значений). `-r [--Reset]` — сбросить параметр в значение по умолчанию. `<значение>` в этом случае в команде не указывается, а если указано — игнорируется. Опции не являются обязательными. Если они не указаны, то текущее значение параметра (в том числе список значений) заменяется на указанное значение. Для секций, описывающих индивидуальные параметры точек подключения компонента Dr.Web ClamD, применение опции `-r` приводит к замене значения параметра в индивидуальной секции на значение, указанное у

Команда	Описание
	соответствующего «родительского» параметра в секции настроек компонента. Если требуется добавить новую точку подключения *<point>* для Dr.Web ClamD, используйте команду `cfset ClamD.Endpoint.<point> -a`, например: `cfset ClamD.Endpoint.point1 -a` Для выполнения этой команды требуется, чтобы `drweb-ctl` была запущена от имени суперпользователя (пользователя *root*). При необходимости используйте команды `su` или `sudo`.
`cfshow [<секция>[.<параметр>]]`	**Назначение**: Вывести на экран параметры текущей конфигурации Dr.Web Gateway Security Suite. Для вывода параметров по умолчанию используется формат *<секция>.<параметр> = <значение>*. Секции и параметры не установленных компонентов по умолчанию не выводятся. **Аргументы** • *<секция>* — имя секции конфигурационного файла, параметры которой нужно вывести на экран. Необязательный аргумент. Если не указан, то на экран выводятся параметры всех секций конфигурационного файла. • *<параметр>* — имя выводимого параметра. Необязательный аргумент. Если не указан, выводятся все параметры указанной секции, в противном случае выводится только этот параметр. Если указан без имени секции, то выводятся все вхождения этого параметра во все секции конфигурационного файла. **Опции** `--Uncut` — вывести на экран все параметры конфигурации, а не только те, которые используются текущим установленным набором компонентов. Если не указано, то выводятся только те параметры, которые используются имеющимися компонентами. `--Changed` — вывести только те параметры, значения которых отличаются от значений по умолчанию. `--Ini` — вывести значения параметров в формате файла `.ini`: сначала в отдельной строке выводится имя секции, заключенное в квадратные скобки, после чего параметры, принадлежащие секции, перечисляются в виде пар *<параметр> = <значение>* (по одному в строке).

Команда	Описание
	`--Value` — вывести только значение указанного параметра. В этом случае аргумент <*параметр*> обязателен.
`reload`	**Назначение**: Перезагрузить конфигурацию Dr.Web Gateway Security Suite. При этом демон управления конфигурацией Dr.Web ConfigD выполняет следующие действия: • перечитывает конфигурацию и рассылает ее изменения всем компонентам Dr.Web Gateway Security Suite; • переоткрывает журнал Dr.Web Gateway Security Suite; • запускает компоненты, использующие вирусные базы (включая антивирусное ядро); • пытается запустить компоненты, работа которых была нештатно завершена. **Аргументы**: Нет. **Опции**: Нет

3.4. Команды управления угрозами и карантином

Доступны следующие команды управления угрозами и карантином:

Команда	Описание
`threats [`<*действие*> <*объект*>`]`	**Назначение**: Выполнить указанное действие с обнаруженными ранее угрозами по их идентификаторам. Тип действия определяется указанной опцией команды. Если действие не указано, то вывести на экран информацию об обнаруженных, но не обезвреженных угрозах. Информация об угрозах выводится в соответствии с форматом, заданным необязательной опцией `--Format`. Если опция `--Format` не указана, то для каждой угрозы выводится следующая информация: • идентификатор, присвоенный угрозе (порядковый номер); • полный путь к инфицированному файлу; • информация об угрозе (имя, тип по классификации компании «Доктор Веб»); • информация о файле: размер, пользователь-владелец, дата последнего изменения; • история действий с инфицированным файлом: обнаружение, применявшиеся действия и т. п. **Аргументы**: Нет.

Команда	Описание
	Опции `--Format "<строка формата>"` — выводить информацию об угрозах в указанном формате. Описание строки формата приведено ниже. Если эта опция указана совместно с любой из опций-действий, она игнорируется. `-f [--Follow]` — ожидать поступления новых сообщений об угрозах и выводить их сразу при поступлении (CTRL+C прерывает ожидание). Если эта опция указана совместно с любой из опций-действий, она игнорируется. `--Cure <список угроз>` — выполнить попытку лечения перечисленных угроз (идентификаторы угроз перечисляются через запятую); `--Quarantine <список угроз>` — выполнить перемещение в карантин перечисленных угроз (идентификаторы угроз перечисляются через запятую); `--Delete <список угроз>` — выполнить удаление перечисленных угроз (идентификаторы угроз перечисляются через запятую); `--Ignore <список угроз>` — игнорировать перечисленные угрозы (идентификаторы угроз перечисляются через запятую). Если требуется применить действие ко всем обнаруженным угрозам, вместо *<список угроз>* укажите `All`. Например, команда: `$ drweb-ctl threats --Quarantine All` перемещает в карантин все обнаруженные объекты с угрозами. `--Directory <список каталогов>` — выводить только те угрозы, которые были обнаружены в файлах в каталогах из *<списка каталогов>*. Если эта опция указана совместно с любой из опций, приведенных ниже, она игнорируется.
`quarantine [<действие> <объект>]`	**Назначение**: Применить действие к указанному объекту, находящемуся в карантине. Если действие не указано, то вывести на экран информацию об объектах, находящихся в карантине, с указанием их идентификаторов и краткой информации об исходных файлах, перемещенных в карантин. Информация об изолированных объектах выводится в соответствии с форматом, заданным необязательной опцией `--Format`. Если опция `--Format` не указана, то для каждого изолированного объекта выводится следующая информация: • идентификатор, присвоенный изолированному объекту в карантине; • исходный путь к файлу, перемещенному в карантин; • дата перемещения файла в карантин;

Команда	Описание
	• информация о файле: размер, пользователь-владелец, дата последнего изменения; • информация об угрозе (имя, тип по классификации компании «Доктор Веб»). **Аргументы**: Нет. **Опции** `--Format "<`*строка формата*`>"` — выводить информацию об объектах, находящихся в карантине, в указанном формате. Описание строки формата приведено ниже. Если эта опция указана совместно с любой из опций-действий, она игнорируется. `-f [--Follow]` — ожидать поступления новых сообщений об угрозах и выводить их сразу при поступлении (CTRL+C прерывает ожидание). Если эта опция указана совместно с любой из опций-действий, она игнорируется. `-a [--Autonomous]` — запустить автономный экземпляр компонента проверки файлов Dr.Web File Checker для выполнения заданного действия с карантином, завершив работу компонента после окончания действия. Эта опция может быть применена совместно с любой из опций, указанных ниже. `--Discovery [<`*список каталогов*`>,]` — произвести поиск каталогов карантина в указанном списке каталогов и добавить их к консолидированному карантину в случае обнаружения. Если `<`*список каталогов*`>` не указан, то произвести поиск каталогов карантина в стандартных местах файловой системы (точки монтирования томов и домашние каталоги пользователей). Эта опция может быть указана совместно не только с опцией `-a` (`--Autonomous`) (см. выше), но и с любой из опций-действий, перечисленных ниже. Более того, если команда `quarantine` запускается в режиме автономного экземпляра, т. е. с опцией `-a` (`--Autonomous`), но без опции `--Discovery`, то это равносильно вызову: `quarantine --Autonomous --Discovery` `--Delete <`*объект*`>` — удалить указанный объект, помещенный в карантин. ⚠ Удаление объекта, помещенного в карантин — необратимая операция. `--Restore <`*объект*`>` — восстановить указанный объект из карантина в исходное место.

Команда	Описание
	Для выполнения этого действия может потребоваться, чтобы `drweb-ctl` была запущена от имени суперпользователя (пользователя *root*). Восстановить файл из карантина можно, даже если он инфицирован. `--Cure` <*объект*> — попытаться вылечить указанный объект в карантине. Даже если объект был успешно вылечен, то он все равно останется в карантине. Для извлечения объекта из карантина воспользуйтесь опцией восстановления `--Restore`. `--TargetPath` <*путь*> — восстановить объект из карантина в указанное место: как файл с указанным именем, если <*путь*> — это путь к файлу, или в указанный каталог (если <*путь*> — это путь к каталогу). Может быть указан как абсолютный путь, так и относительный (относительно текущего каталога). Опция применяется только совместно с опцией восстановления `--Restore`. В качестве <*объект*> используется идентификатор объекта в карантине. Если требуется применить действие ко всем объектам, находящимся в карантине, вместо <*объект*> укажите `All`. Например, команда `$ drweb-ctl quarantine --Restore All --TargetPath test` восстанавливает из карантина все имеющиеся в нем объекты, помещая их в подкаталог `test`, находящийся в текущем каталоге, из которого запущена команда `drweb-ctl`. Если для варианта `--Restore All` указана дополнительная опция `--TargetPath`, то она должна задавать путь к каталогу, а не к файлу.

Форматированный вывод данных для команд threats и quarantine

Формат вывода задается строкой формата, указанной в качестве аргумента необязательной опции `--Format`. Строка формата обязательно указывается в кавычках. Строка формата может включать в себя как обычные символы (будут выведены на экран «как есть»), так и специализированные маркеры, которые при выводе будут заменены на соответствующую информацию. Доступны следующие маркеры:

1. Общие для команд `threats` и `quarantine`:

Маркер	Описание
`%{n}`	Перевод строки
`%{t}`	Табуляция
`%{threat_name}`	Имя обнаруженной угрозы по классификации компании «Доктор Веб»
`%{threat_type}`	Тип угрозы («known virus» и т. д.) по классификации компании «Доктор Веб»
`%{size}`	Размер исходного файла
`%{origin}`	Полное имя исходного файла с путем
`%{path}`	Синоним `%{origin}`
`%{ctime}`	Дата/время модификации исходного файла в формате "*%Y-%b-%d %H:%M:%S*" (например, "`2018-Jul-20 15:58:01`")
`%{timestamp}`	То же, что и `%{ctime}`, но в формате времени *Unix timestamp*
`%{owner}`	Пользователь-владелец исходного файла
`%{rowner}`	Удаленный пользователь-владелец исходного файла (если не применимо или значение неизвестно — заменяется на `?`)

2. Специфические для команды `threats`:

Маркер	Описание
`%{hid}`	Идентификатор записи об угрозе в реестре истории событий, связанных с угрозой
`%{tid}`	Идентификатор угрозы
`%{htime}`	Дата/время события, связанного с угрозой
`%{app}`	Идентификатор компонента Dr.Web Gateway Security Suite, обработавшего угрозу
`%{event}`	Последнее событие, связанное с угрозой: • `FOUND` — угроза была обнаружена; • `CURE` — угроза была вылечена; • `QUARANTINE` — файл с угрозой был перемещен в карантин;

Маркер	Описание
	• `DELETE` — файл с угрозой был удален; • `IGNORE` — угроза была проигнорирована; • `RECAPTURED` — угроза была обнаружена другим компонентом
`%{err}`	Текст сообщения об ошибке (если ошибки нет — заменяется на пустую строку)

3. Специфические для команды `quarantine`:

Маркер	Описание
`%{qid}`	Идентификатор объекта в карантине
`%{qtime}`	Дата/время перемещения объекта в карантин
`%{curetime}`	Дата/время попытки лечения объекта, перемещенного в карантин (если не применимо или значение неизвестно — заменяется на `?`)
`%{cureres}`	Результат попытки лечения объекта, перемещенного в карантин: • `cured` — угроза вылечена; • `not cured` — угроза не вылечена либо попыток лечения не производилось

Пример

```
$ drweb-ctl quarantine --Format "{%{n} %{origin}: %{threat_name} - %{qtime}%{n}}"
```

Данная команда выведет содержимое карантина в виде записей следующего вида:

```
{
 <путь к файлу>: <имя угрозы> - <дата перемещения в карантин>
}
…
```

3.5. Информационные команды

Доступны следующие информационные команды:

Команда	Описание
`appinfo`	**Назначение**: Вывести на экран информацию о работающих компонентах Dr.Web Gateway Security Suite. Для каждого запущенного компонента выводится следующая информация: • внутреннее имя; • идентификатор процесса GNU/Linux (PID);

Команда	Описание
	• состояние (запущен, остановлен и т. п.); • код ошибки, если работа компонента завершена вследствие ошибки; • дополнительная информация (опционально); Для демона управления конфигурацией (`drweb-configd`) в качестве дополнительной информации выводятся: • перечень установленных компонентов — *Installed*; • перечень компонентов, запуск которых должен быть обеспечен демоном — *Should run*. **Аргументы**: Нет. **Опции** `-f [--Follow]` — ожидать поступления новых сообщений об изменении состояния модулей и выводить их на экран сразу при поступлении (CTRL+C прерывает ожидание)
`baseinfo`	**Назначение**: Вывести на экран информацию о текущей версии антивирусного ядра и состоянии вирусных баз. Выводится следующая информация: • версия антивирусного ядра; • дата и время выпуска используемых вирусных баз; • число доступных записей об угрозах; • момент последнего успешного обновления вирусных баз и антивирусного ядра; • момент следующего запланированного автоматического обновления. **Аргументы**: Нет. **Опции** `-l [--List]` — вывести полный список загруженных файлов вирусных баз данных и число записей об угрозах в каждом файле
`certificate`	**Назначение**: Вывести на экран содержимое доверенного сертификата Dr.Web, который используется Dr.Web Gateway Security Suite для доступа к защищенным соединениям с целью их проверки, если эта проверка включена в настройках. Чтобы сохранить сертификат в файл <*cert_name*>`.pem`, используйте команду: `$ drweb-ctl certificate > <cert_name>.pem` **Аргументы**: Нет. **Опции**: Нет

Команда	Описание
`events`	**Назначение**: Просмотреть события Dr.Web Gateway Security Suite. Кроме этого, команда позволяет выполнить управление событиями (отметка как «прочитанные», удаление). **Аргументы**: Нет. **Опции** `--Report` <*тип*> — тип отчета о событиях. Возможные значения: • `BRIEF` — краткий отчет; • `DEBUG` — подробный отчет; • `JSON` — сериализованный отчет в формате JSON. `-f [--Follow]` — ожидать поступления новых событий и выводить их на экран сразу при поступлении (нажатие CTRL+C прерывает ожидание). `--ShowSeen` — показать также и уже прочитанные события; `-s [--Since]` <*дата, время*> — показывать события, произошедшие не ранее указанного момента времени (<*дата, время*> указывается в формате "`YYYY-MM-DD hh:mm:ss`"). `-u [--Until]` <*дата, время*> — показывать события, произошедшие не позднее указанного момента времени (<*дата, время*> указывается в формате "`YYYY-MM-DD hh:mm:ss`"). `-t [--Types]` <*список типов*> — показывать события только перечисленных типов (типы событий перечисляются через запятую). Доступен следующий тип событий: `UnexpectedAppTermination` — неожиданное завершение работы какого-либо компонента. Для вывода событий всех типов используйте `All`. `--Show` <*список событий*> — вывести на экран перечисленные события (идентификаторы событий перечисляются через запятую); `--Delete` <*список событий*> — удалить перечисленные события (идентификаторы событий перечисляются через запятую); `--MarkAsSeen` <*список событий*> — отметить перечисленные события как «прочитанные» (идентификаторы событий перечисляются через запятую).

Команда	Описание
	Если требуется отметить как «прочитанные» или удалить все события, вместо <*список событий*> укажите `All`. Например, команда `$ drweb-ctl events --MarkAsSeen All` отметит как «прочитанные» все имеющиеся события
`report` <*тип*>	**Назначение**: Сформировать отчет о событиях Dr.Web Gateway Security Suite в виде страницы HTML (тело страницы выводится в указанный файл). **Аргументы** <*тип*> — тип событий, для которых формируется отчет (указывается один тип). Возможные значения см. в описании опции `--Types` команды `events` выше. Обязательный аргумент. **Опции** `-o [--Output]` <*путь к файлу*> — сохранить отчет в указанный файл. Обязательная опция. `-s [--Since]` <*дата, время*> — включить в отчет события, произошедшие не ранее указанного момента времени (<*дата, время*> указывается в формате "`YYYY-MM-DD hh:mm:ss`"). `-u [--Until]` <*дата, время*> — включить в отчет события, произошедшие не позднее указанного момента времени (<*дата, время*> указывается в формате "`YYYY-MM-DD hh:mm:ss`"). `--TemplateDir` <*путь к каталогу*> — путь к каталогу, в котором находятся файлы шаблонов HTML-страницы отчета. Опции `-s`, `-u` и `--TemplateDir` являются необязательными.
`license`	**Назначение**: Вывести на экран информацию об активной лицензии, получить демонстрационную лицензию или получить ключевой файл для уже зарегистрированной лицензии (например, на сайте компании). Если не указана ни одна опция, то выводится следующая информация (если используется лицензия для автономного режима работы): • номер лицензии, • дата и время окончания действия лицензии. Если используется лицензия, выданная сервером централизованной защиты (для работы в режиме централизованной защиты или в мобильном режиме), выводится соответствующая информация.

Команда	Описание
	Аргументы: Нет. **Опции** `--GetDemo` — запросить демонстрационный ключ сроком на месяц и получить его, если не нарушены условия получения демонстрационного периода. `--GetRegistered` <*серийный номер*> — получить лицензионный ключевой файл для указанного серийного номера, если не нарушены условия получения нового ключевого файла (например, программа не находится в режиме централизованной защиты, когда лицензией управляет сервер централизованной защиты). `--NetworkTimeout` <*интервал времени*> — тайм-аут в миллисекундах на сетевые операции при использовании команды `license`. Используется для продолжения активации в случае временного обрыва соединения. Если оборванное сетевое соединение будет восстановлено до истечения тайм-аута, то активация будет продолжена. Если указан `0`, то тайм-аута нет. Значение по умолчанию: `0`. `--Proxy http://`<*имя пользователя*>`:`<*пароль*>`@`<*адрес сервера*>`:`<*номер порта*> — получить лицензионный ключ через прокси-сервер (используется только совместно с одной из предыдущих опций — `--GetDemo` или `--GetRegistered`). *Если серийный номер не является серийным номером демонстрационного периода, то он должен быть предварительно зарегистрирован на сайте компании.* Подробнее о лицензировании продуктов Dr.Web см. раздел Лицензирование. Для регистрации серийного номера и для получения демонстрационного периода требуется наличие подключения к интернету.
`log`	**Назначение**: Вывести в консоль (поток *stdout*) последние записи журнала Dr.Web Gateway Security Suite (аналогично команде `tail`). **Аргументы**: Нет. **Опции** `-s [--Size]` <*число*> — число последних записей журнала, которые нужно вывести на экран.

Команда	Описание
	`-c [--Components]` <*список компонентов*> — список идентификаторов компонентов, записи которых будут выведены. Указываются через пробел. Если параметр не указан, выводятся все доступные последние записи, отправленные в журнал любым из компонентов. Актуальные идентификаторы установленных компонентов (т. е. внутренние имена компонентов, выводимые в журнал) вы можете узнать, используя команду `appinfo` (см. выше). `-f [--Follow]` — ожидать поступления новых записей в журнал и выводить их на экран сразу при поступлении (нажатие CTRL+C прерывает ожидание). Для выполнения этой команды требуется, чтобы `drweb-ctl` была запущена от имени суперпользователя (обычно пользователя *root*). При необходимости используйте команды `su` или `sudo`.
`stat`	**Назначение**: Вывести на экран статистику работы компонентов, обрабатывающих файлы, либо агента сетевой проверки данных Dr.Web Network Checker (нажатие CTRL+C или Q прерывает отображение статистики). В статистике отображается: • имя компонента, инициировавшего проверку файлов; • PID компонента; • усредненное количество файлов, обрабатываемых в секунду за последнюю минуту, 5 минут, 15 минут; • процент использования кеша проверенных файлов; • среднее количество ошибок проверки в секунду. Для агента распределенной проверки на экран выводится: • перечень локальных клиентов, инициировавших сканирование; • перечень удаленных узлов, которым переданы файлы на сканирование; • перечень удаленных узлов, от которых получены файлы на сканирование. Для локальных клиентов агента распределенной проверки указывается имя и PID, а для удаленных — адрес и порт узла. Для каждого клиента, как локального, так и удаленного выводится: • среднее за секунду количество проверенных файлов; • среднее за секунду количество переданных и полученных байт; • среднее за секунду количество ошибок.

Команда	Описание
	Аргументы: Нет. **Опции** `-n [--Netcheck]` — вывести на экран статистику работы агента сетевой проверки данных
`lookup <тип>@<тег>[@<шаблон>]`	**Назначение**: Проверить корректность параметров подключения к источнику данных. **Аргументы** <*тип*> — тип источника данных. Может принимать следующие значения: `ldap`, `ad`, `pq`, `sqlite`, `mysql`, `redis`, `allmatch`, `regex`, `cidr`, `mask`. Характеристика этих типов приведена в описании настроек компонента Dr.Web LookupD. <*тег*> — идентификатор источника данных. Например, если создать в объединенном конфигурационном файле секцию `[LookupD.LDAP.auth1]`, то `auth1` будет служить идентификатором источника данных типа LDAP. <*шаблон*> — шаблон (строка) для поиска в источнике данных. Необязательный аргумент. Если шаблон задан, то выполняется его поиск и возвращается значение *true* (найдено) или *false* (не найдено). **Опции** `--User` <*имя пользователя*> — имя пользователя для подключения к источнику данных; `--Domain` <*имя домена*> — имя домена для подключения к источнику данных. ⚠ Опция применяется только совместно с опцией `--User`. `-d [--Debug]` — показывать отладочную информацию. **Примеры** `$ drweb-ctl lookup --user user --domain d1 "mysql@test1"`

9.2.2. Примеры использования

В этом разделе

- Проверка объектов
  - Простые команды проверки
  - Проверка файлов, отобранных по критериям

- Проверка дополнительных объектов
- Управление конфигурацией
- Управление угрозами
- Пример работы в режиме автономного экземпляра

1. Проверка объектов

1.1. Простые команды проверки

1. Выполнить проверку каталога `/home` с параметрами по умолчанию:

```
$ drweb-ctl scan /home
```

2. Выполнить проверку списка путей к файлам, перечисленным в файле `daily_scan` (по одному пути в строке файла):

```
$ drweb-ctl scan --stdin < daily_scan
```

3. Выполнить проверку загрузочной записи на дисковом устройстве *sda*:

```
$ drweb-ctl bootscan /dev/sda
```

4. Выполнить проверку запущенных процессов:

```
$ drweb-ctl procscan
```

1.2. Проверка файлов, отобранных по критериям

В нижеприведенных примерах для формирования выборки файлов, подлежащих проверке, используется результат работы утилиты `find`. Полученный перечень файлов передается команде `drweb-ctl scan` с параметром `--stdin` или `--stdin0`.

1. Выполнить проверку списка файлов, возвращенных утилитой `find`, и разделенных символом NUL (`\0`):

```
$ find -print0 | drweb-ctl scan --stdin0
```

2. Проверить все файлы всех каталогов, начиная с корневого, находящихся на одном разделе файловой системы:

```
$ find / -xdev -type f | drweb-ctl scan --stdin
```

3. Проверить все файлы всех каталогов, начиная с корневого, кроме файлов `/var/log/messages` и `/var/log/syslog`:

```
$ find / -type f ! -path /var/log/messages ! -path /var/log/syslog |
drweb-ctl scan --stdin
```

4. Проверить во всех каталогах, начиная с корневого, файлы, принадлежащие пользователю *root*:

```
$ find / -type f -user root | drweb-ctl scan --stdin
```

5. Проверить во всех каталогах, начиная с корневого, файлы, принадлежащие пользователям *root* и *admin*:

```
$ find / -type f \( -user root -o -user admin \) | drweb-ctl scan --stdin
```

6. Проверить во всех каталогах, начиная с корневого, файлы, принадлежащие пользователям с UID из диапазона 1000–1005:

```
$ find / -type f -uid +999 -uid -1006 | drweb-ctl scan --stdin
```

7. Проверить файлы во всех каталогах, начиная с корневого, но находящихся не более чем на пятом уровне вложенности относительно корневого каталога:

```
$ find / -maxdepth 5 -type f | drweb-ctl scan --stdin
```

8. Проверить файлы в корневом каталоге, не заходя во вложенные каталоги:

```
$ find / -maxdepth 1 -type f | drweb-ctl scan --stdin
```

9. Проверить файлы во всех каталогах, начиная с корневого, при этом следовать по встречающимся символическим ссылкам:

```
$ find -L / -type f | drweb-ctl scan --stdin
```

10. Проверить файлы во всех каталогах, начиная с корневого, при этом не следовать по встречающимся символическим ссылкам:

```
$ find -P / -type f | drweb-ctl scan --stdin
```

11. Проверить во всех каталогах, начиная с корневого, файлы, созданные не позже, чем 1 мая 2017 года:

```
$ find / -type f -newermt 2017-05-01 | drweb-ctl scan --stdin
```

1.3. Проверка дополнительных объектов

Проверка объектов каталога `/tmp` на удаленном узле *192.168.0.1* при подключении к нему через SSH как пользователь *user* с паролем *passw*:

```
$ drweb-ctl remotescan 192.168.0.1 /tmp --Login user --Password passw
```

2. Управление конфигурацией

1. Вывести на экран информацию о запущенных компонентах Dr.Web Gateway Security Suite:

```
$ drweb-ctl appinfo
```

2. Вывести на экран все параметры из секции `[Root]`:

```
$ drweb-ctl cfshow Root
```

3. Задать значение `No` для параметра `Start` в секции `[LinuxSpider]` (это приведет к остановке работы монитора файловой системы SpIDer Guard):

```
# drweb-ctl cfset LinuxSpider.Start No
```

   Для этого требуются полномочия суперпользователя. Пример вызова этой же команды с использованием `sudo` для временного повышения полномочий:

```
$ sudo drweb-ctl cfset LinuxSpider.Start No
```

4. Выполнить принудительное обновление антивирусных компонентов Dr.Web Gateway Security Suite:

```
$ drweb-ctl update
```

5. Выполнить перезагрузку конфигурации для компонентов Dr.Web Gateway Security Suite:

```
# drweb-ctl reload
```

   Для этого требуются полномочия суперпользователя. Пример вызова этой же команды с использованием `sudo` для временного повышения полномочий:

```
$ sudo drweb-ctl reload
```

6. Подключить Dr.Web Gateway Security Suite к серверу централизованной защиты, работающему на узле *192.168.0.1*, при условии, что сертификат сервера располагается в файле `/home/user/cscert.pem`:

```
$ drweb-ctl esconnect 192.168.0.1 --Certificate /home/user/cscert.pem
```

7. Подключить Dr.Web Gateway Security Suite к серверу централизованной защиты, используя файл настроек подключения `install.cfg`:

```
$ drweb-ctl esconnect --cfg <путь к файлу install.cfg>
```

8. Отключить Dr.Web Gateway Security Suite от сервера централизованной защиты:

```
# drweb-ctl esdisconnect
```

Для этого требуются полномочия суперпользователя. Пример вызова этой же команды с использованием `sudo` для временного повышения полномочий:

```
$ sudo drweb-ctl esdisconnect
```

9. Просмотреть последние записи, внесенные компонентами `drweb-update` и `drweb-configd` в журнал Dr.Web Gateway Security Suite:

```
# drweb-ctl log -c Update ConfigD
```

3. Управление угрозами

1. Вывести на экран информацию об обнаруженных угрозах:

```
$ drweb-ctl threats
```

2. Переместить все файлы, содержащие необезвреженные угрозы, в карантин:

```
$ drweb-ctl threats --Quarantine All
```

3. Вывести на экран список файлов, перемещенных в карантин:

```
$ drweb-ctl quarantine
```

4. Восстановить все файлы из карантина:

```
$ drweb-ctl quarantine --Restore All
```

4. Пример работы в режиме автономного экземпляра

Проверить файлы и обработать карантин в режиме автономного экземпляра:

```
$ drweb-ctl scan /home/user -a --OnKnownVirus=QUARANTINE
$ drweb-ctl quarantine -a --Delete All
```

Первая команда проверит файлы в каталоге `/home/user` в режиме автономного экземпляра, и файлы, содержащие известные угрозы, будут помещены в карантин. Вторая команда обработает содержимое карантина (также в режиме автономного экземпляра) и удалит все содержащиеся в нем объекты.

9.2.3. Параметры конфигурации

Утилита управления из командной строки Dr.Web Ctl не имеет собственной секции параметров в объединенном конфигурационном файле Dr.Web Gateway Security Suite. Утилита использует параметры, указанные в секции `[Root]`.

9.3. Веб-интерфейс управления Dr.Web

В этом разделе

- Назначение
- Системные требования веб-интерфейса
- Доступ к управлению через веб-интерфейс
- Главное меню

Назначение

Веб-интерфейс управления Dr.Web Gateway Security Suite позволяет выполнять следующие действия:

- просматривать состояние компонентов Dr.Web Gateway Security Suite, запускать и останавливать работу некоторых из них;
- просматривать состояние обновлений и запускать обновление вручную при необходимости;
- просматривать состояние лицензии и загружать лицензионный ключ при необходимости;
- просматривать перечень обнаруженных угроз и управлять содержимым карантина (отображаются только угрозы, обнаруженные в файлах локальной файловой системы компонентом Dr.Web File Checker);
- выполнять редактирование настроек компонентов Dr.Web Gateway Security Suite;
- подключать Dr.Web Gateway Security Suite к серверу централизованной защиты или переводить его в автономный режим работы;
- запускать проверку локальных файлов по требованию (в том числе перетаскиванием их на страницу, открытую в браузере).

Системные требования веб-интерфейса

Корректная работа веб-интерфейса управления гарантируется в следующих браузерах:

- Microsoft Internet Explorer версии 11 и более поздней;
- Mozilla Firefox версии 25 и более поздней;
- Google Chrome версии 30 и более поздней.

Доступ к управлению через веб-интерфейс

Для доступа к веб-интерфейсу необходимо в адресной строке браузера ввести адрес вида:

```
https://<xocm_drweb>:<nopm>/
```

где *<xocm_drweb>* — IP-адрес или имя узла, на котором работает Dr.Web Gateway Security Suite, в составе которого функционирует сервер веб-интерфейса Dr.Web HTTPD, а *<nopm>* — порт на этом узле, прослушиваемый Dr.Web HTTPD. Для доступа к компонентам Dr.Web Gateway Security Suite, работающего на локальном узле, достаточно использовать IP-адрес `127.0.0.1` или имя `localhost`. При настройках по умолчанию используется порт `4443`.

Таким образом, для доступа к веб-интерфейсу на локальном компьютере при настройках по умолчанию необходимо ввести адрес:

```
https://127.0.0.1:4443/
```

В случае успешного подключения к серверу управления на экране появится стартовая страница, содержащая форму аутентификации. Для доступа к управлению необходимо пройти аутентификацию, введя в соответствующие поля формы логин и пароль пользователя, обладающего административными полномочиями на узле, на котором функционирует Dr.Web Gateway Security Suite.

При необходимости вы можете обеспечить авторизацию на веб-интерфейсе по личному сертификату пользователя. Для этого:

1. Создайте личный сертификат, подписанный сертификатом удостоверяющего центра.
2. Импортируйте подписанный сертификат в качестве удостоверяющего сертификата пользователя в браузер, через который осуществляется подключение к веб-интерфейсу управления.
3. В настройках компонента Dr.Web HTTPD (параметр `AdminSslCA`) укажите путь к файлу сертификата удостоверяющего центра, которым подписан ваш личный сертификат.

При авторизации на веб-интерфейсе по личному сертификату пользователя форма авторизации не показывается при начале работы с веб-интерфейсом, а пользователь авторизуется как пользователь *root*.

При необходимости обратитесь к информации в разделе Приложение Д. Генерация сертификатов SSL.

Главное меню

В левой части страниц веб-интерфейса управления, открывающихся после успешного прохождения аутентификации, расположено главное меню, состоящее из следующих пунктов:

- **Главная** — открывает главную страницу, на которой отображается перечень установленных компонентов Dr.Web Gateway Security Suite и их состояние.
- **Угрозы** — открывает страницу, отображающую все угрозы, обнаруженные на сервере. В этом разделе вы можете осуществлять управление обнаруженными угрозами, в том числе, перемещать инфицированные объекты в карантин, осуществлять повторную проверку, лечение или удаление вредоносных объектов.
- **Настройки** — открывает страницу управления настройками компонентов Dr.Web Gateway Security Suite, установленных на сервере.
- **Информация** — открывает страницу просмотра краткой информации о версии веб-интерфейса и состоянии вирусных баз.
- **Справка** — открывает в новой вкладке браузера справку по продуктам Dr.Web для Unix.
- **Проверить файл** — показывает панель оперативной проверки файлов, которая будет доступна поверх любой страницы веб-интерфейса до момента закрытия панели.
- **Выйти** — завершает сеанс работы текущего пользователя с веб-интерфейсом управления (недоступно, если используется авторизация по личному сертификату пользователя).

9.3.1. Управление компонентами

Просмотр перечня компонентов, входящих в состав Dr.Web Gateway Security Suite, и управление их работой осуществляются на странице **Главная**.

Отображаемые компоненты Dr.Web Gateway Security Suite разделены на две части: основные, выполняющие обнаружение угроз, и сервисные, обеспечивающие корректную работу Dr.Web Gateway Security Suite в целом. Перечень основных компонентов (зависит от поставки) отображается в виде таблицы, расположенной в верхней части страницы. Для каждого компонента указывается:

1. **Название**. Нажмите название, чтобы перейти к странице настроек компонента.
2. **Состояние**. Состояние, в котором находится компонент, иллюстрируется переключателем и текстовой подписью, отображающей текущее состояние, в котором он находится. Чтобы запустить компонент или приостановить его работу, нажмите переключатель. Возможные состояния переключателя:

	Компонент отключен и не используется.
	Компонент включен и корректно функционирует.

	Компонент включен, но не функционирует вследствие произошедшей ошибки.

Если в работе компонента произошла ошибка, вместо состояния выводится сообщение об ошибке. Нажмите , чтобы открыть всплывающее окно с подробной информацией о произошедшей ошибке и рекомендациями по ее устранению.

3. **Нагрузка**. Среднее число файлов, обработанных компонентом за секунду в течение последней минуты, 5 минут, 15 минут (три числа, разделенных косой чертой).
4. **Ошибки**. Среднее число ошибок за секунду, произошедших в работе компонента в течение последней минуты, 5 минут, 15 минут (три числа, разделенных косой чертой).

Наведите указатель на , чтобы получить всплывающую подсказку.

Под таблицей основных компонентов в виде набора плиток перечисляются сервисные компоненты Dr.Web Gateway Security Suite (такие как Dr.Web Scanning Engine, Dr.Web File Checker и др.). Для них также указываются состояние и статистика их работы. Нажмите название компонента, чтобы открыть страницу его настроек. Как правило, эти компоненты запускаются и завершаются автоматически, по мере необходимости. Если какой-либо из них может быть запущен или остановлен пользователем вручную, то, кроме названия и статистики работы, в плитке сервисного компонента доступен выключатель для управления его запуском.

В нижней части страницы указывается информация о вирусных базах и лицензии. Кнопка **Обновить** позволяет начать принудительное обновление вирусных баз, а кнопка **Продлить** (или **Активировать лицензию**, в зависимости от текущего состояния лицензии) — продлить или активировать лицензию путем загрузки на сервер действующего ключевого файла, подходящего для Dr.Web Gateway Security Suite.

9.3.2. Управление угрозами

Обзор перечня обнаруженных угроз и управление ими осуществляются на странице **Угрозы**.

На этой странице приводится полный перечень угроз, обнаруженных компонентами Dr.Web Gateway Security Suite, выполняющими мониторинг и проверку файловой системы. В верхней части страницы располагается меню, позволяющее отфильтровать угрозы по категориям:

- **Все** — отобразить в списке все обнаруженные угрозы (в том числе активные и те, которые были помещены в карантин);
- **Активные** — отобразить в списке только активные угрозы, т. е. такие, которые были обнаружены, но все еще не нейтрализованы;
- **Заблокированные** — отобразить в списке угрозы, которые не нейтрализованы, но файлы, содержащие их, были заблокированы для доступа пользователей;
- **В карантине** — отобразить в списке угрозы, перемещенные в карантин;

- **Ошибки** — отобразить в списке угрозы, при попытке обработки которых произошла ошибка.

Справа от названия каждой категории в меню отображается число, показывающее количество обнаруженных угроз, соответствующих данной категории. Для отображения в списке угроз требуемой категории нажмите ее название в меню.

На странице **Угрозы** не отображаются угрозы, обнаруженные компонентами, проверяющими сетевой трафик (SpIDer Gate, Dr.Web ICAPD), а также компонентом Dr.Web ClamD. Для отслеживания угроз, обнаруженных этими компонентами, вы можете контролировать состояние счетчиков угроз и отслеживать уведомления, доступные по протоколу SNMP (доступ к счетчикам угроз и уведомлениям об инцидентах обеспечивает компонент Dr.Web SNMPD согласно структуре MIB Dr.Web).

В списке угроз для каждой угрозы выводится следующая информация:

- **Файл** — имя файла, содержащего вредоносный объект (путь к файлу не указывается);
- **Владелец** — имя пользователя, являющегося владельцем файла, содержащего угрозу;
- **Компонент** — имя компонента, обнаружившего угрозу;
- **Угроза** — имя вредоносного объекта, обнаруженного в файле, по классификации компании «Доктор Веб».

Для объекта, выделенного в списке, справа от списка выводится подробная информация:

- имя угрозы (выводится в виде ссылки, при нажатии которой в новой вкладке браузера открывается страница Вирусной библиотеки Dr.Web с описанием угрозы);
- размер файла в байтах;
- имя компонента, обнаружившего угрозу;
- дата и время обнаружения угрозы;
- дата и время последнего изменения файла;
- имя пользователя-владельца файла с угрозой;
- имя группы, которой принадлежит пользователь-владелец;
- идентификатор файла с угрозой в карантине, если файл уже был помещен в карантин;
- полный путь к файлу в исходном месте (там, где в нем была обнаружена угроза).

Чтобы выделить объект в списке, нажмите соответствующую строку списка. Чтобы выделить более одного объекта, установите флажки в строках выделяемых объектов. Чтобы за один раз выделить все объекты или снять выделение со всех объектов в списке, установите или снимите флажок, расположенный в поле **Файл** в заголовке списка угроз.

Для применения действий к объектам, выделенным в списке угроз, необходимо нажать соответствующую кнопку на панели инструментов, расположенной непосредственно над списком угроз. В панели инструментов доступны следующие кнопки:

	Удалить отмеченные файлы.
	Восстановить отмеченные файлы из карантина в исходное место.
	Применить дополнительное действие к отмеченным файлам (выбирается из выпадающего списка). Доступны следующие дополнительные действия: • **В карантин** — переместить файлы с угрозами в карантин; • **Лечить** — попытаться вылечить угрозы; • **Игнорировать** — игнорировать угрозы, обнаруженные в отмеченных файлах, и удалить их из списка обнаруженных угроз.

Некоторые из кнопок могут быть недоступны в зависимости от типа выделенных угроз.

На странице **Угрозы** также доступна панель фильтрации списка угроз на основании поискового запроса. Чтобы отфильтровать список угроз, оставив в нем только те объекты, в описании которых присутствует заданная строка, воспользуйтесь строкой поиска. Она расположена в правой части панели инструментов и отмечена значком . Для фильтрации списка следует ввести произвольное слово в строку поиска, при этом из списка угроз будут скрыты все объекты, не содержащие в своем названии или описании указанного слова (поиск выполняется без учета регистра букв). Чтобы очистить результаты поиска и вернуться к исходному списку, нажмите в строке поиска или удалите поисковое слово.

9.3.3. Управление настройками

В этом разделе

- Просмотр и изменение настроек компонента в табличной форме
- Просмотр и изменение настроек компонента в редакторе ini
- Дополнительно

Просмотр и изменение текущих параметров конфигурации компонентов, входящих в состав Dr.Web Gateway Security Suite и перечисленных на главной странице, производятся на странице **Настройки**. Кроме того, на этой странице вы можете переключить Dr.Web Gateway Security Suite в режим *централизованной защиты* или в *автономный* режим работы (подробнее о режимах работы см. раздел Режимы работы).

В левой части страницы располагается меню, в котором перечисляются все компоненты Dr.Web Gateway Security Suite, настройки которых доступны для просмотра и

редактирования. Чтобы просмотреть и изменить настройки компонента, выберите его в меню, нажав его имя. Имя компонента, настройки которого в данный момент просматриваются в редакторе, выделяется в меню слева.

- Пункт меню **Централизованная защита** позволяет перейти на страницу управления работой в режиме централизованной защиты.
- Пункт меню **Общие настройки** соответствует настройкам Dr.Web ConfigD, обеспечивающего общую работу Dr.Web Gateway Security Suite.

Если компонент имеет кроме основной секции настроек также и дополнительные, специфичные секции настроек (например, такие секции имеются у компонента эмуляции интерфейса ClamAV® Dr.Web ClamD — в каждой из них задаются индивидуальные параметры проверки для клиентов, использующих определенный адрес подключения), то слева от имени компонента в меню выводится значок сворачивания/разворачивания дополнительных (подчиненных) секций настроек этого компонента. Если этот значок имеет вид ▸, то дополнительные секции скрыты. Если же этот значок имеет вид ▾, то дополнительные секции также отображаются в меню по одной строке на дополнительную секцию. Чтобы свернуть или развернуть список подчиненных секций компонента, нажмите значок сворачивания/разворачивания сбоку от имени нужного компонента в меню.

- Дополнительные секции настроек компонента отображаются с отступом вправо. Чтобы просмотреть или отредактировать параметры дополнительной секции, нажмите ее название.
- Чтобы добавить для компонента новую подчиненную секцию параметров, если он допускает такую возможность, нажмите +. Этот значок расположен справа от имени компонента и появляется при наведении указателя мыши на имя компонента. Далее укажите уникальное имя (тег) дополнительной секции параметров и нажмите **ОК**. Чтобы отказаться от добавления новой секции, нажмите **Отменить**.
- Чтобы удалить подчиненную секцию параметров, нажмите ×. Этот значок расположен справа от имени (тега) секции и появляется при наведении указателя мыши на имя компонента. Далее подтвердите удаление выбранной секции, нажав **Да**, или откажитесь от удаления, нажав **Нет**.

В верхней части страницы просмотра настроек располагается меню, управляющее режимом просмотра настроек. Доступны следующие режимы:

- **Все** — отобразить в табличном редакторе все параметры конфигурации компонента, доступные для просмотра и изменения;
- **Измененные** — отобразить в табличном редакторе для просмотра и изменения только те параметры конфигурации компонента, которые имеют значения, отличные от значений по умолчанию;
- **Редактор ini** — отобразить параметры конфигурации компонента, которые имеют значения, отличные от значений по умолчанию, в редакторе параметров файла конфигурации (в виде пар `параметр = значение`).

На странице управления настройками доступна также панель фильтрации списка отображаемых параметров на основании поискового запроса. Чтобы отфильтровать список параметров, оставив в нем только те параметры, в описании которых присутствует заданная строка, необходимо воспользоваться строкой поиска. Она расположена в правой части меню, управляющего режимом просмотра, и отмечена значком . Чтобы отфильтровать список параметров, введите произвольное слово в строку поиска, при этом из списка параметров будут скрыты все параметры, не содержащие в своем описании указанного слова (поиск выполняется без учета регистра букв). Чтобы очистить результаты поиска и вернуться к исходному списку параметров, нажмите в строке поиска или удалите поисковое слово.

Фильтрация списка параметров работает только при просмотре списка параметров в табличной форме (режим **Все** или **Измененные**).

Просмотр и изменение настроек компонента в табличной форме

При просмотре списка параметров в табличной форме (режим **Все** или **Измененные**) каждая строка таблицы содержит имя и описание параметра (слева) и его текущее значение (справа). Для параметров логического типа (имеющих только два допустимых значения — «Да» и «Нет») вместо значения параметра отображается флажок (включенное состояние соответствует заданному значению «Да», а выключенное — значению «Нет»).

В режиме просмотра всех параметров, а не только измененных, значения, отличные от значений, определенных для этих параметров по умолчанию, выделены в списке жирным шрифтом.

Общий список параметров разбит на разделы, такие как **Основные**, **Дополнительные** и т. д. Чтобы свернуть или развернуть раздел таблицы, нажмите заголовок раздела. Если раздел свернут, а параметры, входящие в него, не указаны в таблице, то слева от имени раздела отображается . Если раздел развернут и входящие в него параметры указаны в таблице, слева от имени раздела отображается .

Чтобы изменить параметр, нажмите его текущее значение в таблице (для параметра логического типа — установите или снимите соответствующий флажок). Если параметр имеет строго ограниченный набор значений, то при нажатии значения откроется выпадающий список, в котором необходимо выбрать требуемое значение. Если значение параметра — число, то при нажатии оно будет доступно в поле редактирования прямо в таблице. В этом случае следует указать новое требуемое значение и нажать ENTER. Во всех этих случаях измененное значение параметра сразу же фиксируется в настройках компонента.

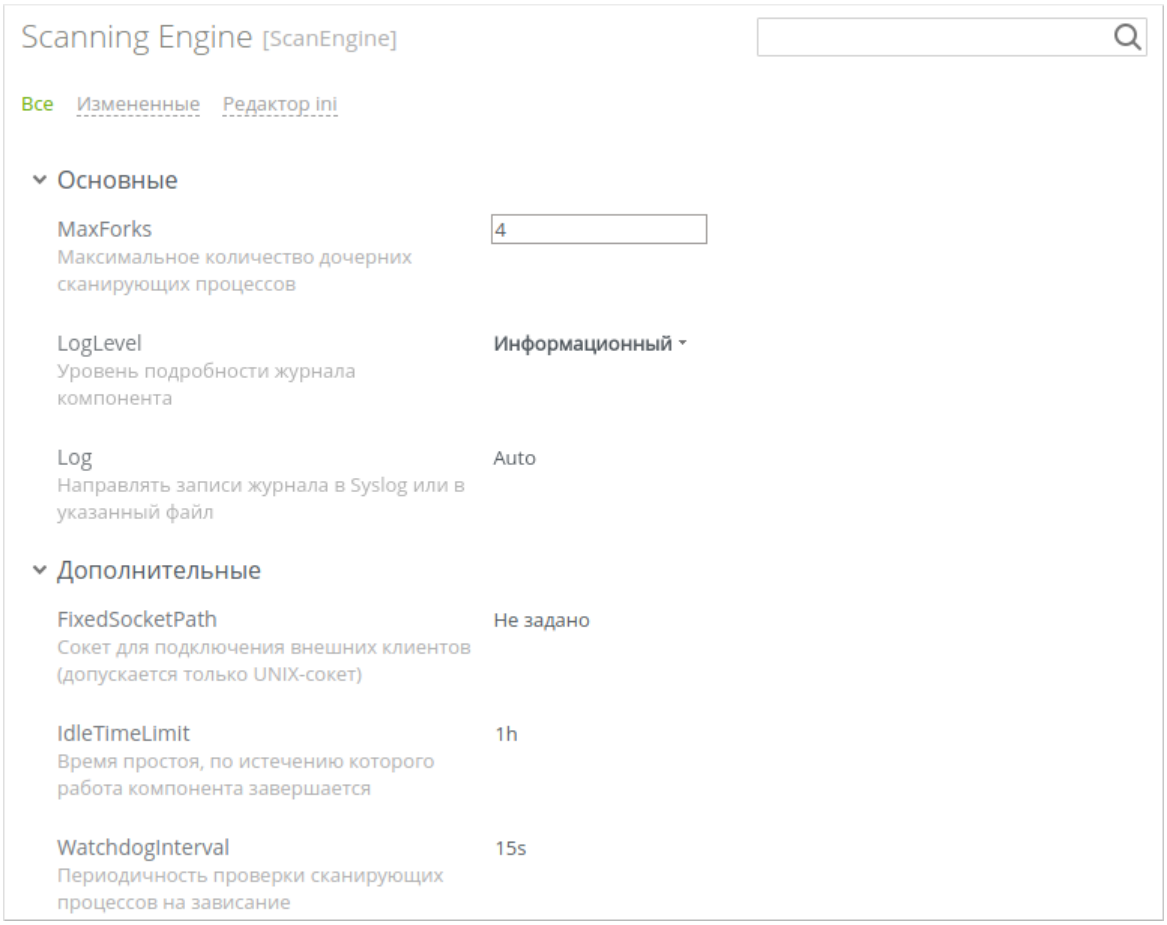

Рисунок 3. Представление настроек компонента в табличной форме

Если параметр принимает строковое значение или список произвольных значений, то при нажатии текущего значения параметра на экране появляется всплывающее окно, в котором можно отредактировать текущее значение параметра. Если параметр принимает список значений, то элементы списка выводятся в многострочном поле редактирования по одному в строке, как показано на рисунке ниже. Чтобы отредактировать элементы списка, измените, удалите или добавьте требуемые строки в поле редактирования.

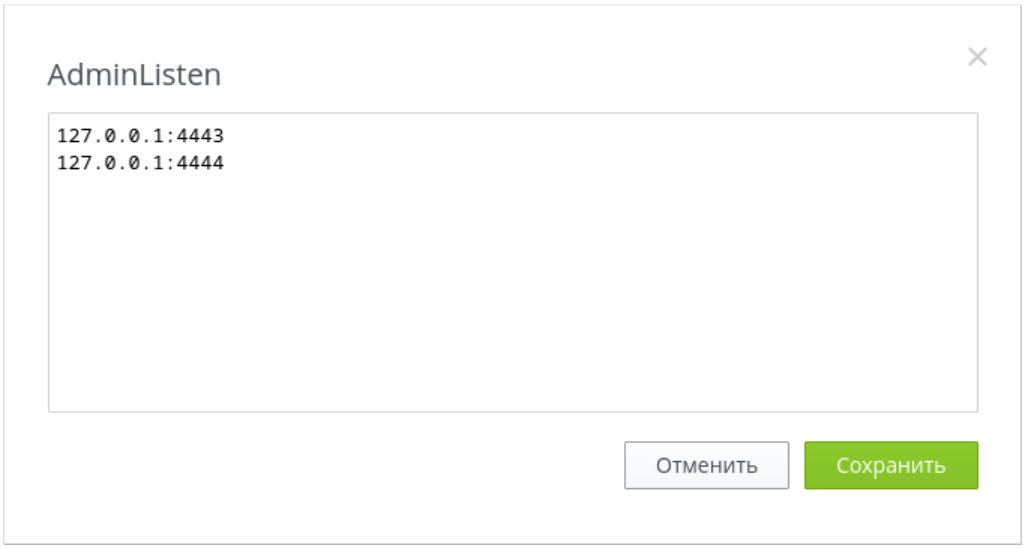

Рисунок 4. Редактирование списка значений

Чтобы сохранить внесенные изменения и закрыть окно, после редактирования значения параметра нажмите **Сохранить**. Чтобы закрыть окно без сохранения внесенных изменений, нажмите **Отменить** или ✕ в верхнем правом углу всплывающего окна.

Просмотр и изменение настроек компонента в редакторе ini

При просмотре параметров в режиме **Редактор ini** они отображаются в редакторе параметров файла конфигурации (в виде пар `параметр = значение`), где `параметр` — имя параметра, задаваемое непосредственно в секции настроек компонента в конфигурационном файле. В этом режиме отображаются только те параметры конфигурации, значения которых отличаются от значений, определенных по умолчанию (т. е. те параметры, значения которых в таблице **Все** выводятся жирным шрифтом). Пример отображения параметров в виде пар показан на рисунке ниже.

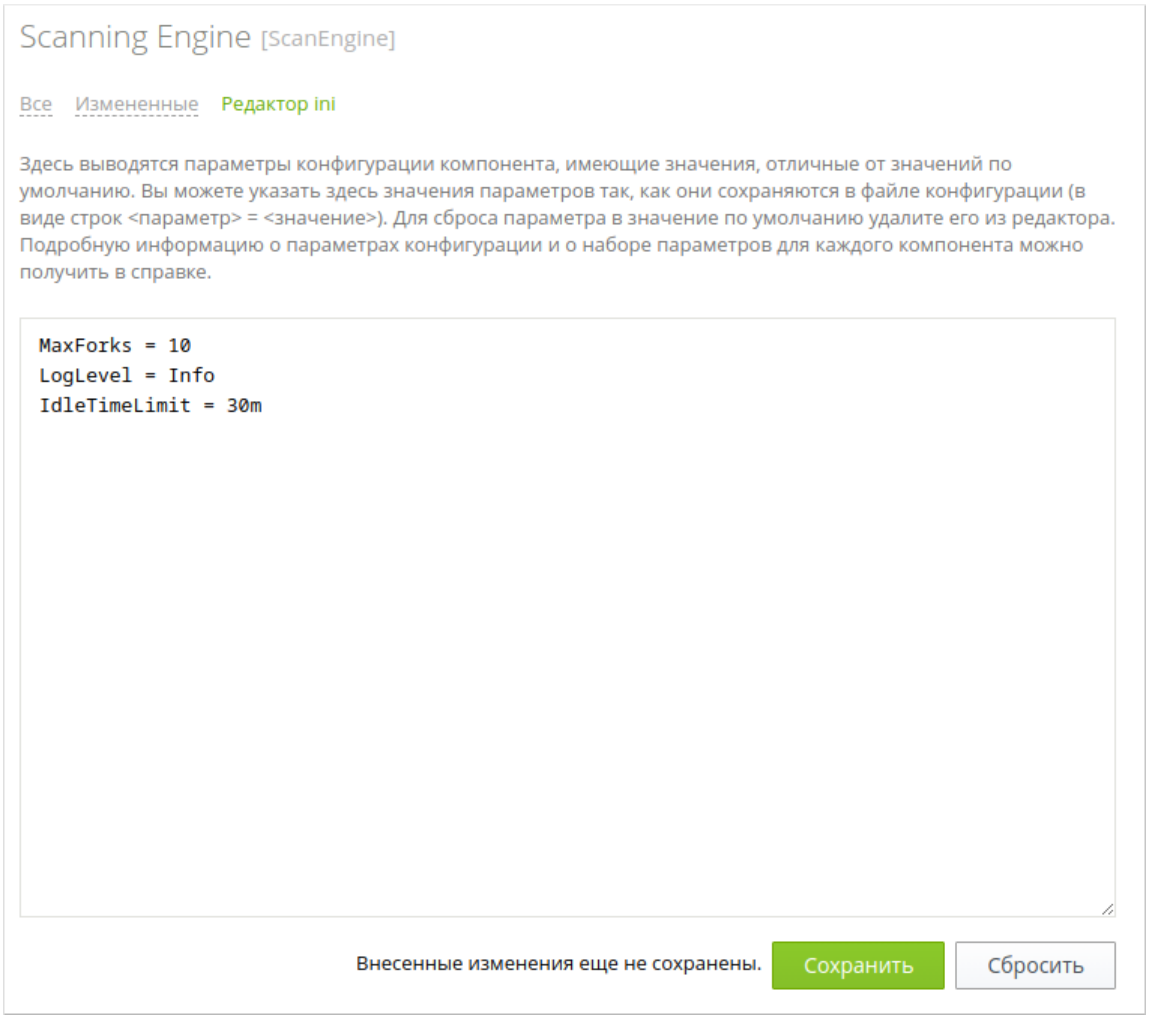

Рисунок 5. Редактирование настроек в формате файла конфигурации

Для внесения изменений необходимо отредактировать текст, учитывая правила формирования файла конфигурации (всегда редактируется только секция файла конфигурации, относящаяся к компоненту, выделенному в меню слева). При необходимости вы можете указать в редакторе любой из параметров, доступных для компонента. В этом случае его значение, установленное по умолчанию, будет заменено на значение, указанное вами в редакторе. Если требуется сбросить параметр в значение по умолчанию, достаточно удалить его строчку из редактора. В этом случае после сохранения изменений параметру будет присвоено значение по умолчанию.

Чтобы сохранить внесенные изменения после редактирования, нажмите **Сохранить**. Чтобы отменить внесенные изменения, нажмите **Отменить**.

При нажатии **Сохранить** выполняется проверка корректности текста, введенного в редакторе: проверяется, что не указаны несуществующие параметры, а также, что все указанные значения параметров допустимы. В случае обнаружения ошибок на экран выдается соответствующее сообщение.

Подробно ознакомиться с общим описанием файла конфигурации, его структурой и особенностями задания значений параметров можно в разделе Приложение Г. Конфигурационный файл Dr.Web Gateway Security Suite.

Дополнительно

- Параметры конфигурации компонента Dr.Web ConfigD (общие настройки).
- Параметры конфигурации компонента Dr.Web ICAPD.
- Параметры конфигурации компонента SpIDer Gate.
- Параметры конфигурации компонента Dr.Web Firewall для Linux.
- Параметры конфигурации компонента Dr.Web ES Agent.
- Параметры конфигурации компонента Dr.Web Updater.
- Параметры конфигурации компонента Dr.Web ClamD.
- Параметры конфигурации компонента Dr.Web File Checker.
- Параметры конфигурации компонента Dr.Web Scanning Engine.
- Параметры конфигурации компонента Dr.Web Network Checker.
- Параметры конфигурации компонента Dr.Web SNMPD.
- Параметры конфигурации компонента Dr.Web CloudD.
- Параметры конфигурации компонента Dr.Web LookupD.
- Параметры конфигурации компонента Dr.Web StatD.
- Управление централизованной защитой.

9.3.3.1. Управление централизованной защитой

Вы можете подключить Dr.Web Gateway Security Suite к серверу централизованной защиты или отключиться от него, переведя продукт в автономный режим работы. Для перехода на страницу управления централизованной защитой выберите пункт **Централизованная защита** в меню настроек на странице **Настройки**.

Чтобы подключить Dr.Web Gateway Security Suite к серверу централизованной защиты или отключиться от него, используйте соответствующий флажок на этой странице.

Подключение к серверу централизованной защиты

При попытке подключения к серверу централизованной защиты на экране появится всплывающее окно, в котором требуется указать параметры подключения к серверу.

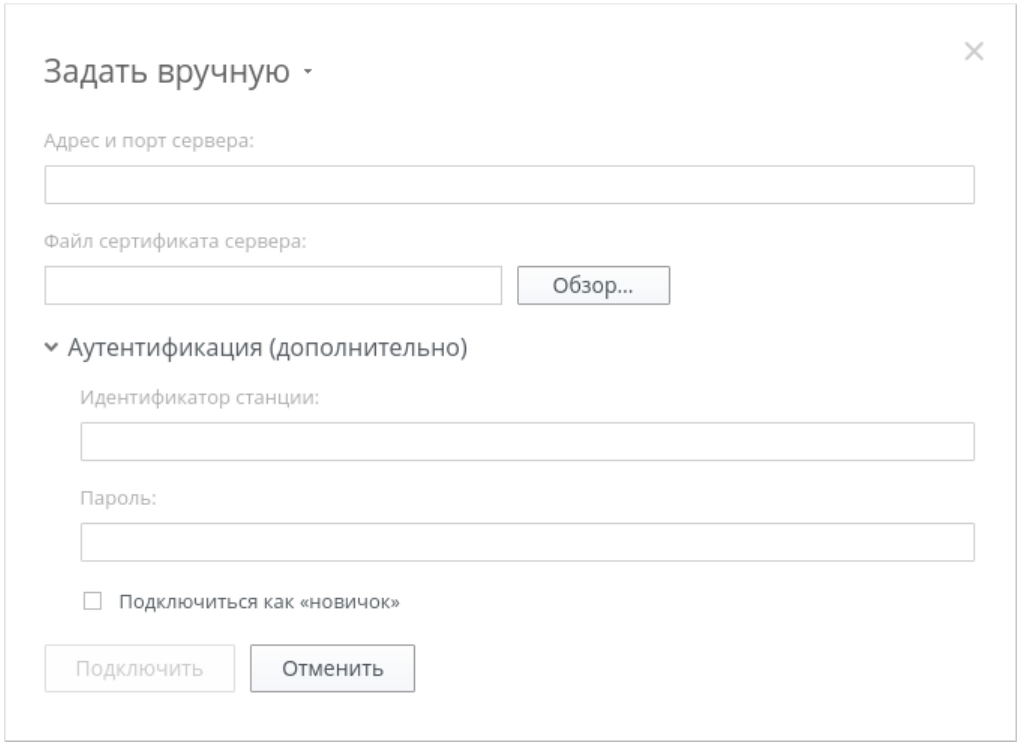

Рисунок 6. Подключение к серверу централизованной защиты

В выпадающем списке, расположенном в верхней части окна, выберите способ подключения к серверу. Доступно три способа:

- *Загрузить из файла*,
- *Задать вручную*,
- *Определить автоматически*.

Если вы выбрали вариант *Загрузить из файла*, укажите в соответствующем поле окна путь к файлу настроек подключения к серверу, предоставленному вам администратором антивирусной сети. При выборе варианта *Задать вручную* следует указать адрес и порт для подключения к серверу централизованной защиты. Кроме того, для способов подключения *Задать вручную* и *Определить автоматически* вы можете также указать путь к файлу публичного ключа сервера, если он у вас имеется (обычно этот файл предоставляется администратором антивирусной сети или провайдером).

Дополнительно, в разделе **Аутентификация (дополнительно)**, вы можете указать идентификатор рабочей станции и пароль для аутентификации на сервере, если они вам известны. Если эти поля заполнены, то подключение к серверу будет успешным только при указании правильной пары идентификатор/пароль. Если эти поля оставить пустыми, то подключение к серверу будет успешным только в случае его одобрения на сервере

(автоматически или администратором антивирусной сети, в зависимости от настроек сервера).

Кроме того, вы можете установить флажок **Подключиться как «новичок»**. Если режим «новичок» для подключения станций разрешен на сервере, то после одобрения подключения он автоматически сгенерирует уникальную пару идентификатор/пароль, которая в дальнейшем будет использоваться для подключения вашего компьютера к этому серверу.

При подключении как «новичок» новая учетная запись для вашего компьютера будет сгенерирована сервером централизованной защиты даже в том случае, если ранее он уже имел учетную запись на этом сервере.

Параметры подключения следует задавать в строгом соответствии с инструкциями, предоставленными администратором антивирусной сети или провайдером.

Для подключения к серверу после указания всех параметров нажмите **Подключить** и дождитесь окончания процесса подключения. Чтобы закрыть окно без подключения к серверу, нажмите **Отменить**.

После того, как вы подключили Dr.Web Gateway Security Suite к серверу централизованной защиты, он будет работать под управлением сервера до тех пор, пока вы его не переведете в автономный режим. Подключение к серверу будет происходить автоматически каждый раз при запуске Dr.Web Gateway Security Suite.

9.3.4. Проверка локальных файлов

В этом разделе

- Открытие панели проверки локальных файлов и настройка параметров проверки
- Запуск проверки локальных файлов

Веб-интерфейс предоставляет возможность оперативной проверки на наличие угроз файлов, находящихся на локальном компьютере, с которого осуществляется доступ к веб-интерфейсу управления. При проверке используется сканирующее ядро, входящее в состав Dr.Web Gateway Security Suite. Проверяемые файлы загружаются на сервер по протоколу HTTP, но после проверки, даже в случае обнаружения угроз, они не сохраняются на сервере и не перемещаются в карантин. Пользователь, отправивший файлы на проверку, будет только проинформирован о ее результате.

Открытие панели проверки локальных файлов и настройка параметров проверки

Выбор и загрузка файлов для проверки осуществляются на панели проверки локальных файлов, которая отображается при выборе пункта **Проверить файл** в главном меню веб-интерфейса. Активированная панель отображается в нижнем правом углу страницы веб-интерфейса. Внешний вид панели проверки локальных файлов показан на рисунке ниже.

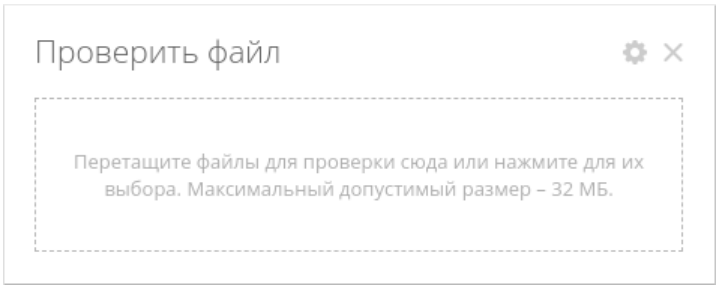

Рисунок 7. Панель проверки локальных файлов

Для закрытия панели нажмите ✕ в верхнем правом углу панели. Нажмите ⚙, чтобы перейти к настройкам проверки локальных файлов, где вы можете указать максимальное время, отведенное на проверку файла (не считая времени его загрузки на север с локального компьютера), разрешить или запретить эвристический анализ, а также указать максимальную степень сжатия для сжатых объектов и глубину вложенности для объектов, упакованных в контейнеры (такие как архивы).

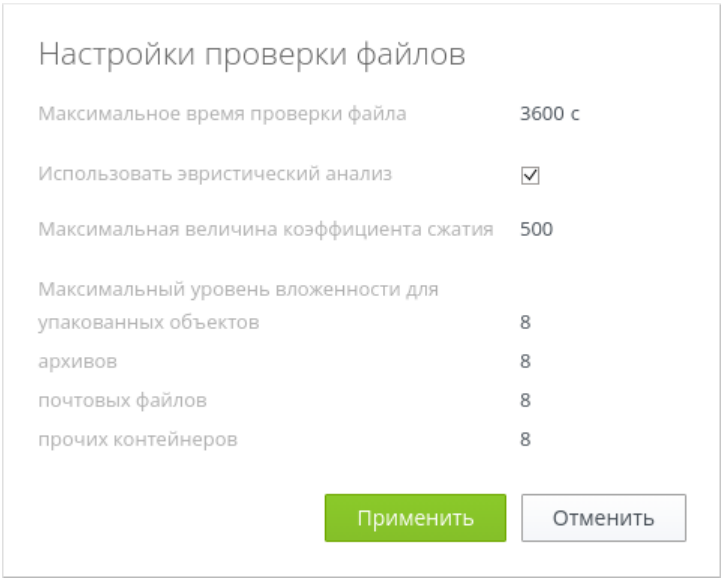

Рисунок 8. Настройка параметров проверки локальных файлов

Для применения измененных настроек и возврата к режиму выбора файлов для проверки нажмите **Применить**. Для возврата к выбору файлов без изменения настроек нажмите **Отменить**.

Запуск проверки локальных файлов

Для начала проверки файлов нажмите надпись-мишень **Перетащите файлы для проверки сюда или нажмите для их выбора**, при этом откроется стандартное окно выбора файлов файлового менеджера. Вы можете выбрать одновременно несколько файлов для проверки.

Выбор каталогов для проверки не допускается.

Вы также можете перетащить выбранные для проверки файлы мышью непосредственно на мишень из окна файлового менеджера. После указания проверяемых файлов начнется их загрузка на сервер с Dr.Web Gateway Security Suite и проверка по мере загрузки. В процессе загрузки и проверки файлов панель проверки отображает общий прогресс процесса проверки.

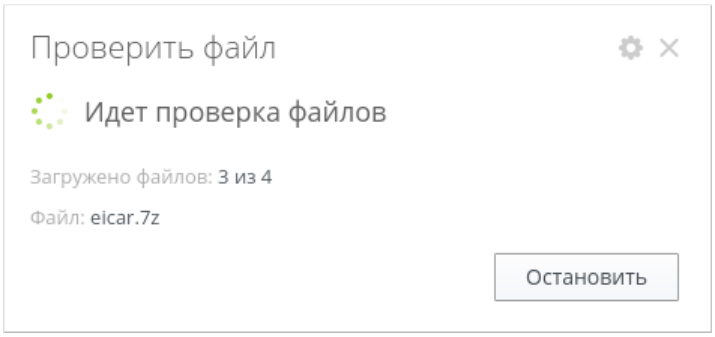

Рисунок 9. Проверка локальных файлов

В случае необходимости вы можете прервать процесс загрузки и проверки файлов, нажав **Остановить**. По окончании проверки на панели отображается отчет о проверке загруженных файлов.

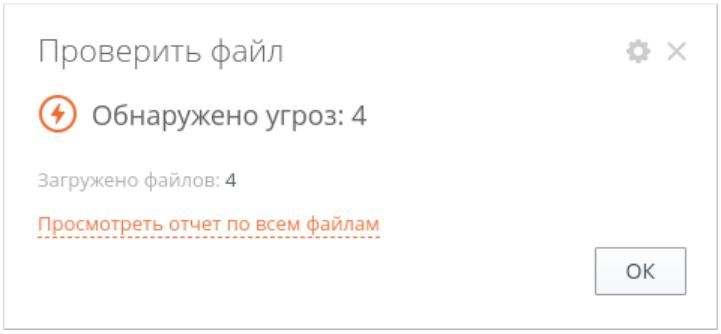

Рисунок 10. Результат проверки локальных файлов

Если вами было загружено более одного файла, будет доступен расширенный отчет о проверке файлов. Чтобы просмотреть расширенный отчет, нажмите **Просмотреть отчет по всем файлам**.

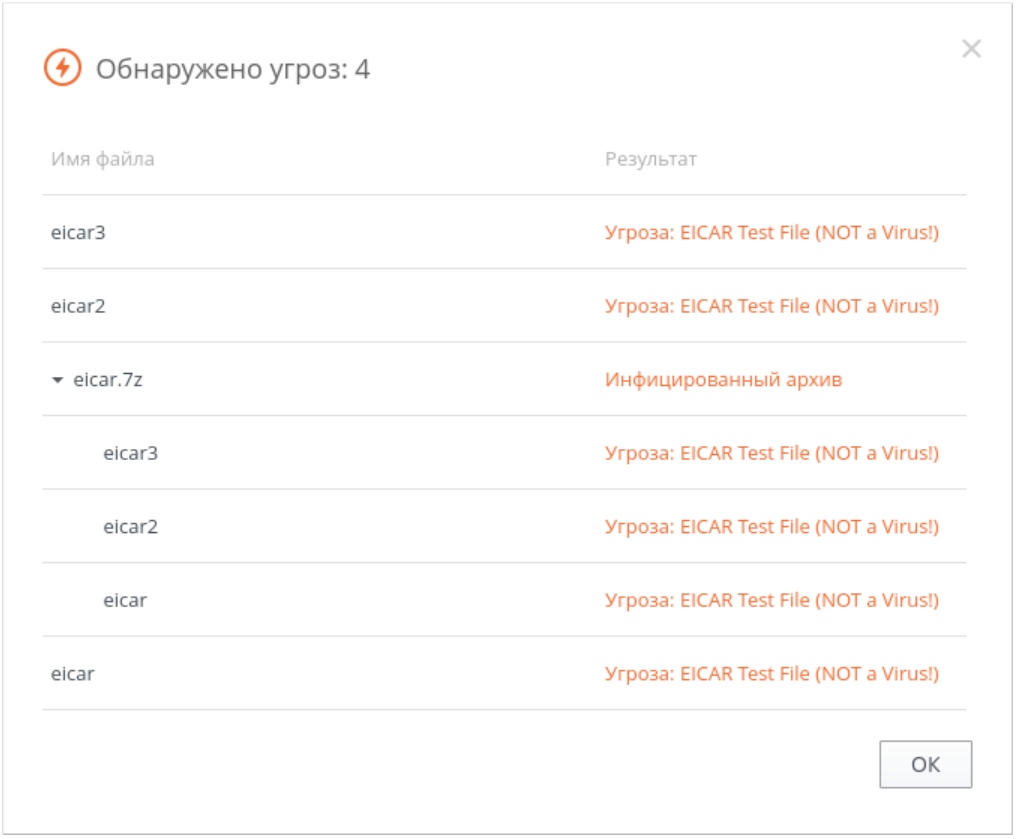

Рисунок 11. Расширенный отчет о проверке локальных файлов

Чтобы закрыть отчет и перевести панель в состояние готовности к выбору новых файлов для проверки, нажмите **OK**.

Запуск проверки локальных файлов с текущими настройками возможен даже тогда, когда панель проверки файлов закрыта. Для начала загрузки и проверки локальных файлов просто перетащите их мышью из окна файлового менеджера на открытую в браузере страницу веб-интерфейса управления.

9.4. Dr.Web ICAPD

Компонент Dr.Web ICAPD предназначен для подключения по протоколу ICAP к прокси-серверу HTTP (такому как Squid), установленному на шлюзе, через который пользователи, находящиеся в локальной сети, осуществляют доступ в интернет. Прокси-сервер использует Dr.Web ICAPD в качестве внешнего фильтра, которому на анализ передаются как запросы пользователей, так и ответы на них от внешних веб-серверов. Если доступ пользователя к какому-либо ресурсу, расположенному во внешней сети, должен быть запрещен, или передаваемые данные (запрос пользователя или ответ, который вернул сервер) содержат угрозу или не могут быть проверены из-за ошибки, Dr.Web ICAPD заставляет прокси-сервер вернуть пользователю HTML-страницу ответа, сформированную Dr.Web ICAPD на основании шаблона.

В случае большой интенсивности проверки файлов, передаваемых по протоколу HTTP, возможно возникновение проблем с проверкой из-за исчерпания компонентом Dr.Web Network Checker числа доступных файловых дескрипторов. В этом случае необходимо увеличить лимит на число файловых дескрипторов, доступных Dr.Web Gateway Security Suite.

9.4.1. Принципы работы

Компонент Dr.Web ICAPD использует протокол ICAP (Internet Content Adaptation Protocol, RFC 3507) для взаимодействия с внешним по отношению к Dr.Web Gateway Security Suite прокси-сервером, обслуживающим соединения узлов локальной сети с веб-серверами по протоколу HTTP/HTTPS.

Протокол ICAP представляет собой легковесный HTTP-подобный протокол. Клиент отправляет на ICAP-сервер запрос, в состав которого входят заголовки, а также инкапсулированный HTTP-запрос, который необходимо проверить. В ответе ICAP-сервер возвращает модифицированный HTTP-запрос в инкапсулированном виде, а также один или несколько заголовков.

Для взаимодействия по протоколу ICAP используются следующие типы запросов (методы):

- `REQMOD` — для проверки и модификации запросов;
- `RESPMOD` — для проверки и модификации ответов;
- `OPTIONS` — для получения информации о параметрах соединения с ICAP-сервером.

В запросах `REQMOD` и `RESPMOD` используются заголовки:

- `X-Client-IP` — IP-адрес, с которого поступил проверяемый HTTP-запрос;
- `X-Server-IP` — IP-адрес, на который направлен проверяемый HTTP-запрос;
- `X-Client-Username` — имя клиента, прошедшего аутентификацию на прокси-сервере (в формате `user` или `user@domain`).

В ответах `REQMOD` и `RESPMOD` используются заголовки:

- `X-Response-Info` — присутствует в ответе, если запрашиваемый ресурс принадлежит к категории нежелательных или потенциально опасных. Всегда имеет значение `Blocked`.
- `X-Infection-Found` — содержит информацию о наличии вирусов и других нежелательных или потенциально опасных объектов.
- `X-Virus-ID` — содержит имя обнаруженной угрозы.
- `X-Violations-Found` — содержит информацию об ошибках, произошедших во время проверки.

В запросе `OPTIONS` может использоваться заголовок `DrWeb-Get-Scan-Status`. Если этот заголовок имеет значение `Yes`, то в ответе будет возвращена информация об используемых версиях антивирусного ядра Dr.Web Virus-Finding Engine, сканирующего ядра Dr.Web Scanning Engine и вирусных баз (см. ниже).

В ответе `OPTIONS` используются заголовки:

- `X-Allow-Out` — содержит список полей заголовков, которые Dr.Web ICAPD может включать в ответы;
- `X-Include` — значения заголовков, полученные из выполненного ранее запроса;
- `DrWeb-Core-Engine` — версия антивирусного ядра Dr.Web Virus-Finding Engine;
- `DrWeb-Scan-Engine` — версия сканирующего ядра Dr.Web Scanning Engine;
- `DrWeb-Scan-Status` — информация о статусе текущей операции сканирования;
- `DrWeb-Database-Timestamp` — метка времени вирусной базы;
- `DrWeb-Virus-Records` — количество записей в базе.

Dr.Web ICAPD также может фильтровать веб-контент и блокировать доступ к нежелательным и потенциально опасным веб-ресурсам. Если пользователь запросит доступ к такому ресурсу, ему будет возвращена страница блокировки, сформированная на основе шаблона. На странице содержится сообщение о запрете доступа с кратким объяснением причины. Такая же страница будет возвращена, если Dr.Web ICAPD обнаружит угрозу или если при проверке передаваемых данных произошла ошибка.

Для проверки URL на предмет принадлежности к нежелательным или потенциально опасным категориям Dr.Web ICAPD использует как базу категорий веб-ресурсов, регулярно обновляемую с серверов обновлений компании «Доктор Веб», так и опрашивает облачный сервис Dr.Web Cloud.

Потенциально опасные категории:

- *InfectionSource* — сайты, содержащие вредоносное ПО («источники распространения угроз»);
- *NotRecommended* — сайты, используемые для мошенничества («социальной инженерии») и не рекомендованные к посещению;

- *AdultContent* — сайты, содержащие материалы порнографического или эротического содержания, сайты знакомств и т. д.;
- *Violence* — сайты, содержащие призывы к насилию, материалы о различных происшествиях с человеческими жертвами и т. д.;
- *Weapons* — сайты, посвященные оружию и взрывчатым веществам, а также материалы с описанием их изготовления и т. д.;
- *Gambling* — сайты, на которых размещены онлайн-игры на деньги, интернет-казино, аукционы, а также принимающие ставки и т. д.;
- *Drugs* — сайты, пропагандирующие употребление, изготовление или распространение наркотиков и т. д.;
- *ObsceneLanguage* — сайты, на которых содержится нецензурная лексика (в названиях разделов, статьях и пр.);
- *Chats* — сайты для обмена сообщениями в режиме реального времени;
- *Terrorism* — сайты, содержащие материалы агрессивно-агитационного характера, описания терактов и т. д.;
- *FreeEmail* — сайты, предоставляющие возможность бесплатной регистрации электронного почтового ящика;
- *SocialNetworks* — социальные сети общего характера, деловые, корпоративные и тематические социальные сети, а также тематические сайты знакомств;
- *DueToCopyrightNotice* — сайты, ссылки на которые указаны правообладателями произведений, защищенных авторскими правами (кинофильмы, музыкальные произведения и т. д.);
- *OnlineGames* — сайты, на которых размещены игры, использующие постоянное соединение с интернет-сетью;
- *Anonymizers* — сайты, позволяющие пользователю скрывать свою личную информацию и предоставляющие доступ к заблокированным сайтам;
- *CryptocurrencyMiningPool* — сайты, предоставляющие доступ к сервисам, объединяющим пользователей с целью добычи (майнинга) криптовалют;
- *Jobs* — сайты, предназначенные для поиска работы.

В настройках компонента системный администратор может определять нежелательные категории веб-ресурсов, а также формировать черные и белые списки. При запросе ресурсов, включенных в черный список, пользователю возвращается страница блокировки. Если же ресурс включен в белый список, то доступ к нему будет всегда разрешен, даже если он относится к одной из нежелательных категорий.

Один сайт может принадлежать к нескольким категориям. Если одна из этих категорий отнесена к нежелательным, доступ к сайту будет заблокирован.

Даже если сайт включен в белый список, отправляемые и загружаемые с него данные все равно проверяются на наличие угроз.

В силу особенностей протокола ICAP, проверка данных большого объема (образы `.iso`, большие архивы, файлы видео и т. п.) может занимать продолжительное время. Рекомендуется настроить ограничения по MIME-типу данных, подлежащих проверке, а также ограничить в настройках прокси-сервера HTTP максимальный размер данных, проверяемых по протоколу ICAP (см. пример для прокси-сервера Squid).

Для регулярного автоматического обновления базы категорий веб-ресурсов с серверов компании «Доктор Веб» используется тот же компонент Dr.Web Updater, который обновляет вирусные базы для сканирующего ядра Dr.Web Scanning Engine. Для обращения к облачному сервису Dr.Web Cloud используется компонент Dr.Web CloudD (использование облачного сервиса задается в основных настройках Dr.Web Gateway Security Suite и при необходимости может быть отключено). Для проверки передаваемых данных Dr.Web ICAPD использует компонент сетевой проверки данных Dr.Web Network Checker, который, в свою очередь, инициирует их проверку сканирующим ядром Dr.Web Scanning Engine.

Для блокирования или пропуска запросов и ответов протокола HTTP компонент Dr.Web ICAPD может использовать как правила, внедренные в настройки, так и скрипт проверки, написанный на языке Lua.

Об интеграции Dr.Web ICAPD с прокси-сервером HTTP см. в разделе Интеграция с прокси-сервером Squid.

9.4.2. Аргументы командной строки

Для запуска компонента Dr.Web ICAPD из командной строки используется следующая команда:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-icapd [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-icapd [<параметры>]
```

Dr.Web ICAPD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-icapd --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web ICAPD.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Gateway Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-icapd`.

9.4.3. Параметры конфигурации

В этом разделе

- Параметры компонента
- Правила проверки трафика и блокировки доступа
  - Просмотр и редактирование правил
  - Просмотр правил с помощью команды drweb-ctl cfshow
  - Редактирование правил с помощью команды drweb-ctl cfset
  - Набор правил по умолчанию
  - Примеры правил проверки трафика и блокировки доступа

Компонент использует параметры конфигурации, заданные в секции `[ICAPD]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

Параметры компонента

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, то используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-icapd` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-icapd`
`Start` *{логический}*	Компонент запускается демоном управления конфигурацией Dr.Web ConfigD. Установка данного параметра в `Yes` предписывает демону управления конфигурацией немедленно запустить компонент, а установка его в значение `No` — немедленно завершить работу компонента. Значение по умолчанию: `No`
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`

Параметр	Описание
`DebugDumpIcap` *{логический}*	Сохранять или не сохранять в журнал содержимое сообщений, передаваемых по протоколу ICAP, если уровень подробности ведения журнала — отладочный (при `LogLevel = DEBUG`). Значение по умолчанию: `No`
`ListenAddress` *{сетевой сокет}*	Сетевой сокет (IP-адрес и порт), прослушиваемый Dr.Web ICAPD в ожидании подключений от прокси-серверов HTTP. Значение по умолчанию: `127.0.0.1:1344`
`TemplatesDir` *{путь к каталогу}*	Путь к каталогу с файлами шаблонов HTML-страниц уведомлений о блокировке веб-ресурсов. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/templates/icapd` • для FreeBSD: `/var/drweb.com/templates/icapd`

`Whitelist`
{список доменов}
	Белый список доменов. Все домены, включенные в список, будут доступны пользователям, даже если они отнесены к нежелательным категориям веб-ресурсов. Доступ ко всем поддоменам этих доменов также будет открыт.
	Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения параметра объединяются в единый список).
	Пример: Добавить в список домены `example.com` и `example.net`.
	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[ICAPD]`
	`Whitelist = "example.com", "example.net"`
	• Две строки (по одному значению в строке):
	`[ICAPD]`
	`Whitelist = example.com`
	`Whitelist = example.net`

Параметр	Описание

	2. Добавление значений через команду `drweb-ctl cfset`:
	`# drweb-ctl cfset ICAPD.Whitelist -a example.com`
	`# drweb-ctl cfset ICAPD.Whitelist -a example.net`
	⚠ Реальное использование списка доменов, указанного в данном параметре, зависит от того, *как* он используется в правилах управления доступом к веб-ресурсам, заданных для Dr.Web ICAPD.
	В перечне правил, заданных по умолчанию (см. ниже), гарантируется, что доступ к доменам (и их поддоменам) из данного списка будет обеспечен, даже если там будут находиться домены из блокируемых категорий веб-ресурсов. Кроме этого, набор правил по умолчанию гарантирует, что данные, загружаемые с доменов из белого списка, *будут проверяться на наличие угроз*.
	Значение по умолчанию: *(не задано)*

`Blacklist`
{список доменов}
	Черный список доменов. Все домены, включенные в этот список, не будут доступны пользователям, даже если они не отнесены к категориям нежелательных веб-ресурсов. Доступ ко всем поддоменам этих доменов также будет заблокирован.
	Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).
	Пример: Добавить в список домены `example.com` и `example.net`.
	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[ICAPD]`
	`Blacklist = "example.com", "example.net"`

Параметр	Описание

	• Две строки (по одному значению в строке):
	`[ICAPD]`
	`Blacklist = example.com`
	`Blacklist = example.net`
	2. Добавление значений через команду `drweb-ctl cfset`:
	`# drweb-ctl cfset ICAPD.Blacklist -a example.com`
	`# drweb-ctl cfset ICAPD.Blacklist -a example.net`
	⚠ Реальное использование списка доменов, указанного в данном параметре, зависит от того, *как* он используется в правилах управления доступом к веб-ресурсам, заданных для Dr.Web ICAPD.
	В перечне правил, заданных по умолчанию (см. ниже), гарантируется, что доступ к доменам (и их поддоменам) из данного списка будет всегда запрещен. Если домен добавлен одновременно в список `Whitelist` и список `Blacklist`, то правила, заданные по умолчанию, гарантируют, что доступ пользователей к нему будет заблокирован.
	Значение по умолчанию: *(не задано)*

`Adlist`
{список строк}
	Список регулярных выражений для описания сайтов. URL, соответствующий любому из приведенных в этом списке регулярных выражений, считается рекламным.
	Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).
	Пример: Добавить в список выражения '`.*ads.+`' и '`.*/ad/.*\.gif$`'.
	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[ICAPD]`
	`Adlist = ".*ads.+", ".*/ad/.*\.gif$"`

Параметр	Описание

	• Две строки (по одному значению в строке):
	`[ICAPD]`
	`Adlist = .*ads.+`
	`Adlist = .*/ad/.*\.gif$`
	2. Добавление значений через команду `drweb-ctl cfset`:
	`# drweb-ctl cfset ICAPD.Adlist -a '.*ads.+'`
	`# drweb-ctl cfset ICAPD.Adlist -a '.*/ad/.*\.gif$'`
	Регулярные выражения записываются с использованием синтаксиса POSIX (BRE, ERE) или Perl (PCRE, PCRE2).
	⚠ Реальное использование списка выражений, указанного в данном параметре, зависит от того, *как* он используется в правилах управления доступом к веб-ресурсам, заданных для Dr.Web ICAPD.
	В перечне правил, заданных по умолчанию (см. ниже), гарантируется, что доступ к URL из данного списка будет запрещен только в том случае, если домены, на которые ведут эти URL, не находятся в списке `Whitelist`.
	Значение по умолчанию: *(не задано)*

`BlockInfectionSource` *{логический}*	Блокировать попытки подключения к сайтам, содержащим вредоносное ПО (входящим в категорию *InfectionSource*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockNotRecommended` *{логический}*	Блокировать попытки подключения к нерекомендуемым сайтам (входящим в категорию *NotRecommended*).

Параметр	Описание
	Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockAdultContent` *{логический}*	Блокировать попытки подключения к сайтам, содержащим материалы для взрослых (входящим в категорию *AdultContent*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockViolence` *{логический}*	Блокировать попытки подключения к сайтам, содержащим сцены насилия (входящим в категорию *Violence*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockWeapons` *{логический}*	Блокировать попытки подключения к сайтам, посвященным оружию (входящим в категорию *Weapons*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockGambling` *{логический}*	Блокировать попытки подключения к сайтам, посвященным азартным играм и играм на деньги (входящим в категорию *Gambling*).

Параметр	Описание
	Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockDrugs` *{логический}*	Блокировать попытки подключения к сайтам, посвященным наркотикам (входящим в категорию *Drugs*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockObsceneLanguage` *{логический}*	Блокировать попытки подключения к сайтам, содержащим нецензурную лексику (входящим в категорию *ObsceneLanguage*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockChats` *{логический}*	Блокировать попытки подключения к сайтам чатов (входящим в категорию *Chats*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockTerrorism` *{логический}*	Блокировать попытки подключения к сайтам, посвященным терроризму (входящим в категорию *Terrorism*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match`

Параметр	Описание
	Значение по умолчанию: `No`
`BlockFreeEmail` *{логический}*	Блокировать попытки подключения к сайтам бесплатных почтовых служб (входящим в категорию *FreeEmail*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockSocialNetworks` *{логический}*	Блокировать попытки подключения к сайтам социальных сетей (входящим в категорию *SocialNetworks*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockDueToCopyrightNotice` *{логический}*	Блокировать попытки подключения к сайтам, ссылки на которые были добавлены по обращению правообладателей (входящим в категорию *DueToCopyrightNotice*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockOnlineGames` *{логический}*	Блокировать попытки подключения к сайтам онлайн-игр (входящим в категорию *OnlineGames*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockAnonymizers` *{логический}*	Блокировать попытки подключения к сайтам анонимайзеров (входящим в категорию *Anonymizers*).

Параметр	Описание
	Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockCryptocurrencyMiningPools` *{логический}*	Блокировать попытки подключения к сайтам, объединяющим пользователей с целью добычи (майнинга) криптовалют (входящим в категорию *CryptocurrencyMiningPool*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockJobs` *{логический}*	Блокировать попытки подключения к сайтам для поиска работы (входящим в категорию *Jobs*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "ICAPD.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockKnownVirus` *{логический}*	Блокировать получение и передачу данных, если они содержат известную угрозу. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "ICAPD.BlockThreat" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockSuspicious` *{логический}*	Блокировать получение и передачу данных, если они содержат неизвестную угрозу, обнаруженную эвристическим анализатором.

Параметр	Описание
	Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "ICAPD.BlockThreat" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockAdware` *{логический}*	Блокировать получение и передачу данных, если они содержат рекламную программу. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "ICAPD.BlockThreat" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockDialers` *{логический}*	Блокировать получение и передачу данных, если они содержат программу дозвона. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "ICAPD.BlockThreat" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockJokes` *{логический}*	Блокировать получение и передачу данных, если они содержат программу-шутку. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "ICAPD.BlockThreat" : BLOCK as _match` Значение по умолчанию: `No`
`BlockRiskware` *{логический}*	Блокировать получение и передачу данных, если они содержат потенциально опасную программу. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "ICAPD.BlockThreat" : BLOCK as _match` Значение по умолчанию: `No`

Параметр	Описание
`BlockHacktools` *{логический}*	Блокировать получение и передачу данных, если они содержат программу взлома. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "ICAPD.BlockThreat" : BLOCK as _match` Значение по умолчанию: `No`
`ScanTimeout` *{интервал времени}*	Тайм-аут на проверку одного файла по запросу Dr.Web ICAPD. Допустимые значения: от 1 секунды (`1s`) до 1 часа (`1h`). Значение по умолчанию: `30s`
`HeuristicAnalysis` *{On | Off}*	Использовать или не использовать эвристический анализ для поиска неизвестных угроз. Эвристический анализ повышает надежность проверки, но увеличивает ее длительность. Действие при срабатывании эвристического анализатора задается параметром `BlockSuspicious`. Допустимые значения: • `On` — использовать эвристический анализ при проверке; • `Off` — не использовать эвристический анализ. Значение по умолчанию: `On`
`PackerMaxLevel` *{целое число}*	Максимальный уровень вложенности для запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`ArchiveMaxLevel` *{целое число}*	Максимальный уровень вложенности для архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены

Параметр	Описание
	архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`MailMaxLevel` *{целое число}*	Максимальный уровень вложенности для файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`ContainerMaxLevel` *{целое число}*	Максимальный уровень вложенности для других типов объектов с вложениями (например, страницы HTML, файлы `.jar` и др.). Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`MaxCompressionRatio` *{целое число}*	Максимальная допустимую степень сжатия запакованных объектов (отношение сжатого объема к несжатому). Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке данных, инициированной по запросу Dr.Web ICAPD. Величина степени сжатия должна быть не менее `2`. Значение по умолчанию: `500`
`BlockUnchecked` *{логический}*	Блокировать получение и передачу данных, если они не могут быть проверены. Значение по умолчанию: `No`
`UsePreview` *{логический}*	Включить или отключить режим *ICAP preview* для Dr.Web ICAPD. *Не изменяйте* значение этого параметра без необходимости.

Параметр	Описание
	Значение по умолчанию: `Yes`
`Use204` *{логический}*	Возвращать код ответа `204` не только в режиме *ICAP preview*. *Не изменяйте* значение этого параметра без необходимости. Значение по умолчанию: `Yes`
`AllowEarlyResponse` *{логический}*	Разрешить или запретить Dr.Web ICAPD использовать режим «раннего» ответа ICAP, т. е. начинать отправлять ответ клиенту, не прочитав до конца запрос от прокси-сервера HTTP. *Не изменяйте* значение этого параметра без необходимости. Значение по умолчанию: `Yes`

`MessageHook`
 	
{путь к файлу | функция Lua}
	Скрипт обработки HTTP-сообщений на языке Lua либо путь к файлу скрипта (см. раздел Обработка HTTP-сообщений на Lua).
	
	Если функция Lua или путь к файлу не указаны, то сообщения будут обрабатываться в соответствии с правилами. Если указанный файл недоступен, то при загрузке компонента будет выдана ошибка.
	
	Значение по умолчанию: *Генерируется автоматически*. Для настроек по умолчанию скрипт выглядит так:
	
	`local dw = require "drweb"`
	`local cfg = require "drweb.config"`
	`local dwl = require "drweb.lookup"`
	`local rx = require "drweb.regex"`
	
	`function message_hook(ctx)`
	`  if ctx.direction == "request" then`
	`    local url = ctx.request.url`
	`    if url.in_list(cfg.blacklist) then`
	`      return "block"`
	`    end`
	`    if not url.in_list(cfg.whitelist) then`
	`      if rx.search(cfg.adlist, url) or rx.search(cfg.adlist, url.raw) then`
	`        return "block"`
	`      end`
	`      if url.in_categories(cfg.block_url_categories) then`
	`        return "block"`
	`      end`
	`    end`
	`  end`

Параметр	Описание

	`if ctx.body.has_threat{category = cfg.block_threats} then`
	`  return "block"`
	`end`
	`if cfg.block_unchecked and ctx.body.scan_error then`
	`  return "block"`
	`end`
	`return "pass"`
	`end`

Правила проверки трафика и блокировки доступа

В дополнение к параметрам, перечисленным выше, в секции присутствует семь *наборов правил* `RuleSet*` (`RuleSet0`, ..., `RuleSet6`), непосредственно управляющих проверкой трафика и блокировкой доступа пользователей к веб-ресурсам, а также загрузкой контента из интернета. Для некоторых значений в условиях (например, диапазоны IP-адресов, перечни категорий сайтов, черные и белые списки сайтов и т. п.) предусмотрена подстановка значений, загружаемых из текстовых файлов, а также извлеченных из внешних источников данных через LDAP (используется компонент Dr.Web LookupD). При обработке соединений все правила проверяются в порядке сверху вниз единым списком до момента нахождения сработавшего правила, содержащего финальную резолюцию. Пропуски в списке правил, если встречаются, игнорируются.

Подробно правила рассмотрены в разделе Правила проверки трафика Приложения Г.

Просмотр и редактирование правил

Для удобства редактирования списка правил по умолчанию в списке оставлены «пустоты», т. е. наборы `RuleSet<i>`, не содержащие правил (где <*i*> — номер набора `RuleSet`).

> Вы не можете добавить элементы списка, отличные от уже имеющихся `RuleSet<i>`, но можете добавить или удалить любое правило в любом элементе `RuleSet<i>`.

Просмотр и редактирование правил могут осуществляться любым из нижеуказанных способов:

- путем просмотра и изменения файла конфигурации в любом текстовом редакторе (помните, что в этом файле сохраняются только те параметры, значение которых отличается от значений по умолчанию);
- через веб-интерфейс управления;

- через интерфейс командной строки Dr.Web Ctl (команды `drweb-ctl cfshow` и `drweb-ctl cfset`).

Если вы редактировали правила, внося изменения в файл конфигурации, для применения внесенных изменений перезапустите Dr.Web Gateway Security Suite. Для этого воспользуйтесь командой `drweb-ctl reload`.

Просмотр правил с помощью команды drweb-ctl cfshow

Для просмотра содержимого набора правил `ICAPD.RuleSet1` используйте команду:

```
# drweb-ctl cfshow ICAPD.RuleSet1
```

Редактирование правил с помощью команды drweb-ctl cfset

Здесь и далее <*правило*> — текст правила.

- Замена всех правил в наборе правил `ICAPD.RuleSet1` на новое правило:

```
# drweb-ctl cfset ICAPD.RuleSet1 '<правило>'
```

- Добавление еще одного правила в набор правил `ICAPD.RuleSet1`:

```
# drweb-ctl cfset -a ICAPD.RuleSet1 '<правило>'
```

- Удаление конкретного правила из набора правил `ICAPD.RuleSet1`:

```
# drweb-ctl cfset -e ICAPD.RuleSet1 '<правило>'
```

- Возврат набора правил `ICAPD.RuleSet1` к значениям по умолчанию:

```
# drweb-ctl cfset -r ICAPD.RuleSet1
```

При использовании утилиты `drweb-ctl` для редактирования правил заключайте строку добавляемого правила <*правило*> в одинарные или двойные кавычки, а внутренние кавычки, если они встречаются в правиле, экранируйте символом обратной косой черты `\`.

Важно помнить следующие особенности хранения правил в переменных конфигурации `RuleSet<i>`:

- При добавлении безусловных правил условная часть и двоеточие могут быть опущены, однако такие правила всегда сохраняются в списке правил в виде строки `' : <действие>'`.
- При добавлении правил, содержащих несколько действий (правила вида `'<условие> : <действие 1>, <действие 2>'`), такие правила будут преобразованы в цепочку элементарных правил `'<условие> : <действие 1>'` и `'<условие> : <действие 2>'`.
- Так как в записи правил не предусмотрено дизъюнкции (логическое «ИЛИ») условий в условной части, для реализации логического «ИЛИ» запишите цепочку правил, в условии каждого из которых будет указано условие-дизъюнкт.

Чтобы добавить в набор правил `ICAPD.RuleSet1` правило безусловного пропуска (действие `PASS`), достаточно выполнить команду:

```
# drweb-ctl cfset -a ICAPD.RuleSet1 'PASS'
```

Однако, чтобы удалить это правило из указанного набора правил, необходимо выполнить команду:

```
# drweb-ctl cfset -e ICAPD.RuleSet1 ' : PASS'
```

Чтобы добавить в набор правил `ICAPD.RuleSet1` правило, изменяющее для соединений, следующих с неразрешенных адресов, путь к стандартным шаблонам и выполняющее блокировку, достаточно выполнить команду:

```
# drweb-ctl cfset -a ICAPD.RuleSet1 'src_ip not in file("/etc/trusted_ip") :
set http_template_dir = "mytemplates", BLOCK'
```

Эта команда, однако, добавит *два правила* в указанный набор правил, поэтому, чтобы удалить их, необходимо выполнить две команды:

```
# drweb-ctl cfset -e ICAPD.RuleSet1 'src_ip not in file("/etc/trusted_ip") :
set http_template_dir = "mytemplates"'
# drweb-ctl cfset -e ICAPD.RuleSet1 'src_ip not in file("/etc/trusted_ip") :
BLOCK'
```

Чтобы добавить в набор правил `ICAPD.RuleSet1` правило вида «Осуществить блокировку, если обнаружен вредоносный объект типа *KnownVirus* или URL из категории *Terrorism*», необходимо добавить в этот набор сразу два правила:

```
# drweb-ctl cfset -a ICAPD.RuleSet1 'threat_category in (KnownVirus) : BLOCK
as _match'
# drweb-ctl cfset -a ICAPD.RuleSet1 'url_category in (Terrorism) : BLOCK as
_match'
```

Для их удаления также потребуется две команды, как в примере выше.

Набор правил по умолчанию

По умолчанию задан следующий набор правил, управляющих блокировкой:

```
RuleSet0 =
RuleSet1 = direction request, url_host in "ICAPD.Blacklist" : BLOCK as
BlackList
RuleSet1 = direction request, url_host not in "ICAPD.Whitelist", url match
"ICAPD.Adlist" : BLOCK as BlackList
RuleSet2 =
RuleSet3 = direction request, url_host not in "ICAPD.Whitelist",
url_category in "ICAPD.BlockCategory" : BLOCK as _match
RuleSet4 =
RuleSet5 = threat_category in "ICAPD.BlockThreat" : BLOCK as _match
RuleSet6 =
```

Первые два правила регламентируют обработку исходящих HTTP-соединений: если узел (или URL), с которым производится попытка установить соединение, включен в черный список, соединение блокируется по причине попадания в черный список, дальнейшие проверки не производятся. Если же узел (URL) не находится в белом списке и относится к любой из категорий сайтов, отмеченной как нежелательные для посещения, или соответствует списку регулярных выражений, описывающих рекламные сайты, то соединение блокируется по причине попадания URL в запрещенную к посещению категорию.

Правило, указанное в `RuleSet5`, проверяет, не содержатся ли в теле проверяемого HTTP-запроса или HTTP-ответа угрозы, относящиеся к категориям, которые следует блокировать, и если да, то соединение блокируется по причине обнаружения угрозы.

Из-за отсутствия условия `direction` по умолчанию проверяются как запросы клиентов (*request*), так и ответы серверов (*response*).

Примеры правил проверки трафика и блокировки доступа

1. Разрешить для пользователей с диапазоном IP-адресов *10.10.0.0–10.10.0.254* доступ к сайтам любых категорий, кроме категории *Chats*:

   ```
   src_ip in (10.10.0.0/24), url_category not in (Chats) : PASS
   ```

Если правило:

```
url_host in "ICAPD.Blacklist" : BLOCK as BlackList
```

разместить в списке правил выше (т. е. раньше) указанного правила, то доступ к доменам из черного списка, т. е. доменам, перечисленным в параметре `ICAPD.Blacklist`, будет блокироваться и для пользователей с диапазоном IP-адресов *10.10.0.0–10.10.0.254*. А если это правило разместить ниже (т. е. позже), то пользователям с диапазоном IP-адресов *10.10.0.0–10.10.0.254* будут доступны также и сайты из черного списка.

Поскольку резолюция `PASS` является конечной, более никакие правила не проверяются, следовательно, проверка загружаемых данных на наличие угроз также производиться не будет.

Чтобы разрешить пользователям с диапазоном IP-адресов *10.10.0.0–10.10.0.254* доступ к сайтам любых категорий, кроме категории *Chats*, если они не находятся в черном списке, но при этом не разрешать загрузку угроз, используйте следующее правило:

```
url_category not in (Chats), url_host not in "ICAPD.Blacklist",
threat_category not in "ICAPD.BlockCategory" : PASS
```

2. Не выполнять проверку содержимого видео-файлов (т. е. данных с типом MIME `video/*`, где `*` соответствует любому типу MIME-класса `video`):

```
content_type in ("video/*") : PASS
```

9.4.4. Обработка HTTP-сообщений на Lua

В этом разделе

- Общие сведения
- Требования к скрипту для обработки сообщений
- Используемые таблицы (MessageContext, ICAP, User, HeaderField, Request, ContentType, Url, RawUrl, UrlCategoryFilter, Response, Body, Virus, ThreatFilter)
- Доступные сервисные модули (drweb, drweb.lookup, drweb.regex, drweb.config)

Общие сведения

Компонент Dr.Web ICAPD поддерживает взаимодействие с интерпретатором программ на языке Lua (используется версия 5.3.4, которая поставляется совместно с Dr.Web Gateway Security Suite). Скрипты на Lua могут использоваться компонентом для анализа и обработки сообщений протокола HTTP.

Анализ HTTP-сообщения (запроса или ответа), поступившего на проверку от прокси-сервера по протоколу ICAP, выполняется при помощи скрипта на языке Lua, указанного

в настройках Dr.Web ICAPD в соответствующем параметре `MessageHook` (может быть указан как текст скрипта, так и путь к файлу скрипта).

Требования к скрипту для обработки сообщений

Скрипт должен содержать глобальную функцию, являющуюся точкой входа в модуль проверки сообщений (эту функцию Dr.Web ICAPD будет вызывать для обработки вновь поступившего сообщения). Функция обработки должна соответствовать следующим соглашениям о вызове:

1. *Имя функции* — `message_hook`.
2. *Единственный аргумент* — таблица MessageContext (предоставляет из функции доступ к информации об обрабатываемом сообщении).
3. *Единственное возвращаемое значение* — строка. Возвращаемое значение определяет вердикт относительно проверяемого сообщения: пропустить или заблокировать. Возможные значения:
   - `pass` — HTTP-сообщение будет передано получателю (HTTP-запрос — серверу, HTTP-ответ — клиенту).
   - `block` — HTTP-сообщение не будет передано получателю, клиент получит HTTP-ответ с веб-страницей блокировки.

Ситуации, когда функция возвращает иное значение или же во время ее выполнения происходит ошибка, интерпретируются как ошибка проверки; ответ клиенту в таких случаях зависит от значения параметра `BlockUnchecked`.

Ниже приведен пример корректного определения функции, которая всегда будет возвращать в Dr.Web ICAPD вердикт `pass` (пропустить) для всех проверяемых HTTP-сообщений (здесь и далее аргумент `ctx` — экземпляр таблицы *MessageContext*):

```
function message_hook(ctx)
  return "pass"
end
```

Следующий скрипт заблокирует доступ ко всем ресурсам, кроме сайта с документацией компании «Доктор Веб» для всех пользователей, кроме членов группы Web Admins в Active Directory:

```
local dwl = require "drweb.lookup"

function message_hook(ctx)

  -- Не блокировать доступ к ресурсам на сайте документации
  -- компании «Доктор Веб»
  if ctx.request.url.in_list{"download.geo.drweb.com"} then
      return "pass"
  end

  -- Разрешить доступ пользователям из группы WebAdmins
  -- в Active Directory
  if dwl.check("WebAdmins", "AD@WinRoot", ctx.icap.user) then
      return "pass"
  end

  -- Заблокировать доступ всем остальным (ко всем ресурсам)
  return "block"

end
```

Используемые таблицы

Таблица MessageContext

Используется как входной аргумент функции `message_hook`, содержит информацию об обрабатываемом HTTP-сообщении (его тип, заголовки, тело, а также информацию об отправителе и получателях, если она доступна).

Поле	Описание	Тип данных
`direction`	Тип HTTP-сообщения: • `request` — HTTP-запрос. • `response` — HTTP-ответ.	Строка
`icap`	Информация о заголовках ICAP-запроса.	Таблица ICAP
`request`	Информация о заголовках HTTP-запроса.	Таблица Request
`response`	Информация о заголовках HTTP-ответа.	Таблица Response
`body`	Информация о теле HTTP-сообщения.	Таблица Body
Переопределенные метаметоды: *Нет*		

Таблица ICAP

Используется как поле `icap` таблицы MessageContext. Хранит информацию об ICAP-запросе от прокси-сервера HTTP.

Поле	Описание	Тип данных
`user`	Информация о пользователе, полученная из заголовка `X-Client-Username` ICAP-запроса.	Таблица User
`src`	IP-адрес клиента, отправившего запрос (содержится в ICAP-запросе от прокси-сервера, в заголовке `X-Client-IP`), либо `nil`, если адрес неизвестен.	Таблица IpAddress
`field`	Массив заголовков ICAP-запроса.	Массив таблиц HeaderField
`search`	Функция для поиска заголовка по регулярному выражению. Принимает один обязательный аргумент `patterns` — шаблоны поиска, т. е. одно (строка) или несколько (массив строк) регулярных выражений в синтаксисе Perl (PCRE). Выполняет поиск по всем имеющимся заголовкам. ⚠ При использовании строк в кавычках символ косой черты необходимо экранировать. Возвращает логическое значение: • `true` — если для хотя бы одного заголовка строка `field.name .. ": " .. field.value.decoded` соответствует хотя бы одному из заданных регулярных выражений; • `false` — если соответствий не обнаружено.	Функция
`value`	Функция, принимающая один обязательный аргумент — имя заголовка (строка). Возвращает значение первого заголовка с указанным именем, либо `nil`, если заголовка с таким именем нет.	Функция
Переопределенные метаметоды: *Нет*		

Таблица User

Таблица содержит имя пользователя и домен; оба ее поля необязательны.

Поле	Описание	Тип данных
`user`	Имя пользователя	Строка
`domain`	Домен пользователя	Строка

Поле	Описание	Тип данных
Переопределенные метаметоды: • `__tostring` — функция, возвращающая содержимое `User` в виде строки (в кодировке UTF-8); • `__concat` — функция, присоединяющая преобразованное в строку значение `User` к строке.		

Таблица HeaderField

Таблица описывает HTTP- или ICAP-сообщения.

Поле	Описание	Тип данных
`name`	Имя заголовка	Строка
`value`	Значение заголовка	Строка
Переопределенные метаметоды: *Нет*		

Таблица Request

Таблица описывает заголовки HTTP-запроса.

Поле	Описание	Тип данных
`method`	Метод протокола HTTP, указанный в запросе (например, `POST`), либо `nil`, если ICAP-запрос не включает заголовок HTTP-запроса.	Строка
`url`	URL ресурса, на который направлен HTTP-запрос.	Таблица Url
`content_type`	Информация, полученная из заголовка `Content-Type` HTTP-запроса.	Таблица ContentType
`field`	Массив заголовков HTTP-запроса.	Массив таблиц HeaderField
`search`	Функция для поиска заголовка по регулярному выражению. Принимает один обязательный аргумент `patterns` — шаблоны поиска, т. е. одно (строка) или несколько (массив строк) регулярных выражений в синтаксисе Perl (PCRE). Выполняет поиск по всем имеющимся заголовкам. ⚠ При использовании строк в кавычках символ косой черты необходимо экранировать. Возвращает логическое значение:	Функция

Поле	Описание	Тип данных
	• `true` — если для хотя бы одного заголовка строка `field.name .. ": " .. field.value.decoded` соответствует хотя бы одному из заданных регулярных выражений; • `false` — если соответствий не обнаружено.	
`value`	Функция, принимающая один обязательный аргумент — имя заголовка (строка). Возвращает значение первого заголовка с указанным именем, либо `nil`, если заголовка с таким именем нет.	Функция
Переопределенные метаметоды: *Нет*		

Таблица ContentType

Таблица описывает значение, полученное из заголовка `Content-Type`.

Поле	Описание	Тип данных
`type`	MIME-тип части сообщения	Строка
`subtype`	Подтип части сообщения	Строка
`param`	Параметры заголовка в виде массива таблиц, содержащих следующие поля: • `name` — имя параметра (строка); • `value` — значение параметра (строка).	Массив таблиц
`match`	Функция, принимающая один обязательный аргумент `media_types` — массив строк, описывающих MIME-типы. Каждая строка должна иметь вид "`тип/подтип`", "`тип/*`" или "`*/*`". Возвращает логическое значение: • `true` — если MIME-тип тела соответствует одной из указанных строк (регистр не учитывается) или переданный массив содержит строку "`*/*`"; • `false` — если соответствий не обнаружено.	Функция
Переопределенные метаметоды: • `__tostring` — функция, возвращающая раскодированное значение заголовка; • `__concat` — функция, присоединяющая раскодированное значение заголовка к строке.		

Таблица Url

Таблица описывает URL.

Поле	Описание	Тип данных
`scheme`	Префикс схемы (протокола), например, `http`. Если отсутствует — `nil`.	Строка
`host`	Имя или IP-адрес узла, например, `example.com`. Если отсутствует — `nil`.	Строка
`port`	Номер порта, например, `80`. Если отсутствует — `nil`.	Число
`path`	Путь к ресурсу, например, `index.html`. Если отсутствует — `nil`.	Строка
`query`	Декодированные параметры запроса. Если отсутствуют — `nil`.	Строка
`legal_url`	В случае принадлежности URL категории `owners_notice` содержит строку с URL, ведущим на сайт правообладателя, иначе — `nil`.	Строка
`in_list`	Функция, принимающая один обязательный аргумент `hosts` — список доменов (массив строк). Возвращает логическое значение: • `true` — если `host` является поддоменом одного из указанных доменов либо совпадает с одним из них; • `false` — если совпадений не обнаружено.	Функция
`categories`	Функция, принимающая один необязательный аргумент `filter` — таблицу UrlCategoryFilter (отсутствие аргумента равносильно использованию пустой таблицы). Возвращает функцию-итератор, с помощью которой можно перебрать все категории, удовлетворяющие заданным с помощью `filter` условиям, к которым относится URL.	Функция
`in_categories`	Функция, принимающая один обязательный аргумент `categories` — список категорий URL (массив строк). Возвращает логическое значение: • `true` — если URL относится хотя бы к одной из указанных категорий; • `false` — если URL не относится ни к одной из категорий. Если массив `categories` пустой, всегда возвращается `false`. Возможные значения категорий см. в описании поля `category` таблицы UrlCategoryFilter.	Функция
`raw`	Нераскодированный URL в «сыром» виде.	Таблица RawUrl
Переопределенные метаметоды: • `__tostring` — функция, возвращающая содержимое `Url` в виде строки (в кодировке UTF-8); • `__concat` — функция, присоединяющая к строке преобразованное в строку значение `Url`.		

Таблица RawUrl

Таблица содержит информацию об URL в нераскодированном виде.

Поле	Описание	Тип данных
`scheme`	Префикс схемы (протокола), например, `http`. Если отсутствует — `nil`.	Строка
`host`	Имя или IP-адрес узла, например, `example.com`. Если отсутствует — `nil`.	Строка
`port`	Номер порта, например, `80`. Если отсутствует — `nil`.	Число
`path`	Путь к ресурсу, например, `index.html`. Если отсутствует — `nil`.	Строка
`query`	Декодированные параметры запроса. Если отсутствуют — `nil`.	Строка
Переопределенные метаметоды: • `__tostring` — функция, возвращающая содержимое `RawUrl` в виде строки (в кодировке UTF-8); • `__concat` — функция, присоединяющая к строке преобразованное в строку значение `RawUrl`.		

Таблица UrlCategoryFilter

Таблица описывает фильтр для категорий URL. Все ее поля являются необязательными.

Поле	Описание	Тип данных
`category`	Список категорий, которым должен соответствовать URL (регистр не учитывается): • `infection_source` — источник распространения угроз; • `not_recommended` — не рекомендуемый к посещению; • `adult_content` — материалы для взрослых; • `violence` — насилие; • `weapons` — оружие; • `gambling` — азартные игры; • `drugs` — наркотики; • `obscene_language` — нецензурная лексика; • `chats` — чаты; • `terrorism` — терроризм; • `free_email` — бесплатная электронная почта; • `social_networks` — социальные сети;	Строка или таблица строк

Поле	Описание	Тип данных
	• `owners_notice` — сайты, добавленные по обращению правообладателей; • `online_games` — онлайн-игры; • `anonymizers` — анонимайзеры; • `cryptocurrency_mining_pools` — пулы майнеров криптовалют; • `jobs` — сайты для поиска работы; • `black_list` — черный список.	
`category_not`	Список категорий, которым не должен соответствовать URL (регистр не учитывается).	Строка или таблица строк
Переопределенные метаметоды: *Нет*		

Если поле фильтра не задано (т. е. указано значение `nil`), то любая угроза соответствует фильтру. Если указаны несколько полей фильтра, то условие объединяется по конъюнкции (логическое «И»). Если тип поля фильтра — это таблица (список), то фильтруемый объект должен соответствовать хотя бы одному из ее элементов.

Таблица Response

Таблица описывает заголовки HTTP-ответа.

Поле	Описание	Тип данных
`status`	Код ответа HTTP либо `nil`, если ICAP-запрос не включает заголовок HTTP-ответа.	Число
`reason`	Пояснение к коду ответа либо `nil`, если отсутствует.	Строка
`content_type`	Содержит информацию, полученную из заголовка `Content-Type` HTTP-ответа.	Таблица ContentType
`field`	Массив заголовков HTTP-ответа	Массив таблиц HeaderField
`search`	Функция для поиска заголовка по регулярному выражению. Принимает один обязательный аргумент `patterns` — шаблоны поиска, т. е. одно (строка) или несколько (массив строк) регулярных выражений в синтаксисе Perl (PCRE). Выполняет поиск по всем имеющимся заголовкам.	Функция

Поле	Описание	Тип данных
	 При использовании строк в кавычках символ косой черты необходимо экранировать. Возвращает логическое значение: • `true` — если для хотя бы одного заголовка строка `field.name .. ": " .. field.value.decoded` соответствует хотя бы одному из заданных регулярных выражений; • `false` — если соответствий не обнаружено.	
`value`	Функция, принимающая один обязательный аргумент — имя заголовка (строка). Возвращает значение первого заголовка с указанным именем либо `nil`, если заголовка с таким именем нет.	Функция
Переопределенные метаметоды: *Hem*		

Таблица Body

Таблица описывает тело HTTP-сообщения.

Поле	Описание	Тип данных
`has_threat`	Функция, принимающая один необязательный аргумент `filter` — таблицу ThreatFilter (отсутствие аргумента равносильно использованию пустой таблицы). Возвращает логическое значение: • `true` — если тело HTTP-сообщения содержит угрозу, соответствующую указанному условию `filter`; • `false` — если соответствий не обнаружено.	Функция
`threats`	Функция, принимающая один необязательный аргумент `filter` — таблицу ThreatFilter (отсутствие аргумента равносильно использованию пустой таблицы). Возвращает функцию-итератор, с помощью которой можно перебрать все угрозы, найденные в теле HTTP-сообщения. Угрозы описываются с помощью таблицы Virus.	Функция
`content_type`	Содержит информацию о MIME-типе тела, полученную из заголовка `Content-Type` HTTP-запроса или ответа (в зависимости от того, тело сообщения какого типа анализируется).	Таблица ContentType

Поле	Описание	Тип данных
scan_error	Ошибка проверки тела, если произошла, иначе — nil. Возможные значения: • path_not_absolute — указан не абсолютный путь; • file_not_found — файл не найден; • file_not_regular — специальный файл; • file_not_block_device — не блочное устройство; • name_too_long — слишком длинное имя; • no_access — нет доступа; • read_error — ошибка чтения; • write_error — ошибка записи; • file_too_large — файл слишком большой; • file_busy — файл используется; • unpacking_error — ошибка распаковки; • password_protected — архив защищен паролем; • arch_crc_error — ошибка CRC архива; • arch_invalid_header — ошибочный заголовок архива; • arch_no_memory — не хватает памяти для распаковки архива; • arch_incomplete — неполный архив; • can_not_be_cured — файл не может быть вылечен; • packer_level_limit — превышение предельного уровня вложенности для упакованного объекта; • archive_level_limit — превышение предельного уровня вложенности для архива; • mail_level_limit — превышение предельного уровня вложенности для почтового файла; • container_level_limit — превышение предельного уровня вложенности для контейнера; • compression_limit — превышение предельной величины коэффициента сжатия; • report_size_limit — превышение предельного размера отчета; • scan_timeout — превышение предельного времени проверки; • engine_crash — сбой антивирусного ядра;	Строка

Поле	Описание	Тип данных
	• engine_hangup — зависание антивирусного ядра; • engine_error — ошибка антивирусного ядра; • no_license — отсутствует действующая лицензия; • multiscan_too_late — ошибка многопоточной проверки; • curing_limit_reached — превышение предельного числа попыток лечения; • non_supported_disk — неподдерживаемый тип диска; • unexpected_error — неожиданная ошибка.	
Переопределенные метаметоды: *Нет*		

Таблица Virus

Таблица описывает угрозу.

Поле	Описание	Тип данных
name	Имя угрозы (по классификации «Доктор Веб»)	Строка
type	Тип угрозы (по классификации «Доктор Веб»). Возможные значения: • known_virus — известная угроза (т. е. угроза, имеющая описание в вирусных базах); • virus_modification — модификация известной угрозы; • unknown_virus — неизвестная угроза, подозрительный объект; • adware — рекламная программа; • dialer — программа дозвона; • joke — программа-шутка; • riskware — потенциально опасное ПО; • hacktool — программа взлома.	Строка
Переопределенные метаметоды: *Нет*		

Таблица ThreatFilter

Таблица описывает фильтр для угроз.

Поле	Описание	Тип данных
`category`	Перечень категорий, которым должна соответствовать угроза (регистр не учитывается), список категорий см. в описании поля `type` таблицы Virus.	Строка или таблица строк
`category_not`	Перечень категорий, которым не должна соответствовать угроза (регистр не учитывается).	Строка или таблица строк
Переопределенные метаметоды: *Нет*		

Если поле фильтра не задано (т. е. указано значение `nil`), то любая угроза соответствует фильтру. Если указаны несколько полей фильтра, то условие объединяется по конъюнкции (логическое «И»). Если тип поля фильтра — это таблица (список), то фильтруемый объект должен соответствовать хотя бы одному из элементов таблицы (списка).

Примеры использования

1. Вывод в журнал перечня всех угроз, найденных в HTTP-сообщении:

```
local dw = require "drweb"

function message_hook(ctx)
  for virus in ctx.body.threats() do
   dw.notice("threat found: " .. virus.name)
  end
  return "pass"
end
```

2. Вывод в журнал перечня угроз, соответствующих фильтру по категории, и имен частей сообщения, в которых они были обнаружены:

```
local dw = require "drweb"

function message_hook(ctx)
  for v in ctx.body.threats({category = "known_virus"}) do
   dw.notice("found known virus: " .. v.name)
  end
  return "pass"
end
```

Доступные сервисные модули

Для взаимодействия с Dr.Web Gateway Security Suite в пространство Lua-программы могут быть импортированы следующие специальные модули, перечисленные в таблице.

Имя модуля	Назначение
drweb	Модуль, предоставляющий функции для записи сообщений из Lua-программы в журнал компонента Dr.Web Gateway Security Suite, запустившего программу на Lua, а также средства асинхронного запуска Lua-процедур
drweb.lookup	Модуль, предоставляющий инструменты для запроса данных из внешних источников путем обращения к модулю Dr.Web LookupD
drweb.regex	Модуль, предоставляющий интерфейс сопоставления строк с регулярными выражениями
drweb.config	Модуль, предоставляющий таблицу, содержащую значения параметров конфигурации Dr.Web ICAPD

Содержимое модуля drweb

1. Функции

Модуль предоставляет набор функций.

- Для записи сообщений из Lua-программы в журнал компонента Dr.Web Gateway Security Suite:
  - `log(`<*уровень*>, <*сообщение*>`)` записывает строку <*сообщение*> в журнал Dr.Web Gateway Security Suite на уровне <*уровень*> (требуемый уровень задается одним из следующих значений (строка): *debug*, *info*, *notice*, *warning*, *error*);
  - `debug(`<*сообщение*>`)` записывает строку <*сообщение*> в журнал Dr.Web Gateway Security Suite на уровне *debug*;
  - `info(`<*сообщение*>`)` записывает строку <*сообщение*> в журнал Dr.Web Gateway Security Suite на уровне *info*;
  - `notice(`<*сообщение*>`)` записывает строку <*сообщение*> в журнал Dr.Web Gateway Security Suite на уровне *notice*;
  - `warning(`<*сообщение*>`)` записывает строку <*сообщение*> в журнал Dr.Web Gateway Security Suite на уровне *warning*;
  - `error(`<*сообщение*>`)` записывает строку <*сообщение*> в журнал Dr.Web Gateway Security Suite на уровне *error*.
- Для управления синхронизацией Lua-процедур:
  - `sleep(`<*сек.*>`)` приостанавливает выполнение экземпляра Lua-процедуры на указанное число секунд;
  - `async(`<*Lua-функция*>`[,` <*список аргументов*>`])` асинхронно запускает указанную функцию с передачей ей заданного списка аргументов. Вызов функции `async` завершается немедленно, возвращаемое значение (таблица `Future`) позволяет получить результат выполнения функции <*Lua-функция*>.

- Для представления информации об IP-адресе в виде таблицы IpAddress:
  - `ip(<адрес>)` представляет IP-адрес (IPv4 или IPv6) в виде таблицы IpAddress.
- Для загрузки внешних данных из текстового файла:
  - `load_set(<путь к файлу>)` формирует из содержимого указанного текстового файла таблицу со значениями `true`; в качестве ключей используются строки, прочитанные из файла. Пустые строки и строки, состоящие только из пробельных символов, будут проигнорированы.
  - `load_array(<путь к файлу>)` формирует из содержимого указанного текстового файла массив строк. Пустые строки и строки, состоящие только из пробельных символов, будут проигнорированы.

2. Таблицы

- Таблица `Future` описывает отложенный результат выполнения функции при помощи функции `async`.

Поле	Описание	Тип данных
`wait`	Функция, возвращающая результат функции, запущенной при помощи функции `async`. Если функция еще не завершила свое выполнение, ожидает завершения и возвращает результат. Если функция завершилась до момента вызова `wait`, результат возвращается немедленно. Если запущенная функция завершилась с ошибкой, вызов `wait` генерирует ту же ошибку.	Функция
Переопределенные метаметоды: *Нет*		

- Таблица IpAddress описывает IP-адрес.

Поле	Описание	Тип данных
`belongs`	Функция для проверки IP-адреса из таблицы `IpAddress` на принадлежность к указанным подсетям (диапазонам IP-адресов). Принимает единственный аргумент — массив строк вида *<IP-адрес>* или *<IP-адрес>*/*<маска>*, где *<IP-адрес>* — адрес узла либо сети (например, `127.0.0.1`), а *<маска>* — маска подсети, которая указывается в виде IP-адреса (например, `255.0.0.0`), либо в виде целого числа (например, `8`). Возвращает логическое значение: • `true` — если адрес совпадает хотя бы с одним из указанных IP-адресов либо принадлежит хотя бы одной из указанных подсетей (диапазону IP-адресов); • `false` — если адрес не совпадает ни с одним из указанных IP-адресов или не принадлежит ни одной из указанных подсетей	Функция

Поле	Описание	Тип данных
Переопределенные метаметоды: • `__tostring` — функция, преобразующая `IpAddress` в строку, например, `127.0.0.1` (IPv4) или `::1` (IPv6); • `__concat` — функция, присоединяющая `IpAddress` к строке; • `__eq` — функция для проверки равенства двух `IpAddress`; • `__band` — функция, позволяющая накладывать маску, например: `dw.ip('192.168.1.2') & dw.ip('255.255.254.0')`		

3. Примеры

- Вывод в журнал сообщений, сформированных процедурой, запускающейся асинхронно:

```
local dw = require "drweb"

-- Функция, возвращающая полученную в качестве аргумента строку
-- по истечении двух секунд ожидания
function out_msg(message)
 dw.sleep(2)
 return message
end

-- "Главная" функция
function intercept(ctx)
 -- Вывод строки на уровне notice в журнал Dr.Web Gateway Security Suite
 dw.notice("Intercept function started.")

 -- Асинхронный запуск двух экземпляров функции out_msg
 local f1 = dw.async(out_msg, "Hello,")
 local f2 = dw.async(out_msg, " world!")

 -- Ожидание завершения исполнения экземпляров функции
 -- out_msg и вывод их результатов в журнал
 -- Dr.Web Gateway Security Suite на уровне debug
 dw.log("debug", f1.wait() .. f2.wait())
end
```

- Создание регулярной процедуры:

```
local dw = require "drweb"

-- Сохранить таблицу Future в глобальную переменную future, чтобы
-- предотвратить ее удаление сборщиком мусора
future = dw.async(function()
   while true do
     -- Каждый день выводить в журнал указанное сообщение
     dw.sleep(60 * 60 * 24)
     dw.notice("A brand new day began")
   end
end)
```

- Преобразование IP-адреса из строки:

```
local dw = require "drweb"

local ipv4 = dw.ip("127.0.0.1")
local ipv6 = dw.ip("::1")
local mapped = dw.ip("::ffff:127.0.0.1")
```

Содержимое модуля drweb.lookup

1. Функции

Модуль предоставляет функции:

- `lookup(`<*запрос*>`, `<*параметры*>`)` запрашивает данные во внешнем хранилище, доступном через модуль Dr.Web LookupD. Аргумент <*запрос*> должен соответствовать секции запроса в настройках Dr.Web LookupD (строка <*имя*>@<*тег*>). Необязательный аргумент <*параметры*> описывает подстановки, которые будут использованы при формировании запроса. Могут быть использованы следующие автоматически разрешаемые маркеры:
  - `$u`, `$U` (заменяется на `user`) — имя пользователя, переданное клиентским компонентом;
  - `$d`, `$D` (заменяется на `domain`) — имя домена, переданное клиентским компонентом.

  Аргументы задаются в виде таблицы, ключи и значения которой должны быть строками. Функция возвращает массив строк, являющихся результатами запроса.
- `check(`<*проверяемая строка*>`, `<*запрос*>`, `<*параметры*>`)` возвращает `true`, если <*проверяемая строка*> найдена во внешнем хранилище, доступном через модуль Dr.Web LookupD. Аргументы <*запрос*> и <*параметры*> полностью аналогичны аргументам функции `lookup` (см. выше). Аргумент <*проверяемая строка*> должен быть строкой или таблицей, имеющей метаметод `__tostring` (т. е. приводимой к строке).

2. Примеры

- Вывод в журнал списка пользователей, извлеченного из источника данных `LookupD.LDAP.users`:

```
local dw = require "drweb"
local dwl = require "drweb.lookup"

-- "Главная" функция
function intercept(ctx)
 -- Запись строки на уровне notice в журнал Dr.Web Gateway Security Suite
 dw.notice("Intercept function started.")

 -- Вывод в журнал Dr.Web Gateway Security Suite результатов запроса
 -- к источнику данных 'ldap@users'
 for _, s in ipairs(dwl.lookup("ldap@users", {user="username"})) do
   dw.notice("Result of request to 'ldap@users': " .. s)
 end

end
```

Содержимое модуля drweb.regex

1. Функции

Модуль предоставляет следующие функции:

- `search(`*<шаблон>*`, `*<текст>*`[, `*<флаги>*`])` — возвращает `true`, если строка *<текст>* содержит подстроку, соответствующую регулярному выражению *<шаблон>*. Необязательный параметр *<флаги>* (целое число) — набор флагов, влияющих на поведение функции, объединенных с помощью логического «ИЛИ» (OR).
- `match(`*<шаблон>*`, `*<текст>*`[, `*<флаги>*`])` — аналогична `search` за исключением того, что регулярному выражению *<шаблон>* должна соответствовать вся строка *<текст>* целиком, а не только ее подстрока.

2. Доступные флаги

- `ignore_case` — игнорировать регистр текста.

3. Примеры

```
local rx = require "drweb.regex"

rx.search("te.?t", "some TexT") -- false
rx.search("te.?t", "some TexT", rx.ignore_case) -- true

rx.match("some.+", "some TexT") -- true
```

Содержимое модуля drweb.config

1. Функции

Модуль не предоставляет функций.

2. Доступные таблицы

Модуль предоставляет таблицу, содержащую следующие поля:

Поле	Описание	Тип данных
`whitelist`	Значение параметра конфигурации `Whitelist`.	Массив строк
`blacklist`	Значение параметра конфигурации `Blacklist`.	Массив строк
`adlist`	Значение параметра конфигурации `Adlist`.	Массив строк
`block_url_categories`	Перечень блокируемых категорий URL (на основе значений параметров `Block*`, установленных в `Yes`).	Массив строк
`block_threats`	Перечень блокируемых категорий угроз (на основе значений параметров `Block*`, установленных в `Yes`).	Массив строк
`block_unchecked`	Значение параметра конфигурации `BlockUnchecked`.	Логический
Переопределенные метаметоды: *Нет*		

3. Пример

```
local cfg = require "drweb.config"

function message_hook(ctx)

  -- Блокировать сообщения, содержащие угрозы
  -- из перечня угроз, подлежащих блокированию
  if ctx.body.has_threat{category = cfg.block_threats} then
    return "block"
  end

  -- Разрешить доступ ко всем прочим ресурсам
  return "pass"

end
```

9.5. SpIDer Gate

Данный компонент поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux.

Компонент проверки сетевого трафика и URL SpIDer Gate предназначен для проверки данных, загружаемых на локальный узел из сети или передаваемых в сеть с локального узла, на наличие угроз и предотвращения соединения с узлами сети, внесенными в нежелательные категории веб-ресурсов и в черные списки, формируемые системным администратором самостоятельно.

Вы можете указать в настройках компонента, протоколы каких типов следует проверять.

Для проверки принадлежности URL той или иной категории (в рамках проверки соединений, использующих протокол HTTP/HTTPS) компонент использует как базу категорий веб-ресурсов, регулярно обновляемую с серверов обновлений компании «Доктор Веб», так и опрашивает облачный сервис Dr.Web Cloud. Компания «Доктор Веб» поддерживает следующие категории веб-ресурсов:

- *InfectionSource* — сайты, содержащие вредоносное ПО («источники распространения угроз»).
- *NotRecommended* — сайты, используемые для мошенничества («социальной инженерии») и не рекомендованные к посещению.
- *AdultContent* — сайты, содержащие материалы порнографического или эротического содержания, сайты знакомств и т. д.
- *Violence* — сайты, содержащие призывы к насилию, материалы о различных происшествиях с человеческими жертвами и т. д.
- *Weapons* — сайты, посвященные оружию и взрывчатым веществам, а также материалы с описанием их изготовления и т. д.
- *Gambling* — сайты, на которых размещены онлайн-игры на деньги, интернет-казино, аукционы, а также принимающие ставки и т. д.
- *Drugs* — сайты, пропагандирующие употребление, изготовление или распространение наркотиков и т. д.
- *ObsceneLanguage* — сайты, на которых содержится нецензурная лексика (в названиях разделов, статьях и пр.).
- *Chats* — сайты для обмена сообщениями в режиме реального времени.
- *Terrorism* — сайты, содержащие материалы агрессивно-агитационного характера, описания терактов и т. д.
- *FreeEmail* — сайты, предоставляющие возможность бесплатной регистрации электронного почтового ящика.
- *SocialNetworks* — социальные сети общего характера, деловые, корпоративные и тематические социальные сети, а также тематические сайты знакомств.

- *DueToCopyrightNotice* — сайты, ссылки на которые указаны правообладателями произведений, защищенных авторскими правами (кинофильмы, музыкальные произведения и т. д.).
- *OnlineGames* — сайты, на которых размещены игры, использующие постоянное соединение с интернетом.
- *Anonymizers* — сайты, позволяющие пользователю скрывать свою личную информацию и предоставляющие доступ к заблокированным сайтам.
- *CryptocurrencyMiningPool* — сайты, предоставляющие доступ к сервисам, объединяющим пользователей с целью добычи (майнинга) криптовалют.
- *Jobs* — сайты, предназначенные для поиска вакансий.

Системный администратор может определять, доступ к узлам каких категорий является нежелательным. Дополнительно пользователь может формировать собственные черные списки узлов, доступ к которым будет блокироваться, а также белые списки узлов, доступ к которым будет разрешаться, даже если они относятся к нежелательным категориям. Для URL, информация о которых отсутствует в локальных черных списках и базе категорий веб-ресурсов, компонент может отправлять запросы в облачный сервис Dr.Web Cloud с целью проверки, не имеется ли информации об их вредоносности, полученной от других продуктов Dr.Web в режиме реального времени.

Один и тот же сайт может принадлежать нескольким категориям одновременно. Доступ к такому сайту будет заблокирован, если он принадлежит хотя бы одной из категорий, доступ к которой нежелателен.

Даже если сайт включен в белый список, то отправляемые и загружаемые с него данные все равно проверяются на наличие угроз.

В случае большой интенсивности проверки файлов, передаваемых по протоколу HTTP, возможно возникновение проблем с проверкой из-за исчерпания компонентом Dr.Web Network Checker числа доступных файловых дескрипторов. В этом случае необходимо увеличить лимит на число файловых дескрипторов, доступных Dr.Web Gateway Security Suite.

В рамках Dr.Web Gateway Security Suite компонент SpIDer Gate в первую очередь может быть использован для организации «барьера» между сервером компании, например, веб-сервером с публичным доступом, и интернетом, поскольку функции управления доступом пользователей локальной сети к интернету по умолчанию делегированы компоненту Dr.Web ICAPD, работающему в связке с прокси-сервером, который обеспечивает доступ к интернету из локальной сети.

9.5.1. Принципы работы

Компонент SpIDer Gate выполняет контроль сетевых соединений, устанавливаемых пользовательскими приложениями. Компонент проверяет, находится ли узел, с которым клиентское приложение собирается установить соединение, в любой из категорий веб-ресурсов, отмеченной в настройках как нежелательная для посещения. Кроме этого компонент может отправлять запросы на проверку URL в облачный сервис Dr.Web Cloud. Если URL обнаружен в какой-либо из нежелательных категорий (в том числе сервисом Dr.Web Cloud) или в черном списке, сформированным системным администратором, то соединение разрывается, а пользователю (если соединение устанавливалось по протоколу HTTP/HTTPS) возвращается HTML-страница с сообщением о запрете соединения, сформированная SpIDer Gate на основании шаблона, поставляемого совместно с компонентом. Данная страница содержит сообщение о невозможности доступа к запрошенному ресурсу и описание причины отказа. Аналогичная страница формируется и возвращается клиенту в случае, если в передаваемых данных SpIDer Gate обнаружит угрозу, подлежащую блокировке. Если соединение использует протокол, отличный от HTTP(S), то компонент выполняет только проверку того, разрешено ли установление соединения с данным узлом.

Перенаправление соединений, устанавливаемых клиентскими приложениями с удаленными серверами, осуществляется прозрачно для клиентских приложений сервисным компонентом Dr.Web Firewall для Linux, выполняющим динамическое управление правилами NetFilter, системного компонента Linux.

В рамках Dr.Web Gateway Security Suite под клиентскими приложениями в первую очередь понимается некоторый защищаемый серверный ресурс компании (например, веб-сервер с публичным доступом), поскольку функции управления доступом пользователей локальной сети к интернету по умолчанию делегированы компоненту Dr.Web ICAPD, работающему в связке с прокси-сервером, который обеспечивает доступ к интернету из локальной сети.

Для регулярного автоматического обновления базы категорий веб-ресурсов с серверов компании «Доктор Веб» используется тот же компонент Dr.Web Updater, который обновляет вирусные базы для сканирующего ядра Dr.Web Scanning Engine. Для обращения к облачному сервису Dr.Web Cloud используется компонент Dr.Web CloudD (использование облачного сервиса задается в основных настройках Dr.Web Gateway Security Suite и при необходимости может быть отключено). Для проверки передаваемых данных SpIDer Gate использует агента сетевой проверки данных Dr.Web Network Checker, который, в свою очередь, инициирует их проверку сканирующим ядром Dr.Web Scanning Engine.

9.5.2. Аргументы командной строки

Для запуска компонента SpIDer Gate из командной строки используется следующая команда:

```
$ /opt/drweb.com/bin/drweb-gated [<параметры>]
```

SpIDer Gate допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-gated --help
```

Данная команда выведет на экран краткую справку компонента SpIDer Gate.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Gateway Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-gated`.

9.5.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[GateD]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-gated` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-gated`
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`
`TemplatesDir` *{путь к каталогу}*	Путь к каталогу, в котором хранятся файлы шаблонов HTML-страниц уведомлений о блокировке веб-ресурсов. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/templates/gated` • для FreeBSD: `/var/drweb.com/templates/gated`
`CaPath` *{путь}*	Путь к каталогу или файлу с перечнем доверенных корневых сертификатов. Значение по умолчанию: *Путь к системному перечню доверенных сертификатов*. Зависит от дистрибутива GNU/Linux.

Параметр	Описание
	• Для Astra Linux, Debian, Linux Mint, SUSE Linux и Ubuntu это обычно путь `/etc/ssl/certs/`. • Для CentOS и Fedora — `/etc/pki/tls/certs/ca-bundle.crt`. • Для других дистрибутивов путь может быть определен через результат вызова команды `openssl version -d`. • Если команда недоступна или дистрибутив ОС опознать не удалось, используется значение `/etc/ssl/certs/`.

Изменения, внесенные в настройки проверки соединений, не влияют на проверку соединений, которые уже были установлены приложениями до внесения изменений.

Другие параметры настройки проверки трафика, включая правила проверки, задаются в настройках сервисного компонента Dr.Web Firewall для Linux.

9.6. Dr.Web Firewall для Linux

Данный компонент поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux.

Для корректной работы компонента ядро ОС должно быть собрано со включением следующих опций:

- *CONFIG_NETLINK_DIAG*, *CONFIG_INET_TCP_DIAG*;
- *CONFIG_NF_CONNTRACK_IPV4*, *CONFIG_NF_CONNTRACK_IPV6*, *CONFIG_NF_CONNTRACK_EVENTS*;
- *CONFIG_NETFILTER_NETLINK_QUEUE*, *CONFIG_NETFILTER_NETLINK_QUEUE_CT*, *CONFIG_NETFILTER_XT_MARK*.

Конкретный набор требуемых опций из указанного перечня может зависеть от используемого дистрибутива ОС GNU/Linux.

Компонент Dr.Web Firewall для Linux является вспомогательным и играет роль менеджера соединений для SplDer Gate. Dr.Web Firewall для Linux обеспечивает прохождение устанавливаемых соединений через SplDer Gate для проверки передаваемого трафика.

9.6.1. Принципы работы

В этом разделе

- Общие сведения
- Механизм перехвата соединений
  - Действия в правилах iptables
  - Метки пакетов и соединений
  - Маршруты и политики маршрутизации (ip rule, ip route)
  - Правила NetFilter (iptables)
- Порядок перехвата соединений

Общие сведения

Компонент Dr.Web Firewall для Linux обеспечивает корректную работу компонента SplDer Gate, анализируя правила маршрутизации, заданные для NetFilter (системного компонента Linux), и модифицируя их таким образом, чтобы устанавливаемые соединения перенаправлялись на SplDer Gate, который выступает в качестве промежуточного звена (прокси) между клиентским приложением и удаленным сервером.

Dr.Web Firewall для Linux может отдельно управлять правилами перенаправления исходящих и входящих, а также транзитных соединений. Для тонкой настройки правил пропуска или перенаправления соединений компонент может использовать как правила, внедренные в настройки, так и скрипт проверки, написанный на языке Lua.

Механизм перехвата соединений

Для перехвата соединений Dr.Web Firewall для Linux использует таблицы маршрутизации, указанные в базе данных политик маршрутизации (см. `man ip`: `ip route`, `ip rule`), а также интерфейс *nf_conntrack* системного компонента NetFilter. Перехваченные соединения и передающиеся по ним пакеты с целью правильной маршрутизации помечаются битовыми метками, которые позволяют Dr.Web Firewall для Linux принимать правильные решения о перенаправлении соединений и обработке передающихся пакетов на различных этапах прохождения ими цепочек в NetFilter (подробнее см. `man iptables`).

Действия в правилах iptables

Dr.Web Firewall для Linux использует следующие действия в правилах `iptables`:

- *MARK* — присвоить пакету указанную числовую метку.
- *CONNMARK* — присвоить соединению указанную числовую метку.
- *TPROXY* — установить изначальный адрес назначения соединения и перенаправить пакет из цепочки *PREROUTING* NetFilter на указанный сетевой сокет (<*IP-адрес*>:<*порт*>), не меняя содержимое пакета.
- *NFQUEUE* — передать пакет из сетевого стека ядра на проверку процессу, работающему вне пространства ядра. Dr.Web Firewall для Linux подключается к очереди *NFQUEUE* с заданным номером через специальный *Netlink*-сокет и получает пакеты, по которым необходимо вынести вердикты по дальнейшей обработке (Dr.Web Firewall для Linux обязан сообщить NetFilter один из следующих вердиктов: *DROP*, *ACCEPT*, *REPEAT*).

Метки пакетов и соединений

Для пометки пакетов Dr.Web Firewall для Linux использует следующие три бита (из доступных 32 бит) в метках пакетов и в метке соединения:

- Бит `LDM` (*Local Delivery Mark*) — признак локального соединения. Пакеты, в метке которых установлен этот бит, с помощью установленных правил маршрутизации направляются на локальный хост.
- Бит `CPM` (*Client Packets Mark*) — признак соединения между клиентом (инициатором соединения) и прокси, т. е. Dr.Web Firewall для Linux.
- Бит `SPM` (*Server Packets Mark*) — признак соединения между прокси, т. е. Dr.Web Firewall для Linux, и сервером (приемником соединения).

Биты `LDM`, `CPM` и `SPM` могут быть любыми *разными* битами, которые не используются для пометки пакетов другими приложениями, выполняющими маршрутизацию соединений. При настройках по умолчанию Dr.Web Firewall для Linux выбирает подходящие (не используемые другими приложениями) биты автоматически.

Маршруты и политики маршрутизации (ip rule, ip route)

Для корректной работы Dr.Web Firewall для Linux (в любом режиме проверки соединений) в системе должна быть настроена политика маршрутизации `ip rule`, использующая таблицу маршрутов с номером 100:

```
from all fwmark <LDM>/<LDM> lookup 100
```

В эту таблицу должен быть добавлен маршрут следующего вида:

```
local default dev lo scope host
```

Данная политика маршрутизации гарантирует, что пакеты, в метке которых установлен бит `LDM`, всегда направляются на локальный узел.

Здесь и далее выражение <*XXX*> для бита `XXX` представляет собой шестнадцатеричное (*hexadecimal*) число, равное 2^N, где *N* — порядковый номер бита `XXX` в метке пакета. Например, если в качестве бита `LDM` выбран самый младший (нулевой) бит метки пакета, то <*LDM*> = 2^0 = *0x1*.

Правила NetFilter (iptables)

Для корректной работы Dr.Web Firewall для Linux (в любом режиме проверки соединений) в таблицах `nat` и `mangle` соответствующих цепочек компонента NetFilter должны присутствовать следующие шесть правил (представлены в формате вывода команды `iptables-save`):

```
*nat
-A POSTROUTING -o lo -m comment --comment drweb-firewall -m mark --mark
<LDM>/<LDM> -j ACCEPT
*mangle
-A PREROUTING -m comment --comment drweb-firewall -m mark --mark
0x0/<CPM+SPM> -m connmark --mark <SPM>/<CPM+SPM> -j MARK --set-xmark
<LDM>/<LDM>
-A PREROUTING -p tcp -m comment --comment drweb-firewall -m mark ! --mark
<CPM+SPM>/<CPM+SPM> -m connmark --mark <CPM>/<CPM+SPM> -j TPROXY --on-port
<порт> --on-ip <IP-адрес> --tproxy-mark <LDM>/<LDM>
-A OUTPUT -m comment --comment drweb-firewall -m mark --mark
<CPM>/<CPM+SPM> -j CONNMARK --set-xmark <CPM>/0xffffffff
-A OUTPUT -m comment --comment drweb-firewall -m mark --mark <SPM>/<CPM+SPM>
-j CONNMARK --set-xmark <SPM>/0xffffffff
-A OUTPUT -m comment --comment drweb-firewall -m mark --mark 0x0/<CPM+SPM> -
m connmark ! --mark 0x0/<CPM+SPM> -j MARK --set-xmark <LDM>/<LDM>
```

В описании ниже этим правилам присвоены порядковые номера 0–5 (в том порядке, в котором они здесь перечислены). Выражение <*X*+*Y*> обозначает число, равное побитовому «ИЛИ» (сумме) соответствующих чисел *X* и *Y*.

Параметры <*IP-адрес*> и <*порт*> в правиле № 2 указывают на сетевой сокет, на котором Dr.Web Firewall для Linux контролирует перехваченные соединения.

Кроме того, при включении в настройках Dr.Web Firewall для Linux режима перехвата соединений (исходящих, входящих и транзитных), в таблицах `mangle` соответствующих цепочек (*OUTPUT*, *INPUT*, *FORWARD*) должны присутствовать следующие дополнительные правила (по одному для каждого из режимов):

- Для перехвата исходящих соединений (*OUTPUT*):

```
-A OUTPUT -p tcp -m comment --comment drweb-firewall -m tcp --tcp-flags
SYN,ACK SYN -m mark --mark 0x0/<CPM+SPM> -j NFQUEUE --queue-num <ONum> --
queue-bypass
```

- Для перехвата входящих соединений (*INPUT*):

```
-A INPUT -p tcp -m comment --comment drweb-firewall -m tcp --tcp-flags
SYN,ACK SYN -m mark --mark 0x0/<CPM+SPM> -j NFQUEUE --queue-num <INum> --
queue-bypass
```

- Для перехвата транзитных соединений (*FORWARD*):

```
-A FORWARD -p tcp -m comment --comment drweb-firewall -m tcp --tcp-flags
SYN,ACK SYN -m mark --mark 0x0/<CPM+SPM> -j NFQUEUE --queue-num <FNum> --
queue-bypass
```

В описании ниже этим правилам присвоены порядковые номера 6, 7 и 8 (в том порядке, в котором они здесь перечислены).

Здесь <*ONum*>, <*INum*> и <*FNum*> — номера очередей в *NFQUEUE*, в которых Dr.Web Firewall для Linux ожидает появления пакетов, сигнализирующих об установке соединений соответствующих направлений (это пакеты с установленным флагом `SYN`, но со снятым флагом `ACK`).

Порядок перехвата соединений

Согласно любому из правил № 6, 7 и 8, пакеты, сигнализирующие о начале нового сетевого соединения соответствующего направления, если они не помечены одновременно битами `CPM` и `SPM`, помещаются NetFilter в соответствующие очереди *NFQUEUE*, откуда они будут прочитаны Dr.Web Firewall для Linux через интерфейс *nf_conntrack*. Правила № 3 и 4 отмечают само соединение как перехватываемое, т. е. в метке соединения устанавливается бит, указывающий направление соединения. Номер этого бита в метке соединения совпадает с номером бита в метке пакета. В результате этого пакеты, посылаемые по этому соединению, благодаря правилам № 1, 2 и 5, будут получены Dr.Web Firewall для Linux. Правило № 0 добавляется в начало цепочки *POSTROUTING* таблицы `nat`, чтобы в случае настроенного NAT не транслировать адреса для маркированных пакетов, так как это нарушит логику перехвата и обработки соединений Dr.Web Firewall для Linux.

При появлении пакета в одной из очередей *NFQUEUE* Dr.Web Firewall для Linux выполняет базовую проверку правильности пакета на тот случай, если в NetFilter установлены неверные правила. Далее Dr.Web Firewall для Linux пытается соединиться с сервером от своего имени с сокета, имеющего метку `PSC`. При этом сработает правило № 4. Правило локальной доставки № 5 не сработает, поскольку на пакете стоит метка `SPM`, а это правило действует только для пакетов с меткой <*CPM*+*SPM*>.

- *Если соединиться с сервером не удалось*, Dr.Web Firewall для Linux формирует для клиента пакет с установленным битом `RST`, заменяя в пакете пару <*IP-адрес*>:<*порт*> на адрес сетевого сокета запрашиваемого сервера. В *NFQUEUE* при этом отправляется вердикт *DROP*. На сокете, с которого будет оправлен пакет с битом `RST`, установлена метка <*CPM*+*SPM*>, так что ни одно из указанных выше правил не сработает, и этот пакет будет доставлен клиенту по обычным правилам маршрутизации.
- *Если соединение с удаленным сервером удалось установить*, Dr.Web Firewall для Linux копирует перехваченный SYN-пакет и повторно отправляет его с сокета, имеющего метку <*LDM*+*CPM*>, чтобы отправленный пакет был перенаправлен на локальный сетевой сокет. Благодаря установленному биту `LDM`, в процессе выбора выходного

интерфейса, согласно заданным правилам маршрутизации, отправленный пакет попадет на интерфейс *loopback*, откуда попадет в цепочку NetFilter *PREROUTING*, где для него сработает правило № 2. Таким образом, отправленный пакет в неизменном виде будет перенаправлен на сетевой сокет Dr.Web Firewall для Linux. Данный прием позволяет Dr.Web Firewall для Linux сохранить полную адресную четверку для соединения (IP-адрес и порт отправителя пакета, IP-адрес и порт получателя пакета).

Для сетевого сокета, на котором Dr.Web Firewall для Linux принимает перехватываемые соединения согласно правилу № 2, установлена опция `IP_TRANSPARENT` и метка *<LDM+CPM>*, благодаря чему пакеты, отправляемые Dr.Web Firewall для Linux с этого сокета, не попадут в очереди *NFQUEUE*. При подключении клиента производится поиск парного сокета по сохраненной адресной четверке (IP-адрес и порт отправителя, IP-адрес и порт получателя). После того, как соединение с клиентом и с сервером установлено, к соединению применяется процедура проверки, заданная в виде процедуры на языке Lua, а также правила проверки, заданные в настройках Dr.Web Firewall для Linux. Если проверки пройдены успешно и соединение не подлежит разрыву, то сопоставленная пара сокетов, соединяющая клиентскую и серверную сторону установленного соединения, передается компоненту SpIDer Gate для анализа передаваемых по соединению данных. Дальнейшее взаимодействие клиента и сервера производится через посредника, роль которого играет SpIDer Gate. Кроме пары сокетов, ассоциированных с клиентской и серверной стороной соединения, SpIDer Gate получает от Dr.Web Firewall для Linux параметры и правила проверки установленного соединения.

Упрощенно схема работы Dr.Web Firewall для Linux показана на рисунке ниже.

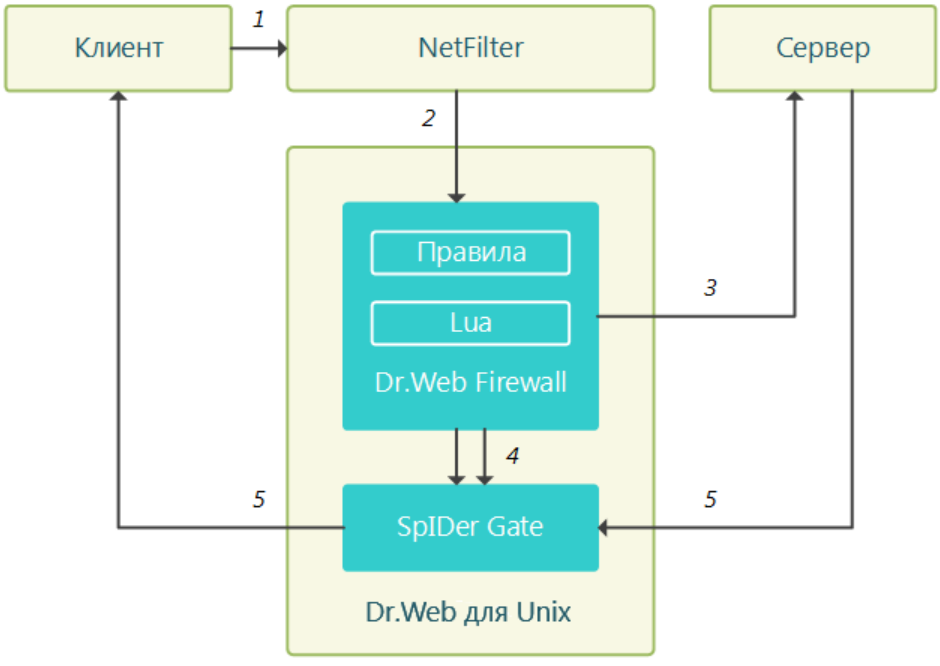

Рисунок 12. Схема работы Dr.Web Firewall для Linux

Цифрами обозначены следующие этапы обработки соединения:

1. Попытка клиента установить соединение с сервером.

2. Перенаправление NetFilter устанавливаемого соединения в Dr.Web Firewall для Linux согласно правилам маршрутизации.
3. Попытка Dr.Web Firewall для Linux установить соединение с сервером от имени клиента и проверка соединения.
4. Передача пары сокетов, ассоциированных с клиентской и серверной сторонами соединения, SpIDer Gate для обслуживания соединения, а также параметров и правил его проверки.
5. Обмен данными между сервером и клиентом через SpIDer Gate в роли посредника.

Для правильной работы компонента Dr.Web Firewall для Linux необходимо наличие указанных правил в таблицах маршрутизации с правильными номерами битов пометки, очередей *NFQUEUE* и адресом сетевого сокета для перехвата соединений. При настройках по умолчанию компонент выполняет надлежащую настройку правил автоматически. Если автоматическая настройка соединений компонентом отключена в его настройках, необходимо обеспечить наличие необходимых правил вручную при начале работы компонента.

9.6.2. Аргументы командной строки

Для запуска компонента Dr.Web Firewall для Linux из командной строки используется следующая команда:

```
$ /opt/drweb.com/bin/drweb-firewall [<параметры>]
```

Dr.Web Firewall для Linux допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-firewall --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web Firewall для Linux.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Gateway Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-firewall`.

9.6.3. Параметры конфигурации

В этом разделе

- Параметры компонента
- Правила проверки трафика и блокировки доступа
  - Просмотр и редактирование правил
  - Просмотр правил с помощью команды drweb-ctl cfshow
  - Редактирование правил с помощью команды drweb-ctl cfset
  - Набор правил по умолчанию
  - Примеры правил проверки трафика и блокировки доступа

Компонент использует параметры конфигурации, заданные в секции `[LinuxFirewall]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

Параметры компонента

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log`	Метод ведения журнала компонента.

Параметр	Описание
{тип журнала}	Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-firewall` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-firewall`
`AutoconfigureIptables` *{Yes | No}*	Включить или отключить режим настройки правил для системного компонента NetFilter через интерфейс `iptables`. Допустимые значения: • `Yes` — автоматически настраивать правила для NetFilter при запуске компонента и удалять их при завершении работы компонента (*рекомендуется*). • `No` — не настраивать правила автоматически. Правила должны быть добавлены администратором вручную перед запуском компонента и удалены, когда он завершит работу. ⚠ Если автоматическая настройка правил для `iptables` не разрешена, необходимо обеспечить наличие необходимых правил `iptables` к моменту начала работы компонента. Значение по умолчанию: `Yes`
`AutoconfigureRouting` *{Yes | No}*	Режим настройки правил и политик маршрутизации `ip route` и `ip rule`. Допустимые значения: • `Yes` — автоматически настраивать правила и политики маршрутизации `ip route` и `ip rule` при запуске компонента и удалять их при завершении работы компонента (*рекомендуется*). • `No` — не настраивать правила автоматически. Правила должны быть добавлены администратором вручную перед запуском компонента и удалены, когда он завершит работу.

Параметр	Описание
	Если автоматическая настройка правил и политик маршрутизации не разрешена, необходимо обеспечить наличие необходимых правил `ip route` и `ip rule` к моменту начала работы компонента. Значение по умолчанию: `Yes`
`LocalDeliveryMark` *{целое число | Auto}*	Метка <*LDM*> для пакетов, перенаправляемых на сетевой сокет Dr.Web Firewall для Linux (определяется параметром `TproxyListenAddress`, см. ниже) для перехвата соединения. Допустимые значения: • <*целое число*> — метка <*LDM*>, присваиваемая пакетам. Численно равна 2^N, где N — номер бита `LDM` в пакете, $0 \leq N \leq 31$. • `Auto` — разрешить Dr.Web Firewall для Linux выбрать подходящий бит в метке пакета автоматически (*рекомендуется*). При назначении числа <*LDM*> вручную убедитесь, что соответствующий бит в метке пакетов не используется никакими другими приложениями, управляющими маршрутизацией соединений и пакетов (в том числе, через NetFilter). Если указано недопустимое значение, запуск компонента завершится ошибкой. Указанное число <*LDM*> должно использоваться в правилах маршрутизации, которые необходимо добавлять вручную, если `AutoconfigureIptables = No` и/или `AutoconfigureRouting = No`. Значение по умолчанию: `Auto`
`ClientPacketsMark` *{целое число | Auto}*	Метка <*CPM*>, которой помечаются пакеты, следующие между клиентом (инициатором соединения) и Dr.Web Firewall для Linux.

Параметр	Описание
	Допустимые значения: • *<целое число>* — метка *<CPM>*, присваиваемая пакетам. Численно равна 2^N, где N — номер бита `CPM` в пакете, $0 \leq N \leq 31$. • `Auto` — разрешить Dr.Web Firewall для Linux выбрать подходящий бит в метке пакета автоматически (*рекомендуется*). При назначении числа *<CPM>* вручную необходимо убедиться, что соответствующий бит в метке пакетов не используется никакими другими приложениями, управляющими маршрутизацией соединений и пакетов (в том числе, через NetFilter). Если указано недопустимое значение, то запуск компонента завершится ошибкой. Указанное число *<CPM>* должно использоваться в правилах маршрутизации, которые необходимо добавлять вручную, если `AutoconfigureIptables = No`. Значение по умолчанию: `Auto`
`ServerPacketsMark` *{целое число | Auto}*	Метка *<SPM>*, которой помечаются пакеты, следующие между Dr.Web Firewall для Linux и сервером (приемником соединения). Допустимые значения: • *<целое число>* — метка *<SPM>*, присваиваемая пакетам. Численно равна 2^N, где N — номер бита `SPM` в пакете, $0 \leq N \leq 31$. • `Auto` —разрешить Dr.Web Firewall для Linux выбрать подходящий бит в метке пакета автоматически (*рекомендуется*).

Параметр	Описание
	 При назначении числа <*SPM*> вручную необходимо убедиться, что соответствующий бит в метке пакетов не используется никакими другими приложениями, управляющими маршрутизацией соединений и пакетов (в том числе, через NetFilter). Если указано недопустимое значение, то запуск компонента завершится ошибкой. Указанное число <*SPM*> должно использоваться в правилах маршрутизации, которые необходимо добавлять вручную, если `AutoconfigureIptables = No` и/или `AutoconfigureRouting = No`. Значение по умолчанию: `Auto`
`TproxyListenAddress` *{сетевой сокет}*	Сетевой сокет (<*IP-адрес*>:<*порт*>), на котором Dr.Web Firewall для Linux принимает перехваченные соединения. Если задан нулевой порт, то сокет выбирается системой автоматически. Необходимо убедиться, что соответствующий сокет не используется никакими другими приложениями. Если указано недопустимое значение, то запуск компонента завершится ошибкой. Указанные IP-адрес и порт должны использоваться в правилах маршрутизации, которые необходимо добавлять вручную, если `AutoconfigureIptables = No`. Значение по умолчанию: `127.0.0.1:0`
`OutputDivertEnable` *{Yes | No}*	Включить или отключить режим перехвата исходящих соединений (т. е. соединений, инициированных приложениями на локальном узле).

Параметр	Описание
	Допустимые значения: • `Yes` — перехватывать и обрабатывать исходящие соединения; • `No` — не перехватывать и не обрабатывать исходящие соединения. Данная настройка добавляет или удаляет правило маршрутизации № 5, которое необходимо добавлять или удалять вручную, если `AutoconfigureIptables = No`. Значение по умолчанию: `No`
`OutputDivertNfqueueNumber` *{целое число | Auto}*	Номер очереди *NFQUEUE*, из которой Dr.Web Firewall для Linux будет извлекать SYN-пакеты, инициирующие исходящие соединения. Допустимые значения: • *<целое число>* — номер очереди *<ONum>* для отслеживания SYN-пакетов перехватываемых исходящих соединений в *NFQUEUE*; • `Auto` —разрешить Dr.Web Firewall для Linux выбрать подходящий номер очереди автоматически (*рекомендуется*). При назначении числа *<ONum>* вручную необходимо убедиться, что соответствующая очередь не используется никакими другими приложениями, контролирующими соединения и пакеты (в том числе через правила NetFilter). Если указано недопустимое значение, то запуск компонента завершится ошибкой. Указанное число *<ONum>* должно использоваться в правиле маршрутизации № 5, которое необходимо добавлять вручную, если `AutoconfigureIptables = No`. Значение по умолчанию: `Auto`

Параметр	Описание
`OutputDivertConnectTransparently` *{Yes | No}*	Включить или отключить режим эмуляции подключения к получателю (серверу) с IP-адреса отправителя перехваченного пакета (клиента) для исходящих соединений. Допустимые значения: • `Yes` — при перехвате соединения подключаться к серверу не со своего адреса, а с адреса клиента, который запросил соединение; • `No` — подключаться к серверу с адреса Dr.Web Firewall для Linux. Поскольку в режиме перехвата исходящих соединений адреса клиента и Dr.Web Firewall для Linux чаще всего совпадают, значение по умолчанию — `No`. Значение по умолчанию: `No`
`OutputDivertMark` *{целое число | Auto | None}*	Метка, которой помечаются пакеты в режиме перехвата исходящих соединений при использовании подсистемы мандатного доступа PARSEC. Допустимые значения: • *<целое число>* — метка, присваиваемая пакетам. Численно равна 2^N, где N — номер бита метки в пакете, $0 \leq N \leq 31$. • `Auto` — разрешить Dr.Web Firewall для Linux выбрать подходящий бит в метке пакета автоматически. • `None` — не устанавливать метку. Значение по умолчанию: `None`
`InputDivertEnable` *{Yes | No}*	Включить или отключить режим перехвата входящих соединений (т. е. соединений, инициированных приложениями на удаленном узле, с приложениями, работающими на локальном узле). Допустимые значения: • `Yes` — перехватывать и обрабатывать входящие соединения; • `No` — не перехватывать и не обрабатывать входящие соединения.

Параметр	Описание
	Данная настройка добавляет или удаляет правило маршрутизации № 6, которое необходимо добавлять или удалять вручную, если `AutoconfigureIptables = No`. Если указано недопустимое значение, то запуск компонента завершится ошибкой. Значение по умолчанию: `No`
`InputDivertNfqueueNumber` *{целое число | Auto}*	Номер очереди *NFQUEUE*, из которой Dr.Web Firewall для Linux будет извлекать SYN-пакеты, инициирующие входящие соединения. Допустимые значения: • *<целое число>* — номер очереди *<INum>* для отслеживания SYN-пакетов перехватываемых входящих соединений в *NFQUEUE*; • `Auto` — разрешить Dr.Web Firewall для Linux выбрать подходящий номер очереди автоматически (*рекомендуется*). При назначении числа *<INum>* вручную необходимо убедиться, что соответствующая очередь не используется никакими другими приложениями, управляющими контролем соединений и пакетов (в том числе через правила NetFilter). Если указано недопустимое значение, то запуск компонента завершится ошибкой. Указанное число *<INum>* должно использоваться в правиле маршрутизации № 6, которое необходимо добавлять вручную, если `AutoconfigureIptables = No`. Значение по умолчанию: `Auto`
`InputDivertConnectTransparently` *{Yes | No}*	Включить или отключить режим эмуляции подключения к получателю (серверу) с IP-адреса отправителя перехваченного пакета (клиента) для входящих соединений.

Параметр	Описание
	Допустимые значения: • `Yes` — при перехвате соединения подключаться к серверу не со своего адреса, а с адреса клиента, который запросил соединение; • `No` — подключаться к серверу с адреса Dr.Web Firewall для Linux. В режиме перехвата входящих соединений весь трафик проходит через Dr.Web Firewall для Linux и можно безопасно подключиться к серверу с фиктивного адреса клиента, поэтому значение по умолчанию — `Yes`. Значение по умолчанию: `Yes`
`InputDivertMark` *{целое число | Auto | None}*	Метка, которой помечаются пакеты в режиме перехвата входящих соединений при использовании подсистемы мандатного доступа PARSEC. Допустимые значения: • *<целое число>* — метка, присваиваемая пакетам. Численно равна 2^N, где N — номер бита метки в пакете, $0 \leq N \leq 31$. • `Auto` — разрешить Dr.Web Firewall для Linux выбрать подходящий бит в метке пакета автоматически. • `None` — не устанавливать метку. Значение по умолчанию: `None`
`ForwardDivertEnable` *{Yes | No}*	Включить или отключить режим перехвата транзитных соединений (т. е. соединений, инициированных приложениями на одном удаленном узле, с приложениями, работающими на другом удаленном узле). Допустимые значения: • `Yes` — перехватывать и обрабатывать транзитные соединения; • `No` — не перехватывать и не обрабатывать транзитные соединения. ⚠ Данная настройка добавляет или удаляет правило маршрутизации № 7, которое необходимо добавлять или удалять вручную, если `AutoconfigureIptables = No`.

Параметр	Описание
	Значение по умолчанию: `No`
`ForwardDivertNfqueueNumber` *{целое число | Auto}*	Номер очереди *NFQUEUE*, из которой Dr.Web Firewall для Linux будет извлекать SYN-пакеты, инициирующие транзитные соединения. Допустимые значения: • *<целое число>* — номер очереди *<FNum>* для отслеживания SYN-пакетов перехватываемых транзитных соединений в *NFQUEUE*; • `Auto` — разрешить Dr.Web Firewall для Linux выбрать подходящий номер очереди автоматически (*рекомендуется*). ⚠ При назначении числа *<FNum>* вручную необходимо убедиться, что соответствующая очередь не используется никакими другими приложениями, управляющими контролем соединений и пакетов (в том числе через правила NetFilter). Если указано недопустимое значение, то запуск компонента завершится ошибкой. Указанное число *<FNum>* должно использоваться в правиле маршрутизации № 7, которое необходимо добавлять вручную, если `AutoconfigureIptables = No`. Значение по умолчанию: `Auto`
`ForwardDivertConnectTransparently` *{Yes | No}*	Включить или отключить режим эмуляции подключения к получателю (серверу) с IP-адреса отправителя перехваченного пакета (клиента) для транзитных соединений. Допустимые значения: • `Yes` — при перехвате соединения подключаться к серверу не со своего адреса, а с адреса клиента, который запросил соединение; • `No` — подключаться к серверу с адреса Dr.Web Firewall для Linux. Поскольку в режиме перехвата транзитных соединений нет гарантии, что весь трафик проходит через один и тот же узел (маршрутизатор), на

Параметр	Описание
	котором установлен Dr.Web Firewall для Linux, для корректной работы значение по умолчанию — `No`. Если конфигурация сети гарантирует, что все защищаемые приложения используют один и тот же маршрутизатор, параметр можно установить в `Yes`, и в этом случае при подключении к серверам Dr.Web Firewall для Linux всегда будет эмулировать подключение с адреса клиента. Значение по умолчанию: `No`
`ForwardDivertMark` *{целое число | Auto | None}*	Метка, которой помечаются пакеты в режиме перехвата транзитных соединений при использовании подсистемы мандатного доступа PARSEC. Допустимые значения: • *<целое число>* — метка, присваиваемая пакетам. Численно равна 2^N, где N — номер бита метки в пакете, $0 \leq N \leq 31$. • `Auto` — разрешить Dr.Web Firewall для Linux выбрать подходящий бит в метке пакета автоматически. • `None` — не устанавливать метку. Значение по умолчанию: `None`

`Whitelist`
 	
{список доменов}
	Белый список доменов (домены, подключение к которым разрешено, даже если они относятся к блокируемым категориям веб-ресурсов. При этом доступ пользователей будет разрешен и ко всем поддоменам доменов, указанных в этом списке).
	
	Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения параметра объединяются в единый список).
	
	Пример: Добавить в список домены `example.com` и `example.net`.
	
	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[LinuxFirewall]`
	`Whitelist = "example.com", "example.net"`

Параметр	Описание

	• Две строки (по одному значению в строке):
	`[LinuxFirewall]`
	`Whitelist = example.com`
	`Whitelist = example.net`
	2. Добавление значений через команду `drweb-ctl cfset`:
	`# drweb-ctl cfset LinuxFirewall.Whitelist -a example.com`
	`# drweb-ctl cfset LinuxFirewall.Whitelist -a example.net`
	⚠ Реальное использование списка доменов, указанного в данном параметре, зависит от того, *как* он используется в правилах проверки, заданных для Dr.Web Firewall для Linux.
	В перечне правил, заданных по умолчанию (см. ниже), гарантируется, что доступ к доменам (и их поддоменам) из данного списка будет обеспечен, даже если там будут находиться домены из блокируемых категорий веб-ресурсов, но только если производится запрос к узлу с использованием протокола HTTP. Кроме этого, условия правил по умолчанию гарантируют, что данные, загружаемые с доменов из белого списка, *будут проверяться на наличие угроз* (так как данные возвращаются в ответе, и переменная `direction` имеет значение `response`).
	Значение по умолчанию: *(не задано)*

`Blacklist` *{список доменов}*	Черный список доменов (домены, подключение к которым запрещено, даже если они не относятся к блокируемым категориям веб-ресурсов. При этом доступ пользователей будет запрещен и ко всем поддоменам доменов, указанных в этом списке).

Параметр	Описание

	Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения параметра объединяются в единый список).
	
	Пример: Добавить в список домены `example.com` и `example.net`.
	
	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[LinuxFirewall]`
	`Blacklist = "example.com", "example.net"`
	• Две строки (по одному значению в строке):
	`[LinuxFirewall]`
	`Blacklist = example.com`
	`Blacklist = example.net`
	2. Добавление значений через команду `drweb-ctl cfset`:
	`# drweb-ctl cfset LinuxFirewall.Blacklist -a example.com`
	`# drweb-ctl cfset LinuxFirewall.Blacklist -a example.net`

Параметр	Описание
	 Реальное использование списка доменов, указанного в данном параметре, зависит от того, *как* он используется в правилах проверки, заданных для Dr.Web Firewall для Linux. Условия правил, заданных по умолчанию (см. ниже), гарантируют, что доступ к доменам (и их поддоменам) из данного списка по протоколу HTTP будет запрещен всегда. Если домен добавлен одновременно в список `Whitelist` и список `Blacklist`, то правила, заданные по умолчанию, гарантируют, что доступ пользователей к домену по протоколу HTTP будет заблокирован. Сайты из черного списка не будут блокироваться, если отключена проверка исходящего трафика (убедитесь, что параметр `OutputDivertEnable` имеет значение `Yes`, `On` или `True`). Если эти сайты используют протокол HTTPS, также установите параметр `UnwrapSsl` в значение `Yes`, `On` или `True`. Значение по умолчанию: *(не задано)*
`InspectHttp` *{On | Off}*	Проверять данные, передаваемые по протоколу HTTP. Данные будут проверены в соответствии с заданными правилами (см. ниже). Значение по умолчанию: `On`
`InspectPop3` *{On | Off}*	Проверять данные, передаваемые по протоколу POP3. Данные будут проверены в соответствии с заданными правилами (см. ниже). Значение по умолчанию: `On`

Параметр	Описание
`InspectImap` *{On | Off}*	Проверять данные, передаваемые по протоколу IMAP. Данные будут проверены в соответствии с заданными правилами (см. ниже). Значение по умолчанию: `On`
`InspectSmtp` *{On | Off}*	Проверять данные, передаваемые по протоколу SMTP. Данные будут проверены в соответствии с заданными правилами (см. ниже). Значение по умолчанию: `On`
`InspectFtp` *{On | Off}*	Проверять данные, передаваемые по протоколу FTP. Данные будут проверены в соответствии с заданными правилами (см. ниже). Значение по умолчанию: `On`

`ExcludedProc`
{путь к файлу}
	Белый список процессов (процессы, сетевая активность которых не контролируется).
	
	Можно указать несколько значений в виде списка. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения параметра объединяются в единый список).
	
	Пример: Добавить в список процессы `wget` и `curl`.
	
	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[LinuxFirewall]`
	`ExcludedProc = "/usr/bin/wget", "/usr/bin/curl"`
	• Две строки (по одному значению в строке):
	`[LinuxFirewall]`
	`ExcludedProc = /usr/bin/wget`
	`ExcludedProc = /usr/bin/curl`

Параметр	Описание

	2. Добавление значений через команду `drweb-ctl cfset`:
	`# drweb-ctl cfset LinuxFirewall.ExcludedProc -a /usr/bin/wget`
	`# drweb-ctl cfset LinuxFirewall.ExcludedProc -a /usr/bin/curl`
	Реальное использование списка процессов, указанного в данном параметре, зависит от того, *как* он используется в правилах проверки, заданных для Dr.Web Firewall для Linux.
	В перечне правил, заданных по умолчанию (см. ниже), гарантируется, что трафик всех процессов, указанных в этом списке пропускается *без какой-либо проверки*.
	Значение по умолчанию: *(не задано)*

`UnwrapSsl` *{логический}*	Проверять или не проверять зашифрованный трафик, передаваемый через SSL. В текущей реализации значение данной переменной не оказывает никакого влияния на проверку защищенного трафика. Для реального управления проверкой нужно создать правило, в котором содержится действие `SET Unwrap_SSL = true/false` (см. ниже). Если значение параметра изменять через команду `cfset` утилиты `drweb-ctl` или через веб-интерфейс управления, то зависимые правила будут перестраиваться автоматически. Значение по умолчанию: `No`

Параметр	Описание
`BlockUnchecked` *{логический}*	Блокировать получение и передачу данных, если они не могут быть проверены. Значение этого параметра влияет на обработку правил, в которых невозможно определить истинность или ложность условия вследствие ошибки: в случае `No` правило будет пропущено как не сработавшее, а в случае `Yes` будет выполнено действие `BLOCK as BlackList`. Значение по умолчанию: `No`
`BlockInfectionSource` *{логический}*	Блокировать попытки подключения к сайтам, содержащим вредоносное ПО (входящим в категорию *InfectionSource*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockNotRecommended` *{логический}*	Блокировать попытки подключения к нерекомендуемым сайтам (входящим в категорию *NotRecommended*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockAdultContent` *{логический}*	Блокировать попытки подключения к сайтам, содержащим материалы для взрослых (входящим в категорию *AdultContent*).

Параметр	Описание
	Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockViolence` *{логический}*	Блокировать попытки подключения к сайтам, содержащим сцены насилия (входящим в категорию *Violence*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockWeapons` *{логический}*	Блокировать попытки подключения к сайтам, посвященным оружию (входящим в категорию *Weapons*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockGambling` *{логический}*	Блокировать попытки подключения к сайтам, посвященным азартным играм и играм на деньги (входящим в категорию *Gambling*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockDrugs` *{логический}*	Блокировать попытки подключения к сайтам, посвященным наркотикам (входящим в категорию *Drugs*).

Параметр	Описание
	Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockObsceneLanguage` *{логический}*	Блокировать попытки подключения к сайтам, содержащим нецензурную лексику (входящим в категорию *ObsceneLanguage*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockChats` *{логический}*	Блокировать попытки подключения к сайтам чатов (входящим в категорию *Chats*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockTerrorism` *{логический}*	Блокировать попытки подключения к сайтам, посвященным терроризму (входящим в категорию *Terrorism*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockFreeEmail` *{логический}*	Блокировать попытки подключения к сайтам бесплатных почтовых служб (входящим в категорию *FreeEmail*).

Параметр	Описание
	Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockSocialNetworks` *{логический}*	Блокировать попытки подключения к сайтам социальных сетей (входящим в категорию *SocialNetworks*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockDueToCopyrightNotice` *{логический}*	Блокировать попытки подключения к сайтам, ссылки на которые были добавлены по обращению правообладателей (входящим в категорию *DueToCopyrightNotice*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockOnlineGames` *{логический}*	Блокировать попытки подключения к сайтам онлайн-игр (входящим в категорию *OnlineGames*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockAnonymizers` *{логический}*	Блокировать попытки подключения к сайтам анонимайзеров (входящим в категорию *Anonymizers*).

Параметр	Описание
	Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockCryptocurrencyMiningPools` *{логический}*	Блокировать попытки подключения к сайтам, объединяющим пользователей с целью добычи (майнинга) криптовалют (входящим в категорию *CryptocurrencyMiningPool*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockJobs` *{логический}*	Блокировать попытки подключения к сайтам, предназначенным для поиска вакансий (входящим в категорию *Jobs*). Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match` Значение по умолчанию: `No`
`BlockKnownVirus` *{логический}*	Блокировать получение и передачу данных, если они содержат известную угрозу. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockSuspicious` *{логический}*	Блокировать получение и передачу данных, если они содержат неизвестную угрозу, обнаруженную эвристическим анализатором.

Параметр	Описание
	Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockAdware` *{логический}*	Блокировать получение и передачу данных, если они содержат рекламную программу. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockDialers` *{логический}*	Блокировать получение и передачу данных, если они содержат программу дозвона. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match` Значение по умолчанию: `Yes`
`BlockJokes` *{логический}*	Блокировать получение и передачу данных, если они содержат программу-шутку. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match` Значение по умолчанию: `No`
`BlockRiskware` *{логический}*	Блокировать получение и передачу данных, если они содержат потенциально опасную программу.

Параметр	Описание
	Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match` Значение по умолчанию: `No`
`BlockHacktools` *{логический}*	Блокировать получение и передачу данных, если они содержат программу взлома. Для блокировки необходимо, чтобы в настройках присутствовало правило вида (см. ниже): `threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match` Значение по умолчанию: `No`
`ScanTimeout` *{интервал времени}*	Тайм-аут на проверку одного файла по запросу SplDer Gate. Допустимые значения: от 1 секунды (`1s`) до 1 часа (`1h`). Значение по умолчанию: `30s`
`HeuristicAnalysis` *{On | Off}*	Использовать или не использовать эвристический анализ для поиска возможных неизвестных угроз при проверке файла, инициированной по запросу SplDer Gate. Использование эвристического анализа повышает надежность проверки, но увеличивает ее длительность. Действие при срабатывании эвристического анализатора задается параметром `BlockSuspicious`. Допустимые значения: • `On` — использовать эвристический анализ при проверке; • `Off` — не использовать эвристический анализ. Значение по умолчанию: `On`
`PackerMaxLevel` *{целое число}*	Максимальный уровень вложенности для запакованных объектов. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX,

Параметр	Описание
	PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`ArchiveMaxLevel` *{целое число}*	Максимальный уровень вложенности для архивов (`.zip`, `.rar` и др.), в которые вложены другие архивы, в которые, в свою очередь, также могут быть вложены архивы, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться. Ограничений уровня вложенности нет. Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`MailMaxLevel` *{целое число}*	Максимальный уровень вложенности для файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться. Ограничений уровня вложенности нет. Значение 0 указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`ContainerMaxLevel` *{целое число}*	Максимальный уровень вложенности для других типов объектов с вложениями (страниц HTML, файлов `.jar` и др.). Задает уровень в иерархии вложенности, после которого объекты внутри объектов будут пропускаться при проверке файла, инициированной по запросу SpIDer Gate. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`MaxCompressionRatio` *{целое число}*	Максимальная допустимая степень сжатия запакованных объектов (отношение сжатого объема

Параметр	Описание
	к несжатому). Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке файла, инициированной по запросу SpIDer Gate. Величина степени сжатия должна быть не менее `2`. Значение по умолчанию: `500`

`InterceptHook`
 	
{путь к файлу | функция Lua}
	Скрипт обработки соединений на языке Lua, либо путь к файлу, хранящему этот скрипт (см. раздел Обработка соединений на Lua).
	
	Если указанный файл недоступен, то при загрузке компонента будет выдана ошибка.
	
	Значение по умолчанию:
	
	`local dwl = require 'drweb.lookup'`
	
	`function intercept_hook(ctx)`
	
	`  -- do not check if group == Root.TrustedGroup`
	`  if ctx.divert == "output" and ctx.group == "drweb"`
	`  then`
	`  return "pass"`
	`  end`
	
	`  -- do not check connections from privileged ports`
	`  -- except FTP active mode`
	`  if ctx.src.port >= 0 and ctx.src.port <= 1024`
	`  and ctx.src.port ~= 20`
	`  then`
	`  return "pass"`
	`  end`
	
	`  return "check"`
	`end`

`XtablesLockPath` *{путь к файлу}*	Путь к файлу блокировки таблиц `iptables` (NetFilter). Если значение параметра не указано, проверяются пути `/run/xtables.lock` и `/var/run/xtables.lock`. Если файл блокировок не обнаружен по указанному пути или путям по умолчанию, запуск компонента завершится ошибкой. Значение по умолчанию: *(не задано)*

Изменения, внесенные в настройки проверки соединений, не влияют на проверку соединений, которые уже были установлены приложениями до внесения изменений. Если необходимо применить их для уже запущенных приложений, необходимо заставить их разорвать и повторно установить сетевое соединение, например, путем перезапуска этих приложений.

Правила проверки трафика и блокировки доступа

В дополнение к параметрам, перечисленным выше, в секции присутствует 11 *наборов правил* `RuleSet*` (`RuleSet0`, ..., `RuleSet10`), непосредственно управляющих проверкой трафика и блокировкой доступа пользователей к веб-ресурсам, а также загрузкой контента из интернета. Для некоторых значений в условиях (например, диапазоны IP-адресов, перечни категорий сайтов, черные и белые списки сайтов и т. п.) предусмотрена подстановка значений, загружаемых из текстовых файлов, а также извлеченных из внешних источников данных через LDAP (используется компонент Dr.Web LookupD). При обработке соединений все правила проверяются в порядке сверху вниз единым списком до момента нахождения сработавшего правила, содержащего финальную резолюцию. Пропуски в списке правил, если встречаются, игнорируются.

Подробно правила рассмотрены в разделе Правила проверки трафика Приложения Г.

Просмотр и редактирование правил

Для удобства редактирования списка правил, по умолчанию в списке оставлены «пустоты», т. е. наборы `RuleSet<i>`, не содержащие правил (где *<i>* — номер набора `RuleSet`).

Вы *не можете* добавить элементы списка, отличные от уже имеющихся `RuleSet<i>`, но можете добавить или удалить любое правило в любом элементе `RuleSet<i>`.

Просматривать и редактировать правила можно любым из следующих способов:

- путем просмотра и изменения файла конфигурации в любом текстовом редакторе (помните, что в этом файле сохраняются только те параметры, значения которых отличаются от значений по умолчанию);
- через веб-интерфейс управления;
- через интерфейс командной строки Dr.Web Ctl (команды `drweb-ctl cfshow` и `drweb-ctl cfset`).

Если вы редактировали правила, внося изменения в файл конфигурации, для применения внесенных изменений перезапустите Dr.Web Gateway Security Suite. Для этого воспользуйтесь командой `drweb-ctl reload`.

Просмотр правил с помощью команды drweb-ctl cfshow

Для просмотра содержимого набора правил `LinuxFirewall.RuleSet1` используйте команду:

```
# drweb-ctl cfshow LinuxFirewall.RuleSet1
```

Редактирование правил с помощью команды drweb-ctl cfset

Здесь и далее <*правило*> — текст правила.

- Замена всех правил в наборе правил `LinuxFirewall.RuleSet1` на новое правило:

  ```
  # drweb-ctl cfset LinuxFirewall.RuleSet1 '<правило>'
  ```

- Добавление еще одного правила в набор правил `LinuxFirewall.RuleSet1`:

  ```
  # drweb-ctl cfset -a LinuxFirewall.RuleSet1 '<правило>'
  ```

- Удаление конкретного правила из набора правил `LinuxFirewall.RuleSet1`:

  ```
  # drweb-ctl cfset -e LinuxFirewall.RuleSet1 '<правило>'
  ```

- Возврат набора правил `LinuxFirewall.RuleSet1` к состоянию по умолчанию:

  ```
  # drweb-ctl cfset -r LinuxFirewall.RuleSet1
  ```

При использовании утилиты `drweb-ctl` для редактирования правил заключайте строку добавляемого правила <*правило*> в одинарные или двойные кавычки, а внутренние кавычки, если они встречаются в правиле, экранируйте символом обратной косой черты `\`.

Важно помнить следующие особенности хранения правил в переменных конфигурации `RuleSet`<*i*>:

- При добавлении безусловных правил условная часть и двоеточие могут быть опущены, однако такие правила всегда сохраняются в списке правил в виде строки '`:` <*действие*>'.
- При добавлении правил, содержащих несколько действий (правила вида '<*условие*> `:` <*действие 1*>`,` <*действие 2*>'), такие правила будут преобразованы в цепочку элементарных правил '<*условие*> `:` <*действие 1*>' и '<*условие*> `:` <*действие 2*>'.
- Так как в записи правил не предусмотрено дизъюнкции (логическое «ИЛИ») условий в условной части, для реализации логического «ИЛИ» запишите цепочку правил, в условии каждого из которых будет указано условие-дизъюнкт.

Чтобы добавить в набор правил `LinuxFirewall.RuleSet1` правило безусловного пропуска (действие `PASS`), достаточно выполнить команду:

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'PASS'
```

Чтобы удалить это правило из указанного набора правил, необходимо выполнить команду:

```
# drweb-ctl cfset -e LinuxFirewall.RuleSet1 ' : PASS'
```

Чтобы добавить в набор правил `LinuxFirewall.RuleSet1` правило, изменяющее для соединений, следующих с неразрешенных адресов, путь к стандартным шаблонам и выполняющее блокировку, достаточно выполнить команду:

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'src_ip not in
file("/etc/trusted_ip") : set http_template_dir = "mytemplates", BLOCK'
```

Эта команда добавит *два правила* в указанный набор правил, поэтому, чтобы удалить их, необходимо выполнить две команды:

```
# drweb-ctl cfset -e LinuxFirewall.RuleSet1 'src_ip not in
file("/etc/trusted_ip") : set http_template_dir = "mytemplates"'
# drweb-ctl cfset -e LinuxFirewall.RuleSet1 'src_ip not in
file("/etc/trusted_ip") : BLOCK'
```

Чтобы добавить в набор правил `LinuxFirewall.RuleSet1` правило вида «Осуществить блокировку, если обнаружен вредоносный объект типа *KnownVirus* или URL из категории *Terrorism*», необходимо добавить в этот набор сразу два правила:

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'threat_category in (KnownVirus)
: BLOCK as _match'
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'url_category in (Terrorism) :
BLOCK as _match'
```

Для их удаления также потребуется две команды, как в примере выше.

Набор правил по умолчанию

По умолчанию задан следующий набор правил, управляющих блокировкой:

```
RuleSet0 =
RuleSet1 = divert output : set HttpTemplatesDir = "output"
RuleSet1 = divert output : set MailTemplatesDir = "firewall"
RuleSet1 = divert input : set HttpTemplatesDir = "input"
RuleSet1 = divert input : set MailTemplatesDir = "server"
RuleSet1 = proc in "LinuxFirewall.ExcludedProc" : PASS
RuleSet1 =  : set Unwrap_SSL = false
RuleSet2 =
```

```
RuleSet3 =
RuleSet4 =
RuleSet5 = protocol in (Http), direction request, url_host in
"LinuxFirewall.Blacklist" : BLOCK as BlackList
RuleSet5 = protocol in (Http), direction request, url_host in
"LinuxFirewall.Whitelist" : PASS
RuleSet6 =
RuleSet7 = protocol in (Http), direction request, url_category in
"LinuxFirewall.BlockCategory" : BLOCK as _match
RuleSet8 =
RuleSet9 = protocol in (Http), divert input, direction request,
threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match
RuleSet9 = protocol in (Http), direction response, threat_category in
"LinuxFirewall.BlockThreat" : BLOCK as _match
RuleSet9 = protocol in (Smtp), threat_category in
"LinuxFirewall.BlockThreat" : REJECT
RuleSet9 = protocol in (Smtp), url_category in "LinuxFirewall.BlockCategory"
: REJECT
RuleSet9 = protocol in (Smtp), total_spam_score gt 0.80 : REJECT
RuleSet9 = protocol in (Pop3, Imap), threat_category in
"LinuxFirewall.BlockThreat" : REPACK as _match
RuleSet9 = protocol in (Pop3, Imap), url_category in
"LinuxFirewall.BlockCategory" : REPACK as _match
RuleSet9 = protocol in (Pop3, Imap), total_spam_score gt 0.80 : REPACK as
_match
RuleSet10 =
```

Первое правило указывает, что если соединение устанавливается процессом, указанным в параметре `ExcludedProc` (см. выше), то соединение пропускается без проверки каких-либо дополнительных условий. Следующее правило (срабатывает безусловно) запрещает проверку защищенных соединений. Это правило, как и все следующие ниже, будет анализироваться только если соединение не связано с исключаемым процессом. Кроме того, поскольку все последующие правила зависят от определения типа протокола, то, если запрещено проверять защищенные соединения, а соединение защищенное, в этом случае все они не сработают из-за невозможности определить истинность условий.

Следующие пять правил регламентируют обработку исходящих HTTP-соединений:

1. Если узел, с которым устанавливается соединение, включен в черный список, соединение блокируется, а дальнейшие проверки не производятся.
2. Если узел находится в белом списке, соединение пропускается, дальнейшие проверки не производятся.
3. Если URL, к которому обращается клиент, относится к категории нежелательных для посещения веб-ресурсов, то соединение блокируется, а дальнейшие проверки не производятся.
4. Если ответ, поступивший от удаленного узла по HTTP, содержит угрозу, относящуюся к категориям, которые следует блокировать, то соединение блокируется, а дальнейшие проверки не производятся.

5. Если данные, передаваемые с локального узла на удаленный сервер, содержат угрозу, относящуюся к категориям, которые следует блокировать, то соединение блокируется, а дальнейшие проверки не производятся.

Эти пять правил будут работать только в том случае, если параметр `InspectHttp` имеет значение `On`. В противном случае ни одно из них не сработает.

Следующие шесть правил, указанных в `RuleSet9`, регламентируют проверку данных, передаваемых по протоколам электронной почты (SMTP, POP3 или IMAP), и срабатывают в следующих случаях:

- сообщение содержит вложения;
- сообщение содержит URL из категорий, подлежащих блокировке;
- сообщение оценено как спам с индексом не менее 0,8.

При этом к письмам, передаваемым по протоколу SMTP, применяется действие, блокирующее передачу письма (т. е. его отправку или прием), а для протоколов IMAP и POP3 производится обработка письма, заключающаяся в удалении из него вредоносного содержимого («перепаковка»).

Если компонент проверки сообщений электронной почты на наличие признаков спама Dr.Web Anti-Spam не установлен, то проверка писем на наличие признаков спама не производится. В этом случае правила, содержащие проверку порога спама (переменную `total_spam_score`), отсутствуют.

Правила проверки электронной почты будут работать только в том случае, если соответствующие параметры `Inspect<`*EmailProtocol*`>` имеют значение `On`. В противном случае ни одно из правил не сработает.

Для непосредственной проверки передаваемого письма на предмет наличия в нем вредоносных вложений, а также для анализа на признаки спама должен быть установлен дополнительный компонент проверки электронной почты — Dr.Web MailD. Если он не установлен, передаваемые сообщения будут блокироваться по причине ошибки *«Невозможно проверить»*. Чтобы разрешить прохождение писем, которые невозможно проверить, установите параметр `BlockUnchecked` в значение `No` (см. выше). Кроме того, при отсутствии компонента проверки электронной почты рекомендуется установить значение `No` для параметров `InspectSmtp`, `InspectPop3` и `InspectImap`.

Dr.Web MailD не входит в состав Dr.Web Gateway Security Suite.

Примеры правил проверки трафика и блокировки доступа

1. Разрешить для пользователей с диапазоном IP-адресов *10.10.0.0–10.10.0.254* доступ по протоколу HTTP к сайтам любых категорий, кроме категории *Chats*:

```
protocol in (HTTP), src_ip in (10.10.0.0/24), url_category not in
(Chats) : PASS
```

Если правило:

```
protocol in (HTTP), url_host in "LinuxFirewall.Blacklist" :
BLOCK as BlackList
```

разместить в списке правил выше (т. е. раньше) указанного правила, то доступ к доменам из черного списка, т. е. доменам, перечисленным в параметре `LinuxFirewall.Blacklist`, будет блокироваться и для пользователей с диапазоном IP-адресов *10.10.0.0–10.10.0.254*. А если это правило разместить ниже (т. е. позже), то пользователям с диапазоном IP-адресов *10.10.0.0–10.10.0.254* будут доступны также и сайты из черного списка.

Так как резолюция `PASS` является конечной, более никакие правила не проверяются, следовательно, проверка загружаемых данных на наличие угроз производиться также не будет.

Чтобы разрешить пользователям с диапазоном IP-адресов *10.10.0.0–10.10.0.254* доступ к сайтам любых категорий, кроме категории *Chats*, если они не находятся в черном списке, но при этом не разрешать загрузку угроз, используйте следующее правило:

```
protocol in (HTTP), url_category not in (Chats), url_host not in
"LinuxFirewall.Blacklist", threat_category not in
"LinuxFirewall.BlockCategory" : PASS
```

2. Не выполнять проверку содержимого *загружаемых из интернета* видеофайлов (т. е. данных с типом MIME `video/*`, где `*` соответствует любому типу MIME-класса `video`):

```
direction response, content_type in ("video/*") : PASS
```

Выгружаемые с локального компьютера файлы (в том числе и с типом MIME `video/*`) будут проверяться, так как они передаются *в запросах, а не ответах*, т. е. для них переменная `direction` имеет значение `request`.

9.6.4. Обработка соединений на Lua

В этом разделе

- Общие сведения

- Требования к скрипту для обработки соединений
- Примеры
- Используемые таблицы (InterceptContext, TcpEndpoint)
- Доступные вспомогательные модули (drweb, drweb.lookup)

Общие сведения

Компонент Dr.Web Firewall для Linux поддерживает взаимодействие с интерпретатором программ на языке Lua (версия 5.3.4 поставляется совместно с Dr.Web Gateway Security Suite). Lua-скрипты могут быть использованы Dr.Web Firewall для Linux для предварительной проверки соединения перед проведением его анализа компонентом SplDer Gate.

Соединение будет проанализировано с помощью скрипта, если в настройках компонента Dr.Web Firewall для Linux (в параметре `InterceptHook`) задан путь к этому скрипту. В противном случае обработка соединения производится с использованием настроек по умолчанию и правил обработки, заданных в настройках компонента (параметры `RuleSet*`).

Дополнительные примеры скриптов для обработки соединений доступны по ссылке: https://github.com/DoctorWebLtd/drweb-lua-examples/tree/master/firewall.

Требования к скрипту для обработки соединений

Скрипт должен содержать глобальную функцию, являющуюся точкой входа в модуль проверки соединения (эту функцию Dr.Web Firewall для Linux будет вызывать для обработки поступающих соединений). Функция обработки должна соответствовать следующим соглашениям о вызове:

- *имя функции* — `intercept_hook`;
- *единственный аргумент* — таблица Lua InterceptContext (предоставляет из функции доступ к информации об обрабатываемом соединении; см. описание таблицы ниже);
- *единственное возвращаемое значение* — строковое значение из таблицы ниже:

Значение	Описание вердикта
`pass`	Пропустить соединение без проверки компонентом SplDer Gate
`check`	Проверить соединение с помощью компонента SplDer Gate
`reject`	Отказать в соединении (клиент, инициировавший соединение, получит TCP-пакет с флагом `RST`)
`drop`	Разорвать соединение (клиент, инициировавший соединение, ничего не получит)

Примеры

1. Простой скрипт передает в Dr.Web Firewall для Linux вердикт `pass`, тем самым указывая, что соединения не нужно проверять:

```
-- Функция проверки соединения, написанная пользователем
function intercept_hook(ctx)
  return "pass" -- не проверять соединение
end
```

2. Скрипт указывает Dr.Web Firewall для Linux направить на проверку все устанавливаемые соединения, кроме:
   - исходящих локальных соединений от приложений, исполняемых с правами пользователя из группы `drweb`;
   - соединений с привилегированных портов (независимо от владельца и направления соединения);
   - исходящих соединений с IP-адресов из локальной подсети.

```
function intercept_hook(ctx)
  -- Не проверять соединения, инициированные с локального
  -- узла (divert == "output") приложением от имени группы
  -- "drweb" (group == "drweb")
  if ctx.divert == "output" and ctx.group == "drweb" then
    return "pass"
  end

  -- Не проверять соединения, инициированные с
  -- привилегированных портов (от 0 до 1024)
  if ctx.src.port >= 0 and ctx.src.port <= 1024 then
    return "pass"
  end

  -- Не проверять соединения с адресов из локальной подсети
  -- (диапазона IP-адресов 127.0.0.1/8)
  if ctx.src.ip.belongs("127.0.0.0/8") then
    return "pass"
  end

  -- По умолчанию соединение проверяется
  return "check"
end
```

Используемые таблицы

Таблица InterceptContext

Таблица используется для передачи в функцию `intercept_hook` данных об обрабатываемом соединении, на основании которых будет выполнено одно из следующих действий:

- пропуск соединения,
- разрыв соединения,
- передача соединения на проверку в SplDer Gate.

Компонент Dr.Web Firewall для Linux заполняет эту таблицу данными. Часть данных в этой таблице известна уже к моменту вызова функции `intercept_hook`, а другая часть (т. н. «ленивые» данные) будет вычислена непосредственно в момент запроса значения соответствующего поля из этой таблицы.

Поле	Описание	Тип данных

`src`	Адрес и порт клиента, инициировавшего соединение
	Пример:
	`if ctx.src.port >= 0 and ctx.src.port <= 1024 then`
	`  return "pass"`
	`end`
		Таблица TcpEndpoint

`dst`	Адрес и порт сервера, соединение к которому запросил клиент
	Пример:
	`if ctx.dst.ip.belongs("10.20.30.41/8") then`
	`  return "reject"`
	`end`
		Таблица TcpEndpoint

`divert`	Тип перехваченного соединения:
	• `output` — исходящее соединение;
	• `input` — входящее соединение;
	• `forward` — транзитное соединение.
	Пример:
	`if ctx.divert == "forward" then`
	`  return "check"`
	`end`
		Строка

`iface_in`	Имя интерфейса, с которого инициировано соединение.	Строка

Поле	Описание	Тип данных
	Если имя интерфейса не удалось определить, имеет значение `nil`.	
`iface_out`	Имя интерфейса, на который были направлены пакеты после инициации соединения. Если имя интерфейса не удалось определить, имеет значение `nil`.	Строка
`uid`	Идентификатор пользователя, от имени которого инициировано исходящее соединение. Если тип соединения (`divert`) не `output`, либо UID не удалось определить, имеет значение `nil`.	Целое число
`gid`	Идентификатор группы, от имени которой инициировано исходящее соединение. Если тип соединения (`divert`) не `output`, либо GID не удалось определить, имеет значение `nil`.	Целое число
`user`	Пользователь, от имени которого инициировано исходящее соединение. Если тип соединения (`divert`) не `output`, либо имя пользователя не удалось определить, имеет значение `nil`.	Строка
`group`	Группа, от имени которой инициировано исходящее соединение. Если тип соединения (`divert`) не `output`, либо имя группы не удалось определить, имеет значение `nil`.	Строка
`pid`	Идентификатор процесса (PID), от имени которого инициировано исходящее соединение. Если тип соединения (`divert`) не `output`, либо PID не удалось определить, имеет значение `nil`.	Целое число
`exe_path`	Путь к исполняемому файлу приложения, инициировавшего исходящее соединение. Если поле `divert` (см. выше) имеет значение `input` или `forward`, а также если путь к исполняемому файлу по тем или иным причинам не удалось определить, имеет значение `nil`.	Строка
Переопределенные метаметоды: *Нет*		

Таблица TcpEndpoint

Таблица описывает адрес точки соединения клиента или сервера.

Поле	Описание	Тип данных
`ip`	IP-адрес	Таблица IpAddress
`port`	Номер порта	Целое число
Переопределенные метаметоды: • `__tostring` — функция, преобразующая `TcpEndpoint` в строку, например, `"127.0.0.1:443"` (IPv4) или `"[::1]:80"` (IPv6); • `__concat` — функция, присоединяющая `TcpEndpoint` к строке		

Доступные вспомогательные модули

Для взаимодействия с Dr.Web Gateway Security Suite в пространство Lua-программы могут быть импортированы следующие специфические модули, перечисленные в таблице.

Имя модуля	Назначение
drweb	Модуль, предоставляющий функции для записи сообщений из Lua-программы в журнал компонента Dr.Web Gateway Security Suite, запустившего эту программу, а также средства асинхронного запуска Lua-процедур
drweb.lookup	Модуль, предоставляющий инструменты для запроса данных из внешних источников путем обращения к модулю Dr.Web LookupD

Содержимое модуля drweb

1. Функции

Модуль предоставляет набор функций.

- Для записи сообщений из Lua-программы в журнал компонента Dr.Web Gateway Security Suite:
  - `log(`<*уровень*>, <*сообщение*>`)` записывает строку <*сообщение*> в журнал Dr.Web Gateway Security Suite на уровне <*уровень*> (требуемый уровень задается одним из следующих значений (строка): *debug*, *info*, *notice*, *warning*, *error*);
  - `debug(`<*сообщение*>`)` записывает строку <*сообщение*> в журнал Dr.Web Gateway Security Suite на уровне *debug*;
  - `info(`<*сообщение*>`)` записывает строку <*сообщение*> в журнал Dr.Web Gateway Security Suite на уровне *info*;

  - `notice(<сообщение>)` записывает строку <*сообщение*> в журнал Dr.Web Gateway Security Suite на уровне *notice*;
  - `warning(<сообщение>)` записывает строку <*сообщение*> в журнал Dr.Web Gateway Security Suite на уровне *warning*;
  - `error(<сообщение>)` записывает строку <*сообщение*> в журнал Dr.Web Gateway Security Suite на уровне *error*.
- Для управления синхронизацией Lua-процедур:
  - `sleep(<сек.>)` приостанавливает выполнение экземпляра Lua-процедуры на указанное число секунд;
  - `async(<Lua-функция>[, <список аргументов>])` асинхронно запускает указанную функцию с передачей ей заданного списка аргументов. Вызов функции `async` завершается немедленно, возвращаемое значение (таблица `Future`) позволяет получить результат выполнения функции <*Lua-функция*>.
- Для представления информации об IP-адресе в виде таблицы IpAddress:
  - `ip(<адрес>)` представляет IP-адрес (IPv4 или IPv6) в виде таблицы IpAddress.
- Для загрузки внешних данных из текстового файла:
  - `load_set(<путь к файлу>)` формирует из содержимого указанного текстового файла таблицу со значениями `true`; в качестве ключей используются строки, прочитанные из файла. Пустые строки и строки, состоящие только из пробельных символов, будут проигнорированы.
  - `load_array(<путь к файлу>)` формирует из содержимого указанного текстового файла массив строк. Пустые строки и строки, состоящие только из пробельных символов, будут проигнорированы.

2. Таблицы

- Таблица `Future` описывает отложенный результат выполнения функции при помощи функции `async`.

Поле	Описание	Тип данных
`wait`	Функция, возвращающая результат функции, запущенной при помощи функции `async`. Если функция еще не завершила свое выполнение, ожидает завершения и возвращает результат. Если функция завершилась до момента вызова `wait`, результат возвращается немедленно. Если запущенная функция завершилась с ошибкой, вызов `wait` генерирует ту же ошибку.	Функция
Переопределенные метаметоды: *Нет*		

- Таблица IpAddress описывает IP-адрес.

Поле	Описание	Тип данных
`belongs`	Функция для проверки IP-адреса из таблицы `IpAddress` на	Функция

Поле	Описание	Тип данных
	принадлежность к указанным подсетям (диапазонам IP-адресов). Принимает единственный аргумент — массив строк вида <*IP-адрес*> или <*IP-адрес*>/<*маска*>, где <*IP-адрес*> — адрес узла либо сети (например, `127.0.0.1`), а <*маска*> — маска подсети, которая указывается в виде IP-адреса (например, `255.0.0.0`), либо в виде целого числа (например, `8`). Возвращает логическое значение: • `true` — если адрес совпадает хотя бы с одним из указанных IP-адресов либо принадлежит хотя бы одной из указанных подсетей (диапазону IP-адресов); • `false` — если адрес не совпадает ни с одним из указанных IP-адресов или не принадлежит ни одной из указанных подсетей	
Переопределенные метаметоды: • `__tostring` — функция, преобразующая `IpAddress` в строку, например, `127.0.0.1` (IPv4) или `::1` (IPv6); • `__concat` — функция, присоединяющая `IpAddress` к строке; • `__eq` — функция для проверки равенства двух `IpAddress`; • `__band` — функция, позволяющая накладывать маску, например: `dw.ip('192.168.1.2') & dw.ip('255.255.254.0')`		

3. Примеры

- Вывод в журнал сообщений, сформированных процедурой, запускающейся асинхронно:

```
local dw = require "drweb"

-- Функция, возвращающая полученную в качестве аргумента строку
-- по истечении двух секунд ожидания
function out_msg(message)
 dw.sleep(2)
 return message
end

-- "Главная" функция
function intercept(ctx)
 -- Вывод строки на уровне notice в журнал Dr.Web Gateway Security Suite
 dw.notice("Intercept function started.")

 -- Асинхронный запуск двух экземпляров функции out_msg
 local f1 = dw.async(out_msg, "Hello,")
 local f2 = dw.async(out_msg, " world!")

 -- Ожидание завершения исполнения экземпляров функции
 -- out_msg и вывод их результатов в журнал
 -- Dr.Web Gateway Security Suite на уровне debug
 dw.log("debug", f1.wait() .. f2.wait())
end
```

- Создание регулярной процедуры:

```
local dw = require "drweb"

-- Сохранить таблицу Future в глобальную переменную future, чтобы
-- предотвратить ее удаление сборщиком мусора
future = dw.async(function()
   while true do
     -- Каждый день выводить в журнал указанное сообщение
     dw.sleep(60 * 60 * 24)
     dw.notice("A brand new day began")
   end
end)
```

- Преобразование IP-адреса из строки:

```
local dw = require "drweb"

local ipv4 = dw.ip("127.0.0.1")
local ipv6 = dw.ip("::1")
local mapped = dw.ip("::ffff:127.0.0.1")
```

Содержимое модуля drweb.lookup

1. Функции

Модуль предоставляет функции:

- `lookup(<запрос>, <параметры>)` запрашивает данные во внешнем хранилище,

доступном через модуль Dr.Web LookupD. Аргумент <*запрос*> должен соответствовать секции запроса в настройках Dr.Web LookupD (строка <*тип*>@<*тег*>). Необязательный аргумент <*параметры*> описывает подстановки, которые будут использованы при формировании запроса. Могут быть использованы следующие автоматически разрешаемые маркеры:

- `$u`, `$U` (заменяется на `user`) — имя пользователя, переданное клиентским компонентом;
- `$d`, `$D` (заменяется на `domain`) — имя домена, переданное клиентским компонентом.

Аргументы задаются в виде таблицы, ключи и значения которой должны быть строками. Функция возвращает массив строк, являющихся результатами запроса.

- `check(`<*проверяемая строка*>`,` <*запрос*>`,` <*параметры*>`)` возвращает `true`, если <*проверяемая строка*> найдена во внешнем хранилище, доступном через модуль Dr.Web LookupD. Аргументы <*запрос*> и <*параметры*> полностью аналогичны аргументам функции `lookup` (см. выше). Аргумент <*проверяемая строка*> должен быть строкой или таблицей, имеющей метаметод `__tostring` (т. е. приводимой к строке).

2. Примеры

- Вывод в журнал списка пользователей, извлеченного из источника данных `LookupD.LDAP.users`:

```
local dw = require "drweb"
local dwl = require "drweb.lookup"

-- "Главная" функция
function intercept(ctx)
 -- Запись строки на уровне notice в журнал Dr.Web Gateway Security Suite
 dw.notice("Intercept function started.")

 -- Вывод в журнал Dr.Web Gateway Security Suite результатов запроса
 -- к источнику данных 'ldap@users'
 for _, s in ipairs(dwl.lookup("ldap@users", {user="username"})) do
   dw.notice("Result of request to 'ldap@users': " .. s)
 end

end
```

9.7. Dr.Web ClamD

Компонент Dr.Web ClamD предназначен для эмуляции интерфейса антивирусного демона `clamd`, являющегося центральным компонентом антивирусного продукта Clam AntiVirus (ClamAV®) от Sourcefire, Inc. Этот интерфейс позволяет внешним приложениям, которые могут использовать антивирусный продукт ClamAV®, проверять файлы с помощью Dr.Web Gateway Security Suite.

9.7.1. Принципы работы

Компонент Dr.Web ClamD позволяет выполнять по запросу от внешних приложений проверку на наличие угроз как содержимого файлов, расположенных в локальной файловой системе, так и непосредственно потоков данных, передаваемых внешним приложением через сокет. Кроме того, компонент может проверять содержимое файлов, для которых внешнее приложение передало отрытый дескриптор через сокет.

Проверка файла по переданному дескриптору осуществляется только через локальный Unix-сокет.

Если внешнее приложение предоставило путь к файлу в локальной файловой системе, компонент передает задание на проверку этого файла компоненту проверки файлов Dr.Web File Checker, иначе он передает данные, полученные от приложения через сокет, агенту распределенной проверки Dr.Web Network Checker.

По умолчанию компонент не запускается автоматически при старте Dr.Web Gateway Security Suite. Чтобы обеспечить запуск компонента, необходимо выполнить не только его включение настройкой `Start`, но и определить не менее одной точки подключения. После запуска компонент ожидает поступления запросов от внешних приложений на проверку указанных файлов или потоков передаваемых данных. В настройках можно определить набор различных точек подключения внешних приложений, указав для каждой свои собственные настройки проверки.

В качестве внешних приложений могут выступать и непосредственно прокси-серверы HTTP (такие как Squid и HAVP), если они оснащены модулем интеграции с Dr.Web ClamD. Подробнее см. в разделе Интеграция с внешними приложениями.

Обнаруженные угрозы *не нейтрализуются* средствами Dr.Web Gateway Security Suite, внешнему приложению только возвращается результат проверки. Таким образом, внешнее приложение само несет ответственность за нейтрализацию обнаруженной угрозы.

9.7.2. Аргументы командной строки

Для запуска компонента Dr.Web ClamD из командной строки используйте команду:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-clamd [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-clamd [<параметры>]
```

Dr.Web ClamD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-clamd --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web ClamD.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости (обычно при загрузке операционной системы). Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Gateway Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-clamd`.

9.7.3. Параметры конфигурации

В этом разделе

- Параметры компонента
- Особенность настроек компонента

Компонент использует параметры конфигурации, заданные в секции `[ClamD]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

Параметры компонента

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-clamd` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-clamd`
`Start` *{логический}*	Компонент запускается демоном управления конфигурацией Dr.Web ConfigD. Установка данного параметра в `Yes` предписывает демону управления конфигурацией немедленно

Параметр	Описание
	запустить компонент, а установка его в значение `No` — немедленно завершить работу компонента. Значение по умолчанию: `No`
`Endpoint.<тег>.ClamdSocket` *{IP-адрес | Unix-сокет}*	Определяет точку подключения с именем *<тег>* и сокет (адрес IPv4 или адрес сокета Unix) для клиентов, желающих проверять файлы на наличие угроз. Для одной точки *<тег>* может быть задан только один сокет. Значение по умолчанию: не задано
`[Endpoint.<тег>.]ReadTimeout` *{интервал времени}*	Тайм-аут на ожидание данных от клиента. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `5s`
`[Endpoint.<тег>.]StreamMaxLength` *{размер}*	Максимальный размер данных, которые могут быть получены от клиента (при передаче данных для проверки в виде потока байтов). Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `25mb`
`[Endpoint.<тег>.]ScanTimeout` *{интервал времени}*	Тайм-аут на проверку одного файла или одной порции данных, поступивших от клиента. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Допустимые значения: от 1 секунды (`1s`) до 1 часа (`1h`). Значение по умолчанию: `3m`
`[Endpoint.<тег>.]HeuristicAnalysis` *{On | Off}*	Использовать эвристический анализ при проверке. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано.

Параметр	Описание
	Значение по умолчанию: `On`
`[Endpoint.<тег>.]PackerMaxLevel` *{целое число}*	Максимальный уровень вложенности для запакованных объектов. Запакованные объекты представляют собой исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Они могут включать другие запакованные объекты, а те, в свою очередь, также могут включать запакованные объекты, и т. д. Максимальный уровень вложенности — это предельный уровень, после которого запакованные объекты внутри запакованных объектов не проверяются. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`[Endpoint.<тег>.]ArchiveMaxLevel` *{целое число}*	Максимальный уровень вложенности для архивов (`.zip`, `.rar` и др.). Архивы могут содержать другие архивы, а те, в свою очередь, также могут содержать архивы, и т. д. Максимальный уровень вложенности — это предельный уровень, после которого архивы внутри архивов не проверяются. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`[Endpoint.<тег>.]MailMaxLevel` *{целое число}*	Максимальный уровень вложенности для файлов почтовых программ (`.pst`, `.tbb` и др.), в которые могут быть вложены объекты, в которые также могут быть вложены объекты, и т. д. Значение этого параметра устанавливает предельный уровень, после которого объекты внутри объектов не будут проверяться. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки

Параметр	Описание
	<тег>, иначе оно определено для всех точек, у которых значение этого параметра не задано. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`[Endpoint.<тег>.]ContainerMaxLevel` *{целое число}*	Максимальный уровень вложенности для других типов объектов, содержащих вложенные объекты (например, страницы HTML или файлы `.jar`). Эти объекты могут содержать другие вложенные объекты, которые, в свою очередь, также могут содержать вложенные объекты, и т. д. Максимальный уровень вложенности — это предельный уровень, после которого объекты внутри объектов не проверяются. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Ограничений уровня вложенности нет. Значение `0` указывает, что вложенные объекты не проверяются. Значение по умолчанию: `8`
`[Endpoint.<тег>.]MaxCompressionRatio` *{целое число}*	Максимальная допустимая степень сжатия запакованных объектов (отношение сжатого объема к несжатому). Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Величина степени сжатия должна быть не менее `2`. Значение по умолчанию: `500`
`[Endpoint.<тег>.]DetectSuspicious` *{логический}*	Сообщать о подозрительных файлах, обнаруженных эвристическим анализатором. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано.

Параметр	Описание
	Значение по умолчанию: `Yes`
`[Endpoint.<тег>.]DetectAdware` *{логический}*	Сообщать о файлах, содержащих рекламные программы. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `Yes`
`[Endpoint.<тег>.]DetectDialers` *{логический}*	Сообщать о файлах, содержащих программы дозвона. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `Yes`
`[Endpoint.<тег>.]DetectJokes` *{логический}*	Сообщать о файлах, содержащих программы-шутки. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `No`
`[Endpoint.<тег>.]DetectRiskware` *{логический}*	Сообщать о файлах, содержащих потенциально опасные программы. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `No`
`[Endpoint.<тег>.]DetectHacktools` *{логический}*	Сообщать о файлах, содержащих программы взлома. Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `No`
`[Endpoint.<тег>.] ReportPasswordProtected`	Сообщать об ошибке, если проверяемые файлы защищены паролем.

Параметр	Описание
{целое число}	Если указан префикс `Endpoint.<тег>`, то значение параметра определено только для точки *<тег>*, иначе оно определено для всех точек, у которых значение этого параметра не задано. Значение по умолчанию: `No`

Особенность настроек компонента

Параметры, отмеченные необязательным префиксом `Endpoint.<тег>`, могут быть сгруппированы. Каждая такая группа определяет *точку подключения* (*endpoint*) с задаваемым уникальным идентификатором *<тег>*, используемую клиентами для подключения к компоненту. Все параметры проверки, включенные в одну группу, определяют параметры, которые будут применяться при проверке данных от клиентов, подключившихся к этой точке. Если параметр указан без префикса `Endpoint.<тег>`, то он определяет значение, применяемое для всех точек подключения. Если из точки подключения удалить параметр, то для точки подключения будет применяться не значение параметра по умолчанию, а значение, указанное в соответствующем одноименном «родительском» параметре (без префикса `Endpoint.<тег>`).

Параметр `ClamdSocket` должен обязательно задаваться с префиксом `Endpoint.<тег>`, поскольку он не только определяет прослушиваемый сокет, но и определяет группу (точку подключения), к которой этот сокет привязывается.

Пример

Пусть требуется организовать две точки подключения для двух групп внешних приложений (серверов) *servers1* и *servers2*. При этом серверы из группы *servers1* могут подключаться через Unix-сокет, а серверы из группы *servers2* — через сетевое соединение. Кроме того, эвристический анализ должен быть выключен по умолчанию, но для серверов из группы *servers2* его нужно использовать. Пример соответствующих настроек:

1) Для задания в файле конфигурации:

```
[ClamD]
HeuristicAnalysis = Off

[ClamD.Endpoint.servers1]
ClamdSocket = /tmp/srv1.socket

[ClamD.Endpoint.servers2]
ClamdSocket = 127.0.0.1:1234
HeuristicAnalysis = On
```

2) Для задания через утилиту командной строки Dr.Web Ctl:

```
# drweb-ctl cfset ClamD.HeuristicAnalysis Off
# drweb-ctl cfset ClamD.Endpoint -a servers1
# drweb-ctl cfset ClamD.Endpoint -a servers2
# drweb-ctl cfset ClamD.Endpoint.servers1.ClamdSocket /tmp/srv1.socket
# drweb-ctl cfset ClamD.Endpoint.servers2.ClamdSocket 127.0.0.1:1234
# drweb-ctl cfset ClamD.Endpoint.servers2.HeuristicAnalysis On
```

Оба способа задания настроек приведут к одинаковому результату, но при ручной правке файла конфигурации необходимо применить измененные настройки с помощью команды `drweb-ctl reload`.

9.7.4. Интеграция с внешними приложениями

За счет использования интерфейса, эмулирующего интерфейс антивирусного демона `clamd`, входящего в состав антивирусного решения ClamAV, Dr.Web ClamD может быть сопряжен с любыми внешними приложениями, способными подключаться к антивирусному демону `clamd`.

В таблице ниже перечислены примеры приложений, которые могут использовать `clamd` для антивирусной проверки:

Продукт	Интеграция
Службы HTTP	
Прокси-сервер HTTP Squid	**Использование clamd** Проверка файлов, получаемых через интернет. **Требование для интеграции** Использование промежуточного компонента `squidclamav` или HAVP. **Ссылки на документацию** Документация по продукту Squid: http://www.squid-cache.org/Doc/. Описание и исходный код `squidclamav`: https://squidclamav.darold.net/

Прокси-сервер HTTP с функциями антивирусной проверки HAVP	**Использование clamd**
	Проверка файлов, получаемых через интернет.
	Требование для интеграции
	Настройка в файле конфигурации HAVP использования `clamd` для антивирусной проверки:
	`ENABLECLAMD true`
	`CLAMDSOCKET <path_to_clamd_Unix_socket>`

Продукт	Интеграция

	или (если вместо Unix-сокета используется TCP-соединение):
	`ENABLECLAMD true`
	`CLAMDSERVER <IP>`
	`CLAMDPORT <port>`
	где *<path_to_clamd_Unix_socket>* или пара *<IP>:<port>* соответствуют сокету точки подключения *(endpoint)*, настроенной в конфигурации Dr.Web ClamD.
	Ссылки на документацию
	Документация по продукту HAVP: http://www.havp.org/documentation/

В настройке компонента, обращающегося непосредственно к Dr.Web ClamD как к антивирусному демону `clamd`, следует указать в качестве адреса подключения к антивирусному демону `clamd` путь к Unix-сокету или TCP-сокету, прослушиваемому Dr.Web ClamD на одной из созданных в его настройках точек подключения *(endpoint)*.

Пример подключения HAVP к Dr.Web ClamD:

1. Настройка Dr.Web ClamD:

```
[ClamD]
Start = yes

[ClamD.Endpoint.proxy]
ClamdSocket = /var/run/drweb.clamd
```

2. Настройка HAVP:

```
ENABLECLAMD true
CLAMDSOCKET /var/run/drweb.clamd
```

Настройки подключения к прочим антивирусным продуктам (параметры вида `ENABLE*`) должны быть установлены в значение `false`.

9.8. Dr.Web File Checker

Компонент проверки файлов Dr.Web File Checker предназначен для проверки файлов и каталогов файловой системы. Он используется другими компонентами Dr.Web Gateway Security Suite для проверки объектов файловой системы. Кроме этого, компонент ведет постоянно хранимый реестр всех угроз, обнаруженных в файловой системе, и выполняет функцию менеджера карантина, управляя содержимым каталогов, в которых располагаются изолированные файлы.

9.8.1. Принципы работы

Компонент Dr.Web File Checker запускается с правами суперпользователя (пользователя *root*) и используется для сканирования объектов файловой системы (файлы, каталоги и загрузочные записи).

Dr.Web File Checker индексирует все проверенные файлы и каталоги и сохраняет данные о проверенных объектах в специальном кеше, чтобы не выполнять повторную проверку объектов, которые уже были проверены ранее и не изменялись с момента последней проверки (в этом случае, если заявка о проверке такого объекта поступает повторно, возвращается результат его предыдущей проверки, извлеченный из кеша).

При поступлении запросов на проверку объектов файловой системы от других компонентов Dr.Web File Checker проверяет, требуется ли проверка запрошенного объекта, и если да, то формирует задание на проверку его содержимого для сканирующего ядра Dr.Web Scanning Engine. Если проверенный объект содержит угрозу, то Dr.Web File Checker заносит его в реестр обнаруженных угроз и применяет к нему нейтрализующее действие (лечение, удаление или перемещение в карантин), если это действие задано клиентским компонентом, инициировавшим проверку, в качестве реакции на угрозу. В качестве инициаторов проверки могут выступать различные компоненты Dr.Web Gateway Security Suite.

В процессе проверки запрошенных объектов файловой системы компонент проверки файлов формирует и отправляет компоненту-клиенту, запросившему проверку, отчеты о результатах проверки и предпринятых действиях по нейтрализации угроз, если они были обнаружены.

Помимо стандартного метода проверки файлов, для внутренних нужд поддерживаются специальные методы проверки файлов:

- *Метод «flow»* — метод потоковой проверки файлов. Компонент, использующий этот метод, один раз инициализирует параметры проверки и обезвреживания угроз, и далее эти параметры будут применяться ко всему потоку заявок на проверку файлов, поступающих от этого компонента.
- *Метод «proxy»* — метод проверки файлов, заключающийся в том, что компонент проверки файлов выполняет только проверку файлов на наличие угроз, не применяя к ним никаких действий, в том числе не выполняя регистрацию обнаруженных угроз

(эти действия целиком возлагаются на компонент, инициировавший проверку). Этот метод проверки используется компонентом Dr.Web ClamD.

Файлы можно проверить методом *«flow»*, используя команду `flowscan` утилиты Dr.Web Ctl (запускается командой `drweb-ctl`), однако для обычной проверки файлов по требованию рекомендуется использовать команду `scan`.

В процессе своей работы компонент проверки файлов не только ведет реестр угроз и управляет карантином, но и собирает общую статистику проверки файлов, усредняя количество файлов, проверенных в течение секунды за последнюю минуту, последние 5 минут, последние 15 минут.

9.8.2. Аргументы командной строки

Для запуска компонента Dr.Web File Checker из командной строки используется следующая команда:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-filecheck [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-filecheck [<параметры>]
```

Dr.Web File Checker допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-filecheck --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web File Checker.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Он запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при поступлении от других компонентов Dr.Web Gateway Security Suite заявок на проверку объектов файловой системы. Для управления параметрами работы компонента, а также для проверки файлов по требованию используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Gateway Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для проверки произвольного файла или каталога компонентом Dr.Web File Checker вы можете воспользоваться командой `scan` утилиты Dr.Web Ctl:

```
$ drweb-ctl scan <путь к файлу или каталогу>
```

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-filecheck`.

9.8.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[FileCheck]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

Эта секция хранит следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-filecheck` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-filecheck`

Параметр	Описание
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`
`DebugClientIpc` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения IPC. Значение по умолчанию: `No`
`DebugScan` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения, поступающие в процессе проверки файлов. Значение по умолчанию: `No`
`DebugFlowScan` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения о проверке файлов методом *«flow»*. Значение по умолчанию: `No`
`DebugProxyScan` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения о проверке файлов методом *«proxy»*. Метод *«proxy»* обычно используется компонентом Dr.Web ClamD. Значение по умолчанию: `No`
`DebugCache` *{логический}*	Сохранять или не сохранять в журнале на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения о состоянии кеша проверенных файлов. Значение по умолчанию: `No`
`MaxCacheSize` *{размер}*	Максимальный разрешенный размер кеша для хранения информации о проверенных файлах. Если указано `0`, то кеширование отключено. Значение по умолчанию: `50mb`
`RescanInterval` *{интервал времени}*	Длительность интервала, в течение которого не производится повторная проверка содержимого файлов, информация о предыдущей проверке которых имеется в кеше (период актуальности кешированной информации). Допустимые значения: от 0 секунд (`0s`) до 1 минуты (`1m`). Если указан интервал менее `1s`, то задержка отсутствует, файл будет проверяться при любом запросе.

Параметр	Описание
	Значение по умолчанию: `1s`

9.9. Dr.Web Network Checker

Компонент сетевой проверки данных Dr.Web Network Checker предназначен для проверки в сканирующем ядре данных, полученных через сеть, а также для организации распределенной проверки файлов на наличие угроз. Он позволяет организовать соединение между набором узлов сети с установленным на них Dr.Web Gateway Security Suite с целью приема и передачи данных (например, содержимого файлов) между узлами сети для проверки этих данных. При взаимодействии узлов компонент организует автоматическое распределение задач на проверку данных (передавая и получая их по сети) на все доступные узлы сети, с которыми настроено соединение, обеспечивая балансировку их нагрузки, вызванной проверкой отправленных данных. Если соединения с удаленными узлами не настроены, компонент передает все полученные данные на проверку локальному сканирующему ядру Dr.Web Scanning Engine.

Данный компонент всегда используется для проверки данных, полученных через сетевые соединения, поэтому, если он отсутствует или недоступен, будет нарушена работоспособность компонентов, отправляющих данные на проверку через сетевое соединение (Dr.Web ClamD, SpIDer Gate, Dr.Web ICAPD).

Данный компонент не предназначен для организации распределенной проверки файлов, расположенных в локальной файловой системе, так как не может заменить компонент проверки файлов Dr.Web File Checker. Для организации распределенной проверки локальных файлов используйте компонент Dr.Web MeshD.

В случае большой интенсивности проверки данных, передаваемых через сеть, возможно возникновение проблем с проверкой из-за исчерпания числа доступных файловых дескрипторов. В этом случае необходимо увеличить лимит на число файловых дескрипторов, доступных Dr.Web Gateway Security Suite.

Обмен проверяемыми данными может производиться как по открытому каналу, так и по защищенному, с использованием SSL/TLS. При использовании защищенного соединения необходимо обеспечить узлы, обменивающиеся файлами, корректными сертификатами и ключами SSL. Для генерации ключей и сертификатов можно воспользоваться утилитой `openssl`. Пример использования утилиты `openssl` для генерации сертификатов и закрытых ключей приведен в разделе Приложение Д. Генерация сертификатов SSL.

9.9.1. Принципы работы

Компонент позволяет передать данные, не представленные в виде файлов в локальной файловой системе, на сканирование в сканирующее ядро Dr.Web Scanning Engine, расположенное на локальном или удаленном узле. С такими данными работают компоненты, отправляющие данные на проверку через сетевое соединение (SpIDer Gate, Dr.Web ICAPD, Dr.Web ClamD).

Эти компоненты всегда используют Dr.Web Network Checker (даже расположенный на локальном узле) для передачи файлов на проверку сканирующему ядру Dr.Web Scanning Engine. Поэтому, если Dr.Web Network Checker недоступен, эти компоненты *не смогут корректно функционировать*.

Кроме этого, Dr.Web Network Checker позволяет организовать соединение Dr.Web Gateway Security Suite с заданным набором узлов в сети с установленным на них Dr.Web Gateway Security Suite (или любым другим решением Dr.Web для Unix версии не ниже 10.1) для организации распределенной проверки на наличие данных, не представленных в виде файлов в локальной файловой системе. За счет этого компонент позволять создать и настроить *сканирующий кластер*, представляющий собой набор узлов сети, обменивающихся данными для проверки (на каждом узле должен быть запущен свой экземпляр агента распределенной проверки Dr.Web Network Checker). На каждом узле сети, включенном в сканирующий кластер, Dr.Web Network Checker выполняет автоматическое распределение задач на проверку данных, передавая их по сети на все доступные узлы, с которыми настроено соединение. При этом осуществляется балансировка нагрузки на узлы, вызванной проверкой данных, в зависимости от количества ресурсов, доступных на удаленных узлах. В качестве индикатора количества ресурсов, доступных для нагрузки, выступает количество дочерних сканирующих процессов, порожденных сканирующим ядром Dr.Web Scanning Engine на узле, включенном в кластер. Также оцениваются длины очередей файлов, дожидающихся проверки на каждом используемом узле.

При этом любой узел сети, включенный в сканирующий кластер, может выступать как в роли клиента сканирования, передающего данные на удаленную проверку, так и в роли сервера сканирования, принимающего с указанных узлов сети данные для проверки. При необходимости агент распределенной проверки можно настроить таким образом, чтобы узел выступал только в качестве сервера сканирования или только в качестве клиента сканирования.

Данные, принятые по сети для проверки, сохраняются в локальную файловую системы в виде временных файлов и передаются на проверку сканирующему ядру Dr.Web Scanning Engine, либо, в случае его недоступности или большой нагруженности, на другой узел сканирующего кластера.

Имеющийся в настройках компонента параметр `InternalOnly` позволяет управлять режимом работы Dr.Web Network Checker, определяя, используется ли он для включения Dr.Web Gateway Security Suite в сканирующий кластер или только для обеспечения внутренних нужд компонентов, работающих локально в составе Dr.Web Gateway Security Suite.

Вы можете создать свой собственный компонент (внешнее приложение), использующий Dr.Web Network Checker для проверки файлов (в том числе путем распределения проверки по узлам сканирующего кластера). Для этого компонент Dr.Web Network Checker предоставляет специализированный API, основанный на технологии Google Protobuf. Описание API Dr.Web Network Checker, а также примеры кода клиентского приложения, использующего Dr.Web Network Checker, поставляются в составе пакета `drweb-netcheck`.

Пример организации сканирующего кластера приведен в разделе Организация сканирующего кластера.

9.9.2. Аргументы командной строки

Чтобы запустить компонент Dr.Web Network Checker из командной строки, используйте команду:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-netcheck [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-netcheck [<параметры>]
```

Dr.Web Network Checker допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-netcheck --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web Network Checker.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Он запускается автоматически демоном управления конфигурацией Dr.Web ConfigD по мере необходимости (обычно при старте операционной системы). При этом, если в настройках компонента задано значение параметра `FixedSocket`, а параметр `InternalOnly` установлен в значение `No`, то компонент будет запущен демоном управления конфигурацией и постоянно доступен клиентам через Unix-сокет. Для управления параметрами работы компонента, а также для запуска сетевого сканирования (при наличии настроенного соединения с другими узлами сети) используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Gateway Security Suite из командной строки. Если соединение с другими узлами сети не настроено, вместо сетевого сканирования будет запущено обычное сканирование на стороне локального сканирующего ядра.

Чтобы запустить утилиту Dr.Web Ctl, используйте команду `drweb-ctl`.

Чтобы проверить произвольный файл или каталог компонентом Dr.Web Network Checker, используйте команду `netscan` утилиты Dr.Web Ctl:

```
$ drweb-ctl netscan <путь к файлу или каталогу>
```

Чтобы получить справку о компоненте из командной строки, используйте команду `man 1 drweb-netcheck`.

9.9.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[NetCheck]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`

Параметр	Описание
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-netcheck` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-netcheck`
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает работу. Если задано значение параметра `LoadBalanceAllowFrom` или `FixedSocket`, то настройка игнорируется (компонент не завершает свою работу по истечении максимального времени простоя). Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`
`FixedSocket` *{путь к файлу | адрес}*	Сокет фиксированного экземпляра агента Dr.Web Network Checker. При задании этого параметра демон управления конфигурацией Dr.Web ConfigD следит за тем, чтобы всегда имелся запущенный экземпляр агента распределенной проверки файлов, доступный клиентам через этот сокет. Возможные значения: • <*путь к файлу*> — путь к файлу локального Unix-сокета; • <*адрес*> — сетевой сокет в виде пары <*IP-адрес*>:<*порт*>.

Параметр	Описание
	Значение по умолчанию: *(не задано)*
`InternalOnly` *{логический}*	Режим работы компонента. Если задано значение `Yes`, то компонент используется только для внутренних нужд компонентов Dr.Web Gateway Security Suite: он не используется для вхождения в сканирующий кластер и для обслуживания внешних (по отношению к Dr.Web Gateway Security Suite) клиентских приложений, вне зависимости от настроек `LoadBalance*` и заданного значения параметра `FixedSocket`. Значение по умолчанию: `No`
`LoadBalanceUseSsl` *{логический}*	Использовать или не использовать SSL/TLS для соединения с другими узлами. Возможные значения: • `Yes` — использовать SSL/TLS; • `No` — не использовать SSL/TLS. Если этот параметр установлен в `Yes`, то для данного узла и для всех узлов, с которыми он взаимодействует, должны быть обязательно заданы соответствующие друг другу сертификат и закрытый ключ (параметры `LoadBalanceSslCertificate` и `LoadBalanceSslKey`). Значение по умолчанию: `No`
`LoadBalanceSslCertificate` *{путь к файлу}*	Путь к файлу сертификата SSL, используемого Dr.Web Network Checker на данном узле для взаимодействия с другими узлами через безопасное соединение SSL/TLS. ⚠ Файл сертификата и файл закрытого ключа (определяется параметром `LoadBalanceSslKey`) должны соответствовать друг другу. Значение по умолчанию: *(не задано)*
`LoadBalanceSslKey` *{путь к файлу}*	Путь к файлу закрытого ключа, используемого Dr.Web Network Checker на данном узле для взаимодействия с другими узлами через безопасное соединение SSL/TLS.

Параметр	Описание
	Файл сертификата (определяется параметром `LoadBalanceSslCertificate`) и файл закрытого ключа должны соответствовать друг другу. Значение по умолчанию: *(не задано)*
`LoadBalanceSslCa` *{путь}*	Путь к каталогу или файлу, в котором располагается перечень доверенных корневых сертификатов. Среди данных сертификатов должен находиться сертификат, удостоверяющий подлинность сертификатов, используемых агентами внутри сканирующего кластера при обмене данными через SSL/TLS. Если значение параметра не задано, то Dr.Web Network Checker, работающий на данном узле, не проверяет подлинность сертификатов взаимодействующих агентов, однако они, в зависимости от заданных для них настроек, могут проверять подлинность сертификата, используемого агентом, работающим на данном узле. Значение по умолчанию: *(не задано)*
`LoadBalanceServerSocket` *{адрес}*	Сетевой сокет (IP-адрес и порт), прослушиваемый Dr.Web Network Checker на данном узле для получения файлов на проверку от удаленных узлов (при работе в качестве сервера сетевого сканирования). Значение по умолчанию: *(не задано)*

`LoadBalanceAllowFrom`
 	
{IP-адрес}
	IP-адрес удаленного узла сети, от которого Dr.Web Network Checker на данном узле может принимать файлы на проверку (как сервер сетевого сканирования).
	
	Может иметь список значений. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).
	
	Пример: Добавить в список адреса узлов 192.168.0.1 и 10.20.30.45.
	
	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[NetCheck]`
	`LoadBalanceAllowFrom = "192.168.0.1", "10.20.30.45"`

Параметр	Описание

	• Две строки (по одному значению в строке):
	`[NetCheck]`
	`LoadBalanceAllowFrom = 192.168.0.1`
	`LoadBalanceAllowFrom = 10.20.30.45`
	2. Добавление значений через команду `drweb-ctl cfset`:
	`# drweb-ctl cfset NetCheck.LoadBalanceAllowFrom -a 192.168.0.1`
	`# drweb-ctl cfset NetCheck.LoadBalanceAllowFrom -a 10.20.30.45`
	Если параметр пуст, то удаленные файлы на проверку не принимаются (узел не работает в режиме сервера).
	Значение по умолчанию: *(не задано)*

`LoadBalanceSourceAddress` *{IP-адрес}*	IP-адрес сетевого интерфейса, используемого Dr.Web Network Checker на данном узле для передачи файлов на удаленную проверку, если узел работает как клиент сетевого сканирования, и если на узле доступно несколько сетевых интерфейсов. Если указать пустое значение, то используемый сетевой интерфейс будет автоматически выбран ядром ОС. Значение по умолчанию: *(не задано)*

`LoadBalanceTo`
{адрес}
	Сокет (IP-адрес и порт) удаленного узла, на который Dr.Web Network Checker на данном узле может отправлять файлы на удаленную проверку (как клиент сетевого сканирования).
	Может иметь список значений. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).
	Пример: Добавить в список сокеты 192.168.0.1:1234 и 10.20.30.45:5678.
	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[NetCheck]`
	`LoadBalanceTo = "192.168.0.1:1234", "10.20.30.45:5678"`

Параметр	Описание

	• Две строки (по одному значению в строке):
	`[NetCheck]`
	`LoadBalanceTo = 192.168.0.1:1234`
	`LoadBalanceTo = 10.20.30.45:5678`
	2. Добавление значений через команду `drweb-ctl cfset`:
	`# drweb-ctl cfset NetCheck.LoadBalanceTo -a 192.168.0.1:1234`
	`# drweb-ctl cfset NetCheck.LoadBalanceTo -a 10.20.30.45:5678`
	Если параметр пуст, то локальные файлы не передаются на удаленную проверку (узел не работает в режиме клиента сетевого сканирования).
	Значение по умолчанию: *(не задано)*

`LoadBalanceStatusInterval` *{интервал времени}*	Интервал времени между рассылками данным узлом информации о своей загруженности для всех агентов распределенной проверки, перечисленных в параметре `LoadBalanceAllowFrom`. Значение по умолчанию: `1s`
`SpoolDir` *{путь к каталогу}*	Каталог в локальной файловой системе, используемый для хранения файлов, принятых Dr.Web Network Checker по сети от клиентов сканирования для проверки. Значение по умолчанию: `/tmp/com.drweb.ncheck`
`LocalScanPreference` *{дробное число}*	Относительный вес (предпочтительность) узла при выборе места для проверки файла (локального или принятого по сети). Если в некоторый момент времени вес локального узла больше суммарного веса всех доступных узлов-серверов сканирования, файл будет оставлен агентом для локальной проверки. Минимальное значение: `1`. Значение по умолчанию: `1`
`LoadBalanceSslCrl` *{путь}*	Путь к каталогу или файлу с перечнем отозванных сертификатов. Если значение параметра не задано, то Dr.Web Network Checker, работающий на данном узле, не проверяет сертификаты взаимодействующих агентов на актуальность, однако они, в зависимости от заданных для

Параметр	Описание
	них настроек, могут проверять актуальность сертификата, используемого агентом, работающим на данном узле. Значение по умолчанию: *(не задано)*

9.9.4. Организация сканирующего кластера

В этом разделе

- Вводные замечания
- Пример организации сканирующего кластера
- Настройка узлов кластера
- Проверка работы кластера

Вводные замечания

Для организации сканирующего кластера, позволяющего выполнять распределенную проверку данных (при сканировании файлов или иных объектов), необходимо иметь набор узлов сети с установленным на каждом из них компонентом Dr.Web Network Checker. Чтобы узел кластера мог не только принимать и передавать данные, подлежащие проверке, необходимо, чтобы на узле также было установлено сканирующее ядро Dr.Web Scanning Engine. Таким образом, для организации узла сканирующего кластера необходимо, чтобы на сервере были установлены как минимум следующие компоненты (прочие компоненты Dr.Web Gateway Security Suite, устанавливаемые автоматически, для обеспечения работоспособности приведенных здесь компонентов, опущены):

1. Dr.Web Network Checker (пакет `drweb-netcheck`) — компонент приема и передачи данных между узлами по сети.
2. Dr.Web Scanning Engine (пакет `drweb-se`) — сканирующее ядро, необходимое для проверки данных, полученных по сети. Может отсутствовать, в этом случае узел будет только передавать данные для проверки на другие доступные узлы сканирующего кластера.

Узлы, составляющие сканирующий кластер, образуют одноранговую (*peer to peer*) сеть, т. е. каждый из них, в зависимости от того, какие настройки заданы у компонента Dr.Web Network Checker на этом узле, может выступать как в роли *клиента сканирования* (передающего данные на проверку в другие узлы), так и в роли *сервера сканирования* (принимающего данные на проверку от других узлов). При соответствующих настройках узел кластера может быть одновременно и клиентом, и сервером сканирования.

Параметры компонента Dr.Web Network Checker, отвечающие за настройку сканирующего кластера, имеют имя, начинающееся с `LoadBalance`.

Пример организации сканирующего кластера

Рассмотрим пример организации сканирующего кластера, показанного на рисунке ниже.

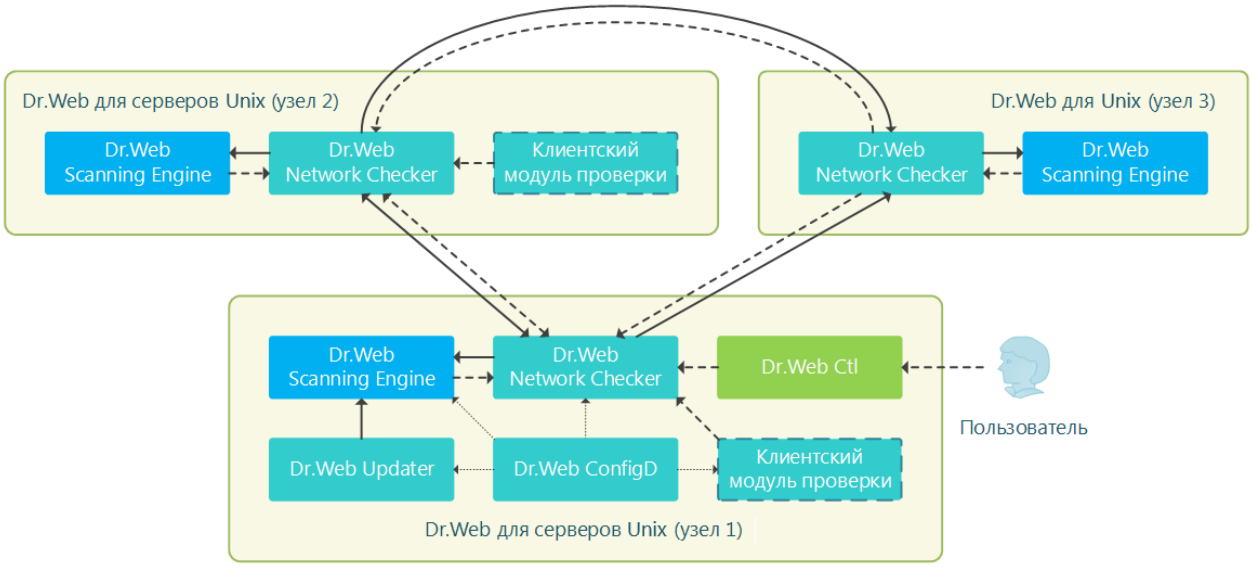

Рисунок 13. Структура сканирующего кластера

В данном случае предполагается, что кластер состоит из трех узлов, обозначенных на рисунке как *узел 1*, *узел 2* и *узел 3*. Узел 1 и узел 2 представляют собой серверы с установленным полноценным продуктом Dr.Web для серверов Unix (например, Dr.Web Gateway Security Suite или Dr.Web Mail Security Suite, тип продукта не имеет значения), а узел 3 используется только для помощи в сканировании файлов, передаваемых с узлов 1 и 2. Поэтому на нем установлен только минимально необходимый комплект компонентов (Dr.Web Network Checker и Dr.Web Scanning Engine, прочие компоненты, устанавливаемые автоматически для обеспечения работоспособности узла, такие как Dr.Web ConfigD, на схеме не обозначены). Узлы 1 и 2 могут функционировать и как серверы, и как клиенты сканирования в отношении друг друга (выполнять взаимное распределение нагрузки, связанной со сканированием), а узел 3 — только в роли сервера, принимая задания с узлов 1 и 2.

«Клиентский модуль проверки» на схеме обозначает компоненты серверов, формирующих компоненту Dr.Web Network Checker на узле задания на проверку, которые будут (в зависимости от соотношения нагрузки) распределены между локальным сканирующим ядром Dr.Web Scanning Engine и узлами-партнерами кластера, выполняющими роль серверов сканирования.

В качестве клиентского модуля проверки могут выступать только компоненты, проверяющие данные, не представленные в виде файла в локальной файловой системе. Это означает, что сканирующий кластер не может быть использован для распределенной проверки файлов монитором файловой системы SpIDer Guard и компонентом проверки файлов Dr.Web File Checker.

Настройка узлов кластера

Для настройки указанной конфигурации кластера необходимо внести изменения в настройки компонента Dr.Web Network Checker на всех трех узлах кластера. Все приведенные ниже фрагменты настроек представлены в формате `.ini` (см. описание формата файла конфигурации).

Узел 1

```
[NetCheck]
InternalOnly = No
LoadBalanceUseSsl = No
LoadBalanceServerSocket = <IP-адрес Узла 1>:<Порт Узла 1>
LoadBalanceAllowFrom = <IP-адрес Узла 2>
LoadBalanceSourceAddress = <IP-адрес Узла 1>
LoadBalanceTo = <IP-адрес Узла 2>:<Порт Узла 2>
LoadBalanceTo = <IP-адрес Узла 3>:<Порт Узла 3>
```

Узел 2

```
[NetCheck]
InternalOnly = No
LoadBalanceUseSsl = No
LoadBalanceServerSocket = <IP-адрес Узла 2>:<Порт Узла 2>
LoadBalanceAllowFrom = <IP-адрес Узла 1>
LoadBalanceSourceAddress = <IP-адрес Узла 2>
LoadBalanceTo = <IP-адрес Узла 1>:<Порт Узла 1>
LoadBalanceTo = <IP-адрес Узла 3>:<Порт Узла 3>
```

Узел 3

```
[NetCheck]
InternalOnly=No
LoadBalanceUseSsl = No
LoadBalanceServerSocket = <IP-адрес Узла 3>:<Порт Узла 3>
LoadBalanceAllowFrom = <IP-адрес Узла 1>
LoadBalanceAllowFrom = <IP-адрес Узла 2>
```

Примечания:

- Прочие (не указанные здесь) параметры Dr.Web Network Checker оставлены без изменения.
- Значения IP-адресов и номеров портов необходимо заменить на актуальные.
- Использование SSL при обмене данными между узлами в данном примере отключено. Чтобы использовать SSL, необходимо задать значение `Yes` для параметра `LoadBalanceUseSsl`, а также задать актуальные значения параметров `LoadBalanceSslCertificate`, `LoadBalanceSslKey` и `LoadBalanceSslCa`.

Проверка работы кластера

Чтобы проверить работу кластера в режиме разделения данных при сканировании, воспользуйтесь на узлах 1 и 2 командой:

```
$ drweb-ctl netscan <путь к файлу или каталогу>
```

При выполнении этой команды компонент Dr.Web Network Checker проверяет файлы из указанного каталога, распределив нагрузку по настроенным узлам кластера. Чтобы просмотреть статистику сетевой проверки на каждом из узлов, перед началом проверки запустите вывод статистики Dr.Web Network Checker командой:

```
$ drweb-ctl stat -n
```

Чтобы прервать вывод статистики, нажмите CTRL+C или Q.

9.10. Dr.Web Scanning Engine

Сканирующее ядро Dr.Web Scanning Engine предназначено для поиска вирусов и других вредоносных объектов в файлах и загрузочных записях (*MBR — Master Boot Record*, *VBR — Volume Boot Record*) дисковых устройств. Компонент выполняет загрузку в память и запуск антивирусного ядра Dr.Web Virus-Finding Engine и вирусных баз Dr.Web, используемых им для поиска угроз.

Сканирующее ядро работает в режиме демона, в качестве сервиса, принимающего от других компонентов Dr.Web Gateway Security Suite запросы на проверку объектов файловой системы на наличие угроз (это компоненты Dr.Web File Checker и Dr.Web Network Checker и, возможно, Dr.Web MeshD). При отсутствии или недоступности компонентов Dr.Web Scanning Engine и Dr.Web Virus-Finding Engine антивирусные проверки на данном узле не производятся (за исключением случаев, когда в составе Dr.Web Gateway Security Suite присутствует компонент Dr.Web MeshD, в настройках которого задано соединение с узлами локального облака, предоставляющими услугу сканирующего ядра).

9.10.1. Принципы работы

Компонент Dr.Web Scanning Engine, работающий в режиме демона, принимает от других компонентов Dr.Web Gateway Security Suite запросы на проверку объектов файловой системы (файлов, загрузочных записей на дисках) на наличие внедренных угроз, формирует очереди задач на проверку объектов и выполняет проверку запрошенных объектов, используя антивирусное ядро Dr.Web Virus-Finding Engine. Если в проверенном объекте обнаружена угроза, и в задании на проверку стоит указание выполнять лечение, сканирующее ядро пытается выполнять лечение, если это действие может быть применено к проверенному объекту.

Сканирующее ядро, антивирусное ядро Dr.Web Virus-Finding Engine и вирусные базы образуют атомарный комплекс и не могут быть разделены. Сканирующее ядро осуществляет загрузку вирусных баз и обеспечивает среду для функционирования кросс-платформенного антивирусного ядра Dr.Web Virus-Finding Engine. Обновление вирусных баз и антивирусного ядра производится компонентом обновлений Dr.Web Updater, входящим в состав Dr.Web Gateway Security Suite, но не являющимся частью сканирующего ядра. Компонент обновлений запускается демоном управления конфигурацией Dr.Web ConfigD периодически или принудительно в ответ на поступившую команду пользователя. Кроме того, если Dr.Web Gateway Security Suite функционирует в режиме централизованной защиты, то функции обновления вирусных баз и антивирусного ядра берет на себя агент централизованной защиты Dr.Web ES Agent, который взаимодействует с сервером централизованной защиты и получает обновления от него.

Dr.Web Scanning Engine может работать как под контролем демона управления конфигурацией Dr.Web ConfigD, так и автономно. В первом случае демон обеспечивает

запуск ядра и своевременное обновление вирусных баз, используемых ядром. Во втором случае запуск ядра и обновление вирусных баз возлагаются на использующее его внешнее приложение. Компоненты Dr.Web Gateway Security Suite, выполняющие запросы к сканирующему ядру на предмет проверки файлов, используют тот же программный интерфейс, что и внешние приложения.

Вы можете создать свой собственный компонент (внешнее приложение), использующий Dr.Web Scanning Engine для проверки файлов. Для этого компонент Dr.Web Scanning Engine предоставляет специализированный API, основанный на технологии Google Protobuf. Для получения описания API Dr.Web Scanning Engine, а также примеров кода клиентского приложения, использующего Dr.Web Scanning Engine, обратитесь в отдел по работе с партнерами компании «Доктор Веб» (https://partners.drweb.com/).

Поступающие задачи на сканирование автоматически распределяются по трем очередям, имеющим различный приоритет (высокий, нормальный и низкий). Очередь, в которую будет помещена задача, определяется исходя из того, какой компонент ее сформировал. Например, задачи, поступающие от мониторов файловых систем, помещаются в очереди высокого приоритета, поскольку при мониторинге важна скорость реакции на действия с объектами файловой системы. Сканирующее ядро ведет статистику своего использования, фиксируя количество поступивших задач на сканирование, а также длины очередей. В качестве показателя средней нагрузки сканирующее ядро определяет среднюю длину очередей в секунду. Этот показатель усредняется для последней минуты, последних 5 минут и последних 15 минут.

Антивирусное ядро Dr.Web Virus-Finding Engine поддерживает как сигнатурный анализ (поиск известных угроз на основе сигнатур, содержащихся в вирусных базах), так и различные технологии эвристического и поведенческого анализа, предназначенные для распознавания потенциальной опасности объекта на основе анализа последовательности содержащихся в нем машинных инструкций и других признаков исполняемого кода.

Эвристический анализ не гарантирует достоверного распознавания угроз и может допускать ошибки первого и второго рода.

- *Ошибки первого рода* — это ложные срабатывания анализатора, когда в качестве вредоносного отмечается безопасный объект.
- *Ошибки второго рода* — это ошибочное признание вредоносного объекта безопасным.

Поэтому угрозы, обнаруженные эвристическим анализом, отнесены в особую категорию «Подозрительные» (*Suspicious*).

Рекомендуется выполнять перемещение подозрительных объектов в карантин с тем, чтобы в дальнейшем, после обновления вирусных баз, проверить их методами сигнатурного анализа. Для предотвращения ошибок второго рода рекомендуется поддерживать вирусные базы в актуальном состоянии.

Антивирусное ядро Dr.Web Virus-Finding Engine позволяет осуществлять проверку и лечение как незапакованных, так и запакованных файлов и объектов, содержащихся в различных контейнерах, таких как архивы, сообщения электронной почты и т. д.

9.10.2. Аргументы командной строки

Для запуска сканирующего ядра Dr.Web Scanning Engine из командной строки используется следующая команда:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-se <сокет> [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-se <сокет> [<параметры>]
```

где обязательный аргумент *<сокет>* указывает адрес сокета, используемого Dr.Web Scanning Engine для обслуживания запросов клиентских компонентов. Может задаваться только в виде пути к файлу (сокет Unix).

Dr.Web Scanning Engine допускает использование следующих параметров:

Параметр	**Описание**
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет
Дополнительные параметры запуска (совпадают с параметрами из конфигурационного файла и замещают их при необходимости):	
`--CoreEnginePath`	Назначение: Путь к файлу библиотеки антивирусного ядра Dr.Web Virus-Finding Engine. Краткий вариант: Нет. Аргументы: *<путь к файлу>* — полный путь к файлу используемой библиотеки.
`--VirusBaseDir`	Назначение: Путь к каталогу, содержащему файлы вирусных баз. Краткий вариант: Нет.

	Аргументы: <*путь к каталогу*> — полный путь к каталогу вирусных баз.
`--TempDir`	Назначение: Путь к каталогу временных файлов. Краткий вариант: Нет. Аргументы: <*путь к каталогу*> — полный путь к каталогу временных файлов.
`--KeyPath`	Назначение: Путь к используемому ключевому файлу. Краткий вариант: Нет. Аргументы: <*путь к файлу*> — полный путь к ключевому файлу.
`--MaxForks`	Назначение: Максимальное разрешенное число дочерних процессов, которые Dr.Web Scanning Engine может породить в процессе проверки. Краткий вариант: Нет. Аргументы: <*число*> — максимальное разрешенное число дочерних процессов.
`--WatchdogInterval`	Назначение: Периодичность, с которой Dr.Web Scanning Engine проверяет работоспособность дочерних процессов, занимающихся проверкой содержимого файлов, для остановки зависших при проверке. Краткий вариант: Нет. Аргументы: <*интервал времени*> — периодичность проверки дочерних процессов.
`--AbortForkOnTimeout`	Назначение: Завершить процессы сканирования при тайм-ауте, послав им сигнал SIGABRT. Краткий вариант: Нет. Аргументы: Нет
`--ShellTrace`	Назначение: Отслеживание оболочки (вывод в журнал расширенной информации о проверке файлов ядром Dr.Web Virus-Finding Engine). Краткий вариант: Нет. Аргументы: Нет
`--LogLevel`	Назначение: Уровень подробности ведения журнала ядром Dr.Web Scanning Engine в процессе работы. Краткий вариант: Нет. Аргументы: <*уровень подробности*>. Возможные значения: • `DEBUG` — самый подробный (отладочный) уровень. Выводятся все сообщения, а также отладочная информация. • `INFO` — выводятся все сообщения. • `NOTICE` — выводятся сообщения об ошибках, предупреждения, уведомления. • `WARNING` — выводятся сообщения об ошибках и предупреждения. • `ERROR` — выводятся только сообщения об ошибках.

`--Log`	Назначение: Способ ведения журнала сообщений компонента.
	Краткий вариант: Нет.
	Аргументы: <*тип журнала*>. Возможные значения:
	• `Stderr[:ShowTimestamp]` — сообщения будут выводиться в стандартный поток ошибок *stderr*.
	Опция `ShowTimestamp` предписывает добавлять к каждому сообщению метку времени.
	• `Syslog[:`<*facility*>`]` — сообщения будут передаваться системной службе журналирования `syslog`.
	Дополнительная метка <*facility*> используется для указания типа журнала, в котором `syslog` будет сохранять сообщения.
	Возможные значения:
	o `DAEMON` — сообщения демонов;
	o `USER` — сообщения пользовательских процессов;
	o `MAIL` — сообщения почтовых программ;
	o `LOCAL0` — сообщения локальных процессов 0;
	...
	o `LOCAL7` — сообщения локальных процессов 7.
	• <*path*> — путь к файлу, в который будут сохраняться сообщения журнала.
	Примеры:
	`--Log /var/opt/drweb.com/log/se.log`
	`--Log Stderr:ShowTimestamp`
	`--Log Syslog:DAEMON`

`--ForkMemoryLimit`	Назначение: Максимальный объем оперативной памяти, выделяемый для работы экземпляра сканирующего ядра. Краткий вариант: Нет. Аргументы: <*число*> — максимальный объем оперативной памяти.
`--EngineDallocLimit`	Назначение: Максимальный объем оперативной памяти, выделяемый для хранения временных файлов. Краткий вариант: Нет. Аргументы: <*число*> — максимальный объем оперативной памяти.

Пример:

```
$ /opt/drweb.com/bin/drweb-se /tmp/drweb.ipc/.se --MaxForks=5
```

Данная команда запустит экземпляр сканирующего ядра Dr.Web Scanning Engine, заставив его создать Unix-сокет `/tmp/drweb.ipc/.se` для взаимодействия с клиентскими компонентами и порождать не более 5 сканирующих дочерних процессов при проверке файлов.

Замечания о запуске

При необходимости может быть запущено произвольное количество экземпляров сканирующего ядра Dr.Web Scanning Engine, предоставляющих сервис по проверке файлов на наличие угроз клиентским приложениям (не обязательно только компонентам Dr.Web Gateway Security Suite). При этом, если в конфигурации компонента задано значение параметра `FixedSocketPath`, то один экземпляр сканирующего ядра всегда будет автоматически запущен демоном управления конфигурацией Dr.Web ConfigD и доступен клиентам через Unix-сокет. Экземпляры сканирующего ядра, запускаемые непосредственно из командной строки, будут работать в автономном режиме, без подключения к демону управления конфигурацией, даже если он запущен. Для управления параметрами работы компонента, а также для проверки файлов по требованию используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Gateway Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для сканирования произвольного файла или каталога компонентом Dr.Web Scanning Engine используйте команду `rawscan` утилиты Dr.Web Ctl:

```
$ drweb-ctl rawscan <путь к каталогу или файлу>
```

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-se`.

9.10.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[ScanEngine]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

Эта секция хранит следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath`	Путь к исполняемому файлу компонента.

Параметр	Описание
{путь к файлу}	Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-se` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-se`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает свою работу. Если задано значение параметра `FixedSocketPath`, то настройка игнорируется (компонент не завершает свою работу по истечению максимального времени простоя). Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `1h`
`FixedSocketPath` *{путь к файлу}*	Путь к файлу Unix-сокета фиксированного экземпляра сканирующего ядра Dr.Web Scanning Engine. При задании этого параметра демон управления конфигурацией Dr.Web ConfigD следит за тем, чтобы всегда имелся запущенный экземпляр сканирующего ядра, доступный клиентам через этот сокет. Значение по умолчанию: *(не задано)*
`MaxForks` *{целое число}*	Максимальное разрешенное количество экземпляров дочерних сканирующих процессов, порождаемых сканирующим ядром Dr.Web Scanning Engine, которые одновременно могут быть запущены. Значение по умолчанию: *Автоматически определяется при старте* как удвоенное число доступных процессорных ядер, или `4`, если полученное число меньше 4.
`ForkMemoryLimit` *{целое число}*	Максимальный объем оперативной памяти, выделяемый для работы экземпляра сканирующего ядра. Значение указывается как целое число с суффиксом (*b, kb, mb, gb*). Если суффикс не указан, то значение интерпретируется как размер в байтах. Допустимые значения: от 1 гигабайта (`1GB`) до 4 гигабайт (`4GB`). Значение по умолчанию: `4GB` ⚠ Этот параметр не задействуется в 32-разрядных дистрибутивах Dr.Web Gateway Security Suite.

Параметр	Описание
`EngineDallocLimit` *{целое число}*	Максимальный объем оперативной памяти, выделяемый для хранения временных файлов. Если указанное значение меньше размера временного файла, то он будет создан на устройстве хранения, что замедлит работу Dr.Web Gateway Security Suite. Значение указывается как целое число с суффиксом (*b, kb, mb, gb*). Если суффикс не указан, то значение интерпретируется как размер в байтах. Допустимые значения: от 50 мегабайт (`50MB`) до 1 гигабайта (`1GB`). Значение по умолчанию: `500MB`
`WatchdogInterval` *{интервал времени}*	Периодичность, с которой Dr.Web Scanning Engine проверяет работоспособность порожденных им дочерних сканирующих процессов для обнаружения зависаний при проверке («сторожевой таймер»). Значение по умолчанию: `15s`
`BufferedIo` *{логическое значение}*	Использовать или не использовать буферизованный ввод-вывод при проверке файлов. Использование буферизованного ввода-вывода в ОС семейства GNU/Linux и ОС FreeBSD может увеличить скорость проверки файлов, расположенных на медленных дисковых устройствах. Возможные значения: • `On`, `Yes`, `True` — использовать буферизованный ввод-вывод; • `Off`, `No`, `False` — не использовать буферизованный ввод-вывод. Значение по умолчанию: `Off`
`AbortForkOnTimeout` *{логическое значение}*	Завершать или не завершать процессы сканирования при тайм-ауте, послав им сигнал SIGABRT. Возможные значения: • `On`, `Yes`, `True` — завершать процессы сканирования при тайм-ауте; • `Off`, `No`, `False` — не завершать процессы сканирования при тайм-ауте. Значение по умолчанию: `Off`

9.11. Dr.Web Updater

Компонент обновлений Dr.Web Updater предназначен для получения обновлений вирусных баз и антивирусного ядра Dr.Web Virus-Finding Engine с серверов обновлений компании «Доктор Веб», а также для синхронизации обновления с локальным облаком продуктов Dr.Web для Unix через компонент Dr.Web MeshD.

Если Dr.Web Gateway Security Suite работает в режиме централизованной защиты, то в качестве источника обновлений используется сервер централизованной защиты, причем все обновления получаются с сервера через Dr.Web ES Agent, а Dr.Web Updater для загрузки обновлений не используется (синхронизация обновлений с локальным облаком продуктов Dr.Web для Unix также не производится).

9.11.1. Принципы работы

Компонент подключается к серверам обновлений компании «Доктор Веб» для проверки наличия и загрузки обновлений вирусных баз и антивирусного ядра Dr.Web Virus-Finding Engine, базы категорий веб-ресурсов. Списки серверов, образующих доступную зону обновлений, хранятся в специальном файле, который подписан с целью невозможности его модификации. При подключении к серверам обновлений через прокси-сервер поддерживается только базовая и дайджест-аутентификация.

Если Dr.Web Gateway Security Suite не подключен к серверу централизованной защиты или подключен к нему в мобильном режиме, то Dr.Web Updater автоматически запускается демоном управления конфигурацией Dr.Web ConfigD с периодичностью, указанной в настройках. Также компонент может быть запущен Dr.Web ConfigD в ответ на поступившую команду пользователя (внеочередное обновление).

При наличии на серверах обновлений доступных обновлений, они загружаются в каталог `/var/opt/drweb.com/cache/` для GNU/Linux или `/var/drweb.com/cache/` для FreeBSD, после чего размещаются в рабочих каталогах Dr.Web Gateway Security Suite.

По умолчанию все обновления загружаются с зоны обновления, общей для всех продуктов Dr.Web. Перечень используемых по умолчанию серверов, входящих в зону обновления, указывается в файлах, находящихся в каталогах, указанных в параметрах `*DrlDir`, сгруппированных по типу выполняемого обновления: для вирусных баз и антивирусного ядра, для базы категорий веб-ресурсов). При необходимости по запросу клиента может быть создана особая зона обновления (для каждого вида обновления), список серверов который указывается в отдельном файле (по умолчанию с именем `custom.drl`), располагающемся в каталоге, указанном в соответствующем параметре `*CustomDrlDir`. В этом случае компонент обновлений будет загружать обновления только с этих серверов, не используя серверы из зоны по умолчанию.

Для отказа от использования особой зоны обновления достаточно очистить значение соответствующего параметра `*CustomDrlDir` в настройках компонента.

Содержимое файлов списков серверов подписано для невозможности их модификации. Если вам необходимо создать особый перечень серверов обновления, обратитесь в техническую поддержку.

Компонент может выполнять сохранение резервных копий обновляемых файлов для последующего отката обновлений по команде пользователя. Место сохранения резервных копий и глубина хранимой истории обновлений задаются в настройках компонента. Откат обновлений выполняется через утилиту управления Dr.Web Gateway Security Suite из командной строки Dr.Web Ctl (запускается командой `drweb-ctl`).

Если Dr.Web Gateway Security Suite подключен к локальному облаку продуктов Dr.Web для Unix и не работает под управлением сервера централизованной защиты, компонент Dr.Web Updater используется также для синхронизации обновлений, получаемых узлами облака, т. е. передает свежие обновления, полученные с серверов обновления, в облако, и получает свежие обновления из облака, что позволяет уменьшить суммарную нагрузку на сервера обновлений Dr.Web. Данная возможность включается и отключается в настройках компонента.

9.11.2. Аргументы командной строки

Для запуска компонента Dr.Web Updater из командной строки используется следующая команда:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-update [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-update [<параметры>]
```

Dr.Web Updater допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-update --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web Updater.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Он запускается демоном управления конфигурацией Dr.Web ConfigD автоматически, по мере необходимости. Для управления параметрами работы компонента, а также для обновления вирусных баз и антивирусного ядра по требованию пользуйтесь утилитой Dr.Web Ctl, предназначенной для управления Dr.Web Gateway Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-update`.

9.11.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[Update]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, то используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-update` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-update`

Параметр	Описание
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, по превышению которого он завершает свою работу. Компонент запускается при очередном обновлении по расписанию. По окончании обновления ждет указанный интервал времени, и, если новых запросов не поступает, то завершает свою работу до следующей попытки обновления. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал `SIGTERM`. Значение по умолчанию: `10m`
`Start` *{логический}*	Запускать или не запускать компонент при загрузке Dr.Web Gateway Security Suite. Этот параметр имеет приоритет над параметром `DwsUpdateEnabled`. Допустимые значения: • `Yes` — запускать компонент при загрузке Dr.Web Gateway Security Suite; • `No` — не запускать компонент при загрузке Dr.Web Gateway Security Suite. Значение по умолчанию: `Yes`
`UpdateInterval` *{интервал времени}*	Частота проверки наличия обновлений на серверах обновления Dr.Web, т. е. период времени, который должен пройти от предыдущей успешной попытки подключения к серверам обновления (автоматического или инициированного пользователем) до следующей попытки выполнить обновление. Значение по умолчанию: `30m`
`NetworkTimeout` *{интервал времени}*	Тайм-аут на сетевые операции компонента при выполнении обновлений с серверов Dr.Web. Используется для ожидания продолжения обновления в случае временного обрыва соединения. Если оборванное

Параметр	Описание
	сетевое соединение будет восстановлено до истечения тайм-аута, то обновление будет продолжено. Не имеет смысла указывать величину тайм-аута более `75s`, т. к. за это время соединение закроется по тайм-ауту TCP. Минимальное значение: `5s`. Значение по умолчанию: `60s`
`RetryInterval` *{интервал времени}*	Частота повторных попыток выполнить обновление с серверов обновления, если очередная попытка выполнить обновление завершилось неудачей. Допустимые значения: от 1 минуты (`1m`) до 30 минут (`30m`). Значение по умолчанию: `3m`
`MaxRetries` *{целое число}*	Количество повторных попыток выполнить обновление с серверов обновления Dr.Web (предпринимаемых через промежутки времени, указанные в параметре `RetryInterval`), если предыдущая попытка обновления закончилась неудачей. Если значение параметра — `0`, то повторные попытки выполнить неудавшееся обновление не производятся (следующее обновление будет производиться через период времени, указанный в параметре `UpdateInterval`). Значение по умолчанию: `3`
`UseHttps` *{Always | ResListOnly | Never}*	Использовать или не использовать протокол HTTPS при скачивании обновлений. Допустимые значения: • `Always` — всегда использовать протокол HTTPS при скачивании обновлений. • `ResListOnly` — использовать протокол HTTPS только при скачивании файла `.lst` со списком файлов обновления. Сами файлы обновления будут скачиваться по протоколу HTTP. • `Never` — всегда использовать протокол HTTP при скачивании обновлений. Значение по умолчанию: `ResListOnly`
`Proxy` *{строка подключения}*	Параметры подключения к прокси-серверу, который используется компонентом обновлений Dr.Web Updater для подключения к серверам обновлений Dr.Web (например, если непосредственное подключение к внешним серверам запрещено политиками безопасности сети).

Параметр	Описание

	Если значение параметра не задано, то прокси-сервер не используется.
	
	Возможные значения:
	
	<*строка подключения*> — строка подключения к прокси-серверу. Имеет следующий формат (URL):
	
	`[`<*протокол*>`://][`<*пользователь*>`:`<*пароль*>`@]`
	<*хост*>`:`<*порт*>
	
	где:
	• <*протокол*> — тип используемого протокола (в текущей версии доступен только `http`);
	• <*пользователь*> — имя пользователя для подключения к прокси-серверу;
	• <*пароль*> — пароль для подключения к прокси-серверу;
	• <*хост*> — адрес узла, на котором работает прокси-сервер (IP-адрес или имя домена, т. е. FQDN);
	• <*порт*> — используемый порт.
	
	Части URL <*протокол*> и <*пользователь*>:<*пароль*> могут отсутствовать. Адрес прокси-сервера <*хост*>:<*порт*> является обязательным.
	
	Если имя пользователя или пароль содержат символы `@`, `%` или `:`, то их следует заменить на соответствующие HEX-коды: `%40`, `%25` и `%3A` соответственно.
	
	Примеры:
	1. В файле конфигурации:
	• Подключение к прокси-серверу на узле `proxyhost.company.org` на порт `123`:
	`Proxy = proxyhost.company.org:123`
	• Подключение к прокси-серверу на узле `10.26.127.0` на порт `3336`, используя протокол HTTP, от имени пользователя `legaluser` с паролем `passw`:
	`Proxy = http://legaluser:passw@10.26.127.0:3336`
	• Подключение к прокси-серверу на узле `10.26.127.0` на порт `3336` от имени пользователя `user@company.com` с паролем `passw%123`:
	`Proxy = user%40company.com:passw%25123%3A@10.26.127.0:3336`

Параметр	Описание

	2. Задание тех же самых значений с использованием команды `drweb-ctl cfset`:
	`# drweb-ctl cfset Update.Proxy proxyhost.company.org:123`
	`# drweb-ctl cfset Update.Proxy http://legaluser:passw@10.26.127.0:3336`
	`# drweb-ctl cfset Update.Proxy user%40company.com:passw%25123%3A@10.26.127.0:3336`
	Значение по умолчанию: *(не задано)*

`ExcludedFiles`
{имя файла}
	Имя файла, который не будет обновляться компонентом обновлений Dr.Web Updater.
	Может иметь список значений. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).
	Пример: Добавить в список файлы `123.vdb` и `456.dws`.
	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[Update]`
	`ExcludedFiles = "123.vdb", "456.dws"`
	• Две строки (по одному значению в строке):
	`[Update]`
	`ExcludedFiles = 123.vdb`
	`ExcludedFiles = 456.dws`
	2. Добавление значений через команду `drweb-ctl cfset`:
	`# drweb-ctl cfset Update.ExcludedFiles -a 123.vdb`
	`# drweb-ctl cfset Update.ExcludedFiles -a 456.dws`
	Значение по умолчанию: `drweb32.lst`

`BaseUpdateEnabled` *{логический}*	Разрешить или запретить обновление вирусных баз и антивирусного ядра. Допустимые значения: • `Yes` — обновление разрешено и будет производиться; • `No` — обновление не разрешено и не будет производиться. Значение по умолчанию: `Yes`

Параметр	Описание
`BaseDrlDir` *{путь к каталогу}*	Путь к каталогу, хранящему файлы для подключения к серверам из стандартной зоны обновления, используемым для обновления вирусных баз и антивирусного ядра. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/drl/bases` • для FreeBSD: `/var/drweb.com/drl/bases`
`BaseCustomDrlDir` *{путь к каталогу}*	Путь к каталогу, хранящему файлы для подключения к серверам особой («клиентской») зоны обновления, используемым для обновления вирусных баз и антивирусного ядра. Если в каталоге, на который указывает параметр, имеется непустой подписанный файл списка серверов (файл `.drl`), то обновление ведется только с этих серверов, а серверы основной зоны (см. выше) не используются для обновления вирусных баз и антивирусного ядра. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/custom-drl/bases` • для FreeBSD: `/var/drweb.com/custom-drl/bases`
`VersionUpdateEnabled` *{логический}*	Разрешить или запретить обновление версий компонентов Dr.Web Gateway Security Suite. Допустимые значения: • `Yes` — обновление разрешено и будет производиться; • `No` — обновление не разрешено и не будет производиться. Значение по умолчанию: `Yes`
`VersionDrlDir` *{путь к каталогу}*	Путь к каталогу, хранящему файлы для подключения к серверам, используемым для обновления версий компонентов Dr.Web Gateway Security Suite. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/drl/version` • для FreeBSD: `/var/drweb.com/drl/version`
`DwsUpdateEnabled` *{логический}*	Разрешить или запретить обновление базы категорий веб-ресурсов. Допустимые значения: • `Yes` — обновление разрешено и будет производиться; • `No` — обновление не разрешено и не будет производиться. Значение по умолчанию: `Yes`

Параметр	Описание
`DwsDrlDir` *{путь к каталогу}*	Путь к каталогу, хранящему файлы для подключения к серверам стандартной зоны обновления, используемым для обновления базы категорий веб-ресурсов. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/drl/dws` • для FreeBSD: `/var/drweb.com/drl/dws`
`DwsCustomDrlDir` *{путь к каталогу}*	Путь к каталогу, хранящему файлы для подключения к серверам особой («клиентской») зоны обновления, используемым для обновления базы категорий веб-ресурсов. Если в каталоге, на который указывает параметр, имеется непустой подписанный файл списка серверов (файл `.drl`), то обновление ведется только с этих серверов, а серверы основной зоны (см. выше) не используются для обновления базы категорий веб-ресурсов. Значение по умолчанию: • для GNU/Linux: `/var/opt/drweb.com/custom-drl/dws` • для FreeBSD: `/var/drweb.com/custom-drl/dws`
`BackupDir` *{путь к каталогу}*	Путь к каталогу, в который сохраняются старые версии обновляемых файлов для возможности отката обновлений. При каждом обновлении сохраняются резервные копии только обновленных файлов. Значение по умолчанию: `/var/opt/drweb.com/backup`
`MaxBackups` *{целое число}*	Максимальное количество сохраняемых предыдущих версий обновляемых файлов. При превышении этой величины самая старая копия удаляется при очередном обновлении. Если значение параметра — `0`, то предыдущие версии файлов для восстановления не сохраняются. Значение по умолчанию: `0`

9.12. Dr.Web ES Agent

Агент централизованной защиты Dr.Web ES Agent предназначен для подключения Dr.Web Gateway Security Suite к серверу централизованной защиты.

Когда Dr.Web Gateway Security Suite подключен к серверу централизованной защиты, Dr.Web ES Agent синхронизирует лицензионный ключевой файл с ключами, хранящимися на сервере централизованной защиты. Кроме того, Dr.Web ES Agent передает на сервер централизованной защиты, к которому он подключен, статистику инцидентов, связанных с вредоносным ПО, перечень запущенных компонентов и их состояние.

Также Dr.Web ES Agent выполняет обновление вирусных баз Dr.Web Gateway Security Suite непосредственно с подключенного сервера централизованной защиты, минуя компонент обновления Dr.Web Updater.

9.12.1. Принципы работы

Компонент Dr.Web ES Agent осуществляет подключение к серверу централизованной защиты, который позволяет администратору сети реализовать на всем пространстве сети единую политику безопасности, в частности, настроить на всех рабочих станциях и серверах сети одинаковые стратегии проверки файлов и других объектов файловой системы и реакции на обнаруженные угрозы. Кроме того, сервер централизованной защиты выполняет в рамках защищаемой сети функции внутреннего сервера обновлений, играя роль хранилища актуальных вирусных баз (обновление в этом случае производится через Dr.Web ES Agent, Dr.Web Updater не используется).

При подключении Dr.Web ES Agent к серверу централизованной защиты агент обеспечивает прием от сервера актуальной версии настроек программных компонентов и лицензионного ключевого файла, которые он передает демону управления конфигурацией Dr.Web ConfigD для применения к управляемым компонентам. Кроме того, он может принимать от сервера централизованной защиты задания на проверку объектов файловой системы на рабочей станции (в том числе по расписанию).

Dr.Web ES Agent собирает и отправляет на сервер, к которому он подключен, статистику обнаружения различных угроз и примененных действий.

Для подключения Dr.Web ES Agent к серверу централизованной защиты требуется иметь пароль и идентификатор узла («рабочей станции» в терминах сервера централизованной защиты), а также файл публичного ключа шифрования, используемого сервером для подтверждения его подлинности. Вместо идентификатора станции можно указать при подключении идентификатор основной и тарифной групп, в которые станцию необходимо включить на сервере. Требуемые идентификаторы и файл публичного ключа можно получить у администратора, управляющего антивирусной защитой сети через сервер централизованной защиты.

Кроме того, к серверу централизованной защиты можно подключить защищаемый узел («рабочую станцию») в режиме «новичок», если данная возможность разрешена сервером централизованной защиты. В этом случае после того, как администратор подтвердит заявку на подключение станции, сервер централизованной защиты автоматически сгенерирует для узла новые идентификатор и пароль и отправит их агенту для использования при последующих подключениях.

9.12.2. Аргументы командной строки

Для запуска компонента Dr.Web ES Agent из командной строки используется следующая команда:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-esagent [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-esagent [<параметры>]
```

Dr.Web ES Agent допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-esagent --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web ES Agent.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически, при старте операционной системы, демоном управления конфигурацией Dr.Web ConfigD. Для управления

параметрами работы компонента, а также для подключения Dr.Web Gateway Security Suite к серверу централизованной защиты используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Gateway Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-esagent`.

9.12.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[ESAgent]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-esagent` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-esagent`
`MobileMode` *{On | Off | Auto}*	Использовать или не использовать мобильный режим Dr.Web Gateway Security Suite при подключении к серверу централизованной защиты. Допустимые значения: • `On` — использовать мобильный режим, если он разрешен сервером централизованной защиты (устанавливать обновления с серверов обновлений компании «Доктор Веб» с помощью Dr.Web Updater); • `Off` — не использовать мобильный режим, оставаться в режиме централизованной защиты (всегда получать обновления только с сервера централизованной защиты); • `Auto` — использовать мобильный режим, если он разрешен сервером централизованной защиты, а обновления устанавливать как с серверов обновлений компании «Доктор Веб» с помощью Dr.Web Updater, так и

Параметр	Описание
	с сервера централизованной защиты, в зависимости от того, какое соединение доступно и качество какого соединения лучше. Поведение данного параметра зависит от разрешений на сервере: если мобильный режим на используемом сервере не разрешен, то параметр не имеет никакого эффекта. Значение по умолчанию: `Auto`
`Discovery` *{On | Off}*	Разрешить или запретить агенту принимать *discovery*-запросы от инспектора сети, встроенного в сервер централизованной защиты (*discovery*-запросы используются инспектором для проверки структуры и состояния антивирусной сети). Допустимые значения: • `On` — разрешать агенту принимать и обрабатывать *discovery*-запросы; • `Off` — запретить агенту принимать и обрабатывать *discovery*-запросы. Данный параметр имеет приоритет над настройками сервера централизованной защиты: если указано значение `Off`, агент не будет принимать discovery-запросы, даже если эта функция включена на сервере. Значение по умолчанию: `On`
`UpdatePlatform` *{название платформы}*	Обозначение платформы, для которой агент будет получать с сервера централизованной защиты обновления для антивирусного ядра. Допустимые значения: • для GNU/Linux: `unix-linux-32`, `unix-linux-64-engine64`, `unix-linux-aarch64`, `unix-linux-e2k`, `unix-linux-e2k-engine64`, `unix-linux-mips`, `unix-linux-ppc64le`; • для FreeBSD: `unix-freebsd-32`, `unix-freebsd-64-engine64`; • для Darwin: `unix-darwin-32`, `unix-darwin-64-engine64`, `unix-darwin-aarch64`. Настоятельно не рекомендуется изменять значение параметра, если вы не уверены, что это действительно необходимо. Значение по умолчанию: *Зависит от используемой платформы*
`DebugIpc` *{логический}*	Включать или не включать в журнал на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения IPC (взаимодействие Dr.Web ES Agent и демона управления конфигурацией Dr.Web ConfigD). Значение по умолчанию: `No`

Параметр	Описание
`SrvMsgAutoremove` *{целое число}*	Срок хранения сообщений. По завершении указанного срока сообщения удаляются из базы. Допустимые значения: от 1 недели (`1w`) до 365 дней (`365d`). Значение параметра указывается в виде целого числа с суффиксом `s`, `m`, `h`, `d`, `w`. Значение по умолчанию: `1w`

9.13. Dr.Web HTTPD

Компонент Dr.Web HTTPD обеспечивает инфраструктуру для локального или удаленного взаимодействия с Dr.Web Gateway Security Suite посредством протокола HTTP (например, через веб-браузер).

Помимо управления Dr.Web Gateway Security Suite через веб-интерфейс Dr.Web, вы можете использовать непосредственно командный интерфейс (HTTP API) Dr.Web HTTPD для взаимодействия с компонентами Dr.Web Gateway Security Suite по протоколу HTTPS. Данная возможность позволяет разработать для Dr.Web Gateway Security Suite собственный управляющий интерфейс.

HTTP API Dr.Web HTTPD описан в соответствующем разделе.

При использовании защищенного соединения HTTPS необходимо обеспечить сервер Dr.Web HTTPD корректным сертификатом и закрытым ключом SSL. По умолчанию для Dr.Web HTTPD серверный сертификат и закрытый ключ SSL генерируются автоматически, в процессе установки, но при необходимости вы можете сгенерировать для сервера собственную пару сертификат/ключ. Также персональный удостоверяющий сертификат пользователя, подписанный доверенным для Dr.Web HTTPD сертификатом удостоверяющего центра, может использоваться для автоматической авторизации клиентов при обращении к Dr.Web HTTPD.

Для генерации ключей и сертификатов можно воспользоваться утилитой `openssl`. Примеры использования утилиты `openssl` для генерации сертификатов и закрытых ключей приведены в разделе Приложение Д. Генерация сертификатов SSL.

9.13.1. Принципы работы

Dr.Web HTTPD представляет собой веб-сервер, специально разработанный для управления работой Dr.Web Gateway Security Suite, позволяя тем самым не использовать для этих целей как сторонние веб-серверы (такие как Apache HTTP Server и Nginx), так и управляющие сервисы наподобие Webmin. Более того, он может работать с ними на одном узле, не препятствуя их функционированию.

Сервер Dr.Web HTTPD обслуживает запросы, поступающие по протоколам HTTP и HTTPS на сокеты, заданные в его настройках, что позволяет ему не конфликтовать с другими веб-серверами, если они также используются на этом узле. Для управления Dr.Web Gateway Security Suite используется безопасный протокол HTTPS.

Веб-интерфейс управления Dr.Web не является обязательным для функционирования Dr.Web Gateway Security Suite и может отсутствовать, поэтому соответствующий блок на схеме обведен пунктирной границей.

Компонент Dr.Web HTTPD формирует управляющие команды к демону управления конфигурацией Dr.Web ConfigD, компоненту проверки файлов Dr.Web File Checker и другим компонентам на основании команд, полученных через HTTP API.

Описание веб-интерфейса управления, использующего Dr.Web HTTPD, приведено в соответствующем разделе.

Если веб-интерфейс управления Dr.Web не включен в состав Dr.Web Gateway Security Suite, вы можете подключить к продукту любой сторонний интерфейс управления, использующий HTTP API (описан в разделе Описание HTTP API) компонента Dr.Web HTTPD.

9.13.2. Аргументы командной строки

Для запуска компонента Dr.Web HTTPD из командной строки используется следующая команда:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-httpd [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-httpd [<параметры>]
```

Dr.Web HTTPD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-httpd --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web HTTPD.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости (обычно при загрузке операционной системы). Если компонент запущен, то для управления работой компонентов Dr.Web Gateway Security Suite достаточно выполнить HTTPS-подключение к одному из адресов, обслуживающих функционирование веб-интерфейса, при помощи любого стандартного браузера. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Gateway Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-httpd`.

9.13.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[HTTPD]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-httpd` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-httpd`
`Start` *{логический}*	Запустить или остановить компонент с помощью демона конфигурации Dr.Web ConfigD.

Параметр	Описание
	Установка данного параметра в `Yes` предписывает демону управления конфигурацией немедленно запустить компонент, а установка его в значение `No` — немедленно завершить работу компонента. Значение по умолчанию: *Зависит от того, установлен ли веб-интерфейс управления*
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`

`AdminListen`
 	
{адрес, ...}
	Список сетевых сокетов (каждый сокет определяется парой *<IP-адрес>:<порт>*), прослушиваемых Dr.Web HTTPD в ожидании подключений по HTTPS от клиентов с административными полномочиями. Используется как для подключения к веб-интерфейсу управления, так и для доступа к HTTP API.
	
	Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).
	
	Пример: Добавить в список сокеты 192.168.0.1:1234 и 10.20.30.45:5678.
	
	1. Добавление значений в конфигурационный файл.
	• Два значения в одной строке:
	`[HTTPD]`
	`AdminListen = "192.168.0.1:1234", "10.20.30.45:5678"`
	• Две строки (по одному значению в строке):
	`[HTTPD]`
	`AdminListen = 192.168.0.1:1234`
	`AdminListen = 10.20.30.45:5678`
	2. Добавление значений через команду `drweb-ctl cfset`:
	`# drweb-ctl cfset HTTPD.AdminListen -a 192.168.0.1:1234`
	`# drweb-ctl cfset HTTPD.AdminListen -a 10.20.30.45:5678`
	
	Если не указано ни одного значения, то использование HTTP API и веб-интерфейса управления невозможно.

Параметр	Описание
	Значение по умолчанию: `127.0.0.1:4443`
`AdminSslCertificate` *{путь к файлу}*	Путь к файлу серверного сертификата, используемого сервером веб-интерфейса управления для взаимодействия с клиентами, подключающимися к административному сокету по протоколу HTTPS. Файл сертификата генерируется автоматически при установке компонента. ⚠ Файл сертификата и файл закрытого ключа (определяется параметром `AdminSslKey`) должны соответствовать друг другу. Значение по умолчанию: • для GNU/Linux: `/etc/opt/drweb.com/certs/serv.crt` • для FreeBSD: `/usr/local/etc/drweb.com/certs/serv.crt`
`AdminSslKey` *{путь к файлу}*	Путь к файлу закрытого ключа, используемого сервером веб-интерфейса управления для взаимодействия с клиентами, подключающимися к административному сокету по протоколу HTTPS. Файл закрытого ключа генерируется автоматически при установке компонента. ⚠ Файл сертификата (определяется параметром `AdminSslCertificate`) и файл закрытого ключа должны соответствовать друг другу. Значение по умолчанию: • для GNU/Linux: `/etc/opt/drweb.com/certs/serv.key` • для FreeBSD: `/usr/local/etc/drweb.com/certs/serv.key`
`AdminSslCA` *{путь к файлу}*	Путь к файлу сертификата доверенного центра сертификации для сертификатов, используемых клиентами, подключающимися к административному сокету по протоколу HTTPS. Если сертификат клиента подписан указанным здесь сертификатом, то для клиента не производится аутентификация указанием пары логин-пароль. Более того, этот метод аутентификации запрещается для клиентов, использующих сертификаты, подписанные этим сертификатом. Клиент, прошедший аутентификацию при помощи сертификата, всегда считается суперпользователем (*root*). Значение по умолчанию: *(не задано)*
`PublicListen` *{адрес, ...}*	Список сетевых сокетов (каждый сокет определяется парой *<IP-адрес>:<порт>*), прослушиваемых Dr.Web HTTPD в ожидании

Параметр	Описание

	подключений по HTTP от клиентов с ограниченными полномочиями.
	
	Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).
	
	Пример: Добавить в список сокеты 192.168.0.1:1234 и 10.20.30.45:5678.
	
	1. Добавление значений конфигурационный файл.
	• Два значения в одной строке:
	`[HTTPD]`
	`PublicListen = "192.168.0.1:1234",`
	`"10.20.30.45:5678"`
	• Две строки (по одному значению в строке):
	`[HTTPD]`
	`PublicListen = 192.168.0.1:1234`
	`PublicListen = 10.20.30.45:5678`
	2. Добавление значений через команду `drweb-ctl cfset`:
	`# drweb-ctl cfset HTTPD.PublicListen -a 192.168.0.1:1234`
	`# drweb-ctl cfset HTTPD.PublicListen -a 10.20.30.45:5678`
	
	Подключиться к HTTP API с полным набором команд и веб-интерфейсу управления, используя данные адреса, невозможно.
	
	Значение по умолчанию: *(не задано)*

`WebconsoleRoot` *{путь к каталогу}*	Путь к каталогу с файлами веб-интерфейса управления (аналог каталога `htdocs` для Apache HTTP Server). Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/share/drweb-httpd/webconsole` • для FreeBSD: `/usr/local/libexec/drweb.com/share/drweb-httpd/webconsole`
`HelpRoot` *{путь к каталогу}*	Путь к каталогу с файлами документации, доступной через веб-интерфейс управления. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/share/doc/html` • для FreeBSD: `/usr/local/libexec/drweb.com/share/doc/html`
`AccessLogPath` *{путь к файлу}*	Путь к журналу запросов HTTP/HTTPS, поступающих от клиентов к серверу веб-интерфейса управления.

Параметр	Описание
	Если параметр не задан, информация о запросах в журнал не сохраняется. Значение по умолчанию: *(не задано)*

9.13.4. Описание HTTP API

В этом разделе

- Общие положения
  - Формат HTTP-ответа на HTTP-запрос
  - Кодировка строк объектов JSON
  - Общие ограничения на передачу данных
- Авторизация и идентификация пользователя
  - С помощью логина и пароля (SCS)
  - Авторизация по личному сертификату
- Управление Dr.Web Gateway Security Suite
- Проверка объектов
- Управление списком угроз
- Управление карантином
- Примеры использования HTTP API

1. Общие положения

HTTP API представляет собой инструмент для интеграции Dr.Web Gateway Security Suite со сторонними приложениями через протокол HTTP (для обеспечения безопасности используется защищенный протокол HTTPS).

Для взаимодействия с API используется протокол HTTP версии 1.0. Во всех запросах используются стандартные методы протокола HTTP — `GET` и `POST`. Все данные, за исключением особо оговоренных случаев, передаются в виде JSON-объектов. При передаче JSON-объекта в теле запроса HTTP POST заголовок `Content-Type:` должен быть установлен в значение `application/json`. Для ясности примеры JSON-объектов, приведенные ниже, снабжены комментариями (начинаются с символов `//`), которые не поддерживаются форматом JSON и при вставке в код должны быть удалены.

Формат HTTP-ответа на HTTP-запрос

- В ответ на все запросы API всегда (за исключением особо оговоренных случаев) возвращает JSON-объект. В случае возникновения ошибки API возвращает JSON-объект Error.

- Если поле ответного JSON-объекта имеет тип «массив», но этот массив не содержит ни одного элемента, то в ответе сервера такое поле опускается.
- Заголовок `Content-Type:` в ответе всегда (за исключением особо оговоренных случаев) имеет значение `application/json`.
- При попытке обращения к несуществующему ресурсу в ответе возвращается JSON-объект Error, в котором поле `code` имеет значение `EC_UNEXPECTED_MESSAGE`.
- Если используется SCS (*Secure Cookie Sessions for HTTP*), то ответы содержат cookie, подтверждающие авторизацию клиента (здесь и далее — *SCS-cookie*).

Кодировка строк объектов JSON

- Строки передаются в кодировке UTF-8 (без BOM). В запросах символы вне таблицы ASCII не экранируются последовательностями типа `\uXXXX`, а передаются в кодировке UTF-8.
- В ответах объекты JSON могут содержать как символы, закодированные в UTF-8, так и экранированные последовательности `\uXXXX`.

Общие ограничения на передачу данных

- В POST-запросах, в теле которых передается JSON-объект, допустимы любые символы, разрешенные RFC 7159.
- В GET-запросах в URI могут использоваться любые символы, разрешенные RFC 1945.
- В любых других частях запроса (заголовки, тела) также могут быть использованы любые символы, разрешенные RFC 1945.

2. Авторизация и идентификация пользователя

Чтобы начать работу с API, клиент должен быть авторизован сервером. Предусмотрены два способа авторизации:

1. Использование SCS согласно RFC 6896.
2. Использование клиентских сертификатов SSL, удостоверенных сертификатом доверенного ЦС на стороне Dr.Web HTTPD. В этом случае клиент считается авторизованным как суперпользователь (используются клиентские сертификаты X.509).

При авторизации с использованием SCS SCS-cookie передаются в следующих HTTP-заголовках: `Cookie:` — в запросе, `Set-Cookie:` — в ответе.
При авторизации с использованием SSL-сертификатов SCS-cookie не требуются.

При авторизации по SCS работа с API начинается с отправки команды `login`. В случае успешного выполнения этой команды клиент получает SCS-cookie, подтверждающий авторизацию.
При авторизации с помощью клиентского сертификата выполнять команду `login` не требуется; при попытке ее выполнения будет возвращен JSON-объект Error.

2.1. С помощью логина и пароля (SCS)

Команды авторизации и идентификации клиента:

Команда API	Описание
`login`	Действие: Выполнить авторизацию клиента по указанным имени пользователя и паролю для дальнейшей работы с HTTP API. В случае успешной аутентификации возвращается SCS-cookie. URI: `/api/10.2/login` Метод HTTP: POST Входные параметры: объект AuthOptions Результат успешного исполнения: пустой объект, SCS-cookie
`logout`	Действие: Отозвать (деактивировать) выданный ранее SCS-cookie. В ответе на запрос с отозванным SCS-cookie будет возвращен объект Error с ошибкой `EC_NOT_AUTHORIZED`. URI: `/api/10.2/logout` Метод HTTP: GET Входные параметры: SCS-cookie Результат исполнения: пустой объект
`whoami`	Действие: Получить имя авторизованного пользователя. URI: `/api/10.2/whoami` Метод HTTP: GET Входные параметры: (SCS-cookie)* Результат исполнения: объект whoami, (SCS-cookie)

*) Здесь и далее SCS-cookie заключен в скобки, поскольку он необходим только при авторизации через SCS.

Команды авторизации `login` и `logout` используются только при авторизации через SCS.

Описание используемых объектов

1) `AuthOptions` — объект, содержащий логин и пароль пользователя:

```
{
 "user": <строка>, //Имя пользователя
 "password": <строка> //Пароль пользователя
}
```

Вы можете указать любого пользователя, входящего в группу администраторов (`sudoers` — в Debian и Ubuntu, `wheel` — в CentOS и Fedora, `astra-admin` — в Astra Linux, и т. п.). Если пользователь не является членом группы `sudoers`, в ответе на запрос возвращается ошибка `EC_NOT_AUTHORIZED`.

2) `whoami` — объект, содержащий имя пользователя, авторизованного для работы с HTTP API:

```
{
 "whoami":
 {
 "user": <строка> //Имя пользователя
 }
}
```

3) `Error` — объект, содержащий информацию о произошедшей ошибке:

```
{
 "error":
 {
 "code": <строка>, //Строковый код ошибки вида EC_XXX
 *"what": <строка> //Описание ошибки
 }
}
```

Символом `*` помечен необязательный параметр.

JSON-объект Error, возвращаемый командами HTTP API при ошибках обработки запросов, в поле `code` содержит не числовой код ошибки, а внутренний строковый код, использующийся компонентами Dr.Web Gateway Security Suite. Этот код представляет собой строку вида `EC_XXX`. Для уточнения числового кода и получения описания ошибки обратитесь к разделу Приложение Е. Описание известных ошибок).

2.2. Авторизация по личному сертификату

Этот способ авторизации предполагает использование личного удостоверяющего сертификата, подписанного сертификатом удостоверяющего центра, который указан в настройках Dr.Web HTTPD как доверенный. При авторизации по сертификату все запросы считаются выполняемыми от имени суперпользователя (пользователя *root*).

Чтобы авторизоваться по личному сертификату пользователя

1. Создайте личный сертификат, подписанный сертификатом удостоверяющего центра.

2. В настройках компонента Dr.Web HTTPD (параметр `AdminSslCA`) укажите путь к файлу сертификата удостоверяющего центра, которым подписан ваш личный сертификат.
3. При каждом подключении к Dr.Web HTTPD при установлении соединения используйте подписанный сертификат.

При необходимости обратитесь к информации в разделе Приложение Д. Генерация сертификатов SSL.

3. Управление Dr.Web Gateway Security Suite

Команды API для просмотра и изменения текущих значений параметров конфигурации:

Команда API	Описание
Команды управления конфигурацией	
`get_lexmap`	Действие: Получить значения параметров текущей конфигурации («лексическая карта» параметров). URI: `/api/10.2/get_lexmap` Метод HTTP: GET Входные параметры: (SCS-cookie) Результат успешного исполнения: объект LexMaps, (SCS-cookie)
`set_lexmap`	Действие: Установить или сбросить значения указанных параметров текущей конфигурации (переданных в виде «лексической карты» параметров). URI: `/api/10.2/set_lexmap` Метод HTTP: POST Входные параметры: (SCS-cookie), объект LexMap Результат успешного исполнения: объект SetOptionResult, (SCS-cookie)
Команды обновления	
`start_update`	Действие: Запустить обновление. URI: `/api/10.2/start_update` Метод HTTP: POST Входные параметры: (SCS-cookie) Результат успешного исполнения: объект StartUpdate, (SCS-cookie)

Команда API	Описание
`stop_update`	Действие: Остановить активный процесс обновления. URI: `/api/10.2/stop_update` Метод HTTP: POST Входные параметры: (SCS-cookie) Результат успешного исполнения: пустой объект, (SCS-cookie)
`baseinfo`	Действие: Просмотреть информацию о загруженных вирусных базах URI: `/api/10.2/baseinfo` Метод HTTP: GET Входные параметры: (SCS-cookie) Результат успешного исполнения: объект BaseInfoResult, содержащий объект VirusBaseInfo, (SCS-cookie)
Команды управления лицензией	
`install_license`	Действие: Установить указанный ключевой файл. URI: `/api/10.2/install_license` Метод HTTP: POST Входные параметры: (SCS-cookie), тело ключевого файла (или архива, содержащего ключевой файл) Результат успешного исполнения: пустой объект, (SCS-cookie)
Команды подключения к серверу централизованной защиты	
`esconnect`	Действие: Включить режим централизованной защиты. URI: `/api/10.2/esconnect` Метод HTTP: POST Входные параметры: (SCS-cookie), объект ESConnection Результат успешного исполнения: пустой объект, (SCS-cookie)
`esdisconnect`	Действие: Выключить режим централизованной защиты. URI: `/api/10.2/esdisconnect` Метод HTTP: POST

Команда API	Описание
	Входные параметры: (SCS-cookie) Результат успешного исполнения: пустой объект, (SCS-cookie)

Конфигурация компонентов возвращается и задается в виде так называемой *лексической карты*, то есть в виде последовательности пар «параметр»/«значение». Объект LexMaps всегда содержит три вложенных объекта LexMap, содержащих следующие лексические карты:

- *active* — активные (актуальные на текущий момент) параметры;
- *hardcoded* — значения по умолчанию (применяются для параметров, значения которых не указаны или указаны некорректно);
- *master* — карта значений параметров конфигурации, заданных клиентом для использования.

Команда `get_lexmap` всегда возвращает все три набора значений параметров конфигурации для всех компонентов, которые могут присутствовать в составе Dr.Web Gateway Security Suite, а не только тех, которые установлены и работают.

Описание используемых объектов JSON

1) `LexMaps` — объект, содержащий активную, предопределенную и определенную пользователем лексические карты параметров:

```
{
 "active": <LexMap>, //Активные значения параметров конфигурации
 "hardcoded": <LexMap>, //Предопределенные значения параметров
конфигурации
 "master": <LexMap> //Значения параметров конфигурации, заданные
пользователем
}
```

   Каждое из указанных полей является объектом LexMap, который, в свою очередь, содержит массив объектов типа LexOption.

2) `LexMap` — объект, содержащий лексическую карту параметров:

```
{
 "option": [<LexOption>] //Массив опций конфигурации
}
```

3) `LexOption` — объект, содержащий параметр или секцию конфигурации (группу параметров):

```
{
 "key": <строка>, //Имя опции (параметра конфигурации или секции)
 *"value": <LexValue>, //Если данная опция является параметром
 *"map": <LexMap> //Если данная опция является секцией
}
```

Символом `*` помечены необязательные параметры.

Объект LexOption представляет собой секцию или параметр конфигурации Dr.Web Gateway Security Suite. Он обязательно содержит поле `key`, соответствующее имени секции или параметра, а также либо поле `value` (если объект — это параметр), либо поле `map` (если это секция). Секция также представляет собой объект типа LexMap, а значение параметра — объект LexValue, содержащий поле `item`, описывающее значение параметра в строковом виде.

4) `LexValue` — объект, содержащий массив значений параметра:

```
{
 "item": [<строка>] //Массив значений параметра
}
```

Команда `set_lexmap` принимает на вход объект LexMap, который должен содержать те параметры, значения которых необходимо заменить на новые или сбросить в значения по умолчанию. Параметры, которые следует сбросить в значения по умолчанию, не должны содержать поля `value`. Параметры, не упомянутые в лексической карте, переданной команде `set_lexmap`, останутся без изменений. В результате исполнения команда `set_lexmap` возвращает объект SetOptionResult, содержащий измененные значения каждого из указанных в команде параметров.

5) `SetOptionResult` — объект, поле `item` которого содержит массив с измененными значениями параметров:

```
{
 "item": [<SetOptionResultItem>] //Массив результатов
}
```

Объект содержит массив объектов SetOptionResultItem, которые содержат измененные значения каждого из указанных в команде параметров.

6) `SetOptionResultItem` — объект, содержащий информацию об изменении значения параметра:

```
{
 "option": <строка>, //Имя параметра
 "result": <строка>, //Результат изменения значения (код ошибки)
 *"lower_limit": <строка>, //Нижняя допустимая граница значений
 *"upper_limit": <строка> //Верхняя допустимая граница значений
}
```

Символом `*` помечены необязательные параметры.

Поле `option` содержит в себе имя параметра, к которому применялось действие, а `result` — результат попытки изменить его значение. Если новое значение было успешно применено, поле имеет значение `EC_OK`. В случае ошибки в объекте могут присутствовать поля `lower_limit` и `upper_limit`, содержащие наибольшее и наименьшее допустимые значения параметра.

7) `StartUpdate` — объект, содержащий информацию о начатом процессе обновления:

```
{
 "start_update":
  {
    "attempt_id": <число> //Идентификатор запущенного процесса обновления
  }
}
```

8) `ESConnection` — объект, содержащий информацию о подключении к серверу централизованной защиты:

```
{
 *"server": <строка>, //<Адрес узла>:<порт> (без префикса http/https)
 "certificate": <строка>, //Ключ сервера в base64
 *"newbie": <булево значение>, //По умолчанию: false
 *"login": <строка>, //Имя пользователя
 *"password": <строка> //Пароль
}
```

Символом `*` помечены необязательные параметры.

Параметры `login` и `password` указываются, если `newbie = true`.
Перед подключением скачайте с сервера централизованной защиты файл сертификата и выполните команду:

```
$ cat certificate.pem | base64
```

Строку, полученную в результате выполнения этой команды, и нужно использовать в качестве значения параметра `certificate`.

9) `BaseInfoResult` — объект, содержащий информацию о загруженных вирусных базах:

```
{
 "vdb_base_stamp": <число>, //Временная метка базы
 "vdb_bases": [<VirusBaseInfo>] //Детальная информация о базе
}
```

10) `VirusBaseInfo` — объект, содержащий подробную информацию о вирусной базе:

```
{
  "path": <строка>, //Путь до файла базы
  "virus_records": <число>, //Количество записей в базе
  "version": <число>, //Версия базы
  "timestamp": <число>, //Временная метка базы
  "md5": <строка>, //MD5-хеш базы
```

```
  "load_result": <строка>, //Результат загрузки базы (в случае успешной
загрузки — EC_OK)
  *"sha1": <строка> //SHA1-хеш базы
}
```

Символом * помечен необязательный параметр.

4. Проверка объектов

Команды API для проверки объектов:

Команда API	Описание
Проверка данных (используется вызов компонента Dr.Web Network Checker)	
scan_request	Действие: Запрос на создание подключения (*endpoint*) для проверки данных с необходимыми параметрами. URI: /api/10.2/scan_request Метод HTTP: POST Входные параметры: (SCS-cookie), объект ScanOptions Результат успешного исполнения: объект ScanEndpoint, (SCS-cookie)
scan_endpoint	Действие: Запуск проверки данных (например, тела файла) на созданном подключении *endpoint*. URI: /api/10.2/scan_endpoint/<*endpoint*> Метод HTTP: POST Входные параметры: (SCS-cookie), проверяемые данные Результат успешного исполнения: объект ScanResult, (SCS-cookie)
scan_path	Действие: Сканирование файла или каталога, расположенного по указанному пути. URI: /api/10.2/scan_path Метод HTTP: POST Входные параметры: (SCS-cookie), объект ScanPathOptions Результат успешного исполнения: объект ScanPathResult, (SCS-cookie)
scan_stat	Действие: Получение статистики сканирования. URI: /api/10.2/scan_stat

Команда API	Описание
	Метод HTTP: GET Входные параметры: (SCS-cookie), формат статистики (JSON или CSV) Результат успешного исполнения: объект ScanStat (если выбран формат JSON), (SCS-cookie) Если выбран формат CSV, в ответ на запрос будет возвращена таблица, столбцы которой соответствуют полям объекта ScanStat.

Описание используемых объектов JSON

1) `ScanOptions` — объект, содержащий параметры, используемые при создании *endpoint* для проверки файлов:

```
{
 "scan_timeout_ms": <число>, //Тайм-аут на проверку файла в мс
 "cure": <булево значение>, //Применять ли лечение к инфицированному файлу
 "heuristic_analysis": <булево значение>, //Использовать ли эвристический
анализ
 "packer_max_level": <число>, //Максимальный уровень вложенности для
запакованных объектов
 "archive_max_level": <число>, //Максимальный уровень вложенности для
архивов
 "mail_max_level": <число>, //Максимальный уровень вложенности для
почтовых объектов
 "container_max_level": <число>, //Максимальный уровень вложенности для
прочих сложных объектов (контейнеров)
 "max_compression_ratio": <число>, //Максимальная величина коэффициента
сжатия архивов
 "min_size_to_scan": <число>, //Минимальный размер объекта для
сканирования
 "max_size_to_scan": <число>, //Максимальный размер объекта для
сканирования
 "threat_hash": <булево значение> //Получать ли хеши обнаруженных угроз
}
```

2) `ScanPathOptions` — объект, содержащий параметры сканирования файла или каталога по указанному пути:

```
{
 "path": <строка>, //Абсолютный путь файла или каталога для сканирования
 *"exclude_path": [<строка>], //Список путей, исключенных из сканирования
(можно использовать маски)
 *"scan_timeout_ms": <число>, //Тайм-аут сканирования одного объекта
 *"archive_max_level": <число>, //Максимальный уровень вложенности для
архивных объектов
 *"packer_max_level": <число>, //Максимальный уровень вложенности для
запакованных объектов
```

```
 *"mail_max_level": <число>, //Максимальный уровень вложенности для
почтовых сообщений
 *"container_max_level": <число>, //Максимальный уровень вложенности для
прочих сложных объектов (контейнеров)
 *"max_compression_ratio": <число>, //Максимальная величина коэффициента
сжатия архивов
 *"heuristic_analysis": <булево значение>, //Использовать ли эвристический
анализ (по умолчанию true)
 *"follow_symlinks": <булево значение>, //Переходить ли по символическим
ссылкам
 *"min_size_to_scan": <число>, //Минимальный размер объекта для
сканирования
 *"max_size_to_scan": <число>, //Максимальный размер объекта для
сканирования
 *"timeout_ms": <число>, //Тайм-аут сканирования всех объектов
 *"threat_hash": <булево значение> //Возвращать ли SHA1- и SHA256-хеши угроз
}
```

Символом * помечены необязательные параметры.

3) ScanPathResult — объект, содержащий результаты сканирования файла или каталога по указанному пути:

```
{
  //ScanPathResult:
  "results": [<ScanResult>], //Результаты сканирования
  *"error": <строка> //Ошибка, если процесс завершился с ошибкой
(например, по тайм-ауту)
}
```

Символом * помечен необязательный параметр.

Если сканирование завершено успешно, строка error будет отсутствовать в ответе.

4) ScanResult — объект, содержащий результаты сканирования:

```
{
 //ScanResult:
 "scan_report": <ScanReport>, //Отчет о сканировании
 *"sha1": <строка>, //Хеш SHA1 угрозы
 *"sha256": <строка> //Хеш SHA256 угрозы
}
```

Символом * помечены необязательные параметры.

5) ScanReport — объект, содержащий информацию о файле с обнаруженной угрозой:

```
{
 //ScanReport:
 "object": <строка>, //Строка, имя просканированного объекта
     // Для файла: абсолютный путь, для вложенного объекта — имя файла
     // Для вызова scan_endpoint будет всегда указывать на временный файл
 *"size": <число>, //Размер объекта
 *"compressed_size": <число>, //Размер объекта в сжатом состоянии
```

```
 *"core_fingerprint": <строка>, //Отпечаток движка
 *"packer": [<строка>], //Список упаковщиков, которыми был запакован
объект
 *"compression_ratio": <число>, //Коэффициент сжатия архива
 *"archive": <Archive>, //Сведения о типе архива (контейнера), если объект
распознан как таковой
 *"virus": [<Virus>], //Угрозы, обнаруженные в объекте (если найдены)
 *"item": [<ScanReport>], //Отчеты о сканировании вложенных объектов (если
они были)
 *"error": <строка>, //Ошибка сканирования (если возникла)
 *"heuristic_analysis": <булево значение>, //Использовался ли эвристический
анализ (true — использовался, false — нет)
 *"cured": <булево значение>, //Вылечен ли объект (true — вылечен, false —
нет)
 *"cured_by_deletion": <булево значение>, //Удален ли объект в ходе лечения
(true — удален, false — нет)
 *"new_path": <строка>, //Новый путь к объекту, переименованному в ходе
лечения
 *"user_time": <число>, //Время, проведенное в пространстве пользователя
 *"system_time": <число> //Время, проведенное в системных вызовах во время
сканирования
}
```

Символом * помечены необязательные параметры.

Поля virus и error могут отсутствовать в ответе, если в ходе сканирования не было найдено никаких угроз или не произошло никаких ошибок. Для вызова scan_endpoint поле scan_endpoint всегда указывает на временный файл, созданный компонентом Dr.Web Network Checker в локальной файловой системе сервера (в этот файл помещаются данные для проверки, отправленные в теле запроса scan_endpoint).

6) ScanEndpoint — объект, содержащий информацию о созданном *endpoint* для проверки файлов:

```
{
 "endpoint": <строка> //Уникальный идентификатор созданного endpoint
}
```

Возвращенный в теле объекта идентификатор endpoint используется для запуска проверки файла командой scan_endpoint (как часть URI).

7) VirusInfo — объект, содержащий информацию об обнаруженной угрозе:

```
{
 "type": <строка>, //Тип выявленной угрозы
 "name": <строка>  //Название угрозы
}
```

Поле type (тип угрозы) — строка вида SE_XXX:

- SE_KNOWN_VIRUS — известная угроза,
- SE_VIRUS_MODIFICATION — модификация известной угрозы,

- SE_UNKNOWN_VIRUS — неизвестная угроза (подозрительный объект),
- SE_ADWARE — рекламная программа,
- SE_DIALER — программа автодозвона,
- SE_JOKE — программа-шутка,
- SE_RISKWARE — потенциально опасное ПО,
- SE_HACKTOOL — программа взлома.

8) Archive — объект, содержащий информацию об архиве, запакованных объектах, почтовых сообщениях и других контейнерах:

```
{
 "type": <строка> //Тип архива, может принимать одно из значений:
         "SE_ARCHIVE" //Архив
         "SE_MAIL" //Письмо
         "SE_CONTAINER" //Другой тип контейнера
,"name": <строка> //Формат архива
}
```

9) ScanStat — объект, содержащий статистику проверок:

```
{
 "origin": <строка>, //Приложение, по запросу которого было выполнено
сканирование
 // Счетчики зараженных объектов:
 "known_virus": <число>, //Количество зараженных известными угрозами
объектов
 "virus_modification": <число>, //Количество объектов, зараженных
модификацией известной угрозы
 "unknown_virus": <число>, //Количество зараженных неизвестными угрозами
объектов
 "adware": <число>, //Количество объектов с SE_ADWARE
 "dialer": <число>, //Количество объектов с SE_DIALER
 "joke": <число>, //Количество объектов с SE_JOKE
 "riskware": <число>, //Количество объектов с SE_RISKWARE
 "hacktool": <число>, //Количество объектов с SE_HACKTOOL
 "cured": <число>, //Количество вылеченных объектов
 "quarantined": <число>, //Количество объектов, помещенных в карантин
 "deleted": <число> //Количество удаленных объектов
}
```

5. Управление списком угроз

Для управления списком угроз, обнаруженных при сканировании, доступны следующие команды HTTP API:

Команда API	Описание
threats	Действие: Получить перечень идентификаторов всех обнаруженных угроз.

Команда API	Описание
	URI: `/api/10.2/threats/` Метод HTTP: GET Входные параметры: (SCS-cookie) Результат успешного исполнения: массив идентификаторов угроз
`threat_info`	Действие: Получить информацию об угрозе с идентификатором <*threat ID*>. URI: `/api/10.2/threat_info/`<*threat ID*> Метод HTTP: GET Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), объект FileThreat
`cure_threat`	Действие: Попытаться вылечить угрозу с идентификатором <*threat ID*>. URI: `/api/10.2/cure_threat/`<*threat ID*> Метод HTTP: POST Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), пустой объект
`delete_threat`	Действие: Удалить файл, содержащий угрозу с идентификатором <*threat ID*>. URI: `/api/10.2/delete_threat/`<*threat ID*> Метод HTTP: POST Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), пустой объект
`ignore_threat`	Действие: Проигнорировать угрозу с идентификатором <*threat ID*>. URI: `/api/10.2/ignore_threat/`<*threat ID*> Метод HTTP: POST Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), пустой объект
`quarantine_threat`	Действие: Переместить в карантин угрозу с идентификатором <*threat ID*>.

Команда API	Описание
	URI: `/api/10.2/quarantine_threat/<threat ID>` Метод HTTP: POST Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), пустой объект

У каждой найденной угрозы имеется уникальный целочисленный идентификатор *<threat ID>*. Список идентификаторов всех обнаруженных угроз возвращается командой `threats`. В командах `threat_info`, `cure_threat`, `delete_threat`, `ignore_threat` и `quarantine_threat` можно использовать только идентификаторы угроз из этого списка.

Всю информацию об отдельной угрозе из списка, включая историю действий с ней, возвращает запрос `threat_info` в виде объекта FileThreat.

Описание используемых объектов JSON

1) `FileThreat` — объект, содержащий в себе следующую информацию:

```
{
 "threat_id": <число>, //Идентификатор угрозы
 "detection_time": <Unix-время>, //Дата и время обнаружения угрозы
 "report": <ScanReport>, //Отчет о проверке файла
 "stat": <FileStat>, //Информация о файле
 "origin": <строка>, //Имя компонента, обнаружившего угрозу
 "origin_pid": <число>, //PID компонента, обнаружившего угрозу
 "task_id": <число>, //Идентификатор задачи на проверку в сканирующем ядре
 "history": [<ActionResult>] //История действий с угрозой (массив)
}
```

Поле `report` содержит объект ScanReport; поле `stat` — объект FileStat, а поле `history` — массив объектов ActionResult (история действий по отношению к файлу).

2) `ScanReport` — объект, содержащий информацию о файле с обнаруженной угрозой:

```
{
 "object": <строка>, //Объект файловой системы с угрозой
 "size": <число>, //Размер файла с угрозой в байтах
 "virus": [<VirusInfo>], //Перечень сведений об обнаруженных угрозах
 *"error": <строка>, //Сообщение об ошибке
 "heuristic_analysis": <булево значение> //Использовался ли эвристический
анализ (true – использовался, false – нет)
}
```

Символом * помечен необязательный параметр.

Поле `virus` представляет собой массив объектов VirusInfo, содержащих информацию обо всех обнаруженных угрозах. Поле `error` присутствует, только если произошла ошибка.

3) `FileStat` — объект, содержащий статистическую информацию о файле:

```
{
 "dev": <число>, //Устройство
 "ino": <число>, //Индексный дескриптор (inode)
 *"size": <число>, //Размер файла
 *"uid": <User>, //Идентификатор пользователя-владельца
 *"gid": <Group>, //Идентификатор группы владельцев
 *"mode": <число>, //Режим доступа к файлу
 *"mtime": <Unix-время>, //Дата и время модификации файла
 *"ctime": <Unix-время>, //Дата и время создания файла
 *"rsrc_size": <число>,
 *"finder_info": <строка>,
 *"ext_finder_info": <строка>,
 *"uchg": <строка>,
 *"volume_name": <строка>, //Имя тома
 *"volume_root": <строка>, //Корень (точка монтирования) тома
 *"xattr": [<Xattr>] //Расширенная информация о файле
}
```

Символом `*` помечены необязательные параметры.

Поле `xattr` представляет собой массив объектов `Xattr`. Этот объект содержит два строковых поля `name` и `value`. Поля `uid` и `gid` представляют собой объекты `User` и `Group`, хранящие информацию о пользователе-владельце и о группе владельцев соответственно. Они содержат по два поля:

- `uid` (`gid`) — числовой идентификатор пользователя (группы);
- `username` (`groupname`) — строковое имя пользователя (группы).

4) `ActionResult` — объект, содержащий информацию о действии по отношению к файлу и его результате:

```
{
 "action": <строка>, //Применяемое действие
 "action_time": <Unix-время>, //Дата и время применения
 "result": <строка>, //Результат применения
 "cure_report": <ScanReport> //Отчет о применении действия
}
```

Команды `cure_threat`, `delete_threat`, `ignore_threat` и `quarantine_threat` возвращают пустой объект в случае успешного выполнения. Если запрошенное действие с угрозой завершилось ошибкой (например, угрозу не удалось нейтрализовать), то вместо пустого объекта будет возвращен объект Error.

6. Управление карантином

Для управления содержимым карантина, хранящего угрозы, доступны следующие команды HTTP API:

Команда API	Описание
`quarantine`	Действие: Получить перечень идентификаторов объектов, помещенных в карантин. URI: `/api/10.2/quarantine/` Метод HTTP: GET Входные параметры: (SCS-cookie) Результат успешного исполнения: (SCS-cookie), массив объектов QuarantineId (объектов в карантине)
`qentry_info`	Действие: Получить информацию об изолированном в карантине объекте с идентификатором <*entry ID*>. URI: `/api/10.2/qentry_info/`<*entry ID*> Метод HTTP: GET Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), объект QEntry
`cure_qentry`	Действие: Выполнить попытку лечения объекта с идентификатором <*entry ID*>, находящегося в карантине. URI: `/api/10.2/cure_qentry/`<*entry ID*> Метод HTTP: POST Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), пустой объект
`delete_qentry`	Действие: Удалить из карантина объект с идентификатором <*entry ID*>. URI: `/api/10.2/delete_qentry/`<*entry ID*> Метод HTTP: POST Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), пустой объект

Команда API	Описание
`restore_qentry`	Действие: Восстановить (в исходное местоположение) из карантина объект с идентификатором *<entry ID>*. URI: `/api/10.2/restore_qentry/`*<entry ID>* Метод HTTP: POST Входные параметры: (SCS-cookie) Результат исполнения: (SCS-cookie), пустой объект

Команда `quarantine` возвращает массив объектов QuarantineId, в котором каждый объект содержит идентификатор объекта, находящегося в карантине. Идентификатор состоит из двух частей: `chunk_id` и `entry_id`.

Описание используемых объектов JSON

1) `QuarantineId` — объект, содержащий части составного идентификатора изолированного объекта:

```
{
 "chunk_id": <строка>,
 "entry_id": <строка>
}
```

Комбинация этих двух полей в виде *<entry_id>@<chunk_id>* представляет собой идентификатор изолированного объекта, находящегося в карантине. Этот идентификатор указывается во всех запросах на выполнение действий с любым объектом в карантине при помощи команд `qentry_info`, `cure_qentry`, `delete_qentry` и `restore_qentry`. Команда `qentry_info` используется для получения подробной информации об изолированном объекте по его идентификатору. Она возвращает объект QEntry.

2) `QEntry` — объект, содержащий информацию об изолированном объекте:

```
{
 "entry_id": <строка>, //Части идентификатора
 *"chunk_id": <строка>, //изолированного объекта
 *"quarantine_dir": <строка>, //Каталог карантина
 "restore_path": <строка>, //Путь, куда будет восстановлен объект
 "creation_time": <Unix-время>, //Дата и время помещения в карантин
 "report": <ScanReport>, //Отчет о проверке объекта (см. ScanReport выше)
 "stat": <FileStat>, //Статистическая информация о файле (см. FileStat выше)
 *"history": [<QEntryOperation>], //История манипуляций с объектом
 *"who": <RemoteUser>, //Удаленный владелец файла (если файл был изолирован
с файлового хранилища с сетевым доступом)
 *"detection_time": <Unix-время>, //Дата и время обнаружения угрозы
```

```
 *"origin": <строка> //Компонент, обнаруживший угрозу
}
```

Символом * помечены необязательные параметры.

Поле report содержит объект ScanReport, поле stat — объект FileStat, а в поле history хранится история действий по отношению к изолированному объекту. Каждая запись о действии описывается объектом QEntryOperation. Необязательное поле who содержит информацию об удаленном пользователе в виде объекта RemoteUser.

3) QEntryOperation — объект, хранящий информацию об операции по отношению к объекту в карантине:

```
{
 "action": <строка>, //Действие, применявшееся к объекту (см. обозначения
ниже)
 "action_time": <Unix-время>, //Дата и время применения действия
 "result": <строка>, //Ошибка применения действия (код вида EC_XXX)
 *"restore_path": <строка>, //Путь восстановления объекта из карантина
(если action = "QENTRY_ACTION_RESTORE")
 *"rescan_report": <ScanReport> //Отчет о повторной проверке (если action =
"QENTRY_ACTION_RESCAN")
}
```

Символом * помечены необязательные параметры.

Поле action может принимать следующие значения:

- QENTRY_ACTION_DELETE — попытка удаления объекта из карантина;
- QENTRY_ACTION_RESTORE — попытка восстановления объекта из карантина;
- QENTRY_ACTION_RESCAN — попытка повторной проверки объекта в карантине;
- QENTRY_ACTION_CURE — попытка лечения объекта в карантине.

4) RemoteUser — объект, содержащий информацию об удаленном пользователе-владельце файла (если файл был изолирован с сетевого хранилища):

```
{
 *"ip": <строка>, //IP-адрес пользователя
 *"user": <строка>, //Имя пользователя
 *"domain": <строка> //Домен пользователя
}
```

Символом * помечены необязательные параметры.

Команды cure_qentry, delete_qentry и restore_qentry возвращают пустой объект в случае успешного выполнения. Если выполнение команды завершилось ошибкой, в ответе возвращается объект Error.

7. Примеры использования HTTP API

Для проверки работы HTTP API можно воспользоваться утилитой `curl`. Структуру и формат запроса можно представить следующим образом:

```
$ curl https://<HTTPD.AdminListen>/<HTTP API URI> -k -X <метод HTTP>
 [-H 'Content-Type: application/json' --data-binary '@<файл JSON-объекта>']
 [-c <cookie-файл> [-b <cookie-файл>]] [> <файл результата>]
```

- опция `-k` указывает, что `curl` может не проверять корректность используемого SSL-сертификата;
- опция `-X` используется для указания используемого метода HTTP (GET или POST);
- опция `-H` используется для добавления заголовка `Content-Type: application/json`;
- опция `--data-binary` (или `-d`) используется для присоединения к телу запроса JSON-объекта, взятого из текстового файла;
- если для авторизации используется SCS, файлы, содержащие передаваемый и принимаемый SCS-cookie, указываются в параметрах `-b` и `-c` соответственно.

Подробную информацию об опциях утилиты `curl` можно получить с помощью команд `curl --help` и `man curl`.

1. **Авторизовать клиента** с указанием имени пользователя и пароля (для SCS).

   В файл `user.json` предварительно должен быть записан объект AuthOptions в формате JSON, например:

   `{"user":"<username>","password":"<passphrase>"}`.

   Запрос:

   ```
   $ curl https://127.0.0.1:4443/api/10.2/login -k -X POST -H 'Content-Type:
   application/json' --data-binary '@user.json' -c cookie.file
   ```

   Ответ:

   ```
   HTTP/1.0 200 OK
   Content-Type: application/json
   Content-Length: 2
   Set-Cookie:
   DWToken=6QXy4wn_JGov9A1GohWP_kvMK3dN6ccKegjNgKcmHpb_AqSrHg9cNX_yFJhxPDgr|
   MTQ2Mjg3Mzg4NQ==|cWd4Ow==|GywBUVOhU4w2LF_BKT5frg==|
   kR_rip5nrpxWjJ2dfZ7Xfmvi3rE=; Secure; HttpOnly; Max-Age: 900; Path=/
   Pragma: no-cache

   {}
   ```

Заголовок `Set-Cookie` содержит SCS-cookie, который нужно использовать во всех последующих запросах к HTTP API. В теле объекта в случае успешной аутентификации возвращается пустой объект. Если пользователь не авторизован, возвращается объект Error:

```
HTTP/1.0 403 Forbidden
Content-Type: application/json
Content-Length: 35
Pragma: no-cache

{"error":{"code":"EC_AUTH_FAILED"}}
```

2. **Получить информацию об угрозе** с *ID = 1*:

   Запрос:

```
$ curl https://127.0.0.1:4443/api/10.2/threat_info/1 -k -X GET -c
cookie.file -b cookie.file
```

   Ответ:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 574
Set-Cookie: DWToken=<…>;
 Secure; HttpOnly; Max-Age: 900; Path=/
Pragma: no-cache

{"threat_id":1,"detection_time":1462881660,
"report":{"object":"/sites/site1/eicar.com.txt","size":68,"packer":[],
"virus":[{"type":"SE_KNOWN_VIRUS","name":"EICAR Test File (NOT a
Virus!)"}],
"heuristic_analysis":true,"core_fingerprint":"0D2DD5A869DAB7AE354153A4D5F7
0F45",
"item":[],"log":[],"user_time":0,"system_time":0},"stat":
{"dev":2049,"ino":898,
"size":68,"uid":{"uid":1000,"username":"user"},"gid":
{"gid":1000,"groupname":"user"},
"mode":33204,"mtime":1441028214,"ctime":1460738554,"xattr":[]},
"origin":"APP_COMMAND_LINE_TOOL","origin_pid":2726,"task_id":1,"history":
[]}
```

3. **Переместить в карантин** угрозу с *ID = 1*:

   Запрос:

```
$ curl -v -c cookie.jar -b cookie.jar -k -X POST -H 'Content-
Type:application/json' https://127.0.0.1:4443/api/10.2/quarantine_threat/1
```

   Ответ:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 2
Set-Cookie: DWToken=<…>; Secure; HttpOnly; Max-Age: 900; Path=/
```

```
Pragma: no-cache

{}
```

4. **Просмотреть информацию об изолированном объекте**:

   Запрос:

```
$ curl -v -k -X GET -c cookie.jar -b cookie.jar
https://127.0.0.1:4443/api/10.2/qentry_info/3070d3ce-7b6e-4143-9d9f-
89ba3473a781@801:2108d
```

   Ответ:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 781
Set-Cookie: DWToken=<…>; Secure; HttpOnly; Max-Age: 900; Path=/
Pragma: no-cache

{"entry_id":"3070d3ce-7b6e-4143-9d9f-
89ba3473a781","chunk_id":"3830313A3231303864",
"quarantine_dir":"2F686F6D652F757365722F2E636F6D2E64727765622E71756172616E
74696E65",
"restore_path":"2E2E2F7473742F65696361722E636F6D2E747874","creation_time":
1462888884,
"report":{"object":"/home/user/tst/eicar.com.txt","size":68,"packer":[],
"virus":[{"type":"SE_KNOWN_VIRUS","name":"EICAR Test File (NOT a
Virus!)"}],
"heuristic_analysis":true,"core_fingerprint":"467CD4C6D423C55448B71CD5B815
2776",
"item":[],"log":[],"user_time":0,"system_time":0},"stat":
{"dev":2049,"ino":898,
"size":68,"uid":{"uid":1000,"username":"user"},"gid":
{"gid":1000,"groupname":"user"},
"mode":33204,"mtime":1441028214,"ctime":1462888421,"xattr":[]},"history":
[],
"detection_time":1462888667,"origin":"APP_COMMAND_LINE_TOOL"}
```

5. **Изменить настройки:** выключить Dr.Web CloudD.

   В файл `lexmap_ls_off.json` предварительно должен быть записан объект LexMap в формате JSON:

```
{"option":[{"key":"Root","map":{"option":
[{"key":"UseCloud","value":{"item":["no"]}}]}}]}
```

   Запрос:

```
$ curl -v -k -c cookie.jar -b cookie.jar -X POST -H 'Content-Type:
application/json' --data-binary '@lexmap_ls_off.json'
https://127.0.0.1:4443/api/10.2/set_lexmap
```

Ответ:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 58
Set-Cookie: DWToken=<…>; Secure; HttpOnly; Max-Age: 900; Path=/
Pragma: no-cache

{"item":[{"option":"Root.UseCloud","result":"EC_OK"}]}
```

6. **Изменить настройки:** включить Dr.Web CloudD.

   В файл `lexmap_ls_on.json` предварительно должен быть записан объект LexMap в формате JSON:

   ```
   {"option":[{"key":"Root","map":{"option":
   [{"key":"UseCloud","value":{"item":["yes"]}}]}}]}]}
   ```

   Запрос:

   ```
   $ curl -v -k -c cookie.jar -b cookie.jar -X POST -H 'Content-Type:
   application/json' --data-binary '@lexmap_ls_on.json'
   https://127.0.0.1:4443/api/10.2/set_lexmap
   ```

   Ответ:

   ```
   HTTP/1.0 200 OK
   Content-Type: application/json
   Content-Length: 58
   Set-Cookie: DWToken=<…>; Secure; HttpOnly; Max-Age: 900; Path=/
   Pragma: no-cache

   {"item":[{"option":"Root.UseCloud","result":"EC_OK"}]}
   ```

9.14. Dr.Web SNMPD

Dr.Web SNMPD — это SNMP-агент, предназначенный для интеграции Dr.Web Gateway Security Suite с системами мониторинга, использующими протокол SNMP. Такая интеграция позволяет отслеживать состояние работы компонентов Dr.Web Gateway Security Suite, а также собирать статистику обнаружения и нейтрализации угроз. Агент поддерживает предоставление системам мониторинга или любым SNMP-менеджерам следующей информации:

- Состояние любого компонента Dr.Web Gateway Security Suite.
- Счетчики количества обнаруженных угроз различных типов (в соответствии с классификацией Dr.Web).

Кроме того, агент может рассылать уведомления SNMP trap по факту обнаружения угроз и по факту ошибок при попытках нейтрализации обнаруженных угроз. Агент поддерживает протокол SNMP версий 2c и 3.

Описание информации, которая может быть предоставлена агентом, содержится в специально сформированном компанией «Доктор Веб» разделе MIB (*Management Information Base*). В разделе MIB, определенном для продуктов Dr.Web для Unix-подобных ОС, описывается следующая информация:

1. Форматы оповещений SNMP trap об обнаружении и нейтрализации угроз, а также об ошибках компонентов Dr.Web Gateway Security Suite.
2. Статистика работы Dr.Web Gateway Security Suite.
3. Состояние компонентов Dr.Web Gateway Security Suite.

Подробнее о данных, которые можно получить, используя протокол SNMP, см. в соответствующем разделе.

9.14.1. Принципы работы

В этом разделе

- Общие сведения
- Интеграция с системным SNMP-агентом

Общие сведения

По умолчанию компонент запускается автоматически при старте Dr.Web Gateway Security Suite. После запуска компонент формирует структуры данных в соответствии со структурой, описанной в Dr.Web SNMP MIB, и начинает ожидать поступление запросов на получение информации от внешних менеджеров SNMP. Компонент получает информацию о статусе компонентов Dr.Web Gateway Security Suite, а также уведомления

об обнаружении угроз непосредственно от демона управления конфигурацией Dr.Web ConfigD.

Обнаружение угроз сканирующим ядром может происходить при проверках файлов, производящихся по запросам от различных компонентов Dr.Web Gateway Security Suite. При обнаружении любой угрозы происходит увеличение счетчика количества обнаруженных угроз, соответствующего типу угрозы, а всем менеджерам SNMP, получающим оповещения, рассылается уведомление SNMP trap с информацией об обнаруженной угрозе.

Накопленные значения счетчиков (например, счетчиков обнаруженных угроз) не сохраняются между запусками Dr.Web SNMPD. Таким образом, при перезапуске Dr.Web SNMPD по любой причине (в том числе при общем перезапуске Dr.Web Gateway Security Suite) накопленные значения счетчиков сбрасываются в ноль.

Интеграция с системным SNMP-агентом

Для корректной работы SNMP-агента Dr.Web в случае, если на сервере уже работает основной системный SNMP-агент `snmpd` (`net-snmp`), необходимо настроить передачу SNMP-запросов по ветке MIB Dr.Web от `snmpd` к Dr.Web SNMPD. Для этого необходимо отредактировать конфигурационный файл `snmpd` (обычно `/etc/snmp/snmpd.conf` для GNU/Linux или `/etc/snmpd.config` для FreeBSD), добавив в него строку следующего вида:

```
proxy -v <версия> -c <community> <адрес>:<порт> <ветвь MIB>
```

Где:

- *<версия>* — используемая версия SNMP (2c, 3);
- *<community>* — «community string», используемая Dr.Web SNMPD;
- *<адрес>:<порт>* — сетевой сокет, прослушиваемый Dr.Web SNMPD;
- *<ветвь MIB>* — OID ветви дерева MIB, содержащей описания переменных и уведомлений SNMP (*trap*), используемых Dr.Web (этот OID равен `.1.3.6.1.4.1.29690`).

При использовании настроек SNMP-агента Dr.Web по умолчанию добавляемая строка имеет следующий вид:

```
proxy -v 2c -c public localhost:50000 .1.3.6.1.4.1.29690
```

Поскольку в этом случае порт 161 будет использоваться стандартным системным `snmpd`, то для Dr.Web SNMPD в параметре `ListenAddress` следует указать другой порт (`50000` в данном примере).

9.14.2. Аргументы командной строки

Для запуска компонента Dr.Web SNMPD из командной строки используется следующая команда:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-snmpd [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-snmpd [<параметры>]
```

Dr.Web SNMPD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-snmpd --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web SNMPD.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости (обычно при загрузке операционной системы). Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Gateway Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-snmpd`.

9.14.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[SNMPD]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, то используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-snmpd` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-snmpd`
`Start` *{логический}*	Запускать или не запускать компонент с помощью демона управления конфигурацией Dr.Web ConfigD. Если параметр имеет значение `Yes`, то демон управления конфигурацией немедленно запустит компонент, а установка его в значение `No` — немедленно завершить работу компонента. Значение по умолчанию: `No`
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`.

Параметр	Описание
	Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`SnmpVersion` *{V2c | V3}*	Используемая версия протокола SNMP (*SNMPv2c* или *SNMPv3*). Значение по умолчанию: `V2c`
`ListenAddress` *{адрес}*	Адрес (IP-адрес и порт), прослушиваемый агентом Dr.Web SNMPD в ожидании подключений от клиентов (менеджеров SNMP). Для совместной работы с `snmpd` необходимо указать порт, отличный от стандартного (`161`). Кроме того, у `snmpd` необходимо настроить проксирование. Значение по умолчанию: `127.0.0.1:161`

`TrapReceiver`
 	
{список адресов}
	Список адресов (IP-адрес и порт), на которые Dr.Web SNMPD отправляет уведомления *SNMP trap* при обнаружении угроз компонентами Dr.Web Gateway Security Suite.
	
	Может иметь список значений. Значения в списке указываются через запятую (каждое значение в кавычках). Допускается повторение параметра в секции (в этом случае все значения объединяются в единый список).
	
	Пример: Добавить в список сокеты 192.168.0.1:1234 и 10.20.30.45:5678.
	
	1. Добавление значений в файл конфигурации.
	• Два значения в одной строке:
	`[SNMPD]`
	`TrapReceiver = "192.168.0.1:1234", "10.20.30.45:5678"`
	• Две строки (по одному значению в строке):
	`[SNMPD]`
	`TrapReceiver = 192.168.0.1:1234`
	`TrapReceiver = 10.20.30.45:5678`

Параметр	Описание

	2. Добавление значений через команду `drweb-ctl cfset`:
	`# drweb-ctl cfset SNMPD.TrapReceiver -a 192.168.0.1:1234`
	`# drweb-ctl cfset SNMPD.TrapReceiver -a 10.20.30.45:5678`
	Значение по умолчанию: *(не задано)*

`V2cCommunity` *{строка}*	Строка «SNMP read community» для аутентификации менеджеров SNMP (протокол *SNMPv2c*) при доступе к переменным MIB Dr.Web для чтения. Параметр используется, если задано `SnmpVersion = V2c`. Значение по умолчанию: `public`
`V3EngineId` *{строка}*	Строка-идентификатор *Engine ID* для *SNMPv3* (согласно RFC 3411). Значение по умолчанию: `800073FA044452574542`
`V3UserName` *{строка}*	Имя пользователя для аутентификации менеджеров SNMP (протокол *SNMPv3*) для доступа к переменным MIB Dr.Web. Параметр используется, если задано `SnmpVersion = V3`. Значение по умолчанию: `noAuthUser`
`V3Auth` *{SHA(<pwd>) | MD5(<pwd>) | None}*	Метод аутентификации менеджеров SNMP (протокол *SNMPv3*) для доступа к переменным MIB Dr.Web. Возможные значения: • `SHA(<PWD>)` — используется SHA-хеш пароля (строки <*PWD*>); • `MD5(<PWD>)` — используется MD5-хеш пароля (строки <*PWD*>); • `None` — аутентификация не производится; где <*PWD*> — пароль в открытом виде (*plain text*). При задании значения параметра из командной строки, некоторые командные интерпретаторы могут потребовать экранирование скобок при помощи символа `\`. Примеры: 1. Значение параметра в файле конфигурации: `V3Auth = MD5(123456)`

Параметр	Описание
	2. Задание этого же значения из командной строки с использованием команды `drweb-ctl cfset`: `drweb-ctl cfset SNMPD.V3Auth MD5\(123456\)` Параметр используется, если задано `SnmpVersion = V3`. Значение по умолчанию: `None`

`V3Privacy`
{DES(<secret>) | AES128(<secret>) | None}
	Метод шифрования содержимого SNMP-сообщений (протокол *SNMPv3*).
	Возможные значения:
	• `DES(<secret>)` — используется алгоритм шифрования DES;
	• `AES128(<secret>)` — используется алгоритм шифрования AES128;
	• `None` — шифрование содержимого SNMP-сообщений не производится;
	где *<secret>* — секрет, разделяемый менеджером и агентом (*plain text*).
	При задании значения параметра из командной строки, некоторые командные интерпретаторы могут потребовать экранирование скобок при помощи символа `\`.
	Примеры:
	1. Значение параметра в файле конфигурации:
	`V3Privacy = AES128(supersecret)`
	2. Задание этого же значения из командной строки с использованием команды `drweb-ctl cfset`:
	`drweb-ctl cfset SNMPD.V3Privacy AES128\(supersecret\)`
	Параметр используется, если задано `SnmpVersion = V3`.
	Значение по умолчанию: `None`

9.14.4. Интеграция с системами мониторинга

В этом разделе

- Интеграция с системой мониторинга Munin
  - Подключение узла к Munin
- Интеграция с системой мониторинга Zabbix

  - Подключение узла к Zabbix
  - Настройка приема уведомлений SNMP trap для Zabbix
- Интеграция с системой мониторинга Nagios
  - Подключение узла к Nagios
  - Настройка Nagios
  - Настройка приема уведомлений SNMP trap для Nagios

SNMP-агент Dr.Web может выступать поставщиком данных для любой системы мониторинга, использующей протокол SNMP версии *2c* или *3*. Перечень данных, доступных для мониторинга, и их структура описаны в файле описания MIB Dr.Web `DRWEB-SNMPD-MIB.txt`, поставляемом совместно с Dr.Web Gateway Security Suite. Этот файл находится в каталоге `/opt/drweb.com/share/drweb-snmpd/mibs` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/mibs` для FreeBSD.

Для удобства настройки совместно с компонентом поставляются необходимые шаблоны настроек для популярных систем мониторинга Munin, Zabbix и Nagios.

Шаблоны настроек для систем мониторинга находятся в каталоге `/opt/drweb.com/share/drweb-snmpd/connectors` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/connectors` для FreeBSD.

Интеграция с системой мониторинга Munin

Система мониторинга Munin состоит из централизованного сервера (мастера) munin, собирающего статистику от клиентов munin-node, располагающихся локально на узлах, подлежащих наблюдению. Каждый клиент мониторинга по запросу от сервера собирает данные о работе наблюдаемого узла, запуская *подключаемые модули* (*plug-ins*), предоставляющие данные для передачи на сервер.

Для подключения Dr.Web SNMPD к системе мониторинга Munin в каталоге `/opt/drweb.com/share/drweb-snmpd/connectors/munin/plugins` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/connectors/munin/plugins` для FreeBSD поставляются готовые подключаемые модули сбора данных Dr.Web, используемые munin-node. Эти модули собирают данные для построения следующих графиков:

- количество обнаруженных угроз;
- статистика проверки файлов.

Указанные модули поддерживают использование протокола SNMP версий 1, 2c и 3. На основе этих шаблонных модулей можно создать любые подключаемые модули, опрашивающие состояние Dr.Web Gateway Security Suite через Dr.Web SNMPD.

В каталоге `/opt/drweb.com/share/drweb-snmpd/connectors/munin` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/connectors/munin` для FreeBSD поставляются следующие файлы.

Файл	Описание
`plugins/snmp__drweb_malware`	Подключаемый модуль `munin-node` для опроса Dr.Web SNMPD через SNMP с целью получения количества угроз, обнаруженных Dr.Web Gateway Security Suite на узле.
`plugins/snmp__drweb_filecheck`	Подключаемый модуль `munin-node` для опроса Dr.Web SNMPD через SNMP с целью получения статистики проверки файлов Dr.Web Gateway Security Suite на узле.
`plugin-conf.d/drweb.cfg`	Пример конфигурации в `munin-node` значений переменных среды исполнения подключаемых модулей Dr.Web.

Подключение узла к Munin

В данной инструкции предполагается, что система мониторинга Munin уже корректно развернута на сервере мониторинга, а на наблюдаемом узле установлены и корректно функционируют Dr.Web SNMPD (возможно, в режиме прокси совместно с snmpd) и `munin-node`.

1. Настройка на наблюдаемом узле
   - Скопируйте файлы `snmp__drweb_*` в каталог библиотек подключаемых модулей `munin-node`. Этот путь зависит от используемой ОС, например, в Debian и Ubuntu это путь `/usr/share/munin/plugins`.
   - Настройте `munin-node`, подключив к нему поставляемые подключаемые модули Dr.Web. Для этого используйте утилиту `munin-node-configure`, которая поставляется совместно с `munin-node`.

     Например, команда:

     ```
     $ munin-node-configure --shell --snmp localhost
     ```

     выведет на экран терминала список команд для создания необходимых символических ссылок на подключаемые модули. Скопируйте и выполните их в командной строке. Указанная команда предполагает, что:

     1) `munin-node` установлена на том же узле в сети, что и Dr.Web SNMPD. Если это не так, то следует указать вместо `localhost` правильный FQDN или IP-адрес наблюдаемого узла.
     2) Dr.Web SNMPD использует протокол SNMP версии 2c. Если это не так, то следует указать правильную версию протокола SNMP в вызове команды `munin-node-`

`configure`. Эта команда имеет набор ключей, которые позволяют гибко настроить подключаемые модули, в том числе указать используемую версию протокола SNMP, порт, используемый SNMP-агентом на наблюдаемом узле, строку *community string* и т. п. При необходимости воспользуйтесь справкой по команде `munin-node-configure`.

- При необходимости определите или переопределите значения параметров среды, в которой должны исполняться установленные подключаемые модули Dr.Web для `munin-node`. В качестве параметров среды используется значение *community string*, используемый SNMP-агентом порт и так далее. Эти параметры необходимо определить в файле `/etc/munin/plugin-conf.d/drweb` (создайте его при необходимости). В качестве примера данного файла используйте поставляемый файл `drweb.cfg`.
- В файле конфигурации `munin-node` (`munin-node.conf`) укажите регулярное выражение, которому должны соответствовать IP-адреса узлов сети, с которых серверам (мастерам) munin разрешено подключаться к `munin-node` на данном узле для получения значений контролируемых параметров, например:

  ```
  allow ^10\.20\.30\.40$
  ```

  В данном случае регулярное выражение разрешает получение параметров этого узла только узлу с IP-адресом `10.20.30.40`.
- Перезапустите `munin-node`, например, командой:

  ```
  # service munin-node restart
  ```

2. Настройка на сервере (мастере) Munin

   В конфигурационный файл мастера Munin (`munin.conf`), который по умолчанию хранится в каталоге `/etc` (в системах Debian и Ubuntu — `/etc/munin/munin.conf`), добавьте запись с адресом и идентификатором наблюдаемого узла:

   ```
   [<ID>;<hostname>.<domain>]
   address <host IP address>
   use_node_name yes
   ```

   где <*ID*> — отображаемый идентификатор узла; <*hostname*> — имя узла; <*domain*> — имя домена; <*host IP address*> — IP-адрес узла.

С официальной документацией по настройке системы мониторинга Munin вы можете ознакомиться по ссылке http://guide.munin-monitoring.org/en/latest.

Интеграция с системой мониторинга Zabbix

Для подключения Dr.Web SNMPD к системе мониторинга Zabbix в каталоге `/opt/drweb.com/share/drweb-snmpd/connectors/zabbix` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/connectors/zabbix` для FreeBSD поставляются следующие файлы шаблонов:

Файл	Описание
`zbx_drweb.xml`	Шаблон описания наблюдаемого узла с установленным Dr.Web Gateway Security Suite.
`snmptt.drweb.zabbix.conf`	Настройки утилиты `snmptt` — приемника уведомлений *SNMP trap*.

Шаблон описания наблюдаемого узла содержит:

- Набор описаний счетчиков («*items*», в терминологии Zabbix). По умолчанию шаблон настроен на использование протокола SNMP v2.
- Набор настроенных графиков: количество проверенных файлов и распределение обнаруженных угроз по типам.

Подключение узла к Zabbix

В данной инструкции предполагается, что система мониторинга Zabbix уже корректно развернута на сервере мониторинга, а на наблюдаемом установлен и корректно функционирует Dr.Web SNMPD (возможно, в режиме прокси совместно с `snmpd`). Кроме того, если планируется получать с наблюдаемого узла оповещения *SNMP trap* (в частности, об обнаружении Dr.Web Gateway Security Suite угроз на защищаемом сервере), на сервере мониторинга также должен быть установлен пакет `net-snmp` (используются стандартные утилиты `snmptt` и `snmptrapd`).

1. В веб-интерфейсе Zabbix на вкладке **Configuration** → **Templates** импортируйте шаблон наблюдаемого узла из файла `/opt/drweb.com/share/drweb-snmpd/connectors/zabbix/zbx_drweb.xml` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/connectors/zabbix/zbx_drweb.xml` для FreeBSD.
2. Добавьте наблюдаемый узел в список узлов (используйте ссылку **Hosts** → **Create host**). Укажите параметры узла и корректные настройки SNMP-интерфейса (должны соответствовать настройкам `drweb-snmpd` и snmpd на узле):
   - Вкладка **Host**:

     Host name: *drweb-host*

     Visible name: *DRWEB_HOST*

     Groups: выберите *Linux servers*

Snmp interfaces: нажмите **Add** и укажите IP-адрес и порт, используемый Dr.Web SNMPD (по умолчанию предполагается, что Dr.Web SNMPD работает на локальном узле, поэтому здесь указан адрес *127.0.0.1*, а в качестве порта указан стандартный порт *161*).

- Вкладка **Templates**:

  Нажмите **Add**, отметьте *DRWEB*, нажмите **Select**.

- Вкладка **Macros**:

  Macro: *{$SNMP_COMMUNITY}*

  Value: укажите *read community* для SNMP V2c (по умолчанию *public*).

  Нажмите **Save**.

Макрос *{$SNMP_COMMUNITY}* можно указать непосредственно в шаблоне узла.

По умолчанию импортированный шаблон *DRWEB* настроен на использование версии SNMP v2. Если требуется использовать другую версию SNMP, его необходимо отредактировать на соответствующей странице редактирования шаблона.

3. После привязки шаблона к наблюдаемому узлу, если настройки SNMP корректны, система мониторинга Zabbix начнет сбор данных для счетчиков (*items*), содержащихся в шаблоне. На вкладках веб-интерфейса **Monitoring** → **Latest Data** и **Monitoring** → **Graphs** будут отображаться собранные данные счетчиков.
4. Специальный элемент (*item*) *drweb-traps* служит для сбора уведомлений *SNMP trap* от Dr.Web SNMPD. Журнал полученных оповещений *SNMP trap* доступен на странице **Monitoring** → **Latest Data** → **drweb-traps** → **history**. Для сбора оповещений Zabbix использует стандартные утилиты `snmptt` и `snmptrapd` из пакета `net-snmp`. Об их настройке для получения уведомлений *SNMP trap* от Dr.Web SNMPD см. ниже.
5. В случае необходимости, вы можете настроить для добавленного наблюдаемого узла триггер, изменяющий свое состояние при получении уведомлений *SNMP trap* от Dr.Web SNMPD. Изменение состояния этого триггера можно использовать как источник событий для формирования соответствующих уведомлений. Триггер для наблюдаемого узла добавляется стандартным способом. Ниже показан пример выражения, указываемого в поле **trigger expression** для описанного триггера.

   - Для Zabbix версии *2.x*:

     ```
     ({TRIGGER.VALUE}=0 &
     {DRWEB:snmptrap[.*\.1\.3\.6\.1\.4\.1\.29690\..*].nodata(60)}=1 )|
     ({TRIGGER.VALUE}=1 &
     {DRWEB:snmptrap[.*\.1\.3\.6\.1\.4\.1\.29690\..*].nodata(60)}=0)
     ```

   - Для Zabbix версии *3.x*:

     ```
     ({TRIGGER.VALUE}=0 and {drweb-host:snmptrap[".29690."].nodata(60)}=1 )
     or
     ({TRIGGER.VALUE}=1 and {drweb-host:snmptrap[".29690."].nodata(60)}=0 )
     ```

Данный триггер срабатывает (устанавливается в значение 1), если журнал уведомлений *SNMP trap*, поступающих от Dr.Web SNMPD, был обновлен в течение минуты. Если же журнал в течение минуты не обновлялся, то триггер выключается (меняет состояние на 0).

В поле **Severity** для этого триггера рекомендуется устанавливать вид уведомления, отличный от *Not classified*, например, *Warning*.

Настройка приема уведомлений SNMP trap для Zabbix

1. На наблюдаемом узле в настройках Dr.Web SNMPD (параметр `TrapReceiver`) указывается адрес, который прослушивается `snmptrapd` на узле с Zabbix, например:

```
SNMPD.TrapReceiver = 10.20.30.40:162
```

2. В конфигурационном файле `snmptrapd` (`snmptrapd.conf`) указывается тот же адрес, а также приложение, которое будет обрабатывать полученные уведомления *SNMP trap* (в данном случае, `snmptthandler`, компонент `snmptt`):

```
snmpTrapdAddr 10.20.30.40:162
traphandle default /usr/sbin/snmptthandler
```

Чтобы `snmptt` не отклонял уведомления *SNMP trap*, отправленные Dr.Web SNMPD, как неизвестные, добавьте также в этот файл строку:

```
outputOption n
```

3. Компонент `snmptthandler` сохраняет принимаемые уведомления *SNMP trap* в файл на диске в соответствии с указанным форматом, который должен соответствовать регулярному выражению, заданному в шаблоне узла для Zabbix (элемент (*item*) *drweb-traps*). Формат сохраняемого сообщения о поступлении уведомления *SNMP trap* поставляется в файле `/opt/drweb.com/share/drweb-snmpd/connectors/zabbix/snmptt.drweb.zabbix.conf` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/connectors/zabbix/snmptt.drweb.zabbix.conf` для FreeBSD, который необходимо скопировать в каталог `/etc/snmp`.
4. Кроме этого, путь к файлам формата необходимо указать в конфигурационном файле `snmptt.ini`:

```
[TrapFiles]
# A list of snmptt.conf files (this is NOT the snmptrapd.conf file).
# The COMPLETE path and filename. Ex: '/etc/snmp/snmptt.conf'
snmptt_conf_files = <<END
/etc/snmp/snmptt.conf
/etc/snmp/snmptt.drweb.zabbix.conf
END
```

После этого, если `snmptt` запущен в режиме демона, то его надо перезапустить.

5. В конфигурационном файле сервера Zabbix (`zabbix-server.conf`) необходимо задать (или проверить наличие) следующих настроек:

```
SNMPTrapperFile=/var/log/snmptt/snmptt.log
StartSNMPTrapper=1
```

   где `/var/log/snmptt/snmptt.log` — файл журнала, в который `snmptt` записывает информацию о поступивших уведомлениях SNMP trap.

Подробнее с официальной документацией по Zabbix вы можете ознакомиться по ссылке https://www.zabbix.com/documentation/current/en.

Интеграция с системой мониторинга Nagios

Для подключения Dr.Web SNMPD к системе мониторинга Nagios в каталоге `/opt/drweb.com/share/drweb-snmpd/connectors/nagios` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-snmpd/connectors/nagios` для FreeBSD поставляются следующие файлы примеров конфигурации Nagios:

Файл	Описание
`nagiosgraph/rrdopts.conf-sample`	Пример конфигурационного файла RRD
`objects/drweb.cfg`	Конфигурационный файл, описывающий объекты *drweb*
`objects/nagiosgraph.cfg`	Конфигурационный файл компонента построения графиков Nagiosgraph, используемого Nagios
`plugins/check_drweb`	Скрипт для сбора данных от узла с Dr.Web Gateway Security Suite
`plugins/eventhandlers/submit_check_result`	Скрипт для обработки уведомлений *SNMP trap*
`snmp/snmptt.drweb.nagios.conf`	Настройки утилиты `snmptt` — приемника уведомлений *SNMP trap*

Подключение узла к Nagios

В данной инструкции предполагается, что система мониторинга Nagios уже корректно развернута на сервере мониторинга, включая настройку веб-сервера и графического средства Nagiosgraph, а на наблюдаемом узле установлен и корректно функционирует Dr.Web SNMPD (возможно, в режиме прокси совместно с snmpd). Кроме того, если планируется получать с наблюдаемого узла уведомления *SNMP trap* (в частности, об обнаружении Dr.Web Gateway Security Suite угроз на защищаемом сервере), на сервере

мониторинга также должен быть установлен пакет `net-snmp` (используются стандартные утилиты `snmptt` и `snmptrapd`).

В данном руководстве по подключению используются следующие соглашения о путях (реальные пути зависят от ОС и установки Nagios):

- <*NAGIOS_PLUGINS_DIR*> — каталог плагинов Nagios, например, `/usr/lib64/nagios/plugins`.
- <*NAGIOS_ETC_DIR*> — каталог настроек Nagios, например, `/etc/nagios`.
- <*NAGIOS_OBJECTS_DIR*> — каталог объектов Nagios, например, `/etc/nagios/objects`.
- <*NAGIOSGRAPH_DIR*> — каталог Nagiosgraph, например, `/usr/local/nagiosgraph`.
- <*NAGIOS_PERFDATA_LOG*> — файл, в который Nagios записывает результаты выполнения команд проверки сервисов (должен совпадать с файлом `perflog` из <*NAGIOSGRAPH_DIR*>`/etc/nagiosgraph.conf`). Записи из этого файла считываются скриптом <*NAGIOSGRAPH_DIR*>`/bin/insert.pl` и записываются в соответствующие RRA-архивы RRDtool.

Настройка Nagios

1. Скопируйте файл `check_drweb` в каталог <*NAGIOS_PLUGINS_DIR*>, а файл `drweb.cfg` — в каталог <*NAGIOS_OBJECTS_DIR*>.
2. Добавьте в группу *drweb* узлы с установленным Dr.Web Gateway Security Suite, подлежащие наблюдению (на них должен быть запущен Dr.Web SNMPD), по умолчанию в данную группу включен только локальный узел *localhost*.
3. Отредактируйте (при необходимости) команду `check_drweb`, в которой указывается обращение к Dr.Web SNMPD на узлах *drweb* через утилиту `snmplwalk`:

   ```
   snmpwalk -c public -v 2c $HOSTADDRESS$:161
   ```

   Укажите правильную версию протокола SNMP и параметры, такие как *community string*, или параметры аутентификации, а также порт. Переменную `$HOSTADDRESS$` необходимо оставить в команде (она автоматически заменяется Nagios на правильный адрес узла при вызове команды). OID в команде указывать не требуется. Рекомендуется также указать команду вместе с полным путем к исполняемому файлу (обычно — `/usr/local/bin/snmpwalk`).
4. Подключите объекты *DrWeb* в конфигурационном файле <*NAGIOS_ETC_DIR*>`/nagios.cfg`, добавив в него строку:

   ```
   cfg_file=<NAGIOS_OBJECTS_DIR>/drweb.cfg
   ```
5. Добавьте настройки RRDtool для графиков *DrWeb* из файла `rrdopts.conf-sample` в файл <*NAGIOSGRAPH_DIR*>`/etc/rrdopts.conf`.

6. Если компонент Nagiosgraph еще не настроен, то выполните его настройку:
   - Скопируйте файл `nagiosgraph.cfg` в каталог <*NAGIOS_OBJECTS_DIR*> и исправьте путь к файлу скрипта `insert.pl` в команде `process-service-perfdata-for-nagiosgraph`, например, так:

     ```
     $ awk '$1 == "command_line" { $2 = "<NAGIOSGRAPH_DIR>/bin/insert.pl" }
     { print }' ./objects/nagiosgraph.cfg >
     <NAGIOS_OBJECTS_DIR>/nagiosgraph.cfg
     ```

   - Подключите этот файл в конфигурационном файле <*NAGIOS_ETC_DIR*>`/nagios.cfg`, добавив в него строку:

     ```
     cfg_file=<NAGIOS_OBJECTS_DIR>/nagiosgraph.cfg
     ```

7. Проверьте значения параметров Nagios в конфигурационном файле <*NAGIOS_ETC_DIR*>`/nagios.cfg`:

```
check_external_commands=1
execute_host_checks=1
accept_passive_host_checks=1
enable_notifications=1
enable_event_handlers=1

process_performance_data=1
service_perfdata_file=/usr/nagiosgraph/var/rrd/perfdata.log
service_perfdata_file_template=$LASTSERVICECHECK$||$HOSTNAME$||$SERVICEDES
C$||$SERVICEOUTPUT$||$SERVICEPERFDATA$
service_perfdata_file_mode=a
service_perfdata_file_processing_interval=30
service_perfdata_file_processing_command=process-service-perfdata-for-
nagiosgraph

check_service_freshness=1
enable_flap_detection=1
enable_embedded_perl=1
enable_environment_macros=1
```

Настройка приема уведомлений SNMP trap для Nagios

1. На наблюдаемом узле в настройках Dr.Web SNMPD (параметр `TrapReceiver`) укажите адрес, который прослушивается `snmptrapd` на узле с Nagios, например:

   ```
   SNMPD.TrapReceiver = 10.20.30.40:162
   ```

2. Проверьте наличие файла скрипта <*NAGIOS_PLUGINS_DIR*>`/eventhandlers/submit_check_result`, который будет вызываться при получении уведомлений *SNMP trap*. Если этого файла нет, то следует скопировать в это место файл `submit_check_result` из каталога `/opt/drweb.com/share/drweb-snmpd/connectors/nagios/plugins/eventhandlers/` для GNU/Linux или `/usr/local/libexec/drweb.com/share/drweb-`

`snmpd/connectors/nagios/plugins/eventhandlers/` для FreeBSD. Необходимо в этом файле исправить путь, указанный в параметре `CommandFile`. Он должен иметь то же значение, что и параметр `command_file` в файле *<NAGIOS_ETC_DIR>*`/nagios.cfg`.

3. Скопируйте файл `snmptt.drweb.nagios.conf` в каталог `/etc/snmp/snmp/`. В этом файле измените путь к файлу скрипта `submit_check_result`, например, используя команду:

```
$ awk '$1 == "EXEC" { $2 =
<NAGIOS_PLUGINS_DIR>/eventhandlers/submit_check_result }{ print}'
./snmp/snmptt.drweb.nagios.conf > /etc/snmp/snmp/snmptt.drweb.nagios.conf
```

4. Добавьте в файл `/etc/snmp/snmptt.ini` строку «`/etc/snmp/snmptt.drweb.nagios.conf`». После этого, если `snmptt` запущен в режиме демона, то его надо перезапустить.

После того как все требуемые файлы конфигурации Nagios были добавлены и отредактированы, необходимо запустить Nagios в режиме отладки командой:

```
# nagios -v <NAGIOS_ETC_DIR>/nagios.cfg
```

В этом случае Nagios проверит наличие ошибок конфигурации. Если ошибки не были найдены при проверке, перезапустите Nagios стандартным способом, например, командой:

```
# service nagios restart
```

Подробнее с официальной документацией по Nagios вы можете ознакомиться по ссылке https://www.nagios.org/documentation.

9.14.5. Dr.Web SNMP MIB

Перечень параметров работы Dr.Web Gateway Security Suite, которые могут быть получены внешними системами мониторинга по протоколу SNMP, представлен в таблице ниже.

Имя параметра	**OID параметра**	**Тип и описание параметра**
Общий префикс имен: `.iso.org.dod.internet.private.enterprises.drweb.drwebSnmpd` Общий префикс OID: `.1.3.6.1.4.1.29690.2`		
alert	**Асинхронные уведомления о событиях (SNMP traps)**	
threatAlert	`.1.1`	Уведомление об обнаруженной угрозе

Имя параметра	OID параметра	Тип и описание параметра
threatAlertFile	.1.1.1	Имя инфицированного файла (строка)
threatAlertType	.1.1.2	Тип угрозы (целое число*)
threatAlertName	.1.1.3	Название угрозы (строка)
threatAlertOrigin	.1.1.4	Идентификатор компонента, обнаружившего угрозу (целое число***)
threatAlertRemoteIp	.1.1.5	IP-адрес удаленного узла, с которого производился доступ к файлу (строка)
threatAlertRemoteUser	.1.1.6	Имя удаленного пользователя, обращавшегося к файлу (строка)
threatAlertRemoteDomain	.1.1.7	Имя удаленного узла (FQDN), с которого производился доступ к файлу (строка)
threatActionErrorAlert	.1.2	Уведомление об ошибке при попытке нейтрализации угрозы
threatActionErrorAlertFile	.1.2.1	Имя инфицированного файла (строка)
threatActionErrorAlertType	.1.2.2	Тип угрозы (целое число*)
threatActionErrorAlertName	.1.2.3	Название угрозы (строка)
threatActionErrorAlertOrigin	.1.2.4	Идентификатор компонента, обнаружившего угрозу (целое число***)
threatActionErrorAlertError	.1.2.5	Описание ошибки (строка)
threatActionErrorAlertErrorCode	.1.2.6	Код ошибки (целое число, соответствует кодам из таблицы каталога ошибок)
threatActionErrorAlertAction	.1.2.7	Действие, попытка совершить которое привела к ошибке (целое число: 1 — лечить; 2 — переместить в карантин; 3 — удалить; 4 — информировать; 5 — игнорировать)

Имя параметра	OID параметра	Тип и описание параметра
componentFailureAlert	.1.3	Уведомление о сбое в работе компонента
componentFailureAlertName	.1.3.1	Идентификатор компонента (целое число***)
componentFailureAlertExitCodeDescription	.1.3.2	Описание кода завершения компонента (строка)
componentFailureAlertExitCode	.1.3.3	Код завершения компонента (целое число, соответствует кодам из таблицы каталога ошибок)
infectedUrlAlert	.1.4	Уведомление о блокировании доступа к веб-ресурсу, содержащему угрозу (для соединений HTTP/HTTPS)
infectedUrlAlertUrl	.1.4.1	Заблокированный URL (строка)
infectedUrlAlertDirection	.1.4.2	Направление HTTP-сообщения (целое число: 1 — запрос, 2 — ответ)
infectedUrlAlertType	.1.4.3	Тип угрозы (целое число*)
infectedUrlAlertName	.1.4.4	Название угрозы (строка)
infectedUrlAlertOrigin	.1.4.5	Идентификатор компонента, обнаружившего угрозу (целое число***)
infectedUrlAlertSrcIp	.1.4.6	IP-адрес источника соединения (строка)
infectedUrlAlertSrcPort	.1.4.7	Порт источника соединения (целое число)
infectedUrlAlertDstIp	.1.4.8	IP-адрес точки назначения соединения (строка)
infectedUrlAlertDstPort	.1.4.9	Порт точки назначения соединения (целое число)
infectedUrlAlertSniHost	.1.4.10	SNI точки назначения соединения (для SSL-соединений) (строка)

Имя параметра	OID параметра	Тип и описание параметра
infectedUrlAlertExePath	.1.4.11	Исполняемый путь программы-инициатора соединения (строка)
infectedUrlAlertUserName	.1.4.12	Имя пользователя, с правами которого исполняется программа-инициатор соединения (строка)
categoryUrlAlert	.1.6	Уведомление о блокировании доступа к веб-ресурсу, входящему в нежелательную категорию
categoryUrlAlertUrl	.1.6.1	Заблокированный URL (строка)
categoryUrlAlertCategory	.1.6.2	Категория веб-ресурсов, к которой относится URL (целое число**)
categoryUrlAlertOrigin	.1.6.3	Идентификатор компонента, обнаружившего угрозу (целое число***)
categoryUrlAlertSrcIp	.1.6.4	IP-адрес источника соединения (строка)
categoryUrlAlertSrcPort	.1.6.5	Порт источника соединения (целое число)
categoryUrlAlertDstIp	.1.6.6	IP-адрес точки назначения соединения (строка)
categoryUrlAlertDstPort	.1.6.7	Порт точки назначения соединения (целое число)
categoryUrlAlertSniHost	.1.6.8	SNI точки назначения соединения (для SSL-соединений) (строка)
categoryUrlAlertExePath	.1.6.9	Исполняемый путь программы-инициатора соединения (строка)
categoryUrlAlertUserName	.1.6.10	Имя пользователя, с правами которого исполняется программа-инициатор соединения (строка)

Имя параметра	OID параметра	Тип и описание параметра
blockedConnectionAlert	.1.9	Уведомление о блокировке сетевого соединения
blockedConnectionAlertOrigin	.1.9.1	Идентификатор компонента, обнаружившего угрозу (целое число***)
blockedConnectionAlertDivert	.1.9.2	Направление соединения (целое число: 1 — входящее; 2 — исходящее)
blockedConnectionAlertSrcIp	.1.9.3	IP-адрес источника соединения (строка)
blockedConnectionAlertSrcPort	.1.9.4	Порт источника соединения (целое число)
blockedConnectionAlertDstIp	.1.9.5	IP-адрес точки назначения соединения (строка)
blockedConnectionAlertDstPort	.1.9.6	Порт точки назначения соединения (целое число)
blockedConnectionAlertSniHost	.1.9.7	SNI точки назначения соединения (для SSL-соединений) (строка)
blockedConnectionAlertProtocol	.1.9.8	Тип протокола (целое число: 1 — SMTP; 2 — POP3; 3 — IMAP; 4 — HTTP)
blockedConnectionAlertExePath	.1.9.9	Исполняемый путь программы-инициатора соединения (строка)
blockedConnectionAlertUserName	.1.9.10	Имя пользователя, с правами которого исполняется программа-инициатор соединения (строка)
expiringLicenseAlert	.1.10	Дней до истечения лицензии (целое число)
outdatedBasesAlert	.1.11	Время последней успешной попытки обновления баз (*Unix time*)
stat	**Статистические показатели работы Dr.Web Gateway Security Suite**	
threatCounters	.2.1	Счетчики обнаруженных угроз

Имя параметра	OID параметра	Тип и описание параметра
knownVirus	.2.1.1	Число обнаруженных известных угроз (счетчик; целое число)
suspicious	.2.1.2	Число обнаруженных подозрительных объектов (счетчик; целое число)
adware	.2.1.3	Число обнаруженных рекламных программ (счетчик; целое число)
dialers	.2.1.4	Число обнаруженных программ дозвона (счетчик; целое число)
joke	.2.1.5	Число обнаруженных шуточных программ (счетчик; целое число)
riskware	.2.1.6	Число обнаруженных потенциально опасных программ (счетчик; целое число)
hacktool	.2.1.7	Число обнаруженных программ взлома (счетчик; целое число)
scanErrors	.2.2	Счетчики произошедших ошибок проверки файлов
sePathNotAbsolute	.2.2.1	Количество возникновений ошибки «Не абсолютный путь» (счетчик; целое число)
seFileNotFound	.2.2.2	Количество возникновений ошибки «Файл не найден» (счетчик; целое число)
seFileNotRegular	.2.2.3	Количество возникновений ошибки «Специальный (не регулярный) файл» (счетчик; целое число)
seFileNotBlockDevice	.2.2.4	Количество возникновений ошибки «Файл — не блочное устройство» (счетчик; целое число)

Имя параметра	OID параметра	Тип и описание параметра
seNameTooLong	.2.2.5	Количество возникновений ошибки «Слишком длинный путь или имя файла» (счетчик; целое число)
seNoAccess	.2.2.6	Количество возникновений ошибки «Доступ запрещен» (счетчик; целое число)
seReadError	.2.2.7	Количество возникновений ошибки «Ошибка чтения» (счетчик; целое число)
seWriteError	.2.2.8	Количество возникновений ошибки «Ошибка записи» (счетчик; целое число)
seFileTooLarge	.2.2.9	Количество возникновений ошибки «Файл слишком большой» (счетчик; целое число)
seFileBusy	.2.2.10	Количество возникновений ошибки «Файл занят» (счетчик; целое число)
seUnpackingError	.2.2.20	Количество возникновений ошибки «Ошибка распаковки» (счетчик; целое число)
sePasswordProtecetd	.2.2.21	Количество возникновений ошибки «Защищено паролем» (счетчик; целое число)
seArchCrcError	.2.2.22	Количество возникновений ошибки «Ошибка контрольной суммы архива» (счетчик; целое число)
seArchInvalidHeader	.2.2.23	Количество возникновений ошибки «Недопустимый заголовок архива» (счетчик; целое число)
seArchNoMemory	.2.2.24	Количество возникновений ошибки «Недостаточно памяти для обработки архива» (счетчик; целое число)

Имя параметра	OID параметра	Тип и описание параметра
seArchIncomplete	.2.2.25	Количество возникновений ошибки «Неожиданный конец архива» (счетчик; целое число)
seCanNotBeCured	.2.2.26	Количество возникновений ошибки «Объект не может быть вылечен» (счетчик; целое число)
sePackerLevelLimit	.2.2.30	Количество возникновений ошибки «Превышение допустимого уровня вложенности для запакованных объектов» (счетчик; целое число)
seArchiveLevelLimit	.2.2.31	Количество возникновений ошибки «Превышение допустимого уровня вложенности для архивов» (счетчик; целое число)
seMailLevelLimit	.2.2.32	Количество возникновений ошибки «Превышение допустимого уровня вложенности для почтовых файлов» (счетчик; целое число)
seContainerLevelLimit	.2.2.33	Количество возникновений ошибки «Превышение допустимого уровня вложенности для контейнеров» (счетчик; целое число)
seCompressionLimit	.2.2.34	Количество возникновений ошибки «Превышение допустимой величины коэффициента сжатия» (счетчик; целое число)
seReportSizeLimit	.2.2.35	Количество возникновений ошибки «Превышение допустимого размера отчета о проверке» (счетчик; целое число)

Имя параметра	OID параметра	Тип и описание параметра
seScanTimeout	.2.2.40	Количество возникновений ошибки «Истекло время на проверку файла» (счетчик; целое число)
seEngineCrash	.2.2.41	Количество возникновений ошибки «Обнаружен сбой сканирующего ядра» (счетчик; целое число)
seEngineHangup	.2.2.42	Количество возникновений ошибки «Перестало отвечать сканирующее ядро» (счетчик; целое число)
seEngineError	.2.2.44	Количество возникновений ошибки «Внутренняя ошибка сканирующего ядра» (счетчик; целое число)
seNoLicense	.2.2.45	Количество возникновений ошибки «Не найдена действующая лицензия» (счетчик; целое число)
seCuringLimitReached	.2.2.47	Количество возникновений ошибки «Достигнут предел попыток лечения» (счетчик; целое число)
seNonSupportedDisk	.2.2.50	Количество возникновений ошибки «Не поддерживаемый диск» (счетчик; целое число)
seUnexpectedError	.2.2.100	Количество возникновений ошибки «Неожиданная ошибка» (счетчик; целое число)
scanLoadAverage	.2.3	Показатели нагрузки проверки файлов
filesScannedTable	.2.3.1	Скорость проверки файлов по запросам от компонентов
filesScannedEntry	.2.3.1.1	Компонент (строка таблицы; запись)
filesScannedIndex	.2.3.1.1.1	Индекс компонента (идентификатор; целое

Имя параметра	OID параметра	Тип и описание параметра
		число***)
filesScannedOrigin	.2.3.1.1.2	Имя компонента
filesScanned1min	.2.3.1.1.3	Среднее (за минуту) количество файлов, проверенных в секунду (строка)
filesScanned5min	.2.3.1.1.4	Среднее (за 5 минут) количество файлов, проверенных в секунду (строка)
filesScanned15min	.2.3.1.1.5	Среднее (за 15 минут) количество файлов, проверенных в секунду (строка)
bytesScannedTable	.2.3.2	Скорость проверки (в байтах) по запросам от компонентов
bytesScannedEntry	.2.3.2.1	Компонент (строка таблицы; запись)
bytesScannedIndex	.2.3.2.1.1	Индекс компонента (идентификатор; целое число***)
bytesScannedOrigin	.2.3.2.1.2	Имя компонента
bytesScanned1min	.2.3.2.1.3	Среднее (за минуту) количество байт, проверенных в секунду (строка)
bytesScanned5min	.2.3.2.1.4	Среднее (за 5 минут) количество байт, проверенных в секунду (строка)
bytesScanned15min	.2.3.2.1.5	Среднее (за 15 минут) количество байт, проверенных в секунду (строка)
cacheHitFilesTable	.2.3.3	Использование кеша проверенных файлов по запросам от компонентов
cacheHitFilesEntry	.2.3.3.1	Компонент (строка таблицы; запись)

Имя параметра	OID параметра	Тип и описание параметра
cacheHitFilesIndex	.2.3.3.1.1	Индекс компонента (идентификатор; целое число***)
cacheHitFilesOrigin	.2.3.3.1.2	Имя компонента
cacheHitFiles1min	.2.3.3.1.3	Среднее (за минуту) количество отчетов о проверке, извлеченных из кеша в секунду (строка)
cacheHitFiles5min	.2.3.3.1.4	Среднее (за 5 минут) количество отчетов о проверке, извлеченных из кеша в секунду (строка)
cacheHitFiles15min	.2.3.3.1.5	Среднее (за 15 минут) количество отчетов о проверке, извлеченных из кеша в секунду (строка)
errorsTable	.2.3.4	Число ошибок проверки по запросам от компонентов
errorsEntry	.2.3.4.1	Компонент (строка таблицы; запись)
errorsIndex	.2.3.4.1.1	Индекс компонента (идентификатор; целое число***)
errorsOrigin	.2.3.4.1.2	Имя компонента
errors1min	.2.3.4.1.3	Среднее (за минуту) количество ошибок в секунду (строка)
errors5min	.2.3.4.1.4	Среднее (за 5 минут) количество ошибок в секунду (строка)
errors15min	.2.3.4.1.5	Среднее (за 15 минут) количество ошибок в секунду (строка)
net	.2.4	Показатели сетевой активности
blockedInfectionSource	.2.4.101	Число заблокированных URL из категории «Источники

Имя параметра	OID параметра	Тип и описание параметра
		распространения угроз» (счетчик; целое число)
blockedNotRecommended	.2.4.102	Число заблокированных URL из категории «Нерекомендуемые» (счетчик; целое число)
blockedAdultContent	.2.4.103	Число заблокированных URL из категории «Сайты для взрослых» (счетчик; целое число)
blockedViolence	.2.4.104	Число заблокированных URL из категории «Насилие» (счетчик; целое число)
blockedWeapons	.2.4.105	Число заблокированных URL из категории «Оружие» (счетчик; целое число)
blockedGambling	.2.4.106	Число заблокированных URL из категории «Азартные игры» (счетчик; целое число)
blockedDrugs	.2.4.107	Число заблокированных URL из категории «Наркотики» (счетчик; целое число)
blockedObsceneLanguage	.2.4.108	Число заблокированных URL из категории «Нецензурная лексика» (счетчик; целое число)
blockedChats	.2.4.109	Число заблокированных URL из категории «Чаты» (счетчик; целое число)
blockedTerrorism	.2.4.110	Число заблокированных URL из категории «Терроризм» (счетчик; целое число)
blockedFreeEmail	.2.4.111	Число заблокированных URL из категории «Бесплатная электронная почта» (счетчик; целое число)

Имя параметра	OID параметра	Тип и описание параметра
blockedSocialNetworks	.2.4.112	Число заблокированных URL из категории «Социальные сети» (счетчик; целое число)
blockedOwnersNotice	.2.4.113	Число заблокированных URL из категории «По обращению правообладателя» (счетчик; целое число)
blockedOnlineGames	.2.4.114	Число заблокированных URL из категории «Онлайн-игры» (счетчик; целое число)
blockedAnonymizers	.2.4.115	Число заблокированных URL из категории «Анонимайзеры» (счетчик; целое число)
blockedCryptocurrencyMiningPools	.2.4.116	Число заблокированных URL из категории «Пулы добычи криптовалют» (счетчик; целое число)
blockedJobs	.2.4.117	Число заблокированных URL из категории "Вакансии" (счетчик; целое число)
blockedBlackList	.2.4.120	Число заблокированных URL из пользовательского черного списка (счетчик; целое число)
info	**Информация о состоянии Dr.Web Gateway Security Suite**	
components	.3.1	Состояние компонентов Dr.Web Gateway Security Suite
configd	.3.1.1	Данные о компоненте drweb-configd
configdState	.3.1.1.1	Состояние компонента (целое число****)
configdExitCode	.3.1.1.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
configdExitTime	.3.1.1.3	Время завершения работы (*Unix time*)

Имя параметра	OID параметра	Тип и описание параметра
configdInstalledApps	.3.1.1.101	Перечень установленных компонентов
configdAppEntry	.3.1.1.101.1	Информация об установленном компоненте (строка таблицы; запись)
configdAppIndex	.3.1.1.101.1.1	Индекс (номер) установленного компонента (целое число)
configdAppName	.3.1.1.101.1.2	Имя установленного компонента (строка)
configdAppExePath	.3.1.1.101.1.3	Путь к исполняемому файлу компонента (строка)
configdAppInstallTime	.3.1.1.101.1.4	Время установки компонента (*Unix time*)
configdAppIniSection	.3.1.1.101.1.5	Имя секции с параметрами компонента в конфигурационном файле (строка)
scanEngine	.3.1.2	Данные о компоненте drweb-se
scanEngineState	.3.1.2.1	Состояние компонента (целое число****)
scanEngineExitCode	.3.1.2.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
scanEngineExitTime	.3.1.2.3	Время завершения работы (*Unix time*)
scanEngineStatus	.3.1.2.101	Состояние Dr.Web Virus-Finding Engine (целое число)
scanEngineVersion	.3.1.2.102	Версия Dr.Web Virus-Finding Engine (строка)
scanEngineVirusRecords	.3.1.2.103	Число записей об угрозах (целое число)
scanEngineMaxForks	.3.1.2.104	Максимальное число дочерних сканирующих процессов (целое число)

Имя параметра	OID параметра	Тип и описание параметра
scanEngineQueues	.3.1.2.105	Очереди задач на проверку
scanEngineQueuesLow	.3.1.2.105.1	Очередь низкоприоритетных задач
scanEngineQueueLowOut	.3.1.2.105.1.1	Число низкоприоритетных задач, извлеченных из очереди, и переданных на обработку (счетчик; целое число)
scanEngineQueueLowSize	.3.1.2.105.1.2	Число низкоприоритетных задач, ожидающих обработки в очереди (счетчик; целое число)
scanEngineQueuesMedium	.3.1.2.105.2	Очередь задач обычного приоритета
scanEngineQueueMediumOut	.3.1.2.105.2.1	Число задач обычного приоритета, извлеченных из очереди, и переданных на обработку (счетчик; целое число)
scanEngineQueueMediumSize	.3.1.2.105.2.2	Число задач обычного приоритета, ожидающих обработки в очереди (счетчик; целое число)
scanEngineQueuesHigh	.3.1.2.105.3	Очередь высокоприоритетных задач
scanEngineQueueHighOut	.3.1.2.105.3.1	Число высокоприоритетных задач, извлеченных из очереди, и переданных на обработку (счетчик; целое число)
scanEngineQueueHighSize	.3.1.2.105.3.2	Число высокоприоритетных задач, ожидающих обработки в очереди (счетчик; целое число)
scanEngineVirusBasesTable	.3.1.2.106	Перечень вирусных баз
scanEngineVirusBasesEntry	.3.1.2.106.1	Информация о вирусной базе (строка таблицы; запись)
scanEngineVirusBaseIndex	.3.1.2.106.1.1	Индекс вирусной базы (целое число)

Имя параметра	OID параметра	Тип и описание параметра
scanEngineVirusBasePath	.3.1.2.106.1.2	Путь к файлу вирусной базы (строка)
scanEngineVirusBaseRecords	.3.1.2.106.1.3	Число записей в вирусной базе (целое число)
scanEngineVirusBaseVersion	.3.1.2.106.1.4	Версия вирусной базы (целое число)
scanEngineVirusBaseTimestamp	.3.1.2.106.1.5	Метка времени для вирусной базы (*Unix time*)
scanEngineVirusBaseMD5	.3.1.2.106.1.6	Контрольная сумма MD5 (строка)
scanEngineVirusBaseLoadResult	.3.1.2.106.1.7	Результат загрузки вирусной базы (строка)
scanEngineQueuesTab	.3.1.2.107	Перечень очередей задач на проверку
scanEngineQueueEntry	.3.1.2.107.1	Информация об очереди (строка таблицы; запись)
scanEngineQueueIndex	.3.1.2.107.1.1	Индекс (номер) очереди (целое число)
scanEngineQueueName	.3.1.2.107.1.2	Имя очереди (строка)
scanEngineQueueOut	.3.1.2.107.1.3	Число задач, извлеченных из очереди, и переданных на обработку (счетчик; целое число)
scanEngineQueueSize	.3.1.2.107.1.4	Число задач, ожидающих обработки в очереди (счетчик; целое число)
fileCheck	.3.1.3	Данные о компоненте drweb-filecheck
fileCheckState	.3.1.3.1	Состояние компонента (целое число****)
fileCheckExitCode	.3.1.3.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
fileCheckExitTime	.3.1.3.3	Время завершения работы (*Unix time*)

Имя параметра	OID параметра	Тип и описание параметра
fileCheckScannedFiles	.3.1.3.101	Число проверенных файлов (счетчик; целое число)
fileCheckScannedBytes	.3.1.3.102	Число проверенных байт (счетчик; целое число)
fileCheckCacheHitFiles	.3.1.3.103	Число отчетов о проверке, извлеченных из кеша проверенных файлов (счетчик; целое число)
fileCheckScanErrors	.3.1.3.104	Число ошибок сканирующего ядра (счетчик; целое число)
fileCheckScanStat	.3.1.3.105	Перечень клиентов
fileCheckClientEntry	.3.1.3.105.1	Информация о клиенте (строка таблицы; запись)
fileCheckClientIndex	.3.1.3.105.1.1	Индекс (номер) клиента (целое число)
fileCheckClientName	.3.1.3.105.1.2	Имя компонента-клиента (строка)
fileCheckClientScannedFiles	.3.1.3.105.1.3	Число файлов, проверенных для данного клиента (счетчик; целое число)
fileCheckClientScannedBytes	.3.1.3.105.1.4	Число байт, проверенных для данного клиента (счетчик; целое число)
fileCheckClientCacheHitFiles	.3.1.3.105.1.5	Число отчетов о проверке для данного клиента, извлеченных из кеша проверенных файлов (счетчик; целое число)
fileCheckClientScanErrors	.3.1.3.105.1.6	Число ошибок сканирующего ядра для данного клиента (счетчик; целое число)
update	.3.1.4	Данные о компоненте drweb-update
updateState	.3.1.4.1	Состояние компонента (целое число****)
updateExitCode	.3.1.4.2	Последний код завершения (целое число, соответствует

Имя параметра	OID параметра	Тип и описание параметра
		кодам из таблицы каталога ошибок)
updateExitTime	.3.1.4.3	Время завершения работы (*Unix time*)
updateBytesSent	.3.1.4.101	Число отправленных байт (счетчик; целое число)
updateBytesReceived	.3.1.4.102	Число принятых байт (счетчик; целое число)
esagent	.3.1.5	Данные о компоненте drweb-esagent
esagentState	.3.1.5.1	Состояние компонента (целое число****)
esagentExitCode	.3.1.5.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
esagentExitTime	.3.1.5.3	Время завершения работы (*Unix time*)
esagentWorkStatus	.3.1.5.101	Режим работы компонента (целое число: 1 — автономный, 2 — подключается, 3 — ожидает подключения, 4 — подключение одобрено)
esagentIsConnected	.3.1.5.102	Подключен ли к серверу (целое число: 0 — нет, 1 — да)
esagentServer	.3.1.5.103	Адрес используемого сервера централизованной защиты (строка)
netcheck	.3.1.6	Данные о компоненте drweb-netcheck
netcheckState	.3.1.6.1	Состояние компонента (целое число****)
netcheckExitCode	.3.1.6.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)

Имя параметра	OID параметра	Тип и описание параметра
netcheckExitTime	.3.1.6.3	Время завершения работы (*Unix time*)
netcheckLocalSeForks	.3.1.6.101	Число ядер сканирования, доступных локально (целое число)
netcheckRemoteSeForks	.3.1.6.102	Число доступных удаленных ядер сканирования (целое число)
netcheckLocalFilesScanned	.3.1.6.103	Число файлов, проверенных локально (счетчик; целое число)
netcheckNetworkFilesScanned	.3.1.6.104	Число файлов, проверенных удаленно (счетчик; целое число)
netcheckLocalBytesScanned	.3.1.6.105	Число байт, проверенных локально (счетчик; целое число)
netcheckNetworkBytesScanned	.3.1.6.106	Число байт, проверенных удаленно (счетчик; целое число)
netcheckLocalBytesIn	.3.1.6.107	Число байт, полученных от локальных клиентов (счетчик; целое число)
netcheckLocalBytesOut	.3.1.6.108	Число байт, отправленных локальным клиентам (счетчик; целое число)
netcheckNetworkBytesIn	.3.1.6.109	Число байт, полученных от удаленных узлов (счетчик; целое число)
netcheckNetworkBytesOut	.3.1.6.110	Число байт, отправленных на удаленные узлы (счетчик; целое число)
netcheckLocalScanErrors	.3.1.6.111	Число ошибок локальных ядер сканирования (счетчик; целое число)
netcheckNetworkScanErrors	.3.1.6.112	Число ошибок удаленных ядер сканирования (счетчик; целое число)

Имя параметра	OID параметра	Тип и описание параметра
httpd	.3.1.7	Данные о компоненте drweb-httpd
httpdState	.3.1.7.1	Состояние компонента (целое число****)
httpdExitCode	.3.1.7.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
httpdExitTime	.3.1.7.3	Время завершения работы (*Unix time*)
snmpd	.3.1.8	Данные о компоненте drweb-snmpd
snmpdState	.3.1.8.1	Состояние компонента (целое число****)
snmpdExitCode	.3.1.8.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
snmpdExitTime	.3.1.8.3	Время завершения работы (*Unix time*)
statd	.3.1.9	Данные о компоненте drweb-statd
statdState	.3.1.9.1	Состояние компонента (целое число****)
statdExitCode	.3.1.9.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
statdExitTime	.3.1.9.3	Время завершения работы (*Unix time*)
statdConnectionsIn	.3.1.9.101	Число принятых соединений (счетчик; целое число)
statdConnectionsCount	.3.1.9.102	Текущее число открытых соединений (счетчик; целое число)
clamd	.3.1.20	Данные о компоненте drweb-clamd

Имя параметра	OID параметра	Тип и описание параметра
clamdState	.3.1.20.1	Состояние компонента (целое число****)
clamdExitCode	.3.1.20.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
clamdExitTime	.3.1.20.3	Время завершения работы (*Unix time*)
icapd	.3.1.21	Данные о компоненте drweb-icapd
icapdState	.3.1.21.1	Состояние компонента (целое число****)
icapdExitCode	.3.1.21.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
icapdExitTime	.3.1.21.3	Время завершения работы (*Unix time*)
icapdConnectionsIn	.3.1.21.101	Число принятых соединений (счетчик; целое число)
icapdConnectionsCount	.3.1.21.102	Текущее число открытых соединений (счетчик; целое число)
icapdOptions	.3.1.21.103	Число запросов *OPTIONS* (счетчик; целое число)
icapdReqmod	.3.1.21.104	Число запросов *REQMOD* (счетчик; целое число)
icapdRespmod	.3.1.21.105	Число запросов *RESPMOD* (счетчик; целое число)
icapdBad	.3.1.21.106	Число некорректных запросов (счетчик; целое число)
gated	.3.1.41	Данные о компоненте drweb-gated
gatedState	.3.1.41.1	Состояние компонента (целое число****)

Имя параметра	OID параметра	Тип и описание параметра
gatedExitCode	.3.1.41.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
gatedExitTime	.3.1.41.3	Время завершения работы (*Unix time*)
gatedInterceptedIn	.3.1.41.101	Число перехваченных соединений (счетчик; целое число)
gatedInterceptedCount	.3.1.41.102	Число соединений, которые находятся под наблюдением в данный момент (счетчик; целое число)
lookupd	.3.1.43	Данные о компоненте drweb-lookupd
lookupdState	.3.1.43.1	Состояние компонента (целое число****)
lookupdExitCode	.3.1.43.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
lookupdExitTime	.3.1.43.3	Время завершения работы (*Unix time*)
urlcheck	.3.1.45	Данные о компоненте drweb-urlcheck
urlcheckState	.3.1.45.1	Состояние компонента (целое число****)
urlcheckExitCode	.3.1.45.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
urlcheckExitTime	.3.1.45.3	Время завершения работы (*Unix time*)
urlcheckConnectionsIn	.3.1.45.101	Число принятых соединений (счетчик; целое число)
urlcheckConnectionsCount	.3.1.45.102	Текущее число открытых соединений (счетчик; целое число)

Имя параметра	OID параметра	Тип и описание параметра
cloudd	.3.1.50	Данные о компоненте drweb-cloudd
clouddState	.3.1.50.1	Состояние компонента (целое число****)
clouddExitCode	.3.1.50.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
clouddExitTime	.3.1.50.3	Время завершения работы (*Unix time*)
meshd	.3.1.52	Данные о компоненте drweb-meshd
meshdState	.3.1.52.1	Состояние компонента (целое число****)
meshdExitCode	.3.1.52.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
meshdExitTime	.3.1.52.3	Время завершения работы (*Unix time*)
linuxfirewall	.3.1.203	Данные о компоненте drweb-firewall (для GNU/Linux)
linuxfirewallState	.3.1.203.1	Состояние компонента (целое число****)
linuxfirewallExitCode	.3.1.203.2	Последний код завершения (целое число, соответствует кодам из таблицы каталога ошибок)
linuxfirewallExitTime	.3.1.203.3	Время завершения работы (*Unix time*)
ctl	.3.1.300	Данные о компоненте drweb-ctl
ctlState	.3.1.300.1	Состояние компонента (целое число****)
ctlExitCode	.3.1.300.2	Последний код завершения (целое число, соответствует

Имя параметра	OID параметра	Тип и описание параметра
		кодам из таблицы каталога ошибок)
ctlExitTime	.3.1.300.3	Время завершения работы (*Unix time*)
license	.3.2	Состояние лицензии
licenseEsMode	.3.2.1	Лицензия выдана сервером централизованной защиты (целое число: 0 — нет, 1 — да)
licenseNumber	.3.2.2	Номер лицензии (целое число)
licenseOwner	.3.2.3	Владелец лицензии (строка)
licenseActivated	.3.2.4	Дата активации лицензии (*Unix time*)
licenseExpires	.3.2.5	Дата прекращения действия лицензии (*Unix time*)

*) Типы угроз:

Код	Тип угрозы
1	Известная угроза (*known virus*)
2	Подозрительный объект (*suspicious*)
3	Рекламная программа (*adware*)
4	Программа дозвона (*dialer*)
5	Программа-шутка (*joke program*)
6	Потенциально опасная программа (*riskware*)
7	Программа взлома (*hacktool*)

**) Категории URL:

Код	Тип угрозы
1	Источник распространения угроз (*infectionSource*)
2	Не рекомендуемый (*notRecommended*)
3	Сайты для взрослых (*adultContent*)

Код	Тип угрозы
4	Насилие (*violence*)
5	Оружие (*weapons*)
6	Азартные игры (*gambling*)
7	Наркотики (*drugs*)
8	Нецензурная лексика (*obsceneLanguage*)
9	Чаты (*chats*)
10	Терроризм (*terrorism*)
11	Бесплатная электронная почта (*freeEmail*)
12	Социальные сети (*socialNetworks*)
13	Добавленные по обращению правообладателя (*ownerNotice*)
14	Онлайн-игры (*onlineGames*)
15	Анонимайзеры (*anonymizers*)
16	Пулы добычи криптовалют (*cryptocurrencyMiningPools*)
17	Вакансии (*Jobs*)
20	Черный список (*blackList*)

***) Коды компонентов Dr.Web:

Код	Компонент
1	Dr.Web ConfigD (`drweb-configd`)
2	Dr.Web Scanning Engine (`drweb-se`)
3	Dr.Web File Checker (`drweb-filecheck`)
4	Dr.Web Updater (`drweb-update`)
5	Dr.Web ES Agent (`drweb-esagent`)
6	Dr.Web Network Checker (`drweb-netcheck`)
7	Dr.Web HTTPD (`drweb-httpd`)
8	Dr.Web SNMPD (`drweb-snmpd`)

Код	Компонент
20	Dr.Web ClamD (`drweb-clamd`)
21	Dr.Web ICAPD (`drweb-icapd`)
41	SpIDer Gate (`drweb-gated`)
43	Dr.Web LookupD (`drweb-lookupd`)
50	Dr.Web CloudD (`drweb-cloudd`)
52	Dr.Web MeshD (`drweb-meshd`)
203	Dr.Web Firewall для Linux (`drweb-firewall`)
300	Dr.Web Ctl (`drweb-ctl`)
400	Сканирование по заданию сервера централизованной защиты (не является компонентом Dr.Web Gateway Security Suite)

****) Состояния компонентов:

Код	Состояние
0	Не установлен
1	Установлен, но не запущен
2	Запускается
3	Работает
4	Завершает работу

Для непосредственного получения значений переменных вы можете воспользоваться утилитой `snmpwalk`:

```
$ snmpwalk -Os -c <community> -v <версия SNMP> <адрес узла> <OID>
```

Например, для получения статистики по обнаруженным угрозам на локальном узле (при настройках Dr.Web SNMPD по умолчанию) используйте следующую команду:

```
$ snmpwalk -Os -c public -v 2c 127.0.0.1 .1.3.6.1.4.1.29690.2.2.1
```

9.15. Dr.Web MeshD

Компонент Dr.Web MeshD представляет собой агент, включающий узел с установленным Dr.Web Gateway Security Suite в «локальное облако», объединяющее узлы, на которых установлены продукты Dr.Web для Unix. Данное облако позволяет решать следующие задачи:

- предоставление одними узлами облака другим услуг по сканированию файлов (услуга по предоставлению сканирующего ядра);
- распространение обновлений вирусных баз среди узлов облака.

Для объединения узлов с установленными продуктами Dr.Web для Unix в составе каждого узла должен присутствовать компонент Dr.Web MeshD, обеспечивающий включение этого узла в облако. Полномочия узла в рамках облака и возможности облака, используемые узлом, гибко регулируются настройками компонента Dr.Web MeshD.

Обмен данными с другими узлами облака производится по защищенному каналу SSH.

9.15.1. Принципы работы

В этом разделе

- Типы подключений
- Режимы работы
- Услуги
  - Обмен обновлениями (Update)
  - Удаленное сканирование файлов (Engine)
  - Передача файлов на проверку (File)
  - Проверка URL (Url)

Dr.Web MeshD играет роль посредника, обеспечивающего взаимодействие между узлом, на котором установлен Dr.Web Gateway Security Suite, и другими узлами облака.

Типы подключений

При работе Dr.Web MeshD использует подключения следующих типов:

- *Клиентские (сервисные)* используются Dr.Web MeshD для подключения к нему других узлов облака, которые являются клиентами услуг, предоставляемых данным узлом.

Компоненты Dr.Web Gateway Security Suite, работающие на узле и использующие услуги, предоставленные облаком, подключаются к Dr.Web MeshD, работающий на этом же узле, через локальный Unix-сокет. Клиентское подключение при этом не используется.

- *Партнерские (одноранговые)* используются Dr.Web MeshD для взаимодействия с равноправными (в рамках некоторой услуги) узлами-партнерами облака. Обычно подобные горизонтальные связи используются для масштабирования и распределения нагрузки при взаимодействии с облаком, а также синхронизации состояния узлов облака.
- *Восходящие* используются Dr.Web MeshD для подключения данного узла в роли клиента к узлам облака, предоставляющим услуги (например, распространение обновлений вирусных баз, передача файлов на проверку и т. д.).

Использование подключений всех трех типов настраивается для разных услуг облака независимо друг от друга. При этом один и тот же узел может быть настроен как сервер для обслуживания клиентских запросов в рамках одной услуги (например, для раздачи свежих обновлений) и как клиент — в рамках другой услуги (например, удаленного сканирования файлов).

В рамках облака узлы осуществляют взаимодействие по защищенному протоколу SSH, т. е. все стороны в рамках каждого межузлового взаимодействия всегда взаимно аутентифицированы. Для аутентификации используются узловые ключи (*host keys*) согласно RFC 4251. Клиентское подключение от локального компонента всегда считается доверенным.

Режимы работы

Dr.Web MeshD может работать как в режиме демона, так и запускаться по запросам от других компонентов Dr.Web Gateway Security Suite, расположенных на локальном узле. Если Dr.Web MeshD настроен на обслуживание клиентских подключений (параметр `ListenAddress` не пуст) и активирована возможность оказания хотя бы одной из услуг, Dr.Web MeshD запускается как демон и ждет подключения со стороны клиентов.

Если Dr.Web MeshD не настроен на обслуживание клиентских подключений (параметр `ListenAddress` пуст) и запросы к нему отсутствуют в течение периода времени, указанного в параметре `IdleTimeLimit`, работа компонента автоматически завершается.

Услуги

Обмен обновлениями (Update)

Данная услуга позволяет узлу подписываться на обновления вирусных и иных баз, рассылать уведомления о наличии свежего обновления, загружать и раздавать файлы обновлений между узлами облака. Настройки использования данной услуги задаются параметрами `Update*`.

Стандартный сценарий использования услуги предполагает, что в локальной сети предприятия на некотором числе машин (исполняющих роль клиентов услуги) установлен Dr.Web MeshD со включенной функцией получения обновлений. Типовые настройки клиента следующие:

```
[MeshD]
ListenAddress =
```

На узле, выполняющем роль локального сервера распространения обновлений, заданы следующие настройки:

```
ListenAddress = <адрес>:<порт>
```

Здесь *<адрес сервера>* в восходящем соединении клиента должен указывать на те *<адрес>* и *<порт>*, которые используются серверным узлом для организации клиентских подключений.

Как только на каком-либо из узлов происходит обновление с серверов обновления (внешних по отношению к локальному облаку — серверов обновления ВСО Dr.Web или с сервера централизованной защиты), узел рассылает уведомление всем заинтересованным клиентам (если он настроен на работу в роли сервера услуги обмена обновлениями), а также сообщает серверному узлу новый список файлов, доступных для раздачи с этого узла. Получив это уведомление, клиентские узлы могут запросить загрузку обновленных файлов с сервера, который, в свою очередь, может запросить файлы у клиента, чтобы сохранить их у себя локально, либо отдать другому клиенту, который запросил эти файлы у сервера.

При использовании такой схемы обновление происходит с меньшей задержкой, поскольку клиенты опрашивают ВСО Dr.Web в разное время, и при этом первый обновившийся клиент сразу же раздает свежие файлы обновлений всем заинтересованным узлам облака. При этом также снижается количество передаваемого трафика и нагрузка на серверы ВСО Dr.Web.

При использовании локального облака для распространения обновлений на узлах помимо компонента Dr.Web MeshD должен присутствовать компонент обновления Dr.Web Updater.

Удаленное сканирование файлов (Engine)

Данная услуга позволяет использовать Dr.Web Scanning Engine для проверки удаленных файлов: узлы, работающие в роли клиентов, отправляют файлы на проверку на серверный узел, а серверные узлы предоставляют услугу по проверке файлов, отправленных клиентскими узлами. Типовые настройки клиента следующие:

```
…
[MeshD]
EngineChannel = On
EngineUplink = <адрес сервера>
ListenAddress =
…
```

На узле, выполняющем роль локального сервера сканирования, заданы следующие настройки:

```
EngineChannel = On
EngineUplink =
ListenAddress = <адрес>:<порт>
```

Здесь *<адрес сервера>* в восходящем соединении клиента должен указывать на те *<адрес>* и *<порт>*, которые используются серверным узлом для организации клиентских подключений.

Передача файлов на проверку (File)

Данная функциональность не используется (функция удаленного сканирования оказывается в рамках услуги *Engine*).

Проверка URL (Url)

Данная услуга предназначена для проверки URL на принадлежность к потенциально опасным и нежелательным категориям: узлы, выступающие в роли клиентов, отправляют URL для проверки на серверный узел. Типовые настройки клиента следующие:

```
…
[MeshD]
UrlChannel = On
UrlUplink = <адрес сервера>
ListenAddress =
…
```

На узле, выступающем в качестве сервера для проверки URL, заданы следующие настройки:

```
UrlChannel = On
UrlUplink =
ListenAddress = <адрес>:<порт>
```

Здесь *<адрес сервера>* в восходящем соединении клиента должен указывать на те *<адрес>* и *<порт>*, которые используются серверным узлом для организации клиентских подключений.

9.15.2. Аргументы командной строки

Для запуска компонента Dr.Web MeshD из командной строки используется следующая команда:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-meshd [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-meshd [<параметры>]
```

Dr.Web MeshD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет

`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-meshd --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web MeshD.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Gateway Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-meshd`.

9.15.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[MeshD]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию:

Параметр	Описание
	• для GNU/Linux: `/opt/drweb.com/bin/drweb-meshd` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-meshd`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`
`DebugSsh` *{логический}*	Сохранять или не сохранять в журнале сообщения протокола SSH (используется для передачи сообщений и данных), полученных и отправленных компонентом Dr.Web MeshD, работающим на данном узле, если установлен уровень подробности журнала `LogLevel = Debug`. Значение по умолчанию: `No`
`ListenAddress` *<IP-адрес>:<порт>*	Сетевой сокет (адрес и порт) клиентского подключения, на котором компонент ожидает поступления соединений от узлов облака, являющихся клиентами услуг, предоставляемых данным узлом облака. Чтобы компонент мог прослушивать интерфейс IPv6 и определять клиентские узлы облака по IPv6, параметр должен быть обязательно установлен. Если значение не задано, то компонент не принимает запросы от клиентов. Значение по умолчанию: `0.0.0.0:7090`, если установлен пакет `drweb-scanning-server`, в противном случае значение не задано
`DnsResolverConfPath` *{путь к файлу}*	Путь к файлу настроек DNS. Значение по умолчанию: `/etc/resolv.conf`
`DiscoveryResponderPort` *{номер порта}*	Порт, на котором вышестоящий узел MeshD отвечает по протоколу UDP на запросы клиентов. Механизм *discovery* работает, только если задан параметр `ListenAddress`. Значение по умолчанию: `18008`
`FileChannel` *{On | Off}*	Разрешить или запретить компоненту Dr.Web MeshD, работающему на данном узле, принимать участие в услуге обмена файлами.

Параметр	Описание
	Если этот параметр установлен в значение `On`, то компонент Dr.Web MeshD будет автоматически запущен демоном управления конфигурацией Dr.Web ConfigD. Значение по умолчанию: `On`
`FileUplink` *{адрес}*	Адрес вышестоящего узла Dr.Web MeshD, принимающего на проверку файлы с этого узла. Возможные значения: • *значение не указано* — сервер для этой услуги не задан, и Dr.Web MeshD не будет ни к кому подключаться. • *<IP-адрес>:<порт>* — Dr.Web MeshD будет подключаться к серверу с указанным адресом и портом. • `dns:`*<имя сервиса>*`[:`*<домен>*`]` — адрес и порт сервера услуги определяются путем поиска SRV-записи DNS домена *<домен>*. Если *<домен>* не указан, он берется из файла конфигурации DNS resolver (путь указан в `ResolverConfPath`) из полей `search` и `domain` в зависимости от того, какое из них встретится в файле конфигурации последним. • `discover` — искать адрес вышестоящего узла с помощью механизма *discovery*. Значение по умолчанию: *(не задано)*
`FileDebugIpc` *{логический}*	Выводить или не выводить отладочную информацию в журнал для услуги обмена файлами, если установлен уровень подробности журнала `LogLevel = Debug`. Значение по умолчанию: `No`
`EngineChannel` *{On | Off}*	Разрешить или запретить компоненту Dr.Web MeshD, работающему на данном узле, принимать участие в услуге предоставления сканирующего ядра. Если этот параметр установлен в значение `On`, то компонент Dr.Web MeshD будет автоматически запущен демоном управления конфигурацией Dr.Web ConfigD. Значение по умолчанию: `On`
`EngineUplink` *{адрес}*	Адрес вышестоящего узла Dr.Web MeshD, предоставляющего услуги сканирующего ядра для данного узла. Возможные значения: • *значение не указано* — сервер для этой услуги не задан, и Dr.Web MeshD не будет ни к кому подключаться. • *<IP-адрес>:<порт>* — Dr.Web MeshD будет подключаться к серверу с указанным адресом и портом. • `dns:`*<имя сервиса>*`[:`*<домен>*`]` — адрес и порт сервера услуги определяются путем поиска SRV-записи DNS домена *<домен>*.

Параметр	Описание
	Если <*домен*> не указан, он берется из файла конфигурации DNS resolver (путь указан в `ResolverConfPath`) из полей `search` и `domain` в зависимости от того, какое из них встретится в файле конфигурации последним. • `discover` — искать адрес вышестоящего узла с помощью механизма *discovery*. Значение по умолчанию: *(не задано)*
`EngineDebugIpc` *{логический}*	Выводить или не выводить отладочную информацию в журнал для услуги сканирования, если установлен уровень подробности журнала `LogLevel = Debug`. Значение по умолчанию: `No`
`UrlChannel` *{On | Off}*	Разрешить или запретить компоненту Dr.Web MeshD, работающему на данном узле, принимать участие в услуге проверки URL. Значение по умолчанию: `On`
`UrlUplink` *{адрес}*	Адрес вышестоящего узла Dr.Web MeshD, проверяющего URL для данного узла. Возможные значения: • *значение не указано* — сервер проверки URL не задан. • <*IP-адрес*>:<*порт*> — Dr.Web MeshD будет подключаться к серверу с указанным адресом и портом. • `dns:`<*имя сервиса*>`[:`<*домен*>`]` — адрес и порт сервера услуги определяются путем поиска SRV-записи DNS домена <*домен*>. Если <*домен*> не указан, он берется из файла конфигурации DNS resolver (путь указан в `ResolverConfPath`) из полей `search` и `domain` в зависимости от того, какое из них встретится в файле конфигурации последним. • `discover` — искать адрес вышестоящего узла с помощью механизма *discovery*. Значение по умолчанию: *(не задано)*
`UrlDebugIpc` *{логический}*	Выводить или не выводить отладочную информацию в журнал для услуги проверки URL, если установлен уровень подробности журнала `LogLevel = Debug`. Значение по умолчанию: `No`

В текущей версии Dr.Web Gateway Security Suite услуга передачи файлов на проверку *File* не используется. Вместо нее следует использовать услугу сканирующего ядра *Engine*.

9.16. Dr.Web URL Checker

Dr.Web URL Checker — вспомогательный компонент, предназначенный для проверки ссылок на вредоносные и нежелательные веб-ресурсы.

Dr.Web URL Checker используется следующими компонентами:

- Dr.Web HTTPD,
- Dr.Web MeshD,
- SpIDer Gate,
- Dr.Web ICAPD

9.16.1. Принципы работы

Компонент Dr.Web URL Checker предназначен для проверки URL на принадлежность к нежелательным или потенциально опасным категориям.

Проверка выполняется либо с помощью специализированных баз ссылок, либо с помощью сервиса Dr.Web CloudD. Чтобы использовать сервис Dr.Web CloudD, выполните команду:

```
# drweb-ctl cfset Root.UseCloud Yes
```

Компонент Dr.Web URL Checker не может быть запущен пользователем. Он запускается демоном управления конфигурацией Dr.Web ConfigD по запросу от других компонентов.

9.16.2. Аргументы командной строки

Для запуска компонента Dr.Web URL Checker из командной строки используется следующая команда:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-urlcheck [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-urlcheck [<параметры>]
```

Dr.Web URL Checker допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента.

	Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-urlcheck --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web URL Checker.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Gateway Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-urlcheck`.

9.16.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[Urlcheck]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`

Параметр	Описание
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-urlcheck` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-urlcheck`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, по превышению которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `None`, если установлен пакет `drweb-scanning-server`, и `10m` в противном случае
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`

9.17. Dr.Web CloudD

Компонент Dr.Web CloudD предназначен для обращения к облачному сервису Dr.Web Cloud компании «Доктор Веб». Сервис Dr.Web Cloud собирает от всех антивирусных продуктов Dr.Web свежую информацию об обнаруженных угрозах с целью ограждения пользователей от посещения нежелательных сайтов и защиты операционных систем серверов и рабочих станций от инфицированных файлов, содержащих новейшие угрозы, описание которых еще не внесено в вирусные базы Dr.Web. Кроме этого, использование облачного сервиса Dr.Web Cloud снижает вероятность ложных срабатываний сканирующего ядра Dr.Web Scanning Engine и компонентов проверки доступа к интернету.

9.17.1. Принципы работы

Компонент предназначен для обращения к облачному сервису Dr.Web Cloud компании «Доктор Веб» с целью проверки содержимого указанного файла на наличие угроз, неизвестных локальному сканирующему ядру Dr.Web Scanning Engine, а также с целью проверки, к каким из предопределенных компанией «Доктор Веб» категорий интернет-ресурсов относится указанный URL. Кроме того, компонент периодически отправляет облачному сервису Dr.Web Cloud статистику обнаружения инфицированных файлов и информацию об операционной системе, на которой запущен Dr.Web Gateway Security Suite.

Dr.Web CloudD автоматически запускается демоном управления конфигурацией в ответ на поступившую команду от пользователя или какого-либо компонента Dr.Web Gateway Security Suite.

Чтобы использовать сервис Dr.Web Cloud, выполните команду:

```
# drweb-ctl cfset Root.UseCloud Yes
```

Через данный компонент запросы к облачному сервису Dr.Web Cloud на проверку URL, к которым обращается пользователь, производит компонент проверки сетевого трафика и URL SpIDer Gate и компонент Dr.Web ICAPD.

Кроме того, компонент используется при проверке файлов по команде от утилиты управления Dr.Web Gateway Security Suite из командной строки Dr.Web Ctl (запускается командой `drweb-ctl`). При обнаружении угроз сканирующее ядро Dr.Web Scanning Engine отправляет отчет о файле в облачный сервис Dr.Web Cloud.

9.17.2. Аргументы командной строки

Для запуска компонента Dr.Web CloudD из командной строки используется следующая команда:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-cloudd [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-cloudd [<параметры>]
```

Dr.Web CloudD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-cloudd --help
```

Эта команда выведет на экран краткую справку компонента Dr.Web CloudD.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Gateway Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-cloudd`.

9.17.3. Параметры конфигурации

Компонент Dr.Web CloudD использует параметры конфигурации, заданные в секции `[CloudD]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-cloudd` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-cloudd`
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `1h`

Параметр	Описание
`FixedSocketPath` *{путь к файлу}*	Путь к файлу Unix-сокета фиксированного экземпляра компонента. При задании этого параметра демон управления конфигурацией Dr.Web ConfigD следит за тем, чтобы всегда имелся запущенный экземпляр компонента, доступный клиентам через этот сокет. Значение по умолчанию: *(не задано)*
`PersistentCache` *{On | Off}*	Включать или нет сохранение на диск кеша ответов, получаемых от Dr.Web Cloud. Значение по умолчанию: `Off`
`DebugSdk` *{логический}*	Включать или нет в журнал на отладочном уровне (при `LogLevel = DEBUG`) подробные сообщения от Dr.Web Cloud. Значение по умолчанию: `No`

9.18. Dr.Web LookupD

Компонент Dr.Web LookupD предназначен для запроса данных из внешних хранилищ данных (текстовых файлов, реляционных баз данных, служб каталогов, поддерживающих обращение по протоколу LDAP). Данные, получаемые компонентом в ответ на запрос из хранилищ данных, могут быть использованы для проверки сетевых соединений (например, для проверки полномочий пользователей и их авторизации), блокировки доступа к URL или сообщения электронной почты в зависимости от выполнения некоторого условия.

В настройках компонента можно указать параметры подключения к нескольким источникам данных. Подключение компонента Dr.Web LookupD к требуемому источнику данных производится только в момент поступления запроса данных от какого-либо компонента Dr.Web Gateway Security Suite.

Компонент Dr.Web LookupD поддерживает обращение к следующим источникам данных:

- текстовые файлы (в режимах *AllMatch*, *Mask*, *Regex*, *Cidr*);
- реляционные базы данных (MySQL, PostgreSQL, SQLite);
- базы данных Redis;
- службы каталогов (Active Directory и иные, обеспечивающие обращение через LDAP, например, OpenLDAP).

Обмен данными по протоколу LDAP может производиться как по открытому каналу, так и по защищенному, с использованием SSL/TLS. При использовании защищенного соединения необходимо обеспечить Dr.Web LookupD корректным сертификатом и ключом SSL. Для генерации ключей и сертификатов, при необходимости, можно воспользоваться утилитой `openssl`. Пример использования утилиты `openssl` для генерации сертификатов и закрытых ключей приведен в разделе Приложение Д. Генерация сертификатов SSL.

9.18.1. Принципы работы

В этом разделе

- Особенности обработки текстовых файлов
- Особенности подключения к БД MySQL

Компонент предназначен для выполнения запросов данных из текстовых файлов, реляционных баз данных, сетевых хранилищ и служб каталогов (таких как Active Directory), поддерживающих протокол LDAP. Получаемые данные (такие как идентификаторы пользователей и их полномочия) передаются затребовавшим их компонентам Dr.Web Gateway Security Suite для использования в различных правилах проверки (например, для разрешения доступа пользователя к запрошенному URL и т. п.).

Данное руководство не описывает механизмы работы реляционных баз данных, сетевой базы данных Redis, служб каталогов и протокол LDAP. При необходимости обратитесь к соответствующим справочным материалам.

Компонент Dr.Web LookupD автоматически запускается демоном управления конфигурацией Dr.Web ConfigD по мере необходимости (при возникновении запросов на получение данных из хранилищ).

При поступлении от некоторого компонента Dr.Web Gateway Security Suite запроса на получение данных, демон управления конфигурацией Dr.Web ConfigD запускает Dr.Web LookupD (если он еще не запущен), после чего компонент выполняет запрос из требуемого источника данных, возвращая ответ. В зависимости от запроса, ответом является список строк, извлеченных из источника данных в соответствии с заданным критерием поиска, либо логическое значение (истина или ложь), указывающее, нашлись ли в результатах поиска строки, соответствующие заданному условию.

В настройках Dr.Web LookupD может быть задано неограниченное число источников данных, при этом, формируя запрос на выборку данных, клиентский компонент Dr.Web Gateway Security Suite должен указать, из какого источника должны быть выбраны данные. После старта и выполнения поступившего запроса, Dr.Web LookupD продолжает работу некоторое время, ожидая поступления новых запросов. В случае их отсутствия Dr.Web LookupD автоматически завершает свою работу после истечения периода ожидания.

Базовый способ использования компонента Dr.Web LookupD другими компонентами Dr.Web Gateway Security Suite — это выборка данных для проверки истинности условий специального вида, указанных в правилах работы компонентов. При проверке правил и определении истинности таких условий запрос данных у Dr.Web LookupD производится автоматически.

Особенности обработки текстовых файлов

1. При обработке текстовых файлов начальные и конечные пробелы в строках отбрасываются. Пустые строки и строки, в которых в качестве первого непробельного символа указан символ #, игнорируются.
2. Текстовые файлы считаются неизменяемыми источниками данных и их содержимое полностью кешируется в памяти. Кроме того, кешируются и результаты запросов к этим файлам на проверку значения. Таким образом, при изменении содержимого файла-источника необходимо заставить Dr.Web LookupD перечитать конфигурацию, для чего можно послать сигнал HUP компоненту Dr.Web ConfigD, например, при помощи команды `drweb-ctl reload`.

Особенности подключения к БД MySQL

Перед соединением с MySQL дополнительно производится чтение параметров из секции `[client]` файла настроек MySQL по умолчанию (данный файл ищется по следующим путям: `/etc/my.cnf`, `/etc/mysql/my.cnf`, `/etc/alternatives/my.cnf`).

9.18.2. Аргументы командной строки

Для запуска компонента Dr.Web LookupD из командной строки используется следующая команда:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-lookupd [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/bin/drweb-lookupd [<параметры>]
```

Dr.Web LookupD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-lookupd --help
```

Данная команда выведет на экран краткую справку компонента Dr.Web LookupD.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами

работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Gateway Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-lookupd`.

9.18.3. Параметры конфигурации

В этом разделе

- Параметры компонента
  - Требования к URI подключения к базам данных
- Секции источников данных
  - Параметры секций типа LDAP
  - Параметры секции типа AD
  - Параметры секций типа AllMatch, Mask, Regex, Cidr
  - Параметры секций типа Pq, Mysql, Sqlite
  - Параметры секций типа Redis
- Добавление секций источников данных

Компонент использует параметры конфигурации, заданные в секции `[LookupD]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

Параметры компонента

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение данного параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию:

Параметр	Описание
	• для GNU/Linux: `/opt/drweb.com/bin/drweb-lookupd` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-lookupd`
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, при превышении которого он завершает работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`
`DebugLibldap` *{логический}*	Включать или не включать в журнал на отладочном уровне (при `LogLevel = DEBUG`) также и отладочные сообщения библиотеки `libldap`. Значение по умолчанию: `No`
`LdapCheckCertificate` *{No | Allow | Try | Yes}*	Режим проверки сертификатов при подключении к LDAP через SSL/TLS. Допустимые значения: • `No` — никогда не запрашивать сертификат сервера. • `Allow` — запрашивать сертификат сервера, и если он не будет предоставлен, то сессия будет продолжена в обычном режиме. Если же серверный сертификат предоставлен, но не может быть проверен (не удалось найти соответствующий корневой сертификат), то сертификат сервера будет проигнорирован и сессия будет продолжена в обычном режиме. • `Try` — запрашивать сертификат сервера, и если он не будет предоставлен, то сессия будет продолжена в обычном режиме. Если же серверный сертификат предоставлен, но не может быть проверен (не удалось найти соответствующий корневой сертификат), то сессия будет прервана. • `Yes` — запрашивать сертификат сервера, и если он не будет предоставлен или серверный сертификат не может быть проверен (не удалось найти соответствующий корневой сертификат), то сессия будет прервана.

Параметр	Описание
	Для источников данных типа `LDAP` влияет на обработку URL по схеме `ldaps://` или с использованием расширения StartTLS. Для источников данных типа `AD` влияет на соединение с сервером, если в соответствующей секции установлено `UseSSL=Yes` (см. ниже). Значение по умолчанию: `Yes`
`LdapCaPath` *{путь}*	Путь к каталогу или файлу, в котором располагается перечень корневых сертификатов, являющихся доверенными при обмене данными по протоколу LDAP через SSL/TLS. Значение по умолчанию: *<путь к системному перечню доверенных сертификатов>*. Зависит от дистрибутива GNU/Linux. • Для Astra Linux, Debian, Linux Mint, SUSE Linux и Ubuntu это обычно путь `/etc/ssl/certs/`. • Для CentOS и Fedora — путь `/etc/pki/tls/certs/ca-bundle.crt`. • Для других дистрибутивов путь может быть определен через результат вызова команды `openssl version -d`. • Если команда недоступна или дистрибутив ОС опознать не удалось, используется значение `/etc/ssl/certs/`.
`LdapCertificatePath` *{путь к файлу}*	Путь к файлу сертификата SSL, используемого для безопасного подключения к серверам LDAP (Active Directory) по SSL/TLS. Файл сертификата и файл закрытого ключа (определяется параметром `LdapKeyPath`) должны соответствовать друг другу. Значение по умолчанию: *(не задано)*
`LdapKeyPath` *{путь к файлу}*	Путь к файлу закрытого ключа, используемого для безопасного подключения к серверам LDAP (Active Directory) по SSL/TLS. Файл сертификата (определяется параметром `LdapCertificatePath`) и файл закрытого ключа должны соответствовать друг другу. Значение по умолчанию: *(не задано)*
`PqDefaultConn` *{URL}*	URI, задающий параметры подключения по умолчанию к базе данных PostgreSQL. Возможные значения: • `tcp://[`*<пользователь>*`[:`*<пароль>*`]@][`*<узел>*`][:`*<порт>*`][/`*<имя базы данных>*`][?`*<параметр>*`=`*<значение>*`[&...]]`; • `unix://[`*<пользователь>*`[:`*<пароль>*`]@]`*<путь к сокету>*`[:`*<имя базы данных>*`][?`*<параметр>*`=`*<значение>*`[&...]]`.

Параметр	Описание
	Необходимо учитывать требования к URI. Значение по умолчанию: *(не задано)*
`SqliteDefaultConn` *{путь к файлу}*	Путь к файлу базы данных SQLite по умолчанию (указывается с префиксом схемы `file://`). Значение по умолчанию: *(не задано)*
`MysqlDefaultConn` *{URL}*	URI, задающий параметры подключения по умолчанию к базе данных MySQL. Возможные значения: • `tcp://[`*<пользователь>*`[:`*<пароль>*`]@][`*<узел>*`][:`*<порт>*`][/`*<имя базы данных>*`][?`*<параметр>*`=`*<значение>*`[&...]]`; • `unix://[`*<пользователь>*`[:`*<пароль>*`]@]`*<путь к сокету>*`[:`*<имя базы данных>*`][?`*<параметр>*`=`*<значение>*`[&...]]`. Необходимо учитывать требования к URI. Значение по умолчанию: *(не задано)*
`RedisDefaultConn` *{URL}*	URL, задающий параметры подключения по умолчанию к базе данных Redis. Возможные значения: • `tcp://[`*<пароль>*`@][`*<узел>*`][:`*<порт>*`][/`*<индекс базы данных>*`];` • `unix://[`*<пароль>*`@]`*<путь к сокету>*`[:`*<индекс базы данных>*`]`. Необходимо учитывать требования к URI. Значение по умолчанию: *(не задано)*
`RedisCaPath` *{путь к файлу}*	Путь к каталогу или файлу, в котором располагается перечень корневых сертификатов, являющихся доверенными при обмене данными с базой данных Redis через SSL/TLS. Значение по умолчанию: *<путь к системному перечню доверенных сертификатов>*. Зависит от дистрибутива GNU/Linux. • Для Astra Linux, Debian, Linux Mint, SUSE Linux и Ubuntu это обычно путь `/etc/ssl/certs/`. • Для CentOS и Fedora — путь `/etc/pki/tls/certs/ca-bundle.crt`.

Параметр	Описание
	• Для других дистрибутивов путь может быть определен через результат вызова команды `openssl version -d`. • Если команда недоступна или дистрибутив ОС опознать не удалось, используется значение `/etc/ssl/certs/`.
`RedisCertificatePath` *{путь к файлу}*	Путь к файлу сертификата SSL, используемого для безопасного подключения к базе данных Redis по SSL/TLS. Файл сертификата и файл закрытого ключа (определяется параметром `RedisKeyPath`) должны соответствовать друг другу. Значение по умолчанию: *(не задано)*
`RedisKeyPath` *{путь к файлу}*	Путь к файлу закрытого ключа, используемого для безопасного подключения к базе данных Redis по SSL/TLS. Файл сертификата (определяется параметром `RedisCertificatePath`) и файл закрытого ключа должны соответствовать друг другу. Значение по умолчанию: *(не задано)*
`DbIdleTimeout` *{интервал времени}*	Период времени ожидания, по окончании которого установленное соединение с базой данных Redis будет разорвано в случае простоя. Значение по умолчанию: `5m`

Требования к URI подключения к базам данных

1. Используются только префиксы схем `tcp://` и `unix://` (для локальных Unix-сокетов). СУБД-специфичные префиксы схемы, такие как `postgresql://` или `mysql://`, не поддерживаются. Путь к файлу БД SQLite указывается с префиксом `file://`.
2. Если поле <*узел*> не указано в URI, или указан узел `localhost`, подставляется адрес узла `127.0.0.1`. В этом случае по умолчанию для БД MySQL и PostgreSQL подключение будет производиться *через локальный Unix-сокет*, несмотря на то, что указано сетевое соединение.
3. При наличии в полях URI (таких как <*пользователь*>, <*пароль*>, <*имя базы данных*> и т. д.) либо в строке параметров подключения специальных символов (пробел, двоеточие и т. п.) необходимо использовать hex-кодирование, например:
   - пробел — %20;
   - : — %3A;
   - / — %2F;
   - @ — %40;

- % — %25.

4. Для БД MySQL строка параметров подключения может включать в себя только следующие параметры:

Имя параметра	Обозначение в документации СУБД	Тип	Описание
`init`	*MYSQL_INIT_COMMAND*	Строка	Команда SQL, которую следует выполнить после подключения к базе данных
`compression`	*MYSQL_OPT_COMPRESS*	Логический	Использовать или не использовать сжатие передаваемых данных
`connect-timeout`	*MYSQL_OPT_CONNECT_TIMEOUT*	Целое число	Тайм-аут разрыва неиспользуемого соединения в секундах
`reconnect`	*MYSQL_OPT_RECONNECT*	Логический	Разрешить или запретить автоматическое переподключение
`read-timeout`	*MYSQL_OPT_READ_TIMEOUT*	Целое число	Тайм-аут на получение пакетов от сервера в секундах
`write-timeout`	*MYSQL_OPT_WRITE_TIMEOUT*	Целое число	Тайм-аут на отправку пакетов серверу в секундах
`charset`	*MYSQL_SET_CHARSET_NAME*	Строка	Кодировка символов, используемая для соединения по умолчанию
`plugin-dir`	*MYSQL_PLUGIN_DIR*	Строка	Путь к каталогу на сервере, хранящему подключаемые модули
`nonblock`	*MYSQL_OPT_NONBLOCK*	Целое число	Размер стека для неблокирующих

Имя параметра	Обозначение в документации СУБД	Тип	Описание
			операций ввода/вывода
`ssl-key`	*MYSQL_OPT_SSL_KEY*	Строка	Путь к закрытому ключу (в формате PEM), использующемуся для организации защищенного соединения
`ssl-cert`	*MYSQL_OPT_SSL_CERT*	Строка	Путь к сертификату открытого ключа (в формате PEM), использующемуся для организации защищенного соединения
`ssl-ca`	*MYSQL_OPT_SSL_CA*	Строка	Путь к файлу (в формате PEM), содержащему доверенные сертификаты CA
`ssl-capath`	*MYSQL_OPT_SSL_CAPATH*	Строка	Путь к каталогу, содержащему доверенные сертификаты CA (в формате PEM)
`ssl-cipher`	*MYSQL_OPT_SSL_CIPHER*	Строка	Список поддерживаемых алгоритмов шифрования для защищенного соединения
`ssl-crl`	*MYSQL_OPT_SSL_CRL*	Строка	Путь к файлу (в формате PEM), содержащему отозванные сертификаты
`ssl-crlpath`	*MYSQL_OPT_SSL_CRLPATH*	Строка	Путь к каталогу, содержащему отозванные сертификаты (в формате PEM)

Имя параметра	Обозначение в документации СУБД	Тип	Описание
`ssl-fp`	*MARIADB_OPT_SSL_FP*	Строка	Хеш SHA1 разрешенного серверного сертификата
`ssl-fp-list`	*MARIADB_OPT_SSL_FP_LIST*	Строка	Путь к файлу, содержащему хеши SHA1 разрешенных серверных сертификатов
`tls-passphrase`	*MARIADB_OPT_TLS_PASSPHRASE*	Строка	Пароль для закрытого ключа клиента, защищенного паролем
`tls-version`	*MARIADB_OPT_TLS_VERSION*	Строка	Список поддерживаемых версий TLS
`server-verify-cert`	*MYSQL_OPT_SSL_VERIFY_SERVER_CERT*	Логический	Разрешить или запретить верификацию серверных сертификатов
`server-public-key-path`	*MYSQL_SERVER_PUBLIC_KEY*	Строка	Путь к файлу (в формате PEM), содержащему открытый ключ RSA сервера

С описанием приведенных параметров вы можете ознакомиться в документации СУБД: https://mariadb.com/kb/en/mysql_optionsv/.

5. Для СУБД PostgreSQL см. дополнительно https://www.postgresql.org/docs/current/libpq-connect.html#LIBPQ-PARAMKEYWORDS.

Секции источников данных

Кроме основной секции `[LookupD]`, в файле конфигурации также задаются секции, описывающие подключения к источникам данных (по одной на каждое подключение). Эти секции именуются по схеме `[LookupD.`<*тип*>`.`<*имя*>`]`, где:

- <*тип*> — тип подключения:
  - `LDAP` — для службы каталогов, использующей LDAP;

- `AD` — для службы каталогов Active Directory;
- `AllMatch` — для текстового файла в режиме *AllMatch* (полное совпадение);
- `Mask` — для текстового файла в режиме *Mask* (соответствие по маске);
- `Regex` — для текстового файла в режиме *Regex* (соответствие регулярному выражению, записанному в стандарте PCRE);
- `Cidr` — для текстового файла в режиме *Cidr* (совпадение IP-адресов и/или диапазонов);
- `Pq` — для базы данных PostgreSQL;
- `Mysql` — для базы данных MySQL;
- `Sqlite` — для базы данных SQLite;
- `Redis` — для базы данных Redis.

- <*имя*> — уникальный идентификатор (тег) подключения для ссылки на него из правил.

Пример: `[LookupD.LDAP.auth1]`.

Секции, описывающие подключение, содержат набор параметров, зависящих от типа источника. Количество секций не ограничено.

1. Параметры секций типа LDAP

Параметр	Описание
`Url` *{строка}*	URL, определяющий используемый сервер LDAP и извлекаемые данные. Согласно RFC 4516, URL строится по схеме: <*scheme*>`://`<*host*>`[:`<*port*>`]/`<*dn*>`[?`<*attrs*>`[?`<*scope*>`[?`<*filter*>`[?`<*extensions*>`]]]]` Здесь: <*scheme*> — способ подключения к серверу (допускаются схемы `ldap`, `ldaps` и `ldapi`); <*host*>`[:`<*port*>`]` — адрес сервера LDAP, к которому направляется запрос; <*dn*> — уникальное имя (distinguished name) объекта, информация о котором получается; <*attrs*> — имена атрибутов записей, значения которых должны быть получены в запросе; <*scope*> — область поиска (`base`, `one`, `sub`); <*filter*> — фильтрующее условие на значения извлекаемых атрибутов; <*extensions*> — перечень используемых в запросе расширений LDAP.

Особенности

- В списке атрибутов <*attrs*> можно использовать спецсимволы выбора `*`, `+` и `1.1`.
- В частях URL <*dn*> и <*filter*> могут быть использованы следующие автоматически разрешаемые маркеры:
  - `$u` — заменяется на `user` — имя пользователя, переданное клиентским компонентом;
  - `$d` — заменяется на `domain` — имя домена, переданное клиентским компонентом;
  - `$D` — цепочка <*subdomain*>.<*domain*>, преобразованная в `dc=`<*subdomain*>`,dc=`<*domain*>;
  - `$$` — символ `$`.
- Если в условии <*filter*> требуется использовать специальные символы (например: `*`, `(`, `)`, `\`, символ с кодом 0) как обычные, то их следует записывать в виде `\XX`. Кроме того, специальные символы в URL LDAP кодируются с помощью последовательностей `%XX`. Например, при использовании символа `/` в URL по схеме `ldapi` в качестве части пути к локальному сокету сервера LDAP этот символ кодируется как `%2f`.
- В качестве допустимых расширений в <*extensions*> поддерживаются только `StartTLS` и `1.3.6.1.4.1.1466.20037`, которые включают использование механизма TLS (т. е. организация защищенного соединения с сервером LDAP, даже если явно не указано использование защищенной схемы `ldaps`). Если перед именем используемого расширения указан символ `!`, то использование TLS *обязательно*, т. е. в случае невозможности установки безопасного соединения запрос *не будет* исполнен. В противном случае запрос будет исполнен, даже если безопасное соединение не будет установлено.

  Указанные расширения не могут применяться в случае использования защищенной схемы `ldaps`. Для получения более подробной информации см. RFC 4516 или `man ldap_search_ext_s`.

Примеры:

```
ldaps://ds.example.com:990/$D?givenName,sn,cn?sub?
(uid=$u)
ldap://ldap.local/o=org,dc=nodomain?
ipNetworkNumber?sub?(objectClass=ipNetwork)?
!StartTLS
```

Значение по умолчанию: *(не задано)*

`BindDn` *{строка}*	Объект в каталоге LDAP, связываемый с пользователем для авторизации. Пример: `cn=admin,dc=nodomain` Значение по умолчанию: *(не задано)*
`BindPassword` *{строка}*	Пароль для аутентификации доступа к серверу LDAP. Значение по умолчанию: *(не задано)*
`ChaseReferrals` *{логический}*	Следовать или не следовать по отсылкам на другие LDAP-серверы, если текущий сервер LDAP присылает их в ответ на запросы. Значение по умолчанию: `No`

2. Параметры секции типа AD

Параметр	Описание
`Host` *{строка}*	Доменное имя (FQDN) или IP-адрес узла, на котором находится сервер службы Active Directory, к которому необходимо подключиться. Пример: `win2012.win.local` Значение по умолчанию: *(не задано)*
`Port` *{целое число}*	Порт на узле, прослушиваемый сервером службы Active Directory. Значение по умолчанию: `389`
`Dn` *{строка}*	*DN* объекта в каталоге Active Directory (аналог части `dn` в URL LDAP). Пример: `dc=win,dc=local` Значение по умолчанию: *(не задано)*
`User` *{строка}*	Полный идентификатор пользователя на сервере. Пример: `Administrator@WIN.LOCAL` Значение по умолчанию: *(не задано)*
`Password` *{строка}*	Пароль для аутентификации доступа к серверу Active Directory. Значение по умолчанию: *(не задано)*
`ChaseReferrals` *{логический}*	Следовать или не следовать по отсылкам на другие LDAP-серверы, если текущий сервер Active Directory присылает их в ответ на запросы. Значение по умолчанию: `No`
`UseSSL` *{логический}*	Использовать или не использовать SSL/TLS при обращении к серверу Active Directory.

	Значение по умолчанию: `No`

3. Параметры секций типа AllMatch, Mask, Regex, Cidr

Параметр	Описание
`File` *{путь}*	Путь к текстовому файлу, содержащему строки для поиска. Пример: `/etc/file1` Значение по умолчанию: *(не задано)*

Особенности

- Строки из файла, указанного в секции типа `AllMatch`, используются для поиска полного совпадения строк без учета регистра символов.
- Строки файла, указанного в секции типа `Mask`, трактуются как маски (*wildcards*). Маски можно рассматривать как упрощенный вариант регулярных выражений, содержащих, помимо стандартных символов, служебные символы. Сравнение строк с масками идет без учета регистра символов. Маски могут содержать следующие служебные символы и выражения:

  `*` — любая последовательность символов;

  `?` — один любой символ;

  `[`<*набор символов*>`]` — один любой символ из указанного набора (например, `[bac]`);

  `[!`<*набор символов*>`]` — один любой символ, не соответствующий ни одному символу из набора (например, `[!cab]`);

  `[[:`<*класс*>`:]]` — один любой символ из указанного POSIX-класса символов (*alnum*, *alpha*, *ascii*, *blank*, *cntrl*, *digit*, *graph*, *lower*, *print*, *punct*, *space*, *upper*, *xdigit*).

Маска, соответствующая некоторой подстроке, должна содержать искомую подстроку, обрамленную символами `*` (например, `*host*`). При необходимости задать в маске один из служебных символов, его необходимо экранировать косой чертой: `\[`, `\]`, `\*`, `\?`. Косая черта, при необходимости, также экранируется: `\\`. Экранирование любых других символов смысла не имеет, то есть строка `\a\b\c\*\d\?\\` будет преобразована в строку `abc*d?\`. Примеры масок:

```
#Соответствует в точности строке name
name

#Соответствует трехсимвольным строкам, у которых
#первый символ — c, второй символ — любой, а третий — t
#Например: cat, cut, cct
c?t

#Соответствует строкам: user, users, us3rr, ussr1 и так далее
#(символьному классу [:alpha:] соответствует любой алфавитный
#символ, а спецсимволу ? — любой символ)
us[[:alpha:]34]r?

#Соответствует строкам: .con, file.col, 3...co! и так далее
#(перед .co - любая последовательность символов, после —
#один любой символ, кроме m и ?)
*.co[!m\?]

#Соответствует любой строке, содержащей в себе часть host,
#например: host, localhost, hostel, ghosts
*host*
```

- Строки из файла, указанного в секции типа `Regex`, трактуются как регулярные выражения PCRE (*Perl Compatible Regular Expressions*). Сопоставление строк с регулярными выражениями производится без учета регистра символов. Примеры регулярных выражений:

```
#IPv4
(\d{1,3}.){3}\d{1,3}

#Адрес электронной почты в домене .com
\w+@\w+\.com
```

- Строки из файла, указанного в секции типа *Cidr*, трактуются как IP-адреса или диапазоны IP-адресов. Допускаются варианты указания как IP-адресов (и диапазонов) IPv4, так и IPv6. Маска подсети может быть указана как в битовом (октетном) формате, так и в нотации CIDR (*Classless Inter-Domain Routing*), например:

```
#IPv4
192.168.0.1
192.168.0.0/12
192.168.0.0/255.255.255.224

#IPv6
fe80::c7e8/32
fe80::c7e8/255.255.255.224
```

4. Параметры секций типа Pq, Mysql, Sqlite

Параметр	Описание
`Conn` *{строка}*	Строка соединения с базой данных.

	Возможные значения:
	• для секций `Mysql` (MySQL) и `Pq` (PostgreSQL):
	`tcp://[`*<пользователь>[:<пароль>]@]<узел>[:<порт>][/<имя базы данных>][?<параметр>=<значение>[&...]]*;
	`unix://[`*<пользователь>[:<пароль>]@]<путь к сокету>[:<имя базы данных>][?<параметр>=<значение>[&...]]*;
	Примеры:
	`tcp://user:pwd@localhost:1234/userdb`
	`unix://user:pwd@/tmp/pgsql.sock:userdb`
	Необходимо учитывать требования к URI.
	• для секции `Sqlite` (SQLite):
	Путь к файлу базы данных (указывается с префиксом схемы `file://`).
	Пример: `file:///home/user/users.db`
	Значение по умолчанию: *определяется значением* соответствующего параметра `*DefaultConn`

`Request` *{строка}*	Строка SQL-запроса (`SELECT`) к базе данных. Как и для источников типа `AD` и `LDAP`, в запросе могут быть использованы следующие автоматически разрешаемые маркеры: • `$u`, `$U` — заменяется на `user` — имя пользователя, переданное клиентским компонентом; • `$d`, `$D` — заменяется на `domain` — имя домена, переданное клиентским компонентом; • `$$` — заменяется на символ `$`. Пример: `SELECT username FROM users INNER JOIN domains ON users.domain = domains.id WHERE domains.name = $d AND users.name = $u` Значение по умолчанию: *(не задано)*

В качестве SQL-запроса может быть указан только запрос типа `SELECT`. После выполнения подстановок запрос передается в базу данных «как есть». Если результат запроса содержит больше одного столбца, то все столбцы, кроме первого, будут проигнорированы.

5. Параметры секций типа Redis

Параметр	Описание
`Conn`	Строка соединения с базой данных Redis.

{строка}	Возможные значения: • `tcp://[`*<пароль>*`@]`*<узел>*`[:`*<порт>*`][/`*<индекс базы данных>*`]`; • `unix://[`*<пароль>*`@]`*<путь к сокету>*`[:`*<индекс базы данных>*`]`; Необходимо учитывать требования к URI. Пример: `tcp://localhost:6379` Значение по умолчанию: *определяется значением* параметра `RedisDefaultConn`
`Request` *{строка}*	Строка запроса данных из базы данных Redis. В запросе могут быть использованы следующие автоматически разрешаемые маркеры: • `$u`, `$U` — заменяется на `user` — имя пользователя, переданное клиентским компонентом; • `$d`, `$D` — заменяется на `domain` — имя домена, переданное клиентским компонентом; • `$$` — заменяется на символ `$`. Пример: `HVALS bad_users` Значение по умолчанию: *(не задано)*
`UseSSL` *{логический}*	Использовать или не использовать SSL/TLS при соединении с базой данных Redis. Значение по умолчанию: `No`

Если результат запроса содержит больше одного столбца, то все столбцы, кроме первого, будут проигнорированы.

Добавление секций источников данных

Чтобы добавить новую секцию параметров для источника данных какого-либо типа с тегом *<имя>* при помощи утилиты Dr.Web Ctl, предназначенной для управления Dr.Web Gateway Security Suite из командной строки (запускается командой `drweb-ctl`), достаточно использовать команду:

```
# drweb-ctl cfset LookupD.<тип> -a <имя>
```

Пример:

```
# drweb-ctl cfset LookupD.AD -a WinAD1
# drweb-ctl cfset LookupD.AD.WinAD1.Host 192.168.0.20
```

Первая команда добавит в файл конфигурации секцию `[LookupD.AD.WinAD1]`, а вторая изменит в ней значение параметра `Host`.

Кроме того, вы можете записать новую секцию непосредственно в файл конфигурации (например, добавив ее в конец файла):

```
[LookupD.AD.WinAD1]
Host = 192.168.0.20
```

Оба способа задания настроек приведут к одинаковому результату, но в случае непосредственной правки файла конфигурации необходимо применить измененные настройки, перезагрузив конфигурацию Dr.Web Gateway Security Suite с помощью команды:

```
# drweb-ctl reload
```

9.19. Dr.Web StatD

Компонент Dr.Web StatD предназначен для накопления статистики событий, возникающих в процессе работы компонентов Dr.Web Gateway Security Suite. Полученные события регистрируются в постоянном хранилище и могут быть получены по запросу.

9.19.1. Принципы работы

Компонент Dr.Web StatD обеспечивает накопление и постоянное хранение событий, поступающих от компонентов Dr.Web Gateway Security Suite в процессе работы. Регистрируются события неожиданного завершения работы компонента.

Dr.Web StatD работает в режиме демона и автоматически запускается демоном управления конфигурацией Dr.Web ConfigD. Просмотр событий и управление ими обеспечивается командой `events` утилиты Dr.Web Ctl.

9.19.2. Аргументы командной строки

Для запуска компонента Dr.Web StatD из командной строки используется следующая команда:

- для GNU/Linux:

```
$ /opt/drweb.com/bin/drweb-statd [<параметры>]
```

- для FreeBSD:

```
$ /usr/local/libexec/drweb.com/drweb-statd [<параметры>]
```

Dr.Web StatD допускает использование следующих параметров:

Параметр	Описание
`--help`	Назначение: Вывод на экран консоли или эмулятора терминала краткой справки по имеющимся параметрам командной строки и завершение работы компонента. Краткий вариант: `-h` Аргументы: Нет
`--version`	Назначение: Вывод на экран консоли или эмулятора терминала информации о версии компонента и завершение работы. Краткий вариант: `-v` Аргументы: Нет

Пример:

```
$ /opt/drweb.com/bin/drweb-statd --help
```

Эта команда выведет на экран краткую справку компонента Dr.Web StatD.

Замечания о запуске

Запуск компонента в автономном режиме непосредственно из командной строки не предусмотрен. Компонент запускается автоматически демоном управления конфигурацией Dr.Web ConfigD при необходимости. Для управления параметрами работы компонента используйте утилиту Dr.Web Ctl, предназначенную для управления Dr.Web Gateway Security Suite из командной строки.

Для запуска утилиты Dr.Web Ctl используйте команду `drweb-ctl`.

Для получения справки о компоненте из командной строки используйте команду `man 1 drweb-statd`.

9.19.3. Параметры конфигурации

Компонент использует параметры конфигурации, заданные в секции `[StatD]` объединенного конфигурационного файла Dr.Web Gateway Security Suite.

В секции представлены следующие параметры:

Параметр	Описание
`LogLevel` *{уровень подробности}*	Уровень подробности ведения журнала компонента. Если значение параметра не указано, используется значение параметра `DefaultLogLevel` из секции `[Root]`. Значение по умолчанию: `Notice`
`Log` *{тип журнала}*	Метод ведения журнала компонента. Значение по умолчанию: `Auto`
`ExePath` *{путь к файлу}*	Путь к исполняемому файлу компонента. Значение по умолчанию: • для GNU/Linux: `/opt/drweb.com/bin/drweb-statd` • для FreeBSD: `/usr/local/libexec/drweb.com/bin/drweb-statd`

Параметр	Описание
`IdleTimeLimit` *{интервал времени}*	Максимальное время простоя компонента, по превышению которого он завершает свою работу. Допустимые значения: от 10 секунд (`10s`) до 30 дней (`30d`). Если установлено значение `None`, то компонент будет работать постоянно; в случае отсутствия активности ему не будет отправлен сигнал SIGTERM. Значение по умолчанию: `10m`
`RunAsUser` *{UID | имя пользователя}*	Пользователь, от имени которого запускается компонент. Вы можете указать числовой идентификатор пользователя (UID) или его имя (логин). Если имя пользователя состоит из цифр (т. е. похоже на числовой UID), то оно указывается с префиксом `name:`, например, `RunAsUser = name:123456`. Если имя пользователя указано некорректно, работа компонента завершается ошибкой сразу после попытки запуска. Значение по умолчанию: `drweb`
`MaxEventStoreSize` *{размер}*	Максимальный разрешенный размер базы событий. Задается в `mb`, например: `MaxEventStoreSize = 100mb`. Минимальное значение: `50mb`. Значение по умолчанию: `1GB`

10. Приложения

10.1. Приложение A. Виды компьютерных угроз

В этом разделе

- Компьютерные вирусы
- Компьютерные черви
- Троянские программы
- Программы взлома
- Рекламные программы
- Программы-шутки
- Программы дозвона
- Потенциально опасные программы
- Подозрительные объекты

Под термином *«угроза»* в этой классификации понимается любое программное средство, косвенно или напрямую способное нанести ущерб компьютеру, сети, информации или правам пользователя (то есть вредоносные и прочие нежелательные программы). В более широком смысле термин «угроза» может означать любую потенциальную опасность для компьютера или сети (то есть ее уязвимость, которая может быть использована для проведения хакерских атак).

Все типы программ, описанные ниже, потенциально обладают способностью подвергнуть опасности данные пользователя или их конфиденциальность. Программы, которые не скрывают своего присутствия в системе (например, некоторые программы для рассылки спама или анализаторы трафика), обычно не принято причислять к компьютерным угрозам, хотя при определенных обстоятельствах они также могут нанести вред пользователю.

Компьютерные вирусы

Данный тип компьютерных угроз характеризуется способностью внедрять свой код в исполняемый код других программ. Такое внедрение называется *инфицированием*. В большинстве случаев инфицированный файл сам становится носителем вируса, а внедренный код не обязательно полностью соответствует оригиналу. Значительное число вирусов создается для повреждения или уничтожения данных.

В компании «Доктор Веб» вирусы классифицируются по типам файлов, которые они инфицируют:

- *Файловые вирусы* инфицируют файлы операционной системы (обычно исполняемые файлы и динамические библиотеки) и активизируются при обращении к инфицированному файлу.
- *Макро-вирусы* инфицируют документы, которые используют программы из пакета Microsoft® Office (и другие программы, которые используют макросы, написанные, например, на языке Visual Basic). *Макросы* — это встроенные программы, написанные на полноценном языке программирования, которые могут запускаться при определенных условиях (например, в Microsoft® Word макросы могут запускаться при открытии, закрытии или сохранении документа).
- *Скрипт-вирусы* пишутся на языках скриптов и в большинстве случаев инфицируют другие файлы скриптов (например, служебные файлы операционной системы). Они также могут инфицировать файлы других типов, которые поддерживают исполнение скриптов, и могут распространяться, например, посредством уязвимых веб-приложений.
- *Загрузочные вирусы* инфицируют загрузочные секторы дисков и разделов, а также главные загрузочные секторы жестких дисков. Они занимают очень мало памяти и остаются готовыми к выполнению своих функций до тех пор, пока не будет произведена выгрузка, перезагрузка или завершение работы системы.

Большинство вирусов обладает определенными механизмами защиты от обнаружения, которые постоянно улучшаются, поэтому для антивирусных программ разрабатываются новые способы преодоления этой защиты. Вирусы можно разделить по принципу защиты от обнаружения:

- *Шифрованные вирусы* шифруют свой код при каждом новом инфицировании, что затрудняет его обнаружение в файле, памяти или загрузочном секторе. Каждый экземпляр таких вирусов содержит только короткий общий фрагмент (процедуру расшифровки), который можно выбрать в качестве сигнатуры.
- *Полиморфные вирусы* используют помимо шифрования кода специальную процедуру расшифровки, изменяющую саму себя в каждом новом экземпляре вируса, что ведет к отсутствию у такого вируса байтовых сигнатур.
- *Стелс-вирусы* (вирусы-невидимки) предпринимают специальные действия для маскировки своей деятельности с целью сокрытия своего присутствия в инфицированных объектах. Такой вирус снимает характеристики объекта перед его инфицированием, а затем передает старые данные при запросе операционной системы или программы, ищущей измененные файлы.

Вирусы также можно классифицировать по языку, на котором они написаны (например, низкоуровневый типа языка ассемблера или высокоуровневый типа языка Go) и по инфицируемым ими операционным системам.

Компьютерные черви

Как и вирусы, программы типа *«компьютерный червь»* способны создавать свои копии, но при этом они не инфицируют другие объекты. Червь проникает на компьютер из сети (чаще всего во вложениях сообщений электронной почты или через интернет) и рассылает свои функциональные копии на другие компьютеры. Черви используют действия пользователя, либо распространяются автоматически.

Черви не обязательно целиком состоят из одного файла (тела червя). У многих червей есть так называемая инфекционная часть (шелл-код), которая загружается в оперативную память компьютера и «догружает» по сети непосредственно само тело червя в виде исполняемого файла. Пока в системе нет тела червя, от него можно избавиться перезагрузкой компьютера (при которой происходит сброс оперативной памяти). Если же в системе оказывается тело червя, то справиться с ним может только антивирус.

За счет интенсивного распространения черви способны вывести из строя целые сети, даже если они не несут никакой полезной нагрузки (не наносят прямой вред системе).

В компании «Доктор Веб» червей классифицируют по способу (среде) распространения:

- *Сетевые черви* распространяются посредством различных сетевых протоколов и протоколов обмена файлами.
- *Почтовые черви* распространяются посредством почтовых протоколов (POP3, SMTP и т. д.).
- *Чат-черви* распространяются, используя популярные системы мгновенного обмена сообщениями (ICQ, IM, IRC и т. д.).

Троянские программы

Вредоносные программы этого типа не способны к саморепликации. Троянские программы выдают себя за одну из популярных программ и выполняют ее функции (или имитируют исполнение этих функций), одновременно производя какие-либо вредоносные действия (повреждение и удаление данных, пересылка конфиденциальной информации и т. д.), либо делая возможным несанкционированное использование компьютера злоумышленником, например, для нанесения вреда третьим лицам.

Эти программы обладают схожими с вирусом маскировочными и вредоносными функциями и даже могут быть модулем вируса, но, как правило, троянские программы распространяются как отдельные исполняемые файлы (выкладываются на файловых сервера, записываются на носители информации или пересылаются в виде вложений в сообщениях электронной почты), которые запускаются либо самим пользователем, либо определенным процессом системы.

Классифицировать троянские программы очень непросто, во-первых, потому что они зачастую распространяются вирусами и червями, во-вторых, вредоносные действия, которые могут выполняться другими типами угроз, принято приписывать только троянским программам. Ниже приведен список некоторых типов троянских программ, которые в компании «Доктор Веб» выделяют в отдельные классы:

- *Бэкдоры* — это троянские программы, которые позволяют получать привилегированный доступ к системе в обход существующего механизма предоставления доступа и защиты. Бэкдоры не инфицируют файлы.
- *Руткиты* предназначены для перехвата системных функций операционной системы с целью сокрытия своего присутствия в системе. Кроме того, руткит может маскировать процессы других программ, каталоги, файлы. Руткит распространяется как самостоятельная программа или как дополнительный компонент в составе другой вредоносной программы. По принципу своей работы руткиты условно разделяют на две группы: руткиты, работающие в режиме пользователя (перехват функций библиотек пользовательского режима) (*User Mode Rootkits — UMR*), и руткиты, работающие в режиме ядра (перехват функций на уровне ядра системы, что значительно усложняет обнаружение и обезвреживание) (*Kernel Mode Rootkits — KMR*).
- *Клавиатурные перехватчики* (*кейлоггеры*) используются для сбора данных, которые пользователь вводит при помощи клавиатуры. Целью таких действий является кража личной информации (например, сетевых паролей, логинов, номеров банковских карт и т. д.).
- *Кликеры* переопределяют ссылки при нажатии на них и таким образом перенаправляют пользователей на определенные (возможно, вредоносные) сайты. Обычно пользователь перенаправляется с целью увеличения рекламного трафика сайтов или для организации распределенных атак отказа в обслуживании (DDoS-атак).
- *Прокси-трояны* предоставляют злоумышленнику анонимный выход в интернет через компьютер жертвы.

Кроме перечисленных выше, троянские программы могут выполнять и другие вредоносные действия, например, изменять стартовую страницу в веб-браузере или удалять определенные файлы. Однако такие действия могут выполняться и угрозами других типов (например, вирусами и червями).

Программы взлома

Программы взлома созданы с целью помочь взломщику. Наиболее распространенным видом подобных программ являются сканеры портов, которые позволяют обнаруживать уязвимости в межсетевых экранах (файерволах, брандмауэрах) и других компонентах, обеспечивающих безопасность компьютера. Кроме хакеров, такими инструментами могут пользоваться администраторы для проверки надежности своих сетей. Иногда к программам взлома относят программы, использующие методы социальной инженерии (элементы социотехники).

Рекламные программы

Чаще всего под этим термином понимают программный код, встроенный в различное бесплатное программное обеспечение, при использовании которого пользователю принудительно показывается реклама. Но иногда такой код может скрытно распространяться посредством других вредоносных программ и демонстрировать рекламу, например, в веб-браузерах. Зачастую рекламные программы работают на основании данных, собранных шпионскими программами.

Программы-шутки

Это тип вредоносных программ, которые, как и рекламные программы, не наносят прямого вреда системе. Чаще всего они генерируют сообщения о несуществующих ошибках и угрожают действиями, которые могут привести к повреждению данных. Их основной функцией является запугивание пользователя, либо навязчивое его раздражение.

Программы дозвона

Это специальные компьютерные программы, разработанные для сканирования некоего диапазона телефонных номеров для нахождения такого, на который ответит модем. В дальнейшем злоумышленники используют найденные номера для накручивания оплаты за телефон или для незаметного подключения пользователя через модем к дорогостоящим платным телефонным службам.

Потенциально опасные программы

Эти программы не создавались для нанесения вреда, но в силу своих особенностей могут представлять угрозу для безопасности системы. К таким программам относятся не только те, которые могут случайно повредить или удалить данные, но и те, которые могут использоваться злоумышленниками или другими программами для нанесения вреда системе. К потенциально опасным программам можно отнести различные программы удаленного общения и администрирования, FTP-серверы и т. д.

Подозрительные объекты

К подозрительным объектам относятся любые потенциальные угрозы, обнаруженные при помощи эвристического анализа. Такие объекты могут относиться к любому типу компьютерных угроз (возможно, даже неизвестному для специалистов по информационной безопасности), а могут оказаться безопасными в случае ложного срабатывания. Файлы, содержащие подозрительные объекты, рекомендуется помещать

в карантин, а также отправлять на анализ специалистам антивирусной лаборатории «Доктор Веб».

10.2. Приложение Б. Устранение компьютерных угроз

В этом разделе

- Методы обнаружения угроз
  - Сигнатурный анализ
  - Origins Tracing™
  - Эмуляция исполнения
  - Эвристический анализ
  - Облачные технологии обнаружения угроз
- Действия с угрозами

Все антивирусные продукты, разработанные компанией «Доктор Веб», применяют целый набор методов обнаружения угроз, что позволяет проверять подозрительные объекты максимально тщательно.

Методы обнаружения угроз

Сигнатурный анализ

Этот метод обнаружения применяется в первую очередь. Он выполняется путем проверки содержимого анализируемого объекта на предмет наличия в нем сигнатур уже известных угроз. Сигнатурой называется непрерывная конечная последовательность байт, необходимая и достаточная для однозначной идентификации угрозы. При этом сравнение содержимого исследуемого объекта с сигнатурами производится не напрямую, а по их контрольным суммам, что позволяет значительно снизить размер записей в вирусных базах, сохранив при этом однозначность соответствия и, следовательно, корректность обнаружения угроз и лечения инфицированных объектов. Записи в вирусных базах Dr.Web составлены таким образом, что благодаря одной и той же записи можно обнаруживать целые классы или семейства угроз.

Origins Tracing™

Это уникальная технология Dr.Web, которая позволяет определять новые и модифицированные угрозы, использующие уже известные и описанные в вирусных базах механизмы инфицирования и нанесения ущерба. Она выполняется по окончании сигнатурного анализа и обеспечивает защиту пользователей, использующих антивирусные решения Dr.Web от таких угроз, как троянская программа-вымогатель Trojan.Encoder.18 (также известная под названием gpcode). Кроме того, использование технологии Origins Tracing™ позволяет значительно снизить количество ложных

срабатываний эвристического анализатора. К названиям угроз, обнаруженных при помощи Origins Tracing™, добавляется постфикс `.Origin`.

Эмуляция исполнения

Метод эмуляции исполнения программного кода используется для обнаружения полиморфных и шифрованных вирусов, когда использование поиска по контрольным суммам сигнатур неприменимо или значительно усложнено из-за невозможности построения надежных сигнатур. Метод состоит в имитации исполнения анализируемого кода при помощи *эмулятора* — программной модели процессора и среды исполнения программ. Эмулятор оперирует с защищенной областью памяти (*буфером эмуляции*). При этом инструкции не передаются на центральный процессор для реального исполнения. Если код, обрабатываемый эмулятором, инфицирован, то результатом его эмуляции станет восстановление исходного вредоносного кода, доступного для сигнатурного анализа.

Эвристический анализ

Работа эвристического анализатора основывается на наборе *эвристик* — предположений о характерных признаках как вредоносного, так и безопасного исполняемого кода, статистическая значимость которых подтверждена опытным путем. Каждый признак кода имеет определенный *вес* (т. е. число, показывающее важность и достоверность этого признака). Вес может быть как положительным, если признак указывает на наличие вредоносного поведения кода, так и отрицательным, если признак не свойственен компьютерным угрозам. На основании суммарного веса, характеризующего содержимое объекта, эвристический анализатор вычисляет вероятность содержания в нем неизвестного вредоносного объекта. Если эта вероятность превышает некоторое пороговое значение, то выдается заключение о том, что анализируемый объект является вредоносным.

Эвристический анализатор также использует технологию FLY-CODE™ — универсальный алгоритм распаковки файлов. Этот механизм позволяет строить эвристические предположения о наличии вредоносных объектов в объектах, сжатых программами упаковки (упаковщиками), причем не только известными разработчикам продукта Dr.Web, но и новыми, ранее не исследованными программами. При проверке запакованных объектов также используется технология анализа их структурной энтропии, которая позволяет обнаруживать угрозы по особенностям расположения участков их кода. Эта технология позволяет на основе одной записи вирусной базы произвести обнаружение набора различных угроз, запакованных одинаковым полиморфным упаковщиком.

Поскольку эвристический анализатор является системой проверки гипотез в условиях неопределенности, то он может допускать ошибки как первого (пропуск неизвестных угроз), так и второго рода (признание безопасной программы вредоносной). Поэтому

объектам, отмеченным эвристическим анализатором как «вредоносные», присваивается статус «подозрительные».

Во время любой из проверок все компоненты антивирусных продуктов Dr.Web используют самую свежую информацию обо всех известных вредоносных программах. Сигнатуры угроз и информация об их признаках и моделях поведения обновляются и добавляются в вирусные базы сразу же, как только специалисты антивирусной лаборатории «Доктор Веб» обнаруживают новые угрозы, иногда до нескольких раз в час. Даже если новейшая вредоносная программа проникает на компьютер, минуя резидентную защиту Dr.Web, то она будет обнаружена в списке процессов и нейтрализована после получения обновленных вирусных баз.

Облачные технологии обнаружения угроз

Облачные методы обнаружения позволяют проверить любой объект (файл, приложение, расширение для браузера и т. п.) по *хеш-сумме*. Она представляет собой уникальную последовательность цифр и букв заданной длины. При анализе по хеш-сумме объекты проверяются по существующей базе и затем классифицируются на категории: чистые, подозрительные, вредоносные и т. д.

Подобная технология оптимизирует время проверки файлов и экономит ресурсы устройства. Благодаря тому, что анализируется не сам объект, а его уникальная хеш-сумма, решение выносится практически моментально. При отсутствии подключения к серверам Dr.Web Cloud, файлы проверяются локально, а облачная проверка возобновляется при восстановлении связи.

Таким образом, облачный сервис Dr.Web Cloud собирает информацию от многочисленных пользователей и оперативно обновляет данные о ранее неизвестных угрозах, тем самым повышая эффективность защиты устройств.

Действия с угрозами

В продуктах Dr.Web реализована возможность применять определенные действия к обнаруженным объектам для обезвреживания компьютерных угроз. Пользователь может оставить автоматически применяемые к определенным типам угроз действия, заданные по умолчанию, изменить их или выбирать нужное действие для каждого обнаруженного объекта отдельно. Ниже приведен список доступных действий. В скобках указан параметр, обозначающий соответствующее действие и используемый в объединенном конфигурационном файле, правилах проверки трафика и командах утилиты Dr.Web Ctl.

- **Сообщать** (`REPORT`) — уведомить о наличии угрозы, но ничего не делать с инфицированным объектом.
- **Лечить** (`CURE`) — попытаться вылечить инфицированный объект, удалив из него вредоносное содержимое, и оставив в целости полезное содержимое.

Это действие применимо не ко всем видам угроз.

- **В карантин** (`QUARANTINE`) — переместить инфицированный объект (если он допускает эту операцию) в специальный каталог карантина с целью его изоляции.
- **Удалить** (`DELETE`) — безвозвратно удалить инфицированный объект.

Если угроза обнаружена в файле, находящемся в контейнере (архив, почтовое сообщение и т. п.), вместо удаления выполняется перемещение контейнера в карантин.

10.3. Приложение B. Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

1. Ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.com/doc/.
2. Прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/.
3. Посетите форумы компании «Доктор Веб» по адресу https://forum.drweb.com/.

Если после этого не удалось решить проблему, вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки компании «Доктор Веб»:

1. Заполните веб-форму в соответствующей секции раздела https://support.drweb.com/.
2. Позвоните по телефону в Москве: +7 (495) 789-45-86 или по бесплатной линии для всей России: 8-800-333-7932.

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте по адресу https://company.drweb.com/contacts/offices/.

Для упрощения работы службы технической поддержки по анализу возникшей у вас проблемы рекомендуется предварительно сформировать пакет информации об установленном у вас продукте, его настройках и системном окружении. Для этого предназначена специализированная утилита, входящая в состав Dr.Web Gateway Security Suite.

Для сбора информации для службы технической поддержки введите следующую команду:

- для GNU/Linux:

```
# /opt/drweb.com/bin/support-report.sh <путь к файлу>
```

- для FreeBSD:

```
# /usr/local/libexec/drweb.com/bin/support-report.sh <путь к файлу>
```

где *<путь к файлу>* — путь к архиву в формате `.tgz`, в котором будет сохранена отладочная информация о продукте и системном окружении, например, `/tmp/report.tgz`. Уже имеющиеся файлы не перезаписываются. Если путь не указан, то архив будет сохранен в каталоге суперпользователя, запустившего утилиту (например, `/root`), и будет называться следующим образом:

```
drweb.report.<timestamp>.tgz
```

где *<timestamp>* — полная метка времени создания отчета, включая миллисекунды, например: 20190618151718.23625.

Утилиту для сбора информации для службы технической поддержки необходимо запускать с правами суперпользователя (*root*). Для получения прав суперпользователя воспользуйтесь командой смены пользователя `su` или командой выполнения от имени другого пользователя `sudo`.

В процессе работы утилита собирает и упаковывает в архив следующую информацию:

- информация об ОС (название, архитектура, вывод команды `uname -a`);
- список установленных в системе пакетов, в том числе пакетов «Доктор Веб»;
- содержимое журналов:
  - журналы Dr.Web Gateway Security Suite (если настроены для отдельных компонентов);
  - журнал, ведущийся демоном журналирования `syslog` (`/var/log/syslog`, `/var/log/messages`);
  - журнал системного пакетного менеджера (`apt`, `yum` и т. п.);
  - журнал `dmesg`;
- результаты запуска команд `df`, `ip a` (`ifconfig -a`), `ldconfig -p`, `iptables-save`, `nft export xml`.
- информация о настройках и конфигурации Dr.Web Gateway Security Suite:
  - перечень загруженных вирусных баз (`drweb-ctl baseinfo -l`);
  - перечень файлов из каталогов Dr.Web Gateway Security Suite и их MD5-хеши;
  - версия и MD5-хеш файла антивирусного ядра Dr.Web Virus-Finding Engine;
  - информация о пользователе и разрешениях, извлеченная из ключевого файла, если Dr.Web Gateway Security Suite работает не в режиме централизованной защиты.

10.4. Приложение Г. Конфигурационный файл Dr.Web Gateway Security Suite

Параметрами конфигурации всех компонентов Dr.Web Gateway Security Suite управляет координирующий демон управления конфигурацией Dr.Web ConfigD. Измененные параметры конфигурации всех компонентов хранятся в едином файле `drweb.ini`, который по умолчанию располагается в каталоге `/etc/opt/drweb.com/` для GNU/Linux или `/usr/local/etc/drweb.com/` для FreeBSD.

В текстовом файле конфигурации хранятся значения только тех параметров, установленные значения которых не совпадают со значением по умолчанию. Если параметр отсутствует в файле конфигурации, то это означает, что он имеет значение по умолчанию.

Просмотреть перечень всех параметров, доступных для изменения, включая те, которые отсутствуют в конфигурационном файле, так как имеют значения по умолчанию, можно при помощи команды:

```
$ drweb-ctl cfshow
```

Изменить значение любого параметра можно двумя способами:

- Выполнив следующую команду:

  ```
  # drweb-ctl cfset <секция>.<параметр> <новое значение>
  ```

  Для выполнения этой команды утилита управления Dr.Web Ctl должна запускаться от имени суперпользователя (пользователя *root*). Для получения прав суперпользователя используйте команду `su` или `sudo`.

  Синтаксис команд `cfshow` и `cfset` утилиты Dr.Web Ctl (модуль `drweb-ctl`) подробнее описан в разделе Dr.Web Ctl.

- Задав этот параметр в конфигурационном файле (отредактировав файл в любом текстовом редакторе) и перезапустив конфигурацию Dr.Web Gateway Security Suite для применения внесенных в файл изменений с помощью команды:

  ```
  # drweb-ctl reload
  ```

10.4.1. Структура файла

Конфигурационный файл сформирован в соответствии с правилами, приведенными ниже.

- Содержимое файла разбито на последовательность именованных секций. Возможные имена секций жестко заданы и не могут быть произвольными. Имя секции указывается в квадратных скобках и совпадает с именем компонента Dr.Web Gateway Security Suite, использующего параметры из этой секции (за исключением секции `[Root]`, в которой хранятся параметры демона управления конфигурацией Dr.Web ConfigD).
- Символы `;` или `#` в начале строк конфигурационного файла обозначают комментарий. Такие строки пропускаются компонентами Dr.Web Gateway Security Suite при чтении параметров из конфигурационного файла.
- В одной строке файла содержится только один параметр:

  ```
  <имя параметра> = <значение>
  ```

- Возможные имена параметров жестко заданы и не могут быть произвольными.
- Все имена секций и параметров регистронезависимы. Значения параметров, за исключением имен каталогов и файлов в путях (для Unix-подобных ОС), также регистронезависимы.
- Значения параметров в конфигурационном файле должны быть заключены в кавычки в том случае, если они содержат пробелы.
- Некоторые параметры могут иметь несколько значений, в этом случае значения параметра разделяются запятой или значение параметра задается несколько раз в разных строках конфигурационного файла. При перечислении значений параметра через запятую пробелы между значением и запятой, если встречаются, игнорируются. Если пробел является частью значения параметра, все значение заключается в кавычки.

  Параметру можно присвоить несколько значений:

  - перечислив их через запятую:

    ```
    Parameter = "Value1", "Value2","Value 3"
    ```

  - в виде последовательности строк:

    ```
    Parameter = Value2
    Parameter = Value1
    Parameter = "Value 3"
    ```

  Порядок значений параметра также несущественен.

Пути к файлам всегда заключаются в кавычки, если они перечисляются через запятую, например:

```
ExcludedPaths = "/etc/file1", "/etc/file2"
```

Описание секций конфигурационного файла приведено в описании использующих его компонентов Dr.Web Gateway Security Suite.

10.4.2. Типы параметров

Параметры конфигурации могут принадлежать к следующим типам:

1. *Адрес* — адрес сетевого соединения в виде пары *<IP-адрес>:<порт>*. В некоторых случаях порт может быть опущен (в каждом случае это указывается в описании параметра).
2. *Логический* — параметр-флаг, принимающий значения `On`, `Yes`, `True` (параметр включен) и `Off`, `No`, `False` (параметр выключен).
3. *Целое число* — неотрицательное целое число.
4. *Дробное число* — в качестве значения параметра может быть указано неотрицательное число, содержащее дробную часть.
5. *Интервал времени* — в качестве значения параметра указывается длина временного интервала, состоящего из целого неотрицательного числа и буквы-суффикса, указывающего заданную единицу измерения. Могут быть использованы суффиксы, задающие единицы измерения:
   - `w` — недели (`1w` = `7d`);
   - `d` — сутки (`1d` = `24h`);
   - `h` — часы (`1h` = `60m`);
   - `m` — минуты (`1m` = `60s`);
   - `s` или без суффикса — секунды.

   Для временного интервала, заданного в секундах, можно указать миллисекунды после точки (не более трех знаков, например, `0.5s` — 500 миллисекунд). В записи одного временного интервала можно использовать совокупность интервалов, измеренных в различных единицах, в этом случае он будет образовываться их суммой (в реальности в параметрах конфигурации всегда сохраняется количество миллисекунд, образующих указанный временной интервал).

   В общем виде любой интервал времени может быть представлен выражением N_1wN_2dN_3hN_4mN_5[.N_6]s, где N_1, ..., N_6 — число соответствующих единиц времени, включенных в данный интервал. Например, год (как 365 суток) можно представить следующим образом (все записи эквивалентны): `365d`, `52w1d`, `52w24h`, `51w7d24h`, `51w7d23h60m`, `8760h`, `525600m`, `31536000s`.

   Примеры задания интервала длиной в 30 минут, 2 секунды, 500 миллисекунд:

   - в файле конфигурации:

```
UpdateInterval = 30m2.5s
```

- с использованием [команды](#) `drweb-ctl cfset`:

```
# drweb-ctl cfset Update.UpdateInterval 1802.5s
```

- задание через параметр командной строки (например, для [сканирующего ядра](#)):
  - для GNU/Linux:

```
# /opt/drweb.com/bin/drweb-se <сокет> --WatchdogInterval 1802.5
```

  - для FreeBSD:

```
# /usr/local/libexec/drweb.com/bin/drweb-se <сокет> --WatchdogInterval
1802.5
```

6. *Размер* — в качестве значения параметра указывается размер какого-либо объекта (файла, буфера, кеша и т. п.), состоящий из целого неотрицательного числа и суффикса, указывающего заданную единицу измерения. Могут быть использованы суффиксы, задающие единицы размера:
   - `mb` — мегабайты (`1mb` = `1024kb`);
   - `kb` — килобайты (`1kb` = `1024b`);
   - `b` — байты.

   Если суффикс опущен, считается, что размер задан в байтах. В записи одного размера можно использовать совокупность размеров, измеренных в различных единицах, в этом случае он будет образовываться их суммой (фактически, в параметрах конфигурации размер всегда сохраняется в байтах).
7. *Путь к каталогу (файлу)* — в качестве значения параметра выступает строка, представляющая собой допустимый путь к каталогу (файлу).

   Путь к файлу должен заканчиваться именем файла.

   В Unix-подобных операционных системах имена каталогов и файлов регистрозависимы. Если это не оговорено непосредственно в описании параметра, в качестве пути нельзя использовать маски, содержащие специальные символы (`?`, `*`).
8. *Уровень подробности* — параметр задает уровень подробности записи в журнал для компонента Dr.Web Gateway Security Suite. Возможные значения:
   - `DEBUG` — самый подробный (отладочный) уровень. Выводятся все сообщения, а также отладочная информация.
   - `INFO` — выводятся все сообщения.
   - `NOTICE` — выводятся сообщения об ошибках, предупреждения, уведомления.

- `WARNING` — выводятся сообщения об ошибках и предупреждения.
- `ERROR` — выводятся только сообщения об ошибках.

9. *Тип журнала* — параметр определяет способ ведения журнала компонентом Dr.Web Gateway Security Suite. Возможные значения:
   - `Stderr[:ShowTimestamp]` — сообщения будут выводиться в стандартный поток ошибок *stderr*. Данное значение может быть использовано *только* в настройках демона управления конфигурацией. При этом, если он работает в фоновом режиме («*daemonized*»), т. е. запущен с указанием параметра `-d`, это значение *не может* быть использовано, поскольку компоненты, работающие в фоновом режиме, не имеют доступа к потокам ввода/вывода терминала). Дополнительный параметр `ShowTimestamp` предписывает добавлять к каждому сообщению метку времени.
   - `Auto` — сообщения для сохранения в журнал передаются демону управления конфигурацией Dr.Web ConfigD, который сохраняет их в единое место в соответствии с собственными настройками (параметр `Log` в секции `[Root]`). Данное значение определено для всех компонентов, *кроме демона управления конфигурацией*, и используется как значение по умолчанию.
   - `Syslog[:`<*facility*>`]` — сообщения будут передаваться компонентом системной службе журналирования `syslog`.
   - Дополнительная метка <*facility*> используется для указания типа журнала, в котором `syslog` будет сохранять сообщения. Возможные значения:
     - `DAEMON` — сообщения демонов,
     - `USER` — сообщения пользовательских процессов,
     - `MAIL` — сообщения почтовых программ,
     - `LOCAL0` — сообщения локальных процессов 0,

     ...
     - `LOCAL7` — сообщения локальных процессов 7.
   - <*путь*> — сообщения будут сохраняться компонентом непосредственно в указанный файл журнала.

   Примеры задания параметра:

   - в файле конфигурации:

```
Log = Stderr:ShowTimestamp
```

   - с использованием команды `drweb-ctl cfset`:

```
# drweb-ctl cfset Root.Log /var/opt/drweb.com/log/general.log
```

   - задание через параметр командной строки (например, для сканирующего ядра):
     - для ОС семейства GNU/Linux:

```
# /opt/drweb.com/bin/drweb-se <сокет> --Log Syslog:DAEMON
```

     - для ОС FreeBSD:

```
# /usr/local/libexec/drweb.com/bin/drweb-se <сокет> --Log Syslog:DAEMON
```

10. *Действие* — действие компонента Dr.Web Gateway Security Suite при обнаружении угроз определенного типа или при возникновении какого-либо другого события. Возможные значения:
    - **Сообщать** (`REPORT`) — только сформировать уведомление об угрозе, не предпринимая никаких других действий;
    - **Лечить** (`CURE`) — попытаться выполнить лечение (удалить из тела файла только вредоносное содержимое);
    - **В карантин** (`QUARANTINE`) — переместить инфицированный файл в карантин;
    - **Удалить** (`DELETE`) — удалить инфицированный файл.

    > ⚠ Некоторые из действий могут быть неприменимы в некоторых случаях (например, для события «Ошибка сканирования» неприменимо действие `CURE`). Перечень разрешенных действий всегда указывается в описании каждого параметра, имеющего тип *действие*.

Прочие типы параметров и их возможные значения указаны непосредственно в описании параметров конфигурации.

10.4.3. Правила проверки трафика

В этом разделе

- Общие сведения
- Формат правил
- Условия
- Действия
- Переменные, используемые в правилах
- Категории нежелательных сайтов и угроз
- Параметры конфигурации, которые можно использовать в условиях правил
- Особенности сохранения правил в файл конфигурации

Общие сведения

Правила представляют собой набор конструкций следующего вида: ЕСЛИ <*условная часть*> ТО <*часть действий*>. В *условной части* перечисляются проверки вида «Переменная (не) имеет заданное значение» или «Значение переменной (не) входит в указанное множество», а *часть действий* содержит набор действий (не менее одного), каждое из которых представляет собой *конечную резолюцию* (пропустить или

заблокировать проверяемый объект) или *модифицирующее действие* вида «Изменить свойства проверяемого объекта», «Присвоить указанной переменной заданное значение» или «Добавить заданное значение к множеству значений указанной переменной».

Указанные в правиле действия выполняются, только если истинна условная часть. Если условная часть правила ложна, то действия, указанные в этом правиле, не выполняются и осуществляется переход к следующему правилу. Правила перебираются сверху вниз до тех пор, пока не сработает какая-либо конечная резолюция. После этого все правила ниже (если имеются) игнорируются.

Действия в *части действий* при срабатывании правила выполняются в порядке их перечисления слева направо, при этом, если в цепочке действий встречается конечная резолюция, прерывающая обработку правил, все следующие за ней действия уже не будут выполнены.

Формат правил

Правила имеют формат:

```
[<условие>[, <условие>[, …]]] : <действие>[, <действие>[, …]]
```

Условная часть правила (перед символом «**:**») может отсутствовать, в этом случае часть действий выполняется безусловно. Если условная часть правила отсутствует, то разделитель «**:**» может быть опущен. Запятая между условиями в условной части и действиями в части действий играет роль конъюнкции (т. е. логического «И»): условная часть считается истинной, только если истинны все перечисленные в ней условия, а все действия, указанные в части действий, выполняются в порядке их перечисления слева направо до момента встречи конечной резолюции, прерывающей обработку правил. Ключевые слова, имена переменных и параметров конфигурации в правилах не чувствительны к регистру.

Условия

В правилах используются следующие условия:

Условие	Комментарий
<переменная> <значение>	Значение указанной переменной совпадает с заданным. Может быть использовано только для переменных, которые не могут принимать множество значений.

Условие	Комментарий
<*переменная*> [not] in <*множество значений*>	Значение переменной содержится в указанном множестве значений (для not — не совпадает ни с одним из значений указанного множества).
<*переменная*> [not] match <*множество значений*>	Значение переменной соответствует регулярному выражению из указанного набора (для not — не соответствует ни одному из выражений в указанном наборе). Регулярные выражения записываются с использованием синтаксиса *POSIX* (*BRE*, *ERE*) или *Perl* (*PCRE*, *PCRE2*).
<*переменная*> [not] gt <*значение*>	Значение указанной переменной (не) больше заданного. Может быть использовано только для переменных, которые принимают единственное числовое значение.
<*переменная*> [not] lt <*значение*>	Значение указанной переменной (не) меньше заданного. Может быть использовано только для переменных, которые принимают единственное числовое значение.

*) Необязательное ключевое слово not обозначает отрицание.

Часть <*множество значений*>, с которым сравнивается переменная, может быть указана следующими способами:

Запись	Смысл
(<*значение 1*>[, <*значение 2*>[, …]])	В скобках перечисляется непосредственно множество проверяемых значений (не менее одного). Для случая с одним значением и использованием условия in скобки можно опустить (получится случай <*переменная*> <*значение*>).
"<*секция*>.<*параметр*>"	Множество параметров конфигурации, где в кавычках указывается имя параметра из конфигурации (с указанием содержащей его секции), значение (или набор значений) которого проверяется.

Запись	Смысл
	Перечни параметров, которые можно использовать в условии, зависят от компонента, для которого заданы правила, и приведены ниже.
`file("<имя файла>")`	Перечень значений считывается из текстового файла *<имя файла>* (одна строка файла — один элемент списка, ведущие и завершающие пробелы в строках не учитываются). Путь к файлу должен быть абсолютным. Кавычки и апострофы, если они встречаются в *<имя файла>*, должны быть экранированы символом косой черты «\». Размер файла не должен быть больше 64 МБ. Содержимое файла считывается и подставляется в правила один раз — при загрузке файла конфигурации. Если указанный файл отсутствует или его размер слишком велик, при загрузке настроек возвращается ошибка x102. Если вы изменили файл, для применения внесенных изменений необходимо перезагрузить конфигурацию Dr.Web Gateway Security Suite, используя команду: `# drweb-ctl reload` Не для всех переменных можно получать множество значений из файла. Для каждой переменной ниже указывается, можно ли использовать для проверки ее значений множество значений, получаемые из файла.
<тип_LOOKUP_запроса> `@<тег>[@<значение>]`	Множество значений запрашивается через Dr.Web LookupD у внешнего источника данных, где *<тип_LOOKUP_запроса>* — тип источника, *<тег>* — имя секции, описывающей подключение для выборки проверяемого параметра, а необязательное *<значение>* — значение, которое должно находиться в множестве значений, извлеченных из источника данных.

Запись	Смысл
	Не для всех переменных можно получать значения через Dr.Web LookupD. Также не для всех переменных используется условие <*проверка*>. Для каждой переменной ниже указывается, можно ли использовать для проверки ее значений значения, получаемые через Dr.Web LookupD.
`dnsxl(`<*DNSxL-сервер 1*>`[: [mask]` <*IP*>`][, …])`	В скобках указывается перечень DNSxL-серверов (DNSBL и т. п.), которые должны проверить вхождение IP-адреса или FQDN (предварительно разрешенного до IP-адреса) в свои списки IP-адресов. Если проверяемый IP-адрес входит в списки одного из перечисленных в скобках DNSxL-серверов, то в ответе этого сервера присутствует одна или более DNS-записей типа A, причем возвращаемый сервером фиктивный IP-адрес может содержать в себе причину, по которой проверяемый IP-адрес был внесен в списки данного сервера (как правило, тип причины определяется значением последнего октета возвращенного фиктивного IP-адреса). Для каждого DNSxL-сервера в списке можно указать проверку на ожидаемое возвращенное значение фиктивного IP-адреса. Проверка указывается после двоеточия в формате: • <*DNSxL-сервер*>`:` <*IP-адрес*> • <*DNSxL-сервер*>`: mask` <*IP-адрес*> В первом случае указывается требование, чтобы возвращенный сервером <*DNSxL-сервер*> фиктивный IP-адрес в точности совпадал бы с указанным адресом <*IP-адрес*>. Во втором случае указывается требование, чтобы возвращенный сервером <*DNSxL-сервер*> фиктивный IP-адрес в точности равнялся бы указанной маске в ее ненулевых октетах. Если параметры проверки не указаны, то условие сработает, если <*DNSxL-сервер*> вернет любой фиктивный IP-адрес в ответ на запрос. Примеры: <*IP*> `in dnsxl("dnsxl.server.org")` — для IP-адреса, содержащегося в переменной <*IP*>, сервер должен вернуть любой фиктивный IP-адрес; <*IP*> `in dnsxl("dnsxl.server.org": 127.0.0.2)` — для IP-адреса, содержащегося в переменной <*IP*>, сервер должен вернуть

Запись	Смысл
	фиктивный IP-адрес `127.0.0.2`; *<IP>* `in dnsxl("dnsxl.server1.org": mask 0.0.0.8, "dnsxl.server2.org": 127.0.0.3, "dnsxl.server3.org")` — для IP-адреса, содержащегося в переменной *<IP>*, либо первый сервер вернет фиктивный IP-адрес с младшим октетом `8`, либо второй — фиктивный IP-адрес `127.0.0.3`, либо третий — любой фиктивный IP-адрес. Использование инструкции проверки *<переменная>* `in dnsxl(`*<список серверов>*`)` допустимо только в том случае, если *<переменная>* представляет собой IP-адрес или доменное имя, которое может быть разрешено службой DNS до IP-адреса (FQDN). Таким образом, в качестве переменной для данного условия могут быть использованы только переменные `src_ip` и `url_host` (см. ниже).

Если переменная имеет множественное значение, то условие *<переменная>* `in` *<множество значений>* истинно, если пересечение множества текущих значений указанной переменной *<переменная>* с указанным множеством *<множество значений>* не пусто. Условие `not in` истинно в противоположном случае.

Например, пусть `X` — переменная, текущее значение которой — множество, содержащее значения *a*, *b*, *c*. Тогда:

- `X in (a, b)` — истинно, так как значения *a* и *b* встречаются в обоих множествах;
- `X in (a, d, e)` — истинно, так как значение *a* встречается в обоих множествах;
- `X in (d, e)` — ложно, так как ни одно из значений переменной (*a*, *b*, *c*) не встречается в множестве (*d*, *e*);
- `X in ()` — ложно, так как множество значений переменной не пусто;
- `X not in ()` — истинно, так как множество значений переменной не пусто;
- `X not in (d, e)` — истинно, так как ни одно из значений переменной (*a*, *b*, *c*) не встречается в множестве (*d*, *e*);
- `X not in (a, d, e)` — ложно, так как значение *a* встречается в обоих множествах.

В описании переменных ниже для каждой переменной указано, может ли она принимать множество значений.

Действия

Действия делятся на *конечные резолюции*, определяющие запрет или разрешение на пропуск объекта, и *действия, изменяющие значения переменных*, что может быть использовано при проверке условий в последующих правилах.

Конечные резолюции

Резолюция	Описание (смысл)
Общие резолюции	
`PASS`	Пропустить трафик (разрешить создание соединения, передать объект получателю). Последующие правила (если имеются) не используются.
`BLOCK as <reason>`	Заблокировать трафик (отказать в создании соединения, передаче объекта получателю). Последующие правила (если имеются) не используются. В журнале фиксируется факт блокировки с указанием причины *<reason>*. Эта же причина используется для определения, какую страницу с уведомлением показать пользователю в браузере. В качестве *<reason>* для `BLOCK` могут быть использованы две стандартные причины: • `BlackList` — данные заблокированы по причине попадания в черный список пользователя. • `_match` — причиной блокировки является попадание веб-ресурса или файла с угрозой в категорию, из-за которой сработало правило (для условий `*_category in (...)`). Переменная `_match` хранит список блокируемых категорий, для которых сработало соответствие.

Особенности обработки конечных резолюций:

- `BLOCK as BlackList` всегда отрабатывает как *«попал в черный список»* (вне зависимости от того, что за условие указано в правиле с данной резолюцией).
- `BLOCK as _match`, если в `_match` не пусто, отрабатывает как *«попал в категорию(и) _match»*.
- `BLOCK as _match`, если в `_match` пусто, отрабатывает как *«попал в черный список»* (вне зависимости от того, что за условие указано в правиле с данной резолюцией).
- Если были просмотрены все правила, но ни одно правило с резолюцией не сработало (или резолюции отсутствуют в правилах), то это равносильно применению к соединению действия `PASS`.

Изменение значения переменной

Для изменения значения переменной используется инструкция:

```
SET <переменная> = ([<значение 1>[, <значение 2>[, …]]])
```

Если в скобках ничего не указано, список значений переменных будет очищен:

```
SET <переменная> = ()
```

Если переменная имеет только одно значение, скобки не используются:

```
SET <переменная> = <значение>
```

Переменные, используемые в правилах

При указании переменных в правилах регистр символов не учитывается. Переменные, название которых состоит из нескольких слов, могут быть записаны с использованием подчеркивания для разделения слов или записаны без подчеркивания. Таким образом, имя переменной может быть указано как `variable_name`, `VariableName` или `variablename`. В данном разделе все переменные записаны с использованием подчеркивания (т. е. используется вариант написания `variable_name`).

Переменная	Описание	Может быть использована в	
		условии	действии (SET)
`protocol`	Тип сетевого протокола, используемого соединением. Переменная может принимать множество значений. Возможные значения: `HTTP`, `SMTP`, `IMAP`, `POP3`. **Особенности использования** • Значение переменной определено, только если не используется SSL/TLS или проверка SSL была разрешена. • В правилах для Dr.Web ICAPD может быть указано только одно значение — `HTTP`.	Да	Нет

Переменная	Описание	Может быть использована в	
		условии	действии (SET)

	• Множество значений для проверки значения переменной можно получать из файла.
	
	Примеры:
	
	`protocol in (HTTP, SMTP)`
	`protocol in (POP3)`
	`protocol in file("/etc/file")`		

`sni_host`	SNI (адрес) узла, с которым устанавливается соединение через SSL/TLS.
	
	Особенности использования
	
	• Если SSL не используется, то значение переменной не определено, условие будет ложным.
	• В правилах для Dr.Web ICAPD переменная не используется (он не обрабатывает SSL, поэтому условие всегда будет ложным).
	• Множество значений для проверки значения переменной можно получать из файла.
	• Переменная может использоваться в паре с переменной `proc` (см. ниже).
	
	Примеры:
	
	`sni_host not in ('vk.com', 'ya.ru')`
	`sni_host in "LinuxFirewall.BlackList"`
	`sni_host in file("/etc/file")`
		Да	Нет

`sni_category`	Список категорий (`AdultContent` и др.), к которым, согласно базам категорий веб-ресурсов, относится узел (определенный по SNI), с которым устанавливается соединение через SSL/TLS. Переменная может принимать множество значений.	Да	Нет

Переменная	Описание	Может быть использована в	
		условии	действии (SET)

	Особенности использования
	• Если SSL не используется, то значение переменной не определено, условие будет ложным.
	• Не имеет смысла использовать в правилах для Dr.Web ICAPD (он не обрабатывает SSL, поэтому условие всегда будет ложным).
	• Для правил, используемых Dr.Web ICAPD, условие с `not in` будет *истинным*, даже если по результатам проверки узел не принадлежит никакой из предопределенных категорий («безопасный» узел). Для правил компонента Dr.Web Firewall для Linux (SplDer Gate) условие в этом случае будет *ложным*.
	• Если базы данных категорий веб-ресурсов не установлены, то переменную нельзя использовать в правилах (попытка проверить истинность условия в правиле будет приводить к ошибке x112).
	• Множество значений для проверки значения переменной можно получать из файла.
	Примеры:
	`sni_category not in (AdultContent, Chats)`
	`sni_category in "LinuxFirewall.BlockCategory"`
	`sni_category in (FreeEmail)`
	`sni_category not in file("/etc/file")`		

`url`	URL, запрошенный клиентом. Может быть сравнен со строкой или регулярным выражением. **Особенности использования** • Можно использовать только в правилах для Dr.Web ICAPD.	Да	Нет

Переменная	Описание	Может быть использована в	
		условии	действии (SET)

	• Для проверки значения переменной можно использовать Dr.Web LookupD.
	• Множество значений для проверки значения переменной можно получать из файла.
	• Может быть использована в паре с переменной `proc` (см. ниже).
	
	Примеры:
	`url match ("drweb.com", "example\..*", "aaa\.ru/")`
	`url match "ICAPD.Adlist"`
	`url not match LDAP@BadURLs`
	`url match file("/etc/file")`		

`url_host`	URL или узел, с которым устанавливается соединение.
	
	Особенности использования
	• Значение переменной определено, только если не используется SSL/TLS или проверка SSL была разрешена.
	• Для проверки значения переменной можно использовать Dr.Web LookupD.
	• Множество значений для проверки значения переменной можно получать из файла.
	
	Примеры:
	`url_host in ('vk.com', 'ya.ru')`
	`url_host not in "ICAPD.Whitelist"`
	`url_host in LDAP@hosts`
	`url_host not in file("/etc/file")`
		Да	Нет

`url_category`	Список категорий, к которым (по базам категорий веб-ресурсов или по ответу из Dr.Web Cloud) относится URL или узел, с которым установлено соединение. Переменная может принимать множество значений.	Да	Нет

Переменная	Описание	Может быть использована в	
		условии	действии (SET)

	Особенности использования
	• Значение переменной определено, только если не используется SSL/TLS или проверка SSL разрешена.
	• Для правил, используемых Dr.Web ICAPD, условие с `not in` будет *истинным*, даже если по результатам проверки URL или узел не принадлежит никакой из предопределенных категорий («безопасный» URL или узел). Для правил компонента Dr.Web Firewall для Linux (SpIDer Gate) условие в этом случае будет *ложным*.
	• Если базы данных категорий веб-ресурсов не установлены, то переменную нельзя использовать в правилах (попытка проверить истинность условия в правиле будет приводить к ошибке x112).
	• Множество значений для проверки значения переменной можно получать из файла.
	Примеры:
	`url_category not in (AdultContent, Chats)`
	`url_category in "LinuxFirewall.BlockCategory"`
	`url_category in (FreeEmail)`
	`url_category in file("/etc/file")`		

`threat_category`	Список категорий, к которым по информации из вирусных баз относится угроза, обнаруженная в передаваемых данных. Переменная может принимать множество значений. **Особенности использования** • Значение переменной определено, только если не используется SSL/TLS или проверка SSL разрешена.	Да	Нет

Переменная	Описание	Может быть использована в	
		условии	действии (SET)

	• Для правил, используемых Dr.Web ICAPD, условие с `not in` будет *истинным*, даже если по результатам проверки объект не содержит угроз ни из одной из предопределенных категорий («безопасный» объект). Для правил компонента Dr.Web Firewall для Linux (SpIDer Gate) условие в этом случае будет *ложным*.
	• Множество значений для проверки значения переменной можно получать из файла.
	Примеры:
	`threat_category in "LinuxFirewall.BlockThreat"`
	`threat_category not in (Joke)`
	`threat_category in file("/etc/file")`		

`user`	Пользователь, от имени которого запущен процесс-отправитель (или получатель) трафика. **Особенности использования** • В правилах для Dr.Web ICAPD имеет смысл для имени пользователя, прошедшего аутентификацию на прокси-сервере (если прокси-сервер поддерживает аутентификацию). Если прокси-сервер не аутентифицирует пользователей, переменная имеет пустое значение. • Для проверки значения переменной можно использовать Dr.Web LookupD. Если требуется проверить, принадлежит ли пользователь к определенной группе, используйте источник данных LDAP или Active Directory, возвращающий список групп. Также запрос должен содержать условие сравнения имени группы, которой принадлежит пользователь, с требуемым (используйте формат *<тип источника LookupD>@<источник групп>@<требуемая группа>*).	Да	Нет

Переменная	Описание	Может быть использована в	
		условии	действии (SET)

	Запросы к Active Directory (AD@) возвращают только перечни групп, поэтому для них использование части *@<требуемая группа>* обязательно.
	• Множество значений для проверки значения переменной можно получать из файла.
	Примеры:
	`user in ('user1', 'user2')`
	`user in AD@Winusergroups@Admins`
	`user in LDAP@AllowedUsers`
	`user not in file("/etc/file")`		

`src_ip`	IP-адрес узла, со стороны которого следует соединение.
	Особенности использования
	• Для проверки значения переменной можно использовать Dr.Web LookupD.
	• Множество значений для проверки значения переменной можно получать из файла.
	Примеры:
	`src_ip not in (127.0.0.1, 10.20.30.41, 198.126.10.0/24)`
	`src_ip in LDAP@AllowedAddresses`
	`src_ip not in file("/etc/file")`
		Да	Нет

`proc`	Процесс, устанавливающий соединение (полный путь к исполняемому файлу). **Особенности использования** • Не имеет смысла использовать в правилах для Dr.Web ICAPD (он не имеет информации о процессах, поэтому условие всегда будет ложным). • Множество значений для проверки значения переменной можно получать из файла.	Да	Нет

Переменная	Описание	Может быть использована в	
		условии	действии (SET)

	• Может быть использована в паре с переменными `sni_host`, `url`, `dst_address` (см. ниже).
	
	Примеры:
	`proc in ('/usr/bin/ls')`
	`proc not in ('/home/user/myapp', '/bin/bin1')`
	`proc in "LinuxFirewall.ExcludedProc"`
	`proc in file("/etc/file")`		

`direction`	Тип трафика, идущего по соединению.
	
	Возможные значения: `request` (клиентский запрос), `response` (ответ сервера).
	
	Переменная не может иметь множества значений, условия типа `match` и `in` неприменимы.
	
	Примеры:
	`direction request`
	`direction not response`
		Да	Нет

`divert`	Направление соединения.
	
	Возможные значения: `input` (входящее — создано или инициировано извне локального узла), `output` (исходящее — создано или инициировано на локальном узле).
	
	Переменная не может иметь множества значений, условия типа `match` и `in` неприменимы.
	
	Примеры:
	`divert input`
	`divert not output`
		Да	Нет

`content_type`	MIME-тип данных, передаваемых по соединению.	Да	Нет

Переменная	Описание	Может быть использована в	
		условии	действии (SET)

	Особенности использования
	• Может быть определен, только если не используется SSL/TLS или проверка SSL разрешена.
	• Выражению "*/*" соответствуют данные любого MIME-типа, а также HTTP-ответы без заголовка Content-Type.
	• Для проверки значения переменной можно использовать Dr.Web LookupD.
	• Множество значений для проверки значения переменной можно получать из файла.
	Примеры:
	`content_type in ("multipart/byteranges", "application/octet-stream")`
	`content_type not in ("text/*", "image/*")`
	`content_type not in ("audio/*")`
	`content_type in ("*/*")`
	`content_type in LDAP@BlockedContent`
	`content_type not in file("/etc/file")`		

(proc, <*переменная*>)	Сетевая активность процесса, где proc — полный путь к исполняемому файлу процесса (см. выше), а <*переменная*> определяет тип сетевой активности и может принимать одно из значений: • sni_host — SNI (адрес) хоста, с которым устанавливается соединение через SSL/TLS (см. выше); • url — URL, запрошенный клиентом (см. выше); • dst_address — сетевой адрес (<*IP-адрес*>:<*порт*>), с которым процесс устанавливает соединение.	Да	Нет

Переменная	Описание	Может быть использована в	
		условии	действии (SET)

	Особенности использования
	• Используется только с условием `match ({<Proc_reg>, <Var_reg>} [, …])`, где <*Proc_reg*> — регулярное выражение для `proc`, а <*Var_reg*> — регулярное выражение для <*переменная*>.
	• Не используется в правилах для Dr.Web ICAPD (он не имеет информации о процессах, поэтому условие всегда будет ложным).
	Примеры:
	`(proc, url) match ({"/usr/bin/wget", "www\.ya\.*"})`
	`(proc, dst_address) match ({"/usr/bin/.*", "192\.168\.1\.\d+:12345"})`		

`unwrap_ssl`	Проверять или не проверять защищенный трафик, передаваемый через SSL/TLS.
	Возможные значения: `true`, `false`.
	Особенности использования
	• Значение переменной не может быть пустым. Инструкция `SET unwrap_ssl = ()` недопустима.
	• Переменная не может использоваться в условиях, а нужна только для управления проверкой SSL (например, чтобы продемонстрировать пользователю веб-страницу с уведомлением о блокировке).
	• Не используется в правилах для Dr.Web ICAPD (он не обрабатывает SSL, изменение значения переменной никак не влияет на обработку правил).
	Примеры:
	`SET unwrap_ssl = TRUE`
	`set Unwrap_SSL = false`
		Нет	Да

Переменная	Описание	Может быть использована в	
		условии	действии (SET)

`http_templates_dir`	Путь к каталогу, в котором хранятся шаблоны страниц блокировки.
	
	Если путь начинается с символа «`/`» — это абсолютный путь, если с любого другого символа, то это относительный путь. Корневым каталогом при этом считается путь из параметра `TemplatesDir`.
	
	Особенности использования
	
	• Может использоваться только для протокола HTTP(S).
	
	Примеры:
	
	`SET http_templates_dir = "/etc/mytemplates"`
	`set http_templates_dir = "templates_for_my_site"`
		Нет	Да

Категории нежелательных сайтов и угроз

1. Категории нежелательных сайтов (для переменных `sni_category`, `url_category`)

Обозначение	Категория сайтов
`InfectionSource`	Сайты, содержащие вредоносное ПО («источники распространения угроз»)
`NotRecommended`	Сайты, используемые для мошенничества («социальной инженерии») и не рекомендованные к посещению
`AdultContent`	Сайты, содержащие материалы порнографического или эротического содержания, сайты знакомств и т. д.
`Violence`	Сайты, содержащие призывы к насилию, материалы о различных происшествиях с человеческими жертвами и т. д.
`Weapons`	Сайты, посвященные оружию и взрывчатым веществам, а также материалы с описанием их изготовления и т. д.
`Gambling`	Сайты, на которых размещены онлайн-игры на деньги, интернет-казино, аукционы, а также принимающие ставки и т. д.

Обозначение	Категория сайтов
Drugs	Сайты, пропагандирующие употребление, изготовление или распространение наркотиков и т. д.
ObsceneLanguage	Сайты, на которых содержится нецензурная лексика (в названиях разделов, статьях и пр.)
Chats	Сайты для обмена сообщениями в режиме реального времени
Terrorism	Сайты, содержащие материалы агрессивно-агитационного характера, описания терактов и т. д.
FreeEmail	Сайты, предоставляющие возможность бесплатной регистрации электронного почтового ящика
SocialNetworks	Социальные сети общего характера, деловые, корпоративные и тематические социальные сети, а также тематические сайты знакомств
DueToCopyrightNotice	Сайты, ссылки на которые указаны правообладателями некоторого произведения, защищенного авторскими правами (кинофильмы, музыкальные произведения и т. д.)
OnlineGames	Сайты, на которых размещены игры, использующие постоянное интернет-соединение
Anonymizers	Сайты, позволяющие пользователю скрывать свою личную информацию и предоставляющие доступ к заблокированным сайтам
CryptocurrencyMiningPool	Сайты, предоставляющие доступ к сервисам, объединяющим пользователей с целью добычи (майнинга) криптовалют
Jobs	Сайты, предназначенные для поиска работы

В качестве значения переменных `sni_category` и `url_category` можно также использовать имена параметров, управляющих блокировкой (см. ниже).

2. Категории угроз (для переменной `threat_category`)

Обозначение	Категория угроз
KnownVirus	Известная угроза
VirusModification	Модификация известной угрозы
UnknownVirus	Неизвестная угроза, подозрительный объект
Adware	Рекламная программа
Dialer	Программа дозвона

Обозначение	Категория угроз
Joke	Программа-шутка
Riskware	Потенциально опасная программа
Hacktool	Программа взлома

В качестве значения переменной threat_category можно также использовать имена параметров, управляющих блокировкой (см. ниже).

Параметры конфигурации, используемые в условиях правил

Параметры, используемые в правилах компонента Dr.Web Firewall для Linux (указываются с префиксом LinuxFirewall.):

Параметр	Описание и пример использования

Whitelist	Белый список — перечень доменов, доступ к которым разрешен, даже если они находятся в базе категорий веб-ресурсов.
	
	Примеры:
	`sni_host in "LinuxFirewall.Whitelist" : PASS`
	`url_host not in "LinuxFirewall.Whitelist" : BLOCK as _match`

Blacklist	Черный список — перечень доменов, доступ к которым запрещен пользователем или администратором.
	
	Примеры:
	`sni_host in "LinuxFirewall.Blacklist" : SET Unwrap_SSL = FALSE`
	`url_host in "LinuxFirewall.Blacklist" : BLOCK as BlackList`

BlockCategory	«Метапараметр»: список категорий (Chats, AdultContent и т. д.), для которых параметры Block* в секции [LinuxFirewall] имеют значение Yes.
	
	Примеры:
	`url_category in "LinuxFirewall.BlockCategory" : BLOCK as _match`
	`sni_category in "LinuxFirewall.BlockCategory" : BLOCK as BlackList`

BlockThreat	«Метапараметр»: список названий типов угроз (KnownVirus, Joke и т. д.), для которых параметры Block* в секции [LinuxFirewall] имеют значение Yes.

Параметр	Описание и пример использования
	Примеры: `threat_category in "LinuxFirewall.BlockThreat" : BLOCK as _match`
`ExcludedProc`	Перечень доверенных процессов, трафик которых не должен проверяться. Примеры: `proc in "LinuxFirewall.ExcludedProc" : PASS`

Параметры, используемые в правилах компонента Dr.Web ICAPD (указываются с префиксом `ICAPD.`):

Параметр	Описание и пример использования
`Whitelist`	Белый список — перечень доменов, доступ к которым разрешается, даже если эти домены находятся в базе категорий веб-ресурсов. Примеры: `url_host not in "ICAPD.Whitelist" : BLOCK as BlackList`
`Blacklist`	Черный список — перечень доменов, доступ к которым запрещен пользователем или администратором. Примеры: `url_host in "ICAPD.Blacklist" : BLOCK as BlackList`
`Adlist`	Рекламный список — перечень регулярных выражений, которые описывают рекламные сайты. Задается пользователем или администратором. Примеры: `url match "ICAPD.Adlist" : BLOCK as BlackList`
`BlockCategory`	«Метапараметр»: список категорий (`Chats`, `AdultContent` и т. д.), для которых параметры `Block*` в секции `[ICAPD]` имеют значение `Yes`. Примеры: `url_category in "ICAPD.BlockCategory" : BLOCK as _match`
`BlockThreat`	«Метапараметр»: список типов угроз (`KnownVirus`, `Joke` и т. д.), для которых соответствующие параметры `Block*` в секции `[ICAPD]` имеют значение `Yes`.

Параметр	Описание и пример использования
	Примеры: `threat_category in "ICAPD.BlockThreat" : BLOCK as _match`

Особенности сохранения правил в файл конфигурации

- В файле конфигурации в секциях настроек компонентов, использующих правила, правила хранятся в переменных типа `RuleSet`, каждая из которых представляет собой набор (последовательность) из неограниченного числа правил. При этом правила в каждом наборе перебираются последовательно (сверху вниз) до момента достижения конечной резолюции.
- При записи в файл конфигурации безусловного правила (правила, содержащего только действия и не содержащего условной части), к нему будет добавлена пустая условная часть и знак разделителя «`:`».

  Например, правило, не содержащее условной части и *состоящее только из действия*:

  ```
  BLOCK as _match
  ```

  будет записано в файл конфигурации в виде:

  ```
  : BLOCK as _match
  ```

- При записи в файл конфигурации правило, содержащее в части действий набор из *нескольких* действий, будет записано в виде последовательности правил с одинаковой условной частью и одним действием в части действий в том же порядке, в каком перечислены действия.

  Например, правило, содержащее *два действия* в части действий:

  ```
  user in ('user1', 'user2') : SET http_templates_dir = "/etc/mytemplates",
  BLOCK as _match
  ```

  будет записано в файл конфигурации в виде *последовательности двух правил*:

  ```
  user in ('user1', 'user2') : SET http_templates_dir = "/etc/mytemplates"
  user in ('user1', 'user2') : BLOCK as _match
  ```

- Так как в записи правил не предусмотрено дизъюнкции (логическое «ИЛИ») условий в условной части, для реализации логического «ИЛИ» надо записать цепочку правил, указав в условии каждого единственное условие-дизъюнкт.

Например, следующие два правила эквивалентны правилу «Осуществить блокировку, если обнаружен вредоносный объект типа `KnownVirus` или URL из категории `Terrorism`»:

```
threat_category in (KnownVirus) : BLOCK as _match
url_category in (Terrorism) : BLOCK as _match
```

так как следующие записи логически эквивалентны: $(a \rightarrow x, b \rightarrow x)$; $((a \rightarrow x) \wedge (b \rightarrow x))$; $((a \vee b) \rightarrow x)$.

Как и для любого параметра конфигурации, значения параметров типа `RuleSet` (т. е. правила) могут быть просмотрены и изменены при помощи команд `cfshow` и `cfset` утилиты управления Dr.Web Ctl (модуль `drweb-ctl`). Подробнее о синтаксисе этих команд см. раздел Dr.Web Ctl.

10.5. Приложение Д. Генерация сертификатов SSL

Для компонентов Dr.Web Gateway Security Suite, использующих для обмена данными защищенный канал передачи данных SSL/TLS и основанные на нем прикладные протоколы, такие как HTTPS, LDAPS, SMTPS и т. п., необходимо обеспечить наличие закрытых ключей SSL и соответствующих им сертификатов. Для некоторых компонентов ключи и сертификаты генерируются автоматически, а для других они должны быть предоставлены пользователем Dr.Web Gateway Security Suite. Все компоненты используют сертификаты, представленные в формате PEM.

Для генерации закрытых ключей и сертификатов, используемых для соединений через SSL/TLS, в том числе для удостоверяющих сертификатов центра сертификации (ЦС) и для подписанных сертификатов, можно использовать утилиту командной строки `openssl` (входит в состав криптографического пакета OpenSSL).

Рассмотрим последовательность действий, необходимых для создания закрытого ключа и соответствующего ему сертификата SSL, а также сертификата SSL, подписанного удостоверяющим сертификатом ЦС.

Чтобы сгенерировать закрытый ключ SSL и сертификат

1. Для генерации закрытого ключа (алгоритм RSA, длина ключа — 2048 бит) выполните команду:

   ```
   $ openssl genrsa -out keyfile.key 2048
   ```

   Если требуется защитить ключ паролем, дополнительно используйте опцию `-des3`. Сгенерированный ключ находится в файле `keyfile.key` в текущем каталоге.

   Для просмотра сгенерированного ключа можно использовать команду:

   ```
   $ openssl rsa -noout -text -in keyfile.key
   ```

2. Для генерации сертификата на указанный срок на основании имеющегося закрытого ключа (в данном примере — на 365 суток) выполните команду:

   ```
   $ openssl req -new -x509 -days 365 -key keyfile.key -out certificate.crt
   ```

   Эта команда запросит данные, идентифицирующие сертифицируемый объект (такие как имя, организация и т. п.). Сгенерированный сертификат будет помещен в файл `certificate.crt`.

   Для проверки содержимого сгенерированного сертификата можно воспользоваться командой:

   ```
   $ openssl x509 -noout -text -in certificate.crt
   ```

Чтобы зарегистрировать сертификат в качестве доверенного сертификата ЦС

1. Переместите или скопируйте файл сертификата в системный каталог доверенных сертификатов (в Debian или Ubuntu — `/etc/ssl/certs`).
2. Создайте в каталоге доверенных сертификатов символическую ссылку на сертификат, именем которой будет являться хеш сертификата.
3. Переиндексируйте содержимое системного каталога сертификатов.

Приведенный ниже пример выполняет все эти три действия. Предполагается, что текущим каталогом является системный каталог доверенных сертификатов `/etc/ssl/certs`, а сертификат, который регистрируется в качестве доверенного, располагается в файле `/home/user/ca.crt`:

```
# cp /home/user/ca.crt .
# ln -s ca.crt `openssl x509 -hash -noout -in ca.crt`.0
# c_rehash /etc/ssl/certs
```

Чтобы создать подписанный сертификат

1. Сгенерируйте файл-запрос на подписание сертификата *(Certificate Signing Request — CSR)* на основании имеющегося закрытого ключа. Если ключа нет, сгенерируйте его.

   Запрос на подписание создается командой:

   ```
   $ openssl req -new -key keyfile.key -out request.csr
   ```

   Эта команда, так же как и команда создания сертификата, запрашивает данные, идентифицирующие сертифицируемый объект. Здесь `keyfile.key` — имеющийся файл закрытого ключа. Полученный запрос будет сохранен в файл `request.csr`.

   Для проверки результата создания запроса воспользуйтесь командой:

   ```
   $ openssl req -noout -text -in request.csr
   ```

2. Для создания подписанного сертификата на основании запроса и имеющегося сертификата ЦС воспользуйтесь командой:

   ```
   $ openssl x509 -req -days 365 -CA ca.crt -CAkey ca.key -set_serial 01 -in request.csr -out sigcert.crt
   ```

   Для создания подписанного сертификата нужно иметь три файла: файл корневого сертификата `ca.crt` и его закрытый ключ `ca.key` (в качестве `ca.crt` и `ca.key` можно использовать сертификат `certificate.crt` и ключ `keyfile.key`, тогда полученный сертификат будет самоподписанными), а также файл запроса на подписание сертификата `request.csr`. Созданный подписанный сертификат будет сохранен в файл `sigcert.crt`.

Для проверки результата воспользуйтесь командой:

```
$ openssl x509 -noout -text -in sigcert.crt
```

Повторите процедуру создания ключа и сертификата (или подписанного сертификата, в зависимости от необходимости) столько раз, сколько уникальных сертификатов вам требуется. Например, с точки зрения соображений безопасности, каждый агент распределенной проверки файлов Dr.Web Network Checker, входящий в сканирующий кластер, должен иметь собственную пару ключ/сертификат.

Преобразование подписанного сертификата

Некоторые браузеры или почтовые клиенты могут потребовать преобразования подписанного сертификата, используемого для удостоверения личности, в формат `PKCS12`.

Указанное преобразование выполняется командой:

```
# openssl pkcs12 -export -in sigcert.crt -out sigcert.pfx -inkey keyfile.key
```

Здесь `sigcert.crt` — имеющийся файл подписанного сертификата, а `keyfile.key` — файл соответствующего ему закрытого ключа. Полученный преобразованный сертификат будет сохранен в файл `sigcert.pfx`.

10.6. Приложение E. Описание известных ошибок

В этом разделе

- Рекомендации по идентификации ошибок
- Коды ошибок
- Ошибки без кода

Если у вас возникла ошибка, описание которой отсутствует в данном разделе, обратитесь в техническую поддержку. Будьте готовы сообщить код ошибки и описать обстоятельства ее возникновения.

Рекомендации по идентификации ошибок

- Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages` в зависимости от используемой ОС). Также вы можете воспользоваться командой:

```
# drweb-ctl log
```

- Для облегчения идентификации ошибки рекомендуется настроить вывод журнала в отдельный файл и разрешить вывод расширенной отладочной информации. Для этого выполните команды:

```
# drweb-ctl cfset Root.Log <путь к файлу журнала>
# drweb-ctl cfset Root.DefaultLogLevel DEBUG
```

- Для возврата настроек ведения журнала по умолчанию выполните команды:

```
# drweb-ctl cfset Root.Log -r
# drweb-ctl cfset Root.DefaultLogLevel -r
```

Коды ошибок

Сообщение об ошибке: *Error on monitor channel (Ошибка связи с монитором)*

Код ошибки: `x1`

Внутреннее обозначение ошибки: `EC_MONITOR_IPC_ERROR`

Описание: Ошибка связи одного или нескольких компонентов с демоном управления конфигурацией Dr.Web ConfigD.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Перезапустите демон управления конфигурацией:

   ```
   # service drweb-configd restart
   ```

2. Убедитесь, что в системе установлен, настроен и корректно функционирует механизм аутентификации PAM. При необходимости установите и настройте его (за подробностями обратитесь к руководствам по администрированию вашего дистрибутива ОС).

3. Если перезапуск демона управления конфигурацией при корректно настроенном PAM не помогает, попробуйте сбросить настройки Dr.Web Gateway Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   - для GNU/Linux:

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```

   - для FreeBSD:

     ```
     # cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
     # echo "" > /usr/local/etc/drweb.com/drweb.ini
     ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

   ```
   # service drweb-configd restart
   ```

4. Если демон управления конфигурацией запустить не удается, попробуйте переустановить пакет `drweb-configd`.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Operation is already in progress (Операция уже выполняется)*

Код ошибки: `x2`

Внутреннее обозначение ошибки: `EC_ALREADY_IN_PROGRESS`

Описание: Запрошенная операция уже выполняется.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Подождите завершения операции и при необходимости повторите требуемое действие позже.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Operation is in pending state (Операция ожидает выполнения)*

Код ошибки: `x3`

Внутреннее обозначение ошибки: `EC_IN_PENDING_STATE`

Описание: Запрошенная операция ожидает выполнения (возможно, в текущий момент устанавливается сетевое соединение или происходит загрузка и инициализация какого-либо компонента, требующая продолжительного времени).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Подождите начала выполнения операции и при необходимости повторите требуемое действие позже.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Interrupted by user (Прервано пользователем)*

Код ошибки: `x4`

Внутреннее обозначение ошибки: `EC_INTERRUPTED_BY_USER`

Описание: Действие было прервано пользователем (возможно, оно выполнялось слишком долго).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Повторите требуемое действие позже.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Operation canceled (Операция отменена)*

Код ошибки: `x5`

Внутреннее обозначение ошибки: `EC_CANCELED`

Описание: Действие было отменено.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Повторите требуемое действие.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *IPC connection terminated (Соединение IPC разорвано)*

Код ошибки: `x6`

Внутреннее обозначение ошибки: `EC_LINK_DISCONNECTED`

Описание: IPC-соединение с одним из компонентов Dr.Web Gateway Security Suite разорвано (возможно, компонент завершил свою работу из-за простоя или по команде пользователя).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Если операция не была завершена, повторите ее позже. В противном случае разрыв соединения не является ошибкой.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid IPC message size (Недопустимый размер сообщения IPC)*

Код ошибки: `x7`

Внутреннее обозначение ошибки: `EC_BAD_MESSAGE_SIZE`

Описание: В процессе обмена данными между компонентами получено сообщение недопустимого размера.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Перезапустите Dr.Web Gateway Security Suite:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid IPC message format (Недопустимый формат сообщения IPC)*

Код ошибки: `x8`

Внутреннее обозначение ошибки: `EC_BAD_MESSAGE_FORMAT`

Описание: В процессе обмена данными между компонентами получено сообщение недопустимого формата.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Перезапустите Dr.Web Gateway Security Suite:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Not ready (Не готов)*

Код ошибки: `x9`

Внутреннее обозначение ошибки: `EC_NOT_READY`

Описание: Требуемое действие не может быть выполнено, потому что запрошенный компонент или устройство еще не инициализированы.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Повторите требуемое действие позже.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Component is not installed (Компонент не установлен)*

Код ошибки: `x10`

Внутреннее обозначение ошибки: `EC_NOT_INSTALLED`

Описание: Компонент, необходимый для выполнения требуемой функции, не установлен.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы

также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Установите или переустановите требуемый компонент. Если неизвестно, какой именно компонент необходим, попробуйте это выяснить, ознакомившись с содержимым журнала.
2. Если установка или переустановка требуемого компонента не помогла, попробуйте переустановить Dr.Web Gateway Security Suite.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Unexpected IPC message (Неожиданное сообщение IPC)*

Код ошибки: `x11`

Внутреннее обозначение ошибки: `EC_UNEXPECTED_MESSAGE`

Описание: В процессе обмена данными между компонентами получено недопустимое сообщение.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Перезапустите Dr.Web Gateway Security Suite, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *IPC protocol violation (Нарушение протокола IPC)*

Код ошибки: `x12`

Внутреннее обозначение ошибки: `EC_PROTOCOL_VIOLATION`

Описание: В процессе обмена данными между компонентами произошло нарушение протокола.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Перезапустите Dr.Web Gateway Security Suite, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Subsystem state is unknown (Неизвестное состояние подсистемы)*

Код ошибки: `x13`

Внутреннее обозначение ошибки: `EC_UNKNOWN_STATE`

Описание: Подсистема Dr.Web Gateway Security Suite, необходимая для выполнения операции, находится в неизвестном состоянии.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Повторите операцию.
2. При повторении ошибки перезапустите Dr.Web Gateway Security Suite, выполнив команду:

   ```
   # service drweb-configd restart
   ```

   после чего повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Path must be absolute (Путь должен быть абсолютным)*

Код ошибки: `x20`

Внутреннее обозначение ошибки: `EC_NOT_ABSOLUTE_PATH`

Описание: Указан относительный путь к файлу или каталогу вместо абсолютного.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Замените относительный путь к файлу или каталогу на абсолютный и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Not enough memory (Недостаточно памяти для завершения операции)*

Код ошибки: `x21`

Внутреннее обозначение ошибки: `EC_NO_MEMORY`

Описание: Недостаточно памяти для выполнения операции.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Попробуйте увеличить объем памяти, доступной процессам Dr.Web Gateway Security Suite (например, изменив лимиты при помощи команды `ulimit`), перезапустить Dr.Web Gateway Security Suite и повторить операцию.

В некоторых случаях системный сервис `systemd` может игнорировать заданные изменения лимита. В этом случае отредактируйте (или создайте, при его отсутствии) файл `/etc/systemd/system/drweb-configd.service.d/limits.conf`, указав в нем измененное значение лимита, например:

```
[Service]
LimitDATA=32767
```

С перечнем доступных лимитов `systemd` можно ознакомиться, выполнив команду `man systemd.exec`.

Для перезапуска Dr.Web Gateway Security Suite выполните команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *IO error (Ошибка ввода-вывода)*

Код ошибки: `x22`

Внутреннее обозначение ошибки: `EC_IO_ERROR`

Описание: Произошла ошибка ввода/вывода (например, дисковое устройство еще не инициализировано или раздел файловой системы более не доступен).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Обеспечьте доступность требуемого устройства ввода/вывода или раздела файловой системы и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *No such file or directory (Нет такого файла или каталога)*

Код ошибки: x23

Внутреннее обозначение ошибки: EC_NO_SUCH_ENTRY

Описание: Попытка обращения к несуществующему файлу или каталогу.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле /var/log/syslog или /var/log/messages, в зависимости от используемой ОС). Вы также можете воспользоваться командой drweb-ctl log.

Устранение ошибки

Проверьте правильность указанного пути. При необходимости исправьте путь и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Permission denied (Доступ запрещен)*

Код ошибки: x24

Внутреннее обозначение ошибки: EC_PERMISSION_DENIED

Описание: Недостаточно прав для доступа к указанному файлу или каталогу.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле /var/log/syslog или /var/log/messages, в зависимости от используемой ОС). Вы также можете воспользоваться командой drweb-ctl log.

Устранение ошибки

Проверьте правильность указанного пути и наличие необходимых прав у компонента. Если доступ к объекту запрещен, измените права доступа к нему или повысьте права компонента и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Not a directory (Не каталог)*

Код ошибки: x25

Внутреннее обозначение ошибки: EC_NOT_A_DIRECTORY

Описание: Указанный объект файловой системы не является каталогом.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле /var/log/syslog или /var/log/messages, в зависимости от используемой ОС). Вы также можете воспользоваться командой drweb-ctl log.

Устранение ошибки

Проверьте правильность пути к объекту. Исправьте путь и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Data file corrupted (Файл данных поврежден)*

Код ошибки: `x26`

Внутреннее обозначение ошибки: `EC_DATA_CORRUPTED`

Описание: Запрашиваемые данные повреждены.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Повторите операцию.
2. При повторении ошибки перезапустите Dr.Web Gateway Security Suite:

   ```
   # service drweb-configd restart
   ```

   после чего повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *File already exists (Файл уже существует)*

Код ошибки: `x27`

Внутреннее обозначение ошибки: `EC_FILE_EXISTS`

Описание: Файл с указанным именем уже существует.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Проверьте правильность написания имени файла. При необходимости исправьте его и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Read-only file system (Файловая система только для чтения)*

Код ошибки: `x28`

Внутреннее обозначение ошибки: `EC_READ_ONLY_FS`

Описание: Файловая система доступна только для чтения.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Проверьте правильность пути к объекту. Исправьте путь так, чтобы он указывал на раздел файловой системы, доступный для записи, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Network error (Ошибка сети)*

Код ошибки: `x29`

Внутреннее обозначение ошибки: `EC_NETWORK_ERROR`

Описание: Ошибка сети (возможно, внезапно перестал отвечать удаленный узел или не удается установить соединение).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Проверьте доступность сети и правильность сетевых настроек. При необходимости исправьте сетевые настройки и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Not a drive (Не дисковое устройство)*

Код ошибки: `x30`

Внутреннее обозначение ошибки: `EC_NOT_A_DRIVE`

Описание: Производится попытка обращения к устройству ввода/вывода, которое не является дисковым устройством.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Проверьте правильность указанного имени устройства. Исправьте путь так, чтобы он вел к дисковому устройству, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Unexpected EOF (Неожиданный конец файла)*

Код ошибки: `x31`

Внутреннее обозначение ошибки: `EC_UNEXPECTED_EOF`

Описание: При чтении данных неожиданно был достигнут конец файла.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Проверьте правильность указанного имени файла. Если нужно, исправьте путь так, чтобы он вел к правильному файлу, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *File was changed (Файл был изменен)*

Код ошибки: `x32`

Внутреннее обозначение ошибки: `EC_FILE_WAS_CHANGED`

Описание: Проверяемый файл был изменен.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Повторите операцию сканирования.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Not a regular file (Объект не является файлом)*

Код ошибки: `x33`

Внутреннее обозначение ошибки: `EC_NOT_A_REGULAR_FILE`

Описание: Запрашиваемый объект файловой системы не является регулярным файлом (он может быть каталогом, сокетом или другим объектом).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Проверьте правильность указанного имени файла. Если нужно, исправьте путь так, чтобы он вел к

регулярному файлу, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Name already in use (Имя уже используется)*

Код ошибки: `x34`

Внутреннее обозначение ошибки: `EC_NAME_ALREADY_IN_USE`

Описание: Объект с указанным именем уже существует.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Проверьте правильность указанного пути. Исправьте путь и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Host is offline (Хост отключен)*

Код ошибки: `x35`

Внутреннее обозначение ошибки: `EC_HOST_OFFLINE`

Описание: Удаленный узел недоступен по сети.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Проверьте доступность требуемого узла сети. При необходимости исправьте адрес узла сети и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Resource limit reached (Достигнут предел использования ресурса)*

Код ошибки: `x36`

Внутреннее обозначение ошибки: `EC_LIMIT_REACHED`

Описание: Достигнут предел использования ресурса.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы

также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Проверьте доступность требуемого ресурса. При необходимости увеличьте лимит на использование ресурса и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Mounting points are different (Различные точки монтирования)*

Код ошибки: `x37`

Внутреннее обозначение ошибки: `EC_CROSS_DEVICE_LINK`

Описание: Восстановление файла предполагает перемещение между двумя точками монтирования.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Выберите другой путь для восстановления файла и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Unpacking error (Ошибка распаковки)*

Код ошибки: `x38`

Внутреннее обозначение ошибки: `EC_UNPACKING_ERROR`

Описание: Не удалось распаковать архив (возможно, он защищен паролем или поврежден).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Убедитесь, что файл не поврежден. Если архив защищен паролем, снимите защиту, указав правильный пароль, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Virus base corrupted (Вирусная база повреждена)*

Код ошибки: `x40`

Внутреннее обозначение ошибки: `EC_BASE_CORRUPTED`

Описание: Вирусные базы повреждены.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр `VirusBaseDir` в секции `[Root]` файла конфигурации).
   - Для просмотра и исправления пути перейдите на страницу **Общие настройки** веб-интерфейса управления.
   - Также вы можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Root.VirusBaseDir
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Root.VirusBaseDir <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset Root.VirusBaseDir -r
   ```

2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Non-supported virus database version (Неподдерживаемая версия вирусных баз)*

Код ошибки: `x41`

Внутреннее обозначение ошибки: `EC_OLD_BASE_VERSION`

Описание: Вирусные базы предназначены для старой версии программы.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его

(параметр `VirusBaseDir` в секции `[Root]` файла конфигурации).

- Для просмотра и исправления пути перейдите на страницу **Общие настройки** веб-интерфейса управления.
- Также вы можете воспользоваться командами утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset Root.VirusBaseDir <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Empty virus database (Вирусная база пуста)*

Код ошибки: `x42`

Внутреннее обозначение ошибки: `EC_EMPTY_BASE`

Описание: Вирусная база пуста.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр `VirusBaseDir` в секции `[Root]` файла конфигурации).
   - Для просмотра и исправления пути перейдите на страницу **Общие настройки** веб-интерфейса управления.
   - Также вы можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Root.VirusBaseDir
   ```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset Root.VirusBaseDir <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Object cannot be cured (Объект не может быть вылечен)*

Код ошибки: `x43`

Внутреннее обозначение ошибки: `EC_CAN_NOT_BE_CURED`

Описание: Действие **Лечить** было применено к неизлечимому объекту.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Выберите действие, допустимое для данного объекта, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Non-supported virus database combination (Неподдерживаемая комбинация вирусных баз)*

Код ошибки: `x44`

Внутреннее обозначение ошибки: `EC_INVALID_BASE_SET`

Описание: Несовместимые вирусные базы.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр `VirusBaseDir` в секции `[Root]` файла конфигурации).

- Для просмотра и исправления пути перейдите на страницу **Общие настройки** веб-интерфейса управления.
- Также вы можете воспользоваться командами утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset Root.VirusBaseDir <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Scan limit reached (Достигнут предел проверки)*

Код ошибки: `x45`

Внутреннее обозначение ошибки: `EC_SCAN_LIMIT_REACHED`

Описание: При сканировании объекта превышены заданные ограничения (например, на величину распакованного файла, на глубину уровней вложенности и т. п.).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Измените ограничения для сканирования объектов (в настройках соответствующего компонента) любым удобным вам способом:
   - используя страницу настроек этого компонента в веб-интерфейсе управления;
   - при помощи команд `drweb-ctl cfshow` и `drweb-ctl cfset`.
2. После изменения настроек повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Authentication failed (Неверные учетные данные пользователя)*

Код ошибки: x47

Внутреннее обозначение ошибки: EC_AUTH_FAILED

Описание: Попытка пройти аутентификацию с неверными учетными данными пользователя.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле /var/log/syslog или /var/log/messages, в зависимости от используемой ОС). Вы также можете воспользоваться командой drweb-ctl log.

Устранение ошибки

Повторите попытку аутентификации, указав правильные учетные данные пользователя, имеющего необходимые полномочия.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Authorization failed (Пользователь не имеет требуемых прав)*

Код ошибки: x48

Внутреннее обозначение ошибки: EC_NOT_AUTHORIZED

Описание: Текущий пользователь не имеет прав на выполнение требуемой операции.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле /var/log/syslog или /var/log/messages, в зависимости от используемой ОС). Вы также можете воспользоваться командой drweb-ctl log.

Устранение ошибки

Повторите попытку авторизации, указав правильные учетные данные пользователя, имеющего необходимые полномочия.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Access token is invalid (Недопустимый токен доступа)*

Код ошибки: x49

Внутреннее обозначение ошибки: EC_INVALID_TOKEN

Описание: Компонент Dr.Web Gateway Security Suite предъявил некорректный токен авторизации при попытке выполнения операции, требующей повышенные права.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле /var/log/syslog или /var/log/messages, в зависимости от используемой ОС). Вы также можете воспользоваться командой drweb-ctl log.

Устранение ошибки

Пройдите аутентификацию, указав правильные учетные данные пользователя, имеющего необходимые полномочия, и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *DBMS general error (Общая ошибка СУБД)*

Код ошибки: `x50`

Внутреннее обозначение ошибки: `EC_DB_COMMON_ERROR`

Описание: Компонент Dr.Web LookupD не смог успешно выполнить запрос к СУБД.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Ознакомьтесь также с журналами сервера СУБД.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Cannot open database (Невозможно открыть базу данных)*

Код ошибки: `x51`

Внутреннее обозначение ошибки: `EC_DB_OPEN_ERROR`

Описание: База данных, к которой пытается подключиться компонент Dr.Web LookupD, недоступна.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Ознакомьтесь также с логами сервера СУБД.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Connection closed by DBMS (Соединение закрыто сервером базы данных)*

Код ошибки: `x52`

Внутреннее обозначение ошибки: `EC_DB_CONN_CLOSED`

Описание: Соединение было закрыто сервером СУБД.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Ознакомьтесь также с логами сервера СУБД.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid argument (Недопустимый аргумент)*

Код ошибки: `x60`

Внутреннее обозначение ошибки: `EC_INVALID_ARGUMENT`

Описание: Команда не может быть выполнена, так как указан недопустимый аргумент.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность написания и формат команды.
2. Повторите требуемое действие, указав допустимый аргумент.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid operation (Недопустимая операция)*

Код ошибки: `x61`

Внутреннее обозначение ошибки: `EC_INVALID_OPERATION`

Описание: Совершена попытка выполнить недопустимую команду.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Повторите требуемое действие, указав допустимую команду.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Superuser privileges required (Требуются полномочия суперпользователя)*

Код ошибки: `x62`

Внутреннее обозначение ошибки: `EC_ROOT_ONLY`

Описание: Для выполнения требуемого действия требуются полномочия суперпользователя.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Повысьте свои права до суперпользователя и повторите требуемое действие. Для повышения прав можно воспользоваться командой `su` или `sudo`.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Not allowed in centralized protection mode (Не разрешено в режиме централизованной защиты)*

Код ошибки: `x63`

Внутреннее обозначение ошибки: `EC_STANDALONE_MODE_ONLY`

Описание: Требуемое действие можно выполнить только при работе Dr.Web Gateway Security Suite в автономном режиме.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Переведите Dr.Web Gateway Security Suite в автономный режим и повторите операцию снова.

Для перевода Dr.Web Gateway Security Suite в автономный режим:

- сбросьте флажок **Включить режим централизованной защиты** на странице настроек **Централизованная защита** веб-интерфейса управления;
- или выполните команду:

```
# drweb-ctl esdisconnect
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Non-supported OS (Неподдерживаемая ОС)*

Код ошибки: `x64`

Внутреннее обозначение ошибки: `EC_NON_SUPPORTED_OS`

Описание: Операционная система, установленная на узле, не поддерживается Dr.Web Gateway Security Suite.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Установите операционную систему из списка, указанного в системных требованиях.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Feature not implemented (Функция не реализована)*

Код ошибки: `x65`

Внутреннее обозначение ошибки: `EC_UNKNOWN_OPTION`

Описание: Запрашиваемые функции компонента отсутствуют в текущей версии.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Попробуйте сбросить настройки Dr.Web Gateway Security Suite в значения по умолчанию.

Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

- для GNU/Linux:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

- для FreeBSD:

```
# cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
# echo "" > /usr/local/etc/drweb.com/drweb.ini
```

После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Unknown option (Неизвестный параметр)*

Код ошибки: `x66`

Внутреннее обозначение ошибки: `EC_UNKNOWN_OPTION`

Описание: Файл конфигурации содержит параметры, неизвестные или не поддерживаемые в текущей версии Dr.Web Gateway Security Suite.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Откройте файл `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD в любом текстовом редакторе, удалите строку, содержащую недопустимый параметр, сохраните файл и перезапустите демон управления конфигурацией Dr.Web ConfigD, выполнив команду:

   ```
   # service drweb-configd restart
   ```

2. Если это не поможет, попробуйте сбросить настройки Dr.Web Gateway Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   - для GNU/Linux:

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```

   - для FreeBSD:

     ```
     # cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
     # echo "" > /usr/local/etc/drweb.com/drweb.ini
     ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

   ```
   # service drweb-configd restart
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Unknown section (Неизвестная секция)*

Код ошибки: `x67`

Внутреннее обозначение ошибки: `EC_UNKNOWN_SECTION`

Описание: Файл конфигурации содержит секции, неизвестные или не поддерживаемые в текущей версии Dr.Web Gateway Security Suite.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Откройте файл `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD в любом текстовом редакторе и удалите неизвестную секцию, после чего сохраните файл и перезапустите демон управления конфигурацией Dr.Web ConfigD, выполнив команду:

   ```
   # service drweb-configd restart
   ```

2. Если это не поможет, попробуйте сбросить настройки Dr.Web Gateway Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   - для GNU/Linux:

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```

   - для FreeBSD:

     ```
     # cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
     # echo "" > /usr/local/etc/drweb.com/drweb.ini
     ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

   ```
   # service drweb-configd restart
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid option value (Недопустимое значение параметра)*

Код ошибки: `x68`

Внутреннее обозначение ошибки: `EC_INVALID_OPTION_VALUE`

Описание: Для одного или нескольких параметров в файле конфигурации указано недопустимое значение.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Измените значение параметра любым удобным для вас способом:
   - используя страницу настроек этого компонента в веб-интерфейсе управления;
   - при помощи команд `drweb-ctl cfshow` и `drweb-ctl cfset`.

   Если вы не знаете, какое значение параметра допустимо, обратитесь к справке по компоненту,

использующему данный параметр, или попытайтесь сбросить значение этого параметра в значение по умолчанию.

2. Также можно отредактировать непосредственно файл конфигурации `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD. Для этого откройте его в любом текстовом редакторе, найдите строку, содержащую недопустимое значение параметра, задайте допустимое значение, сохраните файл и перезапустите демон управления конфигурацией Dr.Web ConfigD, выполнив команду:

   ```
   # service drweb-configd restart
   ```

3. Если предыдущие шаги не помогли, попробуйте сбросить настройки Dr.Web Gateway Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   - для GNU/Linux:

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```

   - для FreeBSD:

     ```
     # cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
     # echo "" > /usr/local/etc/drweb.com/drweb.ini
     ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

   ```
   # service drweb-configd restart
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid state (Недопустимое состояние)*

Код ошибки: `x69`

Внутреннее обозначение ошибки: `EC_INVALID_STATE`

Описание: Недопустимое состояние компонента или Dr.Web Gateway Security Suite в целом для выполнения запрошенной операции.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Повторите требуемое действие через некоторое время.

2. При повторении ошибки перезапустите Dr.Web Gateway Security Suite, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Only one value allowed (Разрешено только одно значение)*

Код ошибки: `x70`

Внутреннее обозначение ошибки: `EC_NOT_LIST_OPTION`

Описание: В файле конфигурации для параметра, который может иметь только одно значение, задано значение в виде списка.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Измените значение параметра любым удобным для вас способом:
   - используя страницу настроек этого компонента в веб-интерфейсе управления;
   - при помощи команд `drweb-ctl cfshow` и `drweb-ctl cfset`.

   Если вы не знаете, какое значение параметра допустимо, обратитесь к справке по компоненту, использующему данный параметр, или попытайтесь сбросить значение этого параметра в значение по умолчанию.
2. Также можно отредактировать непосредственно файл конфигурации `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD. Для этого откройте его в любом текстовом редакторе, найдите строку, содержащую недопустимое значение параметра, задайте допустимое значение, сохраните файл и перезапустите демон управления конфигурацией Dr.Web ConfigD, выполнив команду:

```
# service drweb-configd restart
```

3. Если предыдущие шаги не помогли, попробуйте сбросить настройки Dr.Web Gateway Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:
   - для GNU/Linux:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

   - для FreeBSD:

```
# cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
```

```
# echo "" > /usr/local/etc/drweb.com/drweb.ini
```

После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Tag value is invalid (Недопустимое имя тега)*

Код ошибки: `x71`

Внутреннее обозначение ошибки: `EC_INVALID_TAG`

Описание: В имени источника данных, с которым взаимодействует компонент Dr.Web LookupD, использован некорректный или несуществующий тег.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Проверьте правильность написания тега. Если в написании допущена ошибка, отредактируйте соответствующую секцию в файле конфигурации.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Record not found (Запись не найдена)*

Код ошибки: `x80`

Внутреннее обозначение ошибки: `EC_RECORD_NOT_FOUND`

Описание: Информация о найденной угрозе отсутствует (возможно, угроза уже была обработана другим компонентом).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Обновите список угроз через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Record is in process now (Запись обрабатывается в данный момент)*

Код ошибки: `x81`

Внутреннее обозначение ошибки: `EC_RECORD_BUSY`

Описание: Угроза уже обрабатывается другим компонентом.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Обновите список угроз через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *File has already been quarantined (Файл уже находится в карантине)*

Код ошибки: `x82`

Внутреннее обозначение ошибки: `EC_QUARANTINED_FILE`

Описание: Файл уже находится в карантине. Возможно, угроза уже была обработана другим компонентом.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Обновите список угроз через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Update zone is not provided by cloud (Зона обновления в облаке недоступна)*

Код ошибки: `x83`

Внутреннее обозначение ошибки: `EC_NO_ZONE_IN_CLOUD`

Описание: Попытка обновления с помощью Dr.Web Cloud завершилась неудачей.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Повторите требуемое действие через некоторое время.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Update zone is not provided on disk (Зона обновления на диске недоступна)*

Код ошибки: `x84`

Внутреннее обозначение ошибки: `EC_NO_ZONE_ON_DISK`

Описание: Попытка обновления вирусных баз в режиме оффлайн завершилась неудачей.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Убедитесь, что путь к устройству, с которого производится обновление, указан верно.
2. Убедитесь, что пользователь, от имени которого выполняется обновление, обладает правами на чтение каталога с обновлениями.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Cannot backup before update (Не удалось сохранить резервную копию перед обновлением)*

Код ошибки: `x89`

Внутреннее обозначение ошибки: `EC_BACKUP_FAILED`

Описание: Перед началом загрузки обновлений с сервера обновлений не удалось сохранить резервную копию подлежащих обновлению файлов.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу, хранящему резервные копии обновляемых файлов и при необходимости исправьте его (параметр `BackupDir` в секции `[Update]` файла конфигурации).
   - Для просмотра и исправления пути перейдите на страницу настроек **Updater** веб-интерфейса управления.
   - Вы также можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Update.BackupDir
   ```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset Update.BackupDir <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset Update.BackupDir -r
```

2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```
3. Если ошибка повторяется, проверьте, что пользователь, от имени которого исполняется компонент, имеет права на запись в каталог, указанный в параметре `BackupDir`. Имя пользователя указано в параметре `RunAsUser`. При необходимости измените имя пользователя, изменив значение параметра `RunAsUser`, или предоставьте недостающие права в свойствах каталога.
4. Если ошибка повторяется, переустановите пакет `drweb-update`.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid DRL file (Недопустимый DRL-файл)*

Код ошибки: `x90`

Внутреннее обозначение ошибки: `EC_BAD_DRL_FILE`

Описание: Нарушена структура одного из файлов со списками серверов обновлений.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к файлу списка серверов и при необходимости исправьте его (параметры с именем вида `*DrlDir` в секции `[Update]` файла конфигурации).
   - Для просмотра и исправления пути перейдите на страницу настроек **Updater** веб-интерфейса управления.
   - Вы также можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду (<**DrlDir*> нужно заменить на имя конкретного параметра. Если имя параметра неизвестно, просмотрите значения всех параметров в секции, опустив часть команды, заключенную в квадратные скобки):

   ```
   $ drweb-ctl cfshow Update[.<*DrlDir>]
   ```

Для установки нового значения параметра введите команду (<*DrlDir> нужно заменить на имя конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlDir> <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду (<*DrlDir> нужно заменить на имя конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlDir> -r
```

2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```
3. Если ошибка повторяется, переустановите пакет `drweb-update`.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid LST file (Недопустимый LST-файл)*

Код ошибки: `x91`

Внутреннее обозначение ошибки: `EC_BAD_LST_FILE`

Описание: Нарушена структура файла с перечнем обновляемых вирусных баз.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Обновите вирусные базы повторно через некоторое время:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```
2. Если ошибка повторяется, переустановите пакет `drweb-update`.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid compressed file (Недопустимый сжатый файл)*

Код ошибки: x92

Внутреннее обозначение ошибки: EC_BAD_LZMA_FILE

Описание: Нарушена структура загруженного файла с обновлениями.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле /var/log/syslog или /var/log/messages, в зависимости от используемой ОС). Вы также можете воспользоваться командой drweb-ctl log.

Устранение ошибки

Обновите вирусные базы повторно через некоторое время:

- нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
- или выполните команду:

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Proxy authentication error (Ошибка аутентификации на прокси-сервере)*

Код ошибки: x93

Внутреннее обозначение ошибки: EC_PROXY_AUTH_ERROR

Описание: Не удалось подключиться к серверам обновлений через прокси-сервер, указанный в настройках.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле /var/log/syslog или /var/log/messages, в зависимости от используемой ОС). Вы также можете воспользоваться командой drweb-ctl log.

Устранение ошибки

1. Проверьте правильность параметров подключения к прокси-серверу (задаются в параметре с именем Proxy в секции [Update] файла конфигурации).
   - Для просмотра и задания параметров подключения перейдите на страницу настроек **Updater** веб-интерфейса управления.
   - Вы также можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Update.Proxy
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Update.Proxy <новые параметры>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset Update.Proxy -r
   ```

2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *No update servers available (Нет доступных серверов обновлений)*

Код ошибки: `x94`

Внутреннее обозначение ошибки: `EC_NO_UPDATE_SERVERS`

Описание: Не удалось подключиться ни к одному из серверов обновлений.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте доступность сети и исправьте при необходимости сетевые настройки.
2. Если доступ к сети возможен только через прокси-сервер, задайте параметры подключения к прокси-серверу (задаются в параметре с именем `Proxy` в секции `[Update]` файла конфигурации).
   - Для просмотра и задания параметров подключения перейдите на страницу настроек **Updater** веб-интерфейса управления.
   - Вы также можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Update.Proxy
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Update.Proxy <новые параметры>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset Update.Proxy -r
   ```
3. Если параметры сетевого подключения, в том числе используемого прокси-сервера, правильные, а ошибка происходит, убедитесь в том, что вы используете доступный список серверов обновления. Перечень используемых серверов обновления указывается в параметрах вида `*DrlDir` в секции `[Update]` файла конфигурации.

Если параметры вида `*CustomDrlDir` указывают на существующий корректный файл списка серверов, то указанные там серверы будут использоваться вместо серверов стандартной зоны обновления (значение, указанное в соответствующем параметре `*DrlDir`, игнорируется).

- Для просмотра и задания параметров подключения перейдите на страницу настроек **Updater** веб-интерфейса управления.
- Вы также можете воспользоваться командами утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду (<**DrlDir*> нужно заменить на имя конкретного параметра. Если имя параметра неизвестно, просмотрите значение всех параметров в секции, опустив часть команды, заключенную в квадратные скобки):

```
$ drweb-ctl cfshow Update[.<*DrlDir>]
```

Для установки нового значения параметра введите команду (<**DrlDir*> нужно заменить на имя конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlDir> <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду (<**DrlDir*> нужно заменить на имя конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlDir> -r
```

4. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

     ```
     $ drweb-ctl update
     ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid key file format (Недопустимый формат ключевого файла)*

Код ошибки: `x95`

Внутреннее обозначение ошибки: `EC_BAD_KEY_FORMAT`

Описание: Нарушен формат ключевого файла.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте наличие ключевого файла и правильности пути к нему. Путь к ключевому файлу задается в параметре `KeyPath` в секции `[Root]` файла конфигурации.
   - Для просмотра и задания пути к ключевому файлу перейдите на страницу **Общие настройки**

веб-интерфейса управления.

- Вы также можете воспользоваться командами утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow Root.KeyPath
```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset Root.KeyPath <путь к файлу>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset Root.KeyPath -r
```

2. Если у вас отсутствует ключевой файл, или используемый ключевой файл поврежден, приобретите и установите его. Описание ключевого файла, способы приобретения и установки описаны в разделе Лицензирование.
3. Для установки имеющегося у вас ключевого файла вы можете воспользоваться также формой активации лицензии, расположенной в нижней части страницы **Главная** веб-интерфейса управления.
4. Параметры текущей лицензии можно просмотреть в личном кабинете **Мой Dr.Web** по ссылке https://support.drweb.com/get+cabinet+link/.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *License is already expired (Срок действия лицензии истек)*

Код ошибки: `x96`

Внутреннее обозначение ошибки: `EC_EXPIRED_KEY`

Описание: Срок действия лицензии истек.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе Лицензирование.
2. Для установки приобретенного ключевого файла вы также можете воспользоваться формой активации лицензии, расположенной в нижней части страницы **Главная** веб-интерфейса управления.
3. Параметры текущей лицензии можно просмотреть в личном кабинете **Мой Dr.Web** по ссылке https://support.drweb.com/get+cabinet+link/.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Network operation timed out (Истек тайм-аут сетевой операции)*

Код ошибки: `x97`

Внутреннее обозначение ошибки: `EC_NETWORK_TIMEDOUT`

Описание: Истекло время ожидания сетевого соединения (возможно, внезапно перестал отвечать удаленный узел или не удается установить требуемое соединение).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Проверьте доступность сети и правильность сетевых настроек. При необходимости исправьте сетевые настройки и повторите операцию.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid checksum (Недопустимая контрольная сумма)*

Код ошибки: `x98`

Внутреннее обозначение ошибки: `EC_BAD_CHECKSUM`

Описание: Неверная контрольная сумма загруженного файла с обновлениями.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Обновите вирусные базы повторно через некоторое время:

- нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
- или выполните команду:

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid trial license (Недопустимый демонстрационный ключевой файл)*

Код ошибки: `x99`

Внутреннее обозначение ошибки: `EC_BAD_TRIAL_KEY`

Описание: Демонстрационный ключевой файл недействителен (например, он был получен для другого компьютера).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с

содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Запросите новый демонстрационный период для данного компьютера, или приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе Лицензирование.
2. Для установки приобретенного ключевого файла вы также можете воспользоваться формой активации лицензии, расположенной в нижней части страницы **Главная** веб-интерфейса управления.
3. Параметры текущей лицензии можно просмотреть в личном кабинете **Мой Dr.Web** по ссылке https://support.drweb.com/get+cabinet+link/.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Blocked license key (Лицензионный ключевой файл заблокирован)*

Код ошибки: `x100`

Внутреннее обозначение ошибки: `EC_BLOCKED_LICENSE`

Описание: Текущая лицензия заблокирована (возможно, нарушены условия лицензионного соглашения на использование Dr.Web Gateway Security Suite).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе Лицензирование.
2. Для установки приобретенного ключевого файла можно воспользоваться формой активации лицензии, расположенной в нижней части страницы **Главная** веб-интерфейса управления.
3. Параметры текущей лицензии можно просмотреть в личном кабинете **Мой Dr.Web** по ссылке https://support.drweb.com/get+cabinet+link/.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid license (Недопустимая лицензия)*

Код ошибки: `x101`

Внутреннее обозначение ошибки: `EC_BAD_LICENSE`

Описание: Используемая лицензия предназначена для другого программного продукта или не содержит необходимых разрешений для работы компонентов Dr.Web Gateway Security Suite.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с

содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Приобретите новую лицензию и установите полученный ключевой файл. Способы приобретения лицензии и установки ключевого файла описаны в разделе Лицензирование.
2. Для установки приобретенного ключевого файла можно воспользоваться формой активации лицензии, расположенной в нижней части страницы **Главная** веб-интерфейса управления.
3. Параметры текущей лицензии можно просмотреть в личном кабинете **Мой Dr.Web** по ссылке https://support.drweb.com/get+cabinet+link/.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid configuration (Недопустимая конфигурация)*

Код ошибки: `x102`

Внутреннее обозначение ошибки: `EC_BAD_CONFIG`

Описание: Компонент Dr.Web Gateway Security Suite не может функционировать из-за неправильных настроек конфигурации.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Если имя компонента, вызвавшего ошибку, неизвестно, попытайтесь его определить, ознакомившись с содержимым журнала.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Invalid executable file (Недопустимый исполняемый файл)*

Код ошибки: `x104`

Внутреннее обозначение ошибки: `EC_BAD_EXECUTABLE`

Описание: Невозможно запустить компонент. Исполняемый файл поврежден или путь к нему указан неверно.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Если имя компонента, вызвавшего ошибку, неизвестно, попытайтесь его определить, ознакомившись с содержимым журнала.

2. Проверьте значение пути к исполняемому файлу компонента в конфигурации Dr.Web Gateway Security Suite (параметр `ExePath` в секции компонента), выполнив команду (замените *<секция компонента>* на название соответствующей секции файла конфигурации):

   ```
   $ drweb-ctl cfshow <секция компонента>.ExePath
   ```

3. Сбросьте путь в значение по умолчанию, выполнив команду (замените *<секция компонента>* на название соответствующей секции файла конфигурации):

   ```
   # drweb-ctl cfset <секция компонента>.ExePath -r
   ```

4. Если предыдущие шаги не помогли, переустановите пакет соответствующего компонента.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Core engine is not available (Ядро Virus-Finding Engine недоступно)*

Код ошибки: `x105`

Внутреннее обозначение ошибки: `EC_NO_CORE_ENGINE`

Описание: Файл антивирусного ядра Dr.Web Virus-Finding Engine отсутствует или недоступен.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к файлу антивирусного ядра `drweb32.dll` и при необходимости исправьте его (параметр `CoreEnginePath` в секции `[Root]` файла конфигурации).
   - Для просмотра и исправления пути перейдите на страницу **Общие настройки** веб-интерфейса управления.
   - Вы также можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Root.CoreEnginePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Root.CoreEnginePath <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset Root.CoreEnginePath -r
   ```

2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;

- или выполните команду:

```
$ drweb-ctl update
```

3. Если путь правильный и ошибка повторяется после обновления вирусных баз, переустановите пакет `drweb-bases`.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *No virus databases (Вирусные базы отсутствуют)*

Код ошибки: `x106`

Внутреннее обозначение ошибки: `EC_NO_VIRUS_BASES`

Описание: Вирусные базы отсутствуют.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу вирусных баз и при необходимости исправьте его (параметр `VirusBaseDir` в секции `[Root]` файла конфигурации).
   - Для просмотра и исправления пути перейдите на страницу **Общие настройки** веб-интерфейса управления.
   - Также вы можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

   Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset Root.VirusBaseDir <новый путь>
```

   Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Обновите вирусные базы:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

```
$ drweb-ctl update
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Process terminated by signal (Процесс завершен по сигналу)*

Код ошибки: `x107`

Внутреннее обозначение ошибки: `EC_APP_TERMINATED`

Описание: Компонент завершил работу (возможно, из-за простоя или вследствие команды пользователя).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Если выполнявшаяся операция не была завершена, то повторите ее запуск снова. В противном случае завершение работы не является ошибкой.
2. Если компонент постоянно завершает свою работу, попробуйте сбросить настройки компонента в значения по умолчанию любым удобным для вас способом:
   - используя страницу настроек этого компонента в веб-интерфейсе управления;
   - при помощи команд `drweb-ctl cfshow` и `drweb-ctl cfset`;
   - отредактировав вручную файл конфигурации (удалив все параметры из секции компонента).
3. Если это не помогло, попробуйте сбросить настройки Dr.Web Gateway Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   - для GNU/Linux:

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```

   - для FreeBSD:

     ```
     # cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
     # echo "" > /usr/local/etc/drweb.com/drweb.ini
     ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

   ```
   # service drweb-configd restart
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Unexpected process termination (Непредвиденное завершение процесса)*

Код ошибки: `x108`

Внутреннее обозначение ошибки: `EC_APP_CRASHED`

Описание: Компонент неожиданно завершил работу по причине сбоя.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Повторите выполнявшуюся операцию.
2. Если компонент постоянно аварийно завершает свою работу, сбросьте настройки компонента в значения по умолчанию любым удобным для вас способом:
   - используя страницу настроек этого компонента в веб-интерфейсе управления;
   - при помощи команд `drweb-ctl cfshow` и `drweb-ctl cfset`;
   - отредактировав вручную файл конфигурации (удалив все параметры из секции компонента).
3. Если это не помогло, сбросьте настройки Dr.Web Gateway Security Suite в значения по умолчанию.

   Для этого очистите содержимое файла `/etc/opt/drweb.com/drweb.ini` для GNU/Linux или `/usr/local/etc/drweb.com/drweb.ini` для FreeBSD (при этом рекомендуется сохранить резервную копию конфигурационного файла), например, выполнив команды:

   - для GNU/Linux:

     ```
     # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
     # echo "" > /etc/opt/drweb.com/drweb.ini
     ```

   - для FreeBSD:

     ```
     # cp /usr/local/etc/drweb.com/drweb.ini /usr/local/etc/drweb.com/drweb.ini.save
     # echo "" > /usr/local/etc/drweb.com/drweb.ini
     ```

   После очистки файла конфигурации перезапустите демон управления конфигурацией, выполнив команду:

   ```
   # service drweb-configd restart
   ```

4. Если ошибка повторяется после сброса настроек Dr.Web Gateway Security Suite, переустановите пакет компонента.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Incompatible software detected (Обнаружено несовместимое ПО)*

Код ошибки: `x109`

Внутреннее обозначение ошибки: `EC_INCOMPATIBLE`

Описание: Один или несколько компонентов Dr.Web Gateway Security Suite не могут функционировать корректно. В системе обнаружено программное обеспечение, препятствующее

их работе.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Если ошибка вызвана компонентом SpIDer Gate, то проблема может быть связана с наличием программного обеспечения, формирующего для системного брандмауэра NetFilter правила, которые препятствуют корректной работе SpIDer Gate — например, Shorewall или SuseFirewall2 (в ОС SUSE Linux). Такие приложения периодически выполняют проверку целостности заданной ими системы правил и перезаписывают их.

   Настройте конфликтующее программное обеспечение таким образом, чтобы оно не мешало работе SpIDer Gate. Если сделать это не удается, отключите конфликтующее приложение с запретом его запуска при последующих загрузках ОС. Приложение SuseFirewall2 (в ОС SUSE Linux) можно попытаться настроить следующим образом:

   1) откройте файл конфигурации SuseFirewall2 (по умолчанию это файл `/etc/sysconfig/SuSEfirewall2`);
   2) найдите в файле следующие строки:

```
## Type: yesno
#
# Install NOTRACK target for interface lo in the raw table. Doing so
# speeds up packet processing on the loopback interface. This breaks
# certain firewall setups that need to e.g. redirect outgoing
# packets via custom rules on the local machine.
#
# Defaults to "yes" if not set
#
FW_LO_NOTRACK=""
```

   3) Установите для параметра `FW_LO_NOTRACK` значение `no`:

```
FW_LO_NOTRACK="no"
```

   4) Перезапустите SuseFirewall2:

```
# rcSuSEfirewall2 restart
```

   Если в настройках SuseFirewall2 параметр `FW_LO_NOTRACK` отсутствует, для устранения конфликта остановите это приложение и запретите его запуск при последующих загрузках ОС.

   После изменения настроек или отключения конфликтующего приложения перезапустите SpIDer Gate.

2. Если ошибка вызвана другим компонентом, то отключите или перенастройте конфликтующее программное обеспечение таким образом, чтобы оно не мешало работе Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *No web resource databases (Базы категорий веб-ресурсов отсутствуют)*

Код ошибки: `x112`

Внутреннее обозначение ошибки: `EC_NO_DWS_BASES`

Описание: Отсутствуют базы категорий веб-ресурсов.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к каталогу базы данных категорий веб-ресурсов и при необходимости исправьте его (параметр `DwsDir` в секции `[Root]` файла конфигурации).
   - Для просмотра и исправления пути перейдите на страницу **Общие настройки** веб-интерфейса управления.
   - Вы также можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Root.DwsDir
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Root.DwsDir <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset Root.DwsDir -r
   ```
2. Обновите базы категорий веб-ресурсов:
   - нажмите **Обновить** на странице **Главная** веб-интерфейса управления;
   - или выполните команду:

   ```
   $ drweb-ctl update
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *MeshD is not available (Компонент MeshD недоступен)*

Код ошибки: `x114`

Внутреннее обозначение ошибки: `EC_NO_MESHD`

Описание: Отсутствует компонент Dr.Web MeshD (требуется для распределения нагрузки при проверке файлов).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в

файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-meshd` и при необходимости исправьте его (параметр `ExePath` в секции `[MeshD]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow MeshD.ExePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset MeshD.ExePath <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset MeshD.ExePath -r
   ```

2. При отсутствии настроек компонента Dr.Web MeshD в конфигурации, или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-meshd`.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *LookupD is not available (Компонент LookupD недоступен)*

Код ошибки: `x115`

Внутреннее обозначение ошибки: `EC_NO_LOOKUPD`

Описание: Отсутствует компонент Dr.Web LookupD (требуется для выбора данных из внешних источников).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

1. Проверьте правильность пути к исполняемому файлу `drweb-lookupd` и при необходимости исправьте его (параметр `ExePath` в секции `[LookupD]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow LookupD.ExePath
   ```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset LookupD.ExePath <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset LookupD.ExePath -r
```

2. При отсутствии настроек компонента Dr.Web LookupD в конфигурации, или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-lookupd`.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *UrlCheck is not available (Компонент UrlCheck недоступен)*

Код ошибки: `x116`

Внутреннее обозначение ошибки: `EC_NO_URL_CHECK`

Описание: Отсутствует компонент Dr.Web URL Checker (требуется для проверки URL на принадлежность к запрещенным или потенциально опасным категориям).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-urlcheck` и при необходимости исправьте его (параметр `ExePath` в секции `[URLCheck]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow URLCheck.ExePath
```

   Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset URLCheck.ExePath <новый путь>
```

   Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset URLCheck.ExePath -r
```

2. При отсутствии настроек компонента Dr.Web URL Checker в конфигурации, или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-urlcheck`.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *GateD is not available (SplDer Gate недоступен)*

Код ошибки: `x117`

Внутреннее обозначение ошибки: `EC_NO_GATED`

Описание: Отсутствует компонент SplDer Gate (требуется для проверки сетевых соединений).

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-gated` и при необходимости исправьте его (параметр `ExePath` в секции `[GateD]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow GateD.ExePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset GateD.ExePath <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset GateD.ExePath -r
   ```

2. При отсутствии настроек компонента SplDer Gate в конфигурации или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-gated`.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *ScanEngine is not available (Scanning Engine недоступен)*

Код ошибки: `x119`

Внутреннее обозначение ошибки: `EC_NO_SCAN_ENGINE`

Описание: Компонент Dr.Web Scanning Engine отсутствует или не может быть запущен.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-se` и при необходимости исправьте его (параметр `ExePath` в секции `[ScanEngine]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow ScanEngine.ExePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset ScanEngine.ExePath <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset ScanEngine.ExePath -r
   ```

2. В случае возникновения ошибки при указании правильного пути:

   - Выполните команду:

     ```
     $ drweb-ctl rawscan /
     ```

   Если в выводе на экран присутствует строка «`Error: No valid license provided`», то это означает, что отсутствует действующий ключевой файл. Зарегистрируйте Dr.Web Gateway Security Suite и получите лицензию. Если лицензия вами получена, то проверьте наличие ключевого файла и установите его при необходимости.

   - Если ваша ОС использует подсистему безопасности SELinux, настройте политику безопасности для модуля `drweb-se` (см. раздел Настройка политик безопасности SELinux).

3. При отсутствии настроек компонента Dr.Web Scanning Engine в конфигурации, или если предыдущие шаги не помогли, установите или переустановите пакет `drweb-se`.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *FileCheck is not available (File Checker недоступен)*

Код ошибки: `x120`

Внутреннее обозначение ошибки: `EC_NO_FILE_CHECK`

Описание: Компонент Dr.Web File Checker отсутствует или не может быть запущен.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-filecheck` и при необходимости исправьте его (параметр `ExePath` в секции `[FileCheck]` файла конфигурации).

Вы можете воспользоваться командами утилиты управления из командной строки.

Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow FileCheck.ExePath
```

Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset FileCheck.ExePath <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset FileCheck.ExePath -r
```

2. В случае возникновения ошибки при указании правильного пути:
   - Если ваша ОС использует подсистему безопасности SELinux, настройте политику безопасности для модуля `drweb-filecheck` (см. раздел Настройка политик безопасности SELinux).
3. При отсутствии настроек компонента Dr.Web File Checker в конфигурации, или если предыдущие шаги не помогли, установите или переустановите пакет `drweb-filecheck`.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *ESAgent is not available (ES Agent недоступен)*

Код ошибки: `x121`

Внутреннее обозначение ошибки: `EC_NO_ESAGENT`

Описание: Отсутствует компонент Dr.Web ES Agent, необходимый для подключения к серверу централизованной защиты.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-esagent` и при необходимости исправьте его (параметр `ExePath` в секции `[ESAgent]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

```
$ drweb-ctl cfshow ESAgent.ExePath
```

   Для установки нового значения параметра введите команду:

```
# drweb-ctl cfset ESAgent.ExePath <новый путь>
```

Для сброса значения параметра в значение по умолчанию введите команду:

```
# drweb-ctl cfset ESAgent.ExePath -r
```

2. При отсутствии настроек компонента Dr.Web ES Agent в конфигурации, или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-esagent`.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Firewall is not available (Компонент Firewall для Linux недоступен)*

Код ошибки: `x122`

Внутреннее обозначение ошибки: `EC_NO_FIREWALL`

Описание: Отсутствует компонент Dr.Web Firewall для Linux, необходимый для проверки сетевых соединений.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-firewall` и при необходимости исправьте его (параметр `ExePath` в секции `[LinuxFirewall]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow LinuxFirewall.ExePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset LinuxFirewall.ExePath <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset LinuxFirewall.ExePath -r
   ```

2. При отсутствии настроек компонента Dr.Web Firewall для Linux в конфигурации или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-firewall`.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *NetCheck is not available (Network Checker недоступен)*

Код ошибки: `x123`

Внутреннее обозначение ошибки: `EC_NO_NETCHECK`

Описание: Отсутствует компонент Dr.Web Network Checker, необходимый для проверки файлов по сети.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-netcheck` и при необходимости исправьте его (параметр `ExePath` в секции `[Netcheck]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow Netcheck.ExePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset Netcheck.ExePath <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset Netcheck.ExePath -r
   ```

2. При отсутствии настроек компонента Dr.Web Network Checker в конфигурации или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-netcheck`.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *CloudD is not available (Компонент CloudD недоступен)*

Код ошибки: `x124`

Внутреннее обозначение ошибки: `EC_NO_CLOUDD`

Описание: Отсутствует компонент Dr.Web CloudD, необходимый для обращения к облаку Dr.Web Cloud.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

1. Проверьте правильность пути к исполняемому файлу `drweb-cloudd` и при необходимости исправьте его (параметр `ExePath` в секции `[CloudD]` файла конфигурации).

   Вы можете воспользоваться командами утилиты управления из командной строки.

   Для просмотра текущего значения параметра введите команду:

   ```
   $ drweb-ctl cfshow CloudD.ExePath
   ```

   Для установки нового значения параметра введите команду:

   ```
   # drweb-ctl cfset CloudD.ExePath <новый путь>
   ```

   Для сброса значения параметра в значение по умолчанию введите команду:

   ```
   # drweb-ctl cfset CloudD.ExePath -r
   ```

2. При отсутствии настроек компонента Dr.Web CloudD в конфигурации или в случае возникновения ошибки при указании правильного пути, установите или переустановите пакет `drweb-cloudd`.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Сообщение об ошибке: *Unexpected error (Непредвиденная ошибка)*

Код ошибки: `x125`

Внутреннее обозначение ошибки: `EC_UNEXPECTED_ERROR`

Описание: Возникла непредвиденная ошибка в работе одного или нескольких компонентов.

Для выявления возможной причины и обстоятельств возникновения ошибки ознакомьтесь с содержимым журнала Dr.Web Gateway Security Suite (по умолчанию он находится в файле `/var/log/syslog` или `/var/log/messages`, в зависимости от используемой ОС). Вы также можете воспользоваться командой `drweb-ctl log`.

Устранение ошибки

Перезапустите Dr.Web Gateway Security Suite, выполнив команду:

```
# service drweb-configd restart
```

Если устранить ошибку не удастся, обратитесь в техническую поддержку и сообщите код ошибки.

Ошибки без кода

Симптомы: Такие компоненты, как Dr.Web ClamD, SpIDer Gate, Dr.Web ICAPD, не проверяют

сообщения; в журнале Dr.Web Gateway Security Suite наблюдаются сообщения `Too many open files`.

Описание: В связи большой загрузкой по проверке данных компонент Dr.Web Network Checker исчерпал лимит на число доступных файловых дескрипторов.

Устранение ошибки

1. Увеличьте лимит на число открытых файловых дескрипторов, доступных приложению, используя команду `ulimit -n` (по умолчанию лимит на число дескрипторов для Dr.Web Gateway Security Suite составляет 16384).

   В некоторых случаях системный сервис `systemd` может игнорировать заданные изменения лимита.

   В этом случае отредактируйте (или создайте, при его отсутствии) файл `/etc/systemd/system/drweb-configd.service.d/limits.conf`, указав в нем измененное значение лимита:

   ```
   [Service]
   LimitNOFILE=16384
   ```

   С перечнем доступных лимитов `systemd` можно ознакомиться, выполнив команду `man systemd.exec`.

2. После изменения лимита перезапустите Dr.Web Gateway Security Suite, выполнив команду:

   ```
   # service drweb-configd restart
   ```

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Симптомы: Не удается установить соединение с веб-интерфейсом управления Dr.Web в браузере, компоненты Dr.Web отсутствуют в перечне запущенных процессов (`ps ax | grep drweb`), выполнение любой команды `drweb-ctl <команда>`, за исключением команды `drweb-ctl rawscan`, выводит сообщение об ошибке:

`Error: connect: No such file or directory: "<путь>/.com.drweb.public"`

или

`Error: connect: Connection refused: "<путь>/.com.drweb.public".`

Описание: Dr.Web Gateway Security Suite не может запуститься, поскольку демон управления конфигурацией Dr.Web ConfigD недоступен.

Устранение ошибки

1. Выполните команду:

   ```
   # service drweb-configd restart
   ```

для перезапуска Dr.Web ConfigD и Dr.Web Gateway Security Suite в целом.

2. Если эта команда вернет ошибку или не даст никакого эффекта, выполните отдельную установку пакета `drweb-configd`.

   Это также может означать, что в системе для аутентификации пользователей не используется PAM. Если это так, то установите и настройте его, поскольку без PAM корректная работа Dr.Web Gateway Security Suite невозможна.

3. Если и после этого ошибка повторится, удалите Dr.Web Gateway Security Suite целиком, после чего установите его повторно.

   Инструкции по установке и удалению Dr.Web Gateway Security Suite и его компонентов см. в разделах Установка Dr.Web Gateway Security Suite и Удаление Dr.Web Gateway Security Suite.

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

Симптомы

1. После отключения SpIDer Gate перестают работать сетевые соединения (как исходящие, так, возможно, и входящие — по протоколам SSH, FTP).
2. Поиск в правилах NetFilter (`iptables`) с использованием команды:

   ```
   # iptables-save | grep "comment --comment --comment"
   ```

   выдает непустой результат.

Описание: Данная ошибка связана с некорректной работой NetFilter (`iptables`) версии младше 1.4.15, заключающейся в том, что правила с уникальной меткой (комментарием) добавляются некорректно, вследствие чего SpIDer Gate при завершении своей работы не может удалить добавленные им правила перенаправления сетевых соединений.

Устранение ошибки

1. Повторно включите SpIDer Gate.
2. Если SpIDer Gate требуется оставить выключенным, удалите некорректные правила NetFilter (`iptables`), выполнив команду:

   ```
   # iptables-save | grep -v "comment --comment --comment" | iptables-restore
   ```

   Вызов команд `iptables-save` и `iptables-restore` требует наличия прав суперпользователя. Для получения прав суперпользователя можно воспользоваться командой `su` или `sudo`.

   Указанная команда удалит из перечня правил все правила с некорректно добавленным комментарием (например, добавленные другими приложениями, выполняющими корректировку маршрутизации соединений).

Дополнительная информация

- Для предотвращения возникновения данной ошибки в дальнейшем рекомендуется обновить операционную систему (или, как минимум, NetFilter до версии 1.4.15 или новее).
- Кроме этого, можно включить ручной режим перенаправления соединений для SpIDer Gate, задавая требуемые правила вручную при помощи утилиты `iptables` (не рекомендуется).
- Дополнительные сведения см. в справке `man`: `drweb-firewall(1)`, `drweb-gated(1)`, `iptables(8)`.

Если устранить ошибку не удастся, обратитесь в техническую поддержку.

10.7. Приложение Ж. Список сокращений

В данном руководстве следующие сокращения использованы без расшифровки:

Обозначение	Расшифровка
AD	Microsoft Active Directory
DN	(LDAP) Distinguished Name
FQDN	Fully Qualified Domain Name
GID	Group ID (системный идентификатор группы пользователей)
GNU	Проект GNU (GNU is Not Unix)
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure (через SSL/TLS)
ICAP	Internet Content Adaptation Protocol
ID	Идентификатор
IMA/EVM	Integrity Measurement Architecture and Extended Verification Module (подсистема ядра Linux, позволяющая осуществлять контроль целостности файловой системы)
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
LKM	Loadable Kernel Module (загружаемый модуль ядра)
MBR	Master Boot Record
OID	(SNMP) Object ID
PID	Process ID (системный идентификатор процесса)
PAM	Pluggable Authentication Modules
RPM	Red Hat Package Manager (формат пакетов)
RRA	Round-Robin Archive
RRD	Round-Robin Database
SNI	Server Name Indication

Обозначение	Расшифровка
SNMP	Simple Network Management Protocol
SP	Service Pack
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UID	User ID (системный идентификатор пользователя)
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VBR	Volume Boot Record
ОС	Операционная система

© «Доктор Веб», 2025