Dr.WEB

Enterprise Security Suite

Управление Dr.Web Gateway Security Suite (Unix)

Dr.Web Enterprise Security Suite. Управление Dr.Web Gateway Security Suite (Unix)
Версия 13.0
Руководство администратора
19.02.2025

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

1.1. Назначение документа

Данное руководство является частью пакета документации администратора антивирусной сети, описывающей детали реализации комплексной антивирусной защиты компьютеров и мобильных устройств компании с помощью Dr.Web Enterprise Security Suite.

Руководство адресовано администратору антивирусной сети — сотруднику организации, которому поручено руководство антивирусной защитой рабочих станций и серверов этой сети.

В руководстве приведена информация о централизованной настройке антивирусного ПО рабочих станций, осуществляемой администратором антивирусной сети через Центр управления безопасностью Dr.Web. Руководство описывает настройки антивирусного решения Dr.Web Gateway Security Suite и особенности централизованного управления данным ПО.

Для получения дополнительной информации обращайтесь к следующим руководствам:

- Руководство администратора антивирусного решения Dr.Web Gateway Security Suite содержит информацию о настройке антивирусного ПО, осуществляемой непосредственно на станции.
- Документация администратора антивирусной сети Dr.Web Enterprise Security Suite (включает Руководство администратора, Руководство по установке и Приложения) содержит основную информацию по установке и настройке антивирусной сети и, в частности, по работе с Центром управления безопасностью Dr.Web.

Перед прочтением документов убедитесь, что это последняя версия руководств. Руководства постоянно обновляются, и последнюю их версию можно найти на официальном веб-сайте компании «Доктор Веб».

1.2. Условные сокращения и обозначения

Условные обозначения

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.

Сокращения

В тексте Руководства будут употребляться без расшифровки следующие сокращения:

- BRE — базовый синтаксис регулярных выражений (Basic Regular Expressions),
- CSV — текстовый формат для представления табличных данных (Comma-Separated Values),
- ERE — расширенный синтаксис регулярных выражений (Extended Regular Expressions),
- HTML — язык разметки гипертекста (HyperText Markup Language),
- HTTP — протокол передачи гипертекста (HyperText Transfer Protocol),
- HTTPS — защищенный протокол передачи гипертекста (Hypertext Transfer Protocol Secure),
- ICAP — протокол проверки и контроля трафика (Internet Content Adaptation Protocol),
- IP — протокол интернета (Internet Protocol),
- LKM — модуль ядра Linux (Linux Kernel Module),

- PCRE — синтаксис регулярных выражений в стиле Perl (Perl Compatible Regular Expressions),
- PDF — формат электронных документов (Portable Document Format),
- SNI — индикация имени сервера (Server Name Indication),
- SSL — уровни защищенных сокетов (Secure Socket Layers),
- TCP — протокол управления передачи (Transmission Control Protocol),
- TLS — защищенный транспортный уровень (Transport Layer Security),
- URL — единообразный локатор ресурса (Uniform Resource Locator),
- XML — расширяемый язык разметки (Extensible Markup Language),
- ВСО — Всемирная Система Обновлений Dr.Web,
- ЛВС — Локальная Вычислительная Сеть,
- ОС — Операционная Система,
- ПО — Программное Обеспечение.

2. Dr.Web Enterprise Security Suite

2.1. О продукте

Продукт Dr.Web Enterprise Security Suite предназначен для организации и управления единой и надежной комплексной антивирусной защитой как внутренней сети компании, включая мобильные устройства, так и домашних компьютеров сотрудников.

Совокупность компьютеров и мобильных устройств, на которых установлены взаимодействующие компоненты Dr.Web Enterprise Security Suite, представляет собой единую *антивирусную сеть*.

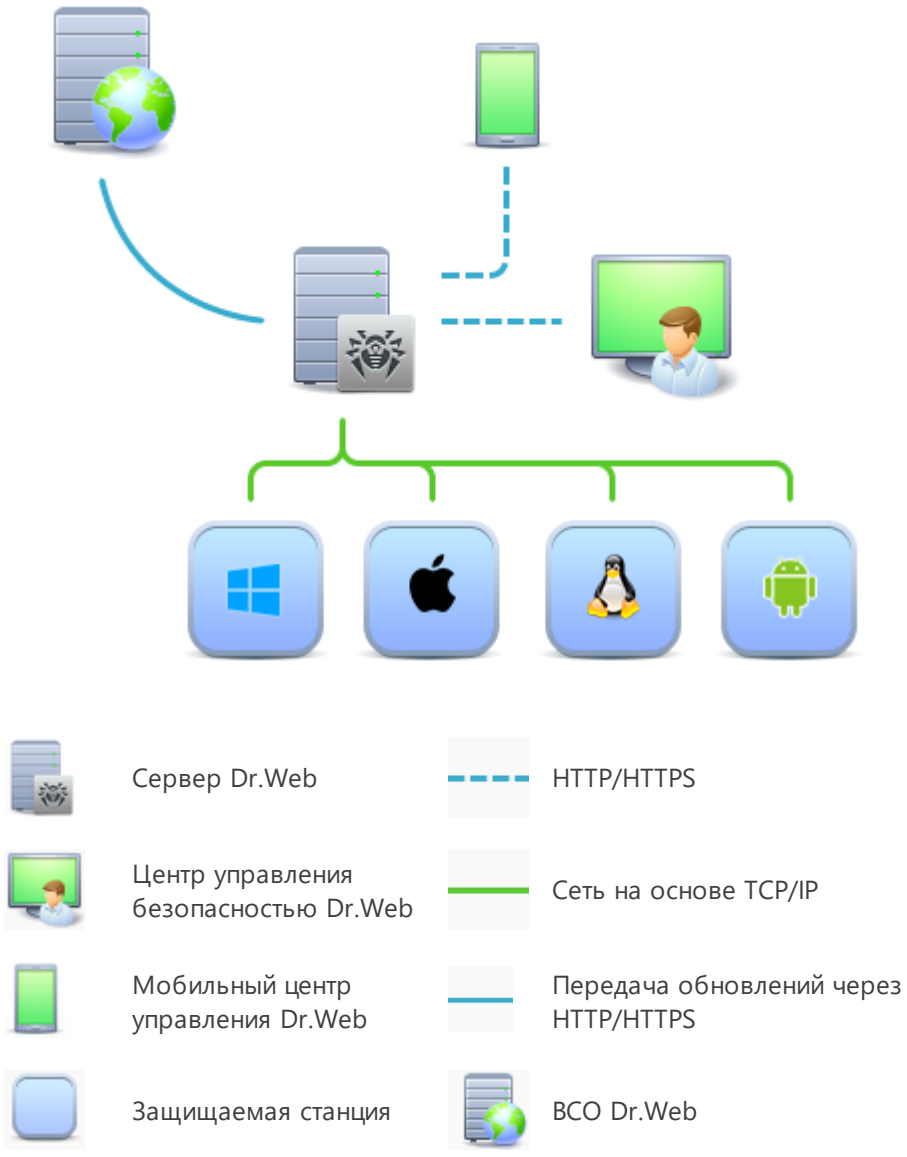

Рисунок 1. Логическая структура антивирусной сети

Антивирусная сеть Dr.Web Enterprise Security Suite имеет архитектуру *клиент-сервер*. Ее компоненты устанавливаются на компьютеры и мобильные устройства пользователей и администраторов, а также на компьютеры, выполняющие функции серверов ЛВС. Компоненты антивирусной сети обмениваются информацией, используя сетевые протоколы TCP/IP. Антивирусное ПО на защищаемые станции возможно устанавливать (и впоследствии управлять ими) как через ЛВС, так и через интернет.

2.2. Защита интернет-шлюзов Unix

Защита интернет-шлюзов Unix осуществляется с помощью антивирусных пакетов Dr.Web.

Рабочей станцией антивирусной сети называется защищаемое устройство с установленным на нем антивирусным пакетом.
Термин «станция» может быть употреблен по отношению к персональному компьютеру, мобильному устройству или серверу локальной сети.

Антивирусные пакеты устанавливаются на защищаемых станциях и подключаются к Серверу Dr.Web. Каждая станция входит в состав одной или нескольких групп, зарегистрированных на этом Сервере. Передача информации с Сервера Dr.Web на защищаемую станцию осуществляется по протоколу, используемому в локальной сети (TCP/IP версии 4 или 6).

Установка

Локальная установка осуществляется непосредственно на защищаемой станции и может быть выполнена как администратором этой станции, так и администратором антивирусной сети.

Подробное описание процедур установки антивирусных пакетов на защищаемые станции приведено в Руководстве по установке Dr.Web Enterprise Security Suite.

Управление

При поддержке связи с Сервером Dr.Web администратору доступны следующие функции, реализуемые антивирусным пакетом на защищаемой станции:

- Централизованная настройка антивирусного пакета на защищаемой станции при помощи Центра управления безопасностью.

  При этом администратор может как запретить, так и оставить возможность пользователям самостоятельно изменять настройки антивирусного пакета на защищаемой станции.
- Настройка расписания антивирусных проверок и других заданий, выполняемых на защищаемой станции.

- Получение статистики сканирования и прочей информации о работе антивирусных компонентов и о состоянии защищаемой станции.
- Запуск и остановка антивирусного сканирования и т. п. (в зависимости от функциональных возможностей антивирусного пакета, установленного на защищаемой станции).

Обновление

Сервер Dr.Web загружает обновления и распространяет их на подключенные к нему защищаемые станции. Таким образом автоматически устанавливается, поддерживается и регулируется оптимальная стратегия защиты от угроз независимо от уровня квалификации администраторов защищаемых станций.

В случае временного отключения защищаемой станции от антивирусной сети, антивирусный пакет на сервере использует локальную копию настроек, антивирусная защита на защищаемой станции сохраняет свою функциональность (в течение срока, не превышающего срок действия пользовательской лицензии), но обновление ПО не производится.

3. Dr.Web Gateway Security Suite

3.1. Функции Dr.Web Gateway Security Suite

В настоящем документе рассматриваются аспекты настройки компонентов, входящих в продукт Dr.Web Gateway Security Suite, предназначенный для работы в ОС GNU/Linux и FreeBSD. Руководство адресовано лицу, отвечающему за антивирусную безопасность и настройку сетей, называемому в данном руководстве «Администратором».

Продукт Dr.Web Gateway Security Suite создан для защиты серверов, работающих под управлением ОС семейства GNU/Linux и FreeBSD от вирусов и всех прочих видов вредоносного программного обеспечения, а также для предотвращения распространения угроз, разработанных для различных платформ.

Основные функции Dr.Web Gateway Security Suite:

1. **Поиск и обезвреживание угроз.** Производится поиск как непосредственно вредоносных программ всех возможных типов (различные вирусы, включая вирусы, инфицирующие почтовые файлы и загрузочные записи дисков, троянские программы, почтовые черви и т. п.), так и нежелательных программ (рекламные программы, программы-шутки, программы автоматического дозвона).

   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;
   - *обращение к сервису Dr.Web Cloud*, собирающему свежую информацию об актуальных угрозах, которая затем рассылается различным антивирусным продуктам «Доктор Веб».

   Обратите внимание, что 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».

   При проверке файловой системы по запросу пользователя имеется возможность как полной проверки всех объектов файловой системы, 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.

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 веб-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.

3.2. Компоненты Dr.Web Gateway Security Suite

Для защиты интернет-шлюзов Unix предоставляются следующие антивирусные компоненты:

Основные

Dr.Web ICAPD

ICAP-сервер, выполняющий анализ запросов и трафика, проходящего через прокси-серверы HTTP (такие, как Squid). Предотвращает передачу инфицированных файлов и доступ к узлам сети, внесенным в нежелательные категории веб-ресурсов или в черные списки, формируемые системным администратором. При запрете доступа к внешним серверам и при обнаружении угроз в передаваемых данных предписывает прокси-серверу вернуть клиенту специальную страницу ответа, содержащую сообщение о невозможности доступа к запрошенному ресурсу или загрузки инфицированного файла.

Центральный компонент Dr.Web Gateway Security Suite. Позволяет интегрировать его с приложениями, использующими протокол ICAP (как правило, это защищаемый прокси-сервер HTTP, использующийся для доступа рабочих станций, включенных в состав ЛВС, к интернету).

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 в нежелательные категории веб-ресурсов и черные списки, формируемые системным администратором.

Поставляется только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux.

Dr.Web ClamD

Компонент, эмулирующий интерфейс антивирусного продукта ClamAV®. Позволяет использовать Dr.Web Gateway Security Suite для антивирусной проверки любым приложениям, которые могут использовать ClamAV®.

Карантин

Используется для изоляции вредоносных и подозрительных объектов.

Служебные

Агент Dr.Web для Unix

Используется для взаимодействия Dr.Web Gateway Security Suite, установленного на станции, с Dr.Web Enterprise Security Suite.

File Checker

Используется Консольным сканером для передачи на проверку в Scanning Engine файлов и управления Карантином на станции.

Network Checker

Используется для передачи на проверку в Scanning Engine данных, отправленных компонентами программного комплекса через сеть. Данный компонент используется для работы всех основных компонентов.

Scanning Engine

Используется компонентами File Checker и Network Checker для антивирусной проверки и управления вирусными базами.

SNMP Agent

Предназначен для интеграции Dr.Web Gateway Security Suite с внешними системами мониторинга посредством протокола SNMP.

Dr.Web ConfigD

Координирует работу всех компонентов Dr.Web Gateway Security Suite.

Dr.Web CloudD

Компонент, получающий сведения о вредоносности посещаемых URL и передаваемых файлов из облачного сервиса.

Dr.Web HTTPD

Веб-сервер управления компонентами Dr.Web Gateway Security Suite. Предоставляет веб-интерфейс управления.

3.3. Режимы работы Dr.Web Gateway Security Suite

Антивирусное решение Dr.Web Gateway Security Suite может работать как в одиночном 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 *одиночном 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 с 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 использования данного режима зависит от разрешений, заданных на сервере централизованной защиты.

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 компонентами Dr.Web Gateway Security Suite), которые обеспечивают антивирусную защиту и поддерживают соединение с сервером централизованной защиты.

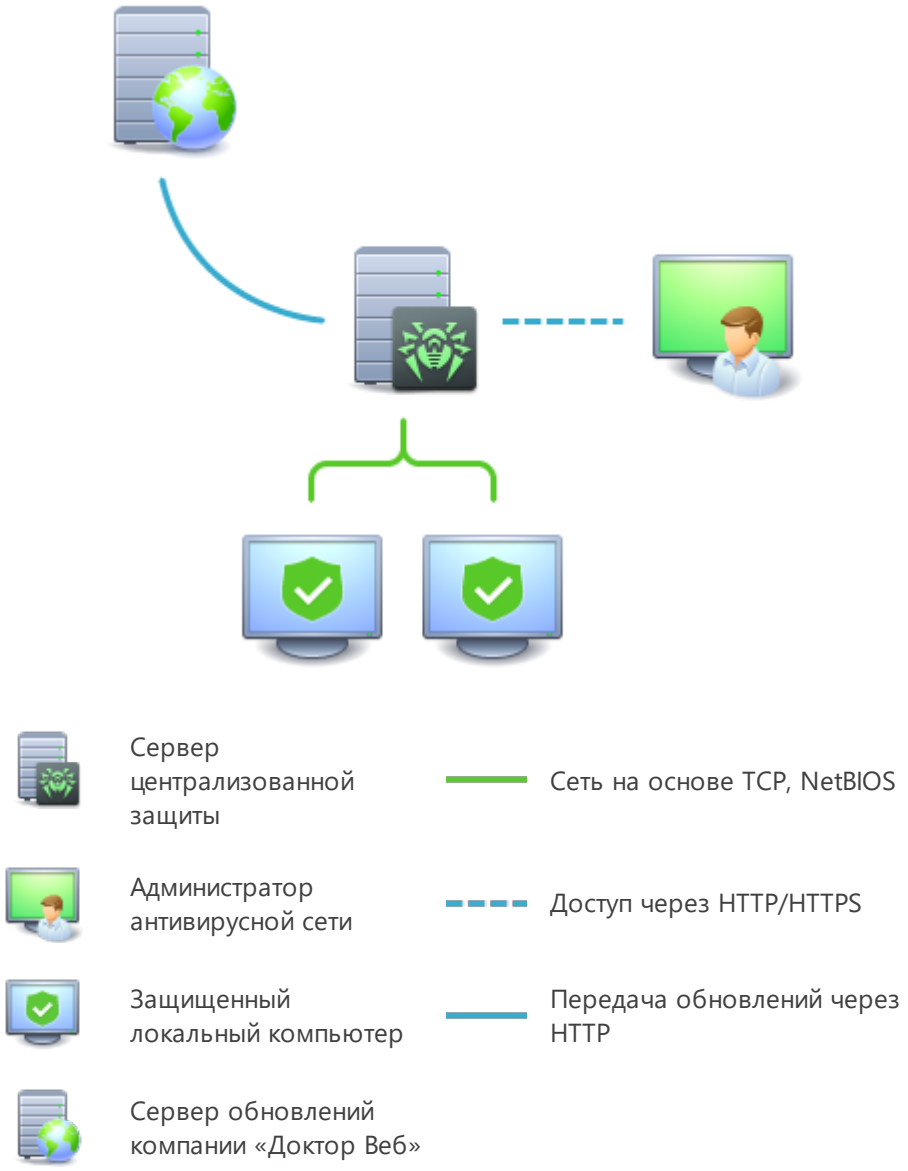

Рисунок 2. Логическая структура антивирусной сети

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, Dr.Web для интернет-шлюзов UNIX версии 5.0). Установка двух антивирусных программ на одном компьютере может привести к отказу системы и потере важных данных.

Продукт Dr.Web Gateway Security Suite версии 11.1, работающий в режиме централизованной защиты, совместим с Dr.Web Enterprise Security Suite версий 11, 12, 13 и 13.0.1.

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`.

3.4. Настройка Dr.Web Gateway Security Suite

Чтобы просмотреть или изменить настройки антивирусных компонентов на рабочей станции:

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления.
2. В открывшемся окне в иерархическом списке нажмите на название станции под требуемой ОС (GNU/Linux или FreeBSD) или группы, содержащей такие станции.
3. В открывшемся управляющем меню в разделе **Конфигурация**, в подразделе требуемой ОС (GNU/Linux или FreeBSD) выберите требуемый компонент.
4. Откроется окно настроек антивирусного компонента.

   Управление настройками антивирусных компонентов через Центр управления имеет некоторые отличия от управления настройками непосредственно через соответствующие компоненты антивируса на станции:

   - для управления отдельными параметрами используйте кнопки, расположенные справа от соответствующих настроек:

     Установить в начальное значение — восстановить значение, которое параметр имел до редактирования (последнее сохраненное значение);

     Сбросить в значение по умолчанию — установить для параметра значение по умолчанию;

   - для управления совокупностью всех параметров раздела используйте кнопки на панели инструментов:

     Установить все параметры в начальные значения — восстановить значения, которые все параметры данного раздела имели до текущего редактирования (последние сохраненные значения);

     Установить все параметры в значения по умолчанию — установить для всех параметров данного раздела значения, заданные по умолчанию;

     Распространить эти настройки на другой объект — скопировать настройки из данного раздела в настройки другой станции, группы или нескольких групп и станций;

     Установить наследование настроек от первичной группы — удалить персональные настройки станций и установить наследование настроек данного раздела от первичной группы;

     Скопировать настройки из первичной группы и установить их в качестве персональных — скопировать настройки данного раздела из первичной группы и

задать их для выбранных станций. Наследование при этом не устанавливается, и настройки станции считаются персональными.

Экспортировать настройки из данного раздела в файл — сохранить все настройки из данного раздела в файл специального формата;

Импортировать настройки в данный раздел из файла — заменить все настройки в данном разделе настройками из файла специального формата.

5. После внесении каких-либо изменений в настройки при помощи Центра управления, для принятия этих изменений, нажмите кнопку **Сохранить**. Настройки будут переданы на станции. Если станции были отключены в момент внесения изменений, настройки будут переданы в момент подключения станций к Серверу.

Администратор может запретить пользователю редактировать настройки на станции (см. раздел **Права пользователей станции** в Руководстве администратора). При этом редактировать настройки сможет только сам администратор через Центр управления.

3.4.1. Настройки Агента Dr.Web для Unix

3.4.1.1. Общие настройки

В данном разделе вы можете управлять настройками работы на защищаемой станции служебного компонента Агент Dr.Web для Unix. Доступны следующие настройки:

- **Собирать информацию о станциях** — разрешить или запретить Агенту Dr.Web для Unix собирать информацию о состоянии станций.
- **Период сбора информации о станциях** — периодичность (в минутах), с которой Агент Dr.Web для Unix отправляет запросы к станциям для сбора информации.
- **Периодичность отправки статистики** — периодичность, с которой Агент Dr.Web для Unix отправляет статистику на сервер.
- **Мобильный режим получения обновлений** — использование мобильного режима получения обновлений. Возможные значения:
  - *Автоматически* — использовать мобильный режим, если он разрешен администратором на сервере Dr.Web Enterprise Security Suite (получать обновления с серверов ВСО, используя локальный компонент обновления, работающий на станции, либо получать обновления от Dr.Web Enterprise Security Suite, в зависимости от того, какое соединение доступно и качество какого соединения лучше).
  - *Использовать* — использовать мобильный режим, если он разрешен администратором на сервере Dr.Web Enterprise Security Suite (получать обновления с серверов ВСО, используя локальный компонент обновления, работающий на станции).
  - *Запретить* — не разрешать Dr.Web Gateway Security Suite на станции получать обновления с серверов ВСО в случае невозможности подключения к серверу Dr.Web Enterprise Security Suite.

- **Обрабатывать discovery-запросы** — разрешить или запретить агенту принимать discovery-запросы от сервера Dr.Web Enterprise Security Suite (используются для проверки структуры и состояния антивирусной сети).
- **Уровень журнала** — уровень подробности ведения журнала компонентом Агент Dr.Web для Unix.
- **Метод ведения журнала** — способ сохранения сообщений Агентом Dr.Web для Unix в журнал. Возможные значения:
  - *Auto* — используются параметры ведения журнала, заданные для всех компонентов в настройках Dr.Web ConfigD.
  - *Syslog* — используется системный сервис syslog для ведения журнала Агента Dr.Web для Unix. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую syslog подсистему (метку) для сохранения сообщений от Агента Dr.Web для Unix.
  - *Path* — сообщения журнала от Агента Dr.Web для Unix сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.

Как правило, для настроек этого компонента по умолчанию заданы оптимальные значения, изменять которые не рекомендуется без необходимости.

3.4.1.2. Конфигурация

В данном разделе вы можете задавать настройки для любого из компонентов Dr.Web Gateway Security Suite, установленного на станции, в формате файла конфигурации `.ini`. Для этого внесите необходимые изменения в поле **Конфигурационный файл drweb.ini**.

Обратите внимание, что:

- Центр управления не поддерживает настройку всех имеющихся параметров. Для детальной настройки компонентов Агента Dr.Web для Unix используйте редактор настроек Dr.Web Gateway Security Suite.
- В редакторе настроек отображаются только те параметры конфигурации, значения которых были изменены на этой странице.
- Значения параметров конфигурации, указанные в редакторе, имеют приоритет по отношению к значениям настроек, задаваемых на страницах настроек компонентов: в случае если на странице настройки задано одно значение некоторого параметра, а на странице **Конфигурация** — другое, на станции будет использовано значение, указанное на странице **Конфигурация**. В частности, для компонентов, секции которых приведены в редакторе **Конфигурационный файл drweb.ini**, неуказанные параметры конфигурации принимают значения по умолчанию.
- Редактор настроек поддерживает контекстную подсказку: нажатие комбинации клавиш CTRL+SPACE открывает выпадающий список доступных параметров (или секций параметров, в зависимости от контекста).

- Имеется возможность импорта и экспорта содержимого редактора в виде файла конфигурации `.ini`. Для этого нажмите соответствующую кнопку, расположенную на странице над редактором настроек.

Для получения полного перечня компонентов на станции, доступных для настройки, а также для ознакомления с описанием их параметров в конфигурационном файле `drweb.ini` обратитесь к руководству администратора продукта, установленного на станции.

3.4.2. Настройки Dr.Web ICAPD

3.4.2.1. Общие настройки

В данном разделе вы можете управлять следующими параметрами работы Dr.Web ICAPD на защищаемой станции (интернет-шлюзе):

- **Запускать компонент при старте** — управляет запуском компонента на защищаемом интернет-шлюзе.
- **Сокет для клиентских подключений** — сетевой сокет (<*IP-адрес*>:<*порт*>), через который ICAP-клиенты (такие, как Squid) будут подключаться к Dr.Web ICAPD.
- **Пользователь** — позволяет указать имя пользователя Unix-подобной ОС, с правами и полномочиями которого работает компонент на защищаемом интернет-шлюзе.

Если имя пользователя не указано, работа компонента завершится ошибкой сразу после попытки его запуска.

- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом Dr.Web ICAPD.
- **Метод ведения журнала** — управляет способом сохранения сообщений Dr.Web ICAPD в журнал. Возможные значения:
  - *Auto* — используются параметры ведения журнала, заданные для всех компонентов в настройках Dr.Web ConfigD.
  - *Syslog* — используется системный сервис syslog для ведения журнала Dr.Web ICAPD. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую syslog подсистему (метку) для сохранения сообщений от Dr.Web ICAPD.
  - *Path* — сообщения журнала от Dr.Web ICAPD сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.

3.4.2.2. Веб-фильтр

В данном разделе вы можете управлять параметрами проверки доступа к сайтам Dr.Web ICAPD на защищаемом интернет-шлюзе:

- Установите флажок **Блокировать сайты, содержащие вредоносное ПО**, чтобы включить блокировку сайтов, которые используются для распространения вирусов и других вредоносных программ.
- Установите флажок **Блокировать нерекомендуемые сайты**, чтобы включить блокировку сайтов, на которых используются методы социальной инженерии для обмана посетителей.
- Установите флажок **Блокировать URL, добавленные по обращению правообладателя**, чтобы заблокировать доступ к сайтам в связи с обращениями правообладателей, обнаруживших нарушения прав на интеллектуальную собственность в интернете.
- Для блокирования сайтов, относящихся к той или иной категории веб-ресурсов установите соответствующие флажки с именами категорий, доступ к которым необходимо заблокировать (**Блокировать сайты для взрослых**, **Блокировать сайты, посвященные насилию** и так далее).
- В разделе **Список рекламных сайтов** укажите список регулярных выражений, которые определяют принадлежность URL к рекламным сайтам. Попытки перехода пользователей по URL, соответствующему любому из указанных здесь регулярных выражений будут блокироваться.

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, гарантируется, что переход по URL, соответствующему любому из указанных здесь регулярных выражений будет заблокирован.

Для добавления нового выражения в список нажмите кнопку  в соответствующей строке списка. Для удаления некоторого выражения из списка нажмите кнопку  в соответствующей строке списка.

3.4.2.3. Исключения

В данном разделе вы можете управлять исключениями в проверке сайтов компонентом Dr.Web ICAPD на защищаемом интернет-шлюзе:

- В разделе **Белый список доменов, подключение к которым разрешено администратором** укажите список доменов, подключение к которым должно быть разрешено пользователям, даже если эти домены относятся к блокируемым

категориям веб-ресурсов. При этом пользователям будет также предоставлен доступ ко всем поддоменам доменов, указанных в этом списке.

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, гарантируется, что доступ к доменам (и их поддоменам) из данного списка будет обеспечен, даже если там будут находиться домены из блокируемых категорий веб-ресурсов. Помимо этого, набор правил по умолчанию гарантирует, что данные, загружаемые с доменов из белого списка, *будут проверяться на наличие угроз*.

- В разделе **Черный список доменов, подключение к которым запрещено администратором** укажите список доменов, подключение к которым должно быть запрещено пользователям, даже если эти домены не относятся к блокируемым категориям веб-ресурсов. При этом пользователям будет также запрещен доступ ко всем поддоменам доменов, указанных в этом списке.

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, гарантируется, что доступ к доменам (и их поддоменам) из данного списка будет запрещен всегда. Если домен добавлен одновременно в белый и черный список доменов, то правила, заданные по умолчанию, гарантируют, что доступ пользователей к нему будет *заблокирован*.

Для добавления нового домена в нужный список нажмите кнопку  в соответствующей строке списка. Для удаления некоторого домена из списка нажмите кнопку  в соответствующей строке списка.

3.4.2.4. Файловый фильтр

В данном разделе вы можете управлять параметрами проверки Dr.Web ICAPD на защищаемом интернет-шлюзе файлов и данных, загружаемых из интернета:

- В разделе **Блокировать файлы** выберите типы небезопасных получаемых объектов, которые будут блокироваться компонентом Dr.Web ICAPD:
  - **Вредоносные** — в проверенном файле обнаружена известная угроза;
  - **Подозрительные** — проверенный файл отмечен как *подозрительный*;
  - **Рекламные программы** — в проверенном файле обнаружена рекламная программа;
  - **Программы дозвона** — в проверенном файле обнаружена программа дозвона;
  - **Программы-шутки** — в проверенном файле обнаружена программа-шутка;

- **Потенциально опасные** — в проверенном файле обнаружена потенциально опасная программа;
- **Программы взлома** — в проверенном файле обнаружена программа взлома;
- **Непроверенные файлы** — файл не удалось проверить.

- **Использовать эвристический анализ** — управляет использованием Dr.Web ICAPD на защищаемом интернет-шлюзе эвристического анализа при проверке файлов «на лету». Использование эвристического анализа замедляет проверку, но повышает ее надежность.
- **Время проверки одного файла** — определяет максимальный период времени, который отводится на проверку одного файла Dr.Web ICAPD на защищаемом интернет-шлюзе. Допустимые значения: от 1 секунды до 1 часа. Значение по умолчанию: 30 секунд.
- В разделе **Максимальный уровень вложенности** вы можете управлять параметрами проверки Dr.Web ICAPD составных файлов, таких как архивы, почтовые файлы, упакованные объекты и прочие контейнеры (т. е. составные файлы, не отнесенные ни к одному из предыдущих типов).

  Для каждого типа файла в соответствующем поле можно указать максимально допустимый уровень вложенности, ниже которого он не должен распаковываться при проверке Dr.Web ICAPD. Например, чтобы проверять содержимое архивов, вложенных в архивы, необходимо указать уровень вложенности для них не менее *2*. Чтобы запретить проверку вложенных объектов, укажите уровень вложенности *0* для соответствующего типа контейнеров.

  Помните, что увеличение уровня вложенности уменьшает скорость проверки.

  Поле **Максимальный коэффициент сжатия архива** устанавливает максимальную допустимую степень сжатия проверяемых объектов (как отношение сжатого объема файла к несжатому). Если степень сжатия проверяемого объекта превысит указанную величину, он будет пропущен при проверке.

3.4.2.5. Дополнительные настройки

В данном разделе вы можете управлять следующими дополнительными параметрами работы Dr.Web ICAPD на защищаемой станции (интернет-шлюзе):

- **Использовать режим ICAP preview** — флажок управляет использованием Dr.Web ICAPD режима ICAP preview.
- **Использовать режим ICAP 204** — флажок определяет, может ли Dr.Web ICAPD возвращать код ответа 204 не только в режиме ICAP preview.
- **Использовать “ранние” ответы ICAP** — флажок определяет, может ли Dr.Web ICAPD использовать режим «раннего» ответа ICAP, т. е. начинать отправлять ответ клиенту, не прочитав до конца запрос от прокси-сервера HTTP.

Как правило, для указанных настроек по умолчанию заданы оптимальные значения,

изменять которые не рекомендуется без необходимости.

3.4.2.6. Правила проверки трафика

В данном разделе вы можете управлять правилами проверки сайтов и данных компонентом Dr.Web ICAPD на защищаемом интернет-шлюзе.

Для добавления нового правила в список нажмите кнопку  в соответствующей строке списка. Для удаления некоторого правила из списка нажмите кнопку  в соответствующей строке списка.

Чтобы ознакомиться с правилами проверки, см. Приложение А. Правила проверки трафика.

В настоящем документе правила проверки трафика приведены в сокращенном виде. Полный вариант опубликован в Руководстве администратора Dr.Web Gateway Security Suite.

3.4.3. Настройки SplDer Gate

3.4.3.1. Общие настройки

В данном разделе вы можете управлять следующими параметрами SplDer Gate на защищаемой станции:

- **Включить SplDer Gate** — управляет запуском SplDer Gate на защищаемой станции.
- **Использовать эвристический анализ** — управляет использованием SplDer Gate на защищаемой станции эвристического анализа для поиска неизвестных угроз. Использование эвристического анализа замедляет проверку, но повышает ее надежность.
- **Время проверки одного файла** — определяет максимальный период времени, который отводится на проверку одного файла SplDer Guard на станции. Допустимые значения: от 1 секунды до 1 часа. Значение по умолчанию: 30 секунд.

3.4.3.2. Действия

В данном разделе вы можете управлять следующими параметрами SplDer Gate на защищаемой станции:

- Установите флажок **Проверять получаемые файлы**, чтобы включить проверку входящего интернет-трафика (в частности, файлов, загруженных из интернета).

- В списках **Блокировать файлы** и **Блокировать дополнительно** выберите типы небезопасных получаемых объектов, которые будут блокироваться компонентом SpIDer Gate.

3.4.3.3. Веб-фильтр

В данном разделе вы можете управлять следующими параметрами SpIDer Gate на защищаемой станции:

- Установите флажок **Проверять URL**, чтобы включить блокировку интернет-ресурсов по категориям.
- Установите флажок **Блокировать нерекомендуемые сайты**, чтобы включить блокировку сайтов, на которых используются методы социальной инженерии для обмана посетителей.
- Установите флажок **Блокировать URL, добавленные по обращению правообладателя**, чтобы заблокировать доступ к сайтам в связи с обращениями правообладателей, обнаруживших нарушения прав на интеллектуальную собственность в интернете.
- В списке **Блокировать следующие категории сайтов** выберите категории интернет-ресурсов, доступ к которым необходимо заблокировать.
- В разделах **Белый список/Черный список** добавьте пути к сайтам, доступ к которым нужно разрешить или ограничить:
  - Чтобы добавить в список определенный сайт, введите полный адрес его домена (например, `www.example.com`). Доступ ко всем ресурсам, расположенным на этом домене, будет определяться данной записью.

3.4.3.4. Контейнеры

В данном разделе вы можете управлять параметрами проверки SpIDer Gate составных файлов, таких, как архивы, почтовые файлы, упакованные объекты и прочие контейнеры (т. е. составные файлы, не отнесенные ни к одному из предыдущих типов).

Для каждого типа файла в соответствующем поле можно указать максимально допустимый уровень вложенности, ниже которого он не должен распаковываться при проверке SpIDer Gate. Например, чтобы проверять содержимое архивов, вложенных в архивы, необходимо указать уровень вложенности для них не менее *2*. Чтобы запретить проверку вложенных объектов, укажите уровень вложенности *0* для соответствующего типа контейнеров.

Помните, что увеличение допустимого уровня вложенности уменьшает скорость проверки.

Поле **Максимальный коэффициент сжатия архива** устанавливает максимальную допустимую степень сжатия проверяемых объектов (как отношение сжатого объема

файла к несжатому). Если степень сжатия проверяемого объекта превысит указанную величину, он будет пропущен при проверке.

3.4.3.5. Дополнительные настройки

В данном разделе вы можете управлять дополнительными настройками работы SpIDer Gate на защищаемой станции.

Доступны следующие дополнительные настройки SpIDer Gate:

- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом SpIDer Gate.
- **Метод ведения журнала** — управляет способом сохранения сообщений SpIDer Gate в журнал. Возможные значения:
  - *Auto* — используются параметры ведения журнала, заданные для всех компонентов в настройках Dr.Web ConfigD.
  - *Syslog* — используется системный сервис syslog для ведения журнала SpIDer Gate. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую syslog подсистему (метку) для сохранения сообщений от SpIDer Gate.
  - *Path* — сообщения журнала от SpIDer Gate сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.

3.4.4. Настройки File Checker

В данном разделе вы можете управлять настройками работы на защищаемой станции служебного компонента File Checker.

Доступны следующие настройки:

- **Размер кэша проверенных файлов** — определяет размер кэша, в котором File Checker временно сохраняет результаты проверки файлов.
- **Период актуальности кэша** — определяет период времени, в течении которого File Checker не проверяет файлы повторно, если информация об их проверке уже содержится в кэше.
- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом File Checker.
- **Метод ведения журнала** — управляет способом сохранения сообщений File Checker в журнал. Возможные значения:
  - *Auto* — используются параметры ведения журнала, заданные для всех компонентов в настройках Dr.Web ConfigD.
  - *Syslog* — используется системный сервис syslog для ведения журнала File Checker. В случае выбора этого значения необходимо также указать в выпадающем списке

Подсистема syslog используемую syslog подсистему (метку) для сохранения сообщений от File Checker.

- *Path* — сообщения журнала от File Checker сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.

Также вы можете указать, какую дополнительную информацию следует записывать в журнал, если он ведется на уровне *Отладка*.

- **IPC** — сохранять в журнал все сообщения внутреннего протокола взаимодействия компонентов.
- **Проверка файлов** — сохранять в журнал сведения о проверке файлов.
- **Мониторинг файлов SpIDer Guard** — сохранять в журнал сведения о запросах от SpIDer Guard.
- **Состояние кэша проверенных файлов** — сохранять в журнал сведения о состоянии кэша проверенных файлов.

Как правило, для настроек этого компонента по умолчанию заданы оптимальные значения, изменять которые не рекомендуется без необходимости.

3.4.5. Настройки Scanning Engine

В данном разделе вы можете управлять настройками работы на защищаемой станции служебного компонента Scanning Engine.

Доступны следующие настройки:

- **Путь к файлу сокета фиксированной копии компонента** — определяет путь к файлу Unix-сокета постоянно работающей копии Scanning Engine. Этот сокет может использоваться для сканирования файлов внешними программами. Если параметр пуст, сканирование недоступно для внешних программ, а Scanning Engine запускается и завершает свою работу автоматически, по мере необходимости.
- **Количество сканирующих процессов** — определяет количество вспомогательных процессов, которые Scanning Engine может создать при сканировании файлов. При изменении значения этого параметра следует учесть количество процессорных ядер, доступных на защищаемой станции.
- **Сторожевой таймер** — определяет период времени, который Scanning Engine использует для автоматического обнаружения зависания вспомогательных сканирующих процессов.
- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом Scanning Engine.
- **Метод ведения журнала** — управляет способом сохранения сообщений Scanning Engine в журнал. Возможные значения:
  - *Auto* — используются параметры ведения журнала, заданные для всех компонентов в настройках Dr.Web ConfigD.

- *Syslog* — используется системный сервис syslog для ведения журнала Scanning Engine. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую syslog подсистему (метку) для сохранения сообщений от Scanning Engine.
- *Path* — сообщения журнала от Scanning Engine сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.

Как правило, для настроек этого компонента по умолчанию заданы оптимальные значения, изменять которые не рекомендуется без необходимости.

3.4.6. Настройки Dr.Web ConfigD

В данном разделе вы можете управлять настройками работы на защищаемой станции служебного управляющего компонента Dr.Web ConfigD.

Доступны следующие настройки:

- **Путь к публичному коммуникационному сокету** — определяет путь к Unix-сокету, который используется для взаимодействия с Dr.Web ConfigD компонентами Dr.Web Gateway Security Suite.
- **Путь к административному коммуникационному сокету** — определяет путь к Unix-сокету, который используется для взаимодействия с Dr.Web ConfigD компонентами Dr.Web Gateway Security Suite, работающими с полномочиями.
- **Путь к каталогу временных файлов** — определяет каталог, в котором компоненты Dr.Web Gateway Security Suite хранят свои временные файлы.
- **Путь к каталогу PID-файлов и файлов коммуникационных сокетов** — определяет каталог, в котором компоненты Dr.Web Gateway Security Suite хранят PID-файлы и Unix-сокеты для внутреннего взаимодействия.
- **Уровень журнала** — управляет уровнем подробности ведения журнала компонентом Dr.Web ConfigD.
- **Метод ведения журнала** — управляет способом сохранения сообщений Dr.Web ConfigD в журнал. Возможные значения:
  - *Syslog* — используется системный сервис syslog для ведения журнала Dr.Web ConfigD. В случае выбора этого значения необходимо также указать в выпадающем списке **Подсистема syslog** используемую syslog подсистему (метку) для сохранения сообщений от Dr.Web ConfigD.
  - *Path* — сообщения журнала от Dr.Web ConfigD сохраняются в отдельный файл. В случае выбора этого значения необходимо указать путь к файлу в поле **Файл журнала**.

Как правило, для настроек этого компонента по умолчанию заданы оптимальные значения, изменять которые не рекомендуется без необходимости.

4. Приложение А. Правила проверки трафика

Правила представляют собой набор конструкций вида ЕСЛИ <*условие*> ТО <*действие*>. При этом в части <*условие*> перечисляются проверки вида *«Переменная (не) имеет заданное значение»* или *«Значение переменной (не) входит в указанное множество»*, а <*действие*> содержит *конечную резолюцию* (пропустить или заблокировать трафик), или действие вида *«Присвоить переменной значение»* или *«Добавить указанное значение к множеству значений переменной»*.

Часть <*действие*> правила выполняется, только если истинна часть <*условие*>. Если <*условие*> ложно, действие не выполняется, осуществляется переход к следующему правилу. Правила перебираются сверху вниз до тех пор, пока не сработает какая-либо конечная резолюция. После этого все правила ниже игнорируются.

Формат правил

Правило имеет формат:

```
[<condition>[, <condition>[, ...]]] : <action>
```

Условная часть правила (перед '**:**') может отсутствовать, в этом случае часть <*действие*> выполняется безусловно. Если условная часть правила отсутствует, то разделитель '**:**' может быть опущен. Запятая между условиями в условной части играет роль конъюнкции (т. е. логического «И»), и условная часть считается истинной, только если истинны все перечисленные в ней условия. Ключевые слова, имена переменных и параметров из конфигурации в правилах не чувствительны к регистру.

Условия

В правилах могут встречаться следующие типы условий:

Условие	**Смысл условия**
<*переменная*> <*значение*>	Значение указанной переменной совпадает с заданным. *Может быть использовано только для переменных, которые не могут принимать множества значений.*
<*переменная*> `[not] in` <*множество значений*>	Значение указанной переменной содержится в указанном множестве значений (*в случае not — не совпадает ни с одним из значений указанного множества*).

Условие	Смысл условия
<*переменная*> `[not] match` <*множество значений*>	Значение указанной переменной соответствует любому регулярному выражению из указанного набора (*в случае 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 указано следующим 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 значений некоторого параметра конфигурации, где в кавычках указывается имя параметра из конфигурации (с указанием содержащей его секции), значение (или набор значений) которого проверяется. Перечни параметров, которые можно использовать в условии, зависят от

Запись	Смысл
	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 будет выдана ошибка `x102`. Если содержимое файла было изменено в процессе работы программного комплекса, для применения внесенных изменений необходимо после сохранения файла перезагрузить Dr.Web Gateway Security Suite. 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.

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 во множестве (*d*, *e*);
- `X in ()` — ложно, так как множество значений переменной не пусто;
- `X not in ()` — истинно, множество значений переменной не пусто;
- `X not in (d, e)` — истинно, так как ни одно из значений переменной (*a*, *b*, *c*) не встречается во 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; *модифицирующие резолюции*, не прерывающие проверку, а фиксирующие действие, которое должно быть применено к соединению или проверяемому объекту по достижении резолюции, разрешающей пропуск трафика и *действия, изменяющие значения некоторой переменной*, что может быть использовано при дальнейшей проверке условий.

Конечные резолюции

Резолюция	Описание (смысл)
Общие резолюции	
`PASS`	Пропустить трафик (разрешить создать соединение, 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, что блокировка случилась по причине <*reason*>. Эта же причина используется для определения, какую страницу с уведомлением показать пользователю в браузере. В

Резолюция	Описание (смысл)
	качестве <*reason*> для блокировки может быть использовано две стандартные причины: • `BlackList` — считается, что 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.
Специальные резолюции для правил обработки почты	
`REJECT ["`<*description*>`"]`	Отклонить письмо (не допустить его прием или отправку). В случае работы с данными, передаваемыми по протоколу SMTP, сформировать код ответа SMTP 541 (класс постоянных ошибок). Необязательный параметр <*description*>, если указан, будет использован в качестве ответа. При проверке письма, поступившего от MTA через интерфейс Spamd/Rspamd, <*description*> будет использовано как значение заголовка *Message*, добавленного к письму после сообщения результатов проверки.
`TEMPFAIL ["`<*description*>`"]`	Ответить отправителю ошибкой типа «временная ошибка». В случае работы с данными, передаваемыми по протоколу SMTP, сформировать код ответа SMTP 451 (класс временных ошибок). Необязательный параметр <*description*>, если указан, будет использован в качестве ответа. При проверке письма, поступившего от MTA через интерфейс Spamd/Rspamd, <*description*> будет использовано как значение заголовка *Message*, добавленного к письму после сообщения результатов проверки.
`DISCARD`	Отвергнуть письмо, т. е. принять его без возврата отправителю кода ошибки и уничтожить вместо передачи получателю.

Модифицирующие резолюции

Модифицирующие резолюции не прерывают проверку правил, а фиксируют действия, которые должны быть применены к проверяемым данным по достижении разрешающей резолюции *PASS*.

Резолюция	Описание (смысл)
`REPACK [`<*reason*>`]`	Перепаковать сообщение, т. е. создать (на основе одного из предопределенных шаблонов) новое сообщение, содержащее содержимое из старого сообщения и некоторый текст, информирующий получателя о наличии

Резолюция	Описание (смысл)
	угроз. Вырезанное нежелательное содержимое помещается в архив, защищенный паролем. Данный архив будет добавлен к сообщению, отправленному получателю, как вложение. Проверка сообщения будет продолжена до достижения резолюции *PASS*. Имеются следующие предопределенные шаблоны перепаковки: 1) сообщение признано спамом; 2) наличие в сообщении одной или более угроз; 3) наличие в сообщении одного или более вредоносных или нежелательных URL; 4) нарушение сообщением политик безопасности, указанных администратором. В журнале фиксируется, что перепаковка случилась по причине <*reason*>. Эта же причина используется для определения, на основании какого из четырех шаблонов сформировать письмо-уведомление получателю. В качестве <*reason*> для `REPACK` могут быть использованы следующие причины: • `as _match` — причиной перепаковки является признание письма спамом, попадание веб-ресурса или файла с угрозой, содержащихся в письме, в категорию, из-за которой сработало правило (для условий `*_category in (...)`). Переменная `_match` хранит список нежелательных категорий, для которых сработало соответствие. Для перепаковки выбирается шаблон 1, 2 или 3 (см. выше), в зависимости от того, что было обнаружено в сообщении: • если сообщение признано спамом, то выбирается шаблон 1; • если найдена хотя бы одна угроза, то выбирается шаблон 2; • если найден хотя бы один вредоносный или нежелательный URL, то выбирается шаблон 3; • если угроз не обнаружено, то выбирается шаблон 4; • "текстовое сообщение" — письмо перепаковано в силу срабатывания настроек, заданных администратором, а сообщение указывает произвольное сообщение от администратора. Пример: *REPACK "Virus found!"*. Для перепаковки будет выбран шаблон 4.

Резолюция	Описание (смысл)
`ADD_HEADER("<Name>","<Value>")`	Добавить в письмо заголовок <*Name*> со значением <*Value*> и продолжить проверку письма до достижения резолюции *PASS*. Пример: `ADD_HEADER ("X-SPAM", "Virus found!")`. Значение перекодируется в ASCII в соответствии с RFC 2047.
`CHANGE_HEADER("<Name>", "<Value>" | _value [+ "<Value>" | _value [+ ...]])`	Заменить значение первого найденного заголовка с именем <*Name*>. Новое значение — конкатенация значений после запятой, разделенных символом +. Каждое значение может быть либо строковым литералом в кавычках, либо специальной переменной *_value*, в которую подставляется исходное значение модифицируемого заголовка. Проверка сообщения будет продолжена до достижения резолюции *PASS*. Например: `CHANGE_HEADER("Subject", "[SPAM] '" + _value + "' (do not read!)")`.

Особенности обработки 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 _match категорию(и)»*.
- `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, а 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 скобки пустые — это означает очистку списка значений переменной. Для случая с одним значением скобки необходимо опустить, т. е. использовать синтаксис

```
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,

записи `variable_name`, `VariableName` и `variablename` представляют одну и ту же переменную. В данном разделе все переменные записаны с использованием подчеркивания (т. е. используется вариант написания `variable_name`).

Переменные общего назначения

Переменная	Описание	Может быть использована в	
		условной части	части действия (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 было разрешено вскрытие SSL.
	• В правилах для Dr.Web ICAPD нет смысла указывать значение, отличное от `HTTP` — для этого компонента протокол может быть только HTTP.
	• Множество значений для проверки значения переменной можно получать из файла.
	
	Примеры:
	`protocol in (HTTP, SMTP)`
	`protocol in (POP3)`
	`protocol in file("/etc/file")`
		Да	Нет

`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. • Нет смысла использовать в правилах для Dr.Web ICAPD (этот компонент не	Да	Нет

Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)

	обрабатывает SSL, поэтому условие всегда будет ложным).
	• Множество значений для проверки значения переменной можно получать из файла.
	• Может быть использована 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")`		

`sni_category`	Список категорий (*AdultContent* и т. п.), к которым в базах категорий веб-ресурсов относится узел (определенный по SNI), с которым устанавливается соединение через SSL/TLS. *Переменная может принимать множество значений.* **Особенности использования:** • Если SSL не используется, то значение переменной не определено, условие будет ложным. • Нет смысла использовать в правилах для Dr.Web ICAPD (этот компонент 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). • 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`).	Да	Нет

Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)

	• 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 с указанной строкой или регулярным выражением.
	Особенности использования:
	• Можно использовать только в правилах для Dr.Web ICAPD.
	• 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")`
		Да	Нет

`url_host`	URL или узел, с которым устанавливается соединение. **Особенности использования:** • Значение переменной определено, только если не используется SSL/TLS или было разрешено вскрытие SSL. • Для проверки значения переменной можно использовать Dr.Web LookupD.	Да	Нет

Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)

	• 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")`		

`url_category`	Список категорий, к которым (по базам категорий веб-ресурсов или по ответу из Dr.Web CloudD) относится URL или узел, с которым установлено соединение.
	Переменная может принимать множество значений.
	Особенности использования:
	• Значение переменной определено, только если не используется SSL/TLS или было разрешено вскрытие SSL.
	• 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).
	• 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`
		Да	Нет

Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)
	`"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 было разрешено вскрытие SSL. • 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). • 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")`	Да	Нет
`user`	Имя пользователя, с правами которого запущен процесс-отправитель (или получатель) трафика. **Особенности использования:** • В правилах для Dr.Web ICAPD имеет смысл использовать имя пользователя, прошедшего аутентификацию на прокси-сервере (если прокси-сервер поддерживает аутентификацию). Если прокси-сервер не аутентифицирует	Да	Нет

Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)

	пользователей, переменная имеет пустое значение.
	• Для проверки значения переменной можно использовать Dr.Web LookupD.
	• Если требуется проверить вхождение пользователя в некоторую группу пользователей, используйте источник данных LDAP или Active Directory, возвращающий перечень групп. Также запрос должен содержать условие сравнения имени группы, которой принадлежит пользователь, с требуемым (используйте формат *<имя источника LookupD>@<источник групп>@<требуемая группа>*). 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`
		Да	Нет

Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)
	`src_ip not in file("/etc/file")`		

`proc`	Процесс, устанавливающий соединение (полный путь к исполняемому файлу).
	
	Особенности использования:
	• Нет смысла использовать в правилах для Dr.Web ICAPD (этот компонент не имеет информации о процессах, поэтому условие всегда будет ложным).
	• Множество значений для проверки значения переменной можно получать из файла.
	• 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")`
		Да	Нет

`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	Да	Нет

Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)

	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`		

`content_type`	MIME-тип данных, передающихся по соединению.
	
	Особенности использования:
	• Может быть определен, только если не используется SSL/TLS или было разрешено вскрытие SSL.
	• 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")`
		Да	Нет

`(proc, <`*переменная*`>)`	Сетевая активность процесса, где `proc` — полный путь к исполняемому файлу	Да	Нет

Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)

	процесса (см. выше), а <*переменная*> определяет тип сетевой активности, и может принимать одно из следующих 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.
	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*>.
	• Нет смысла использовать в правилах для Dr.Web ICAPD (этот компонент 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`	Используется ли раскрытие защищенного трафика, передаваемого через SSL/TLS. **Возможные значения:** `true`, `false`. **Особенности использования:** • Переменная не может не иметь значения, т. е. инструкция `SET unwrap_ssl = ()` недопустима.	Нет	Да

Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)

	• Переменная не может использоваться в условиях, а нужна только для управления вскрытием SSL (например, чтобы продемонстрировать пользователю веб-страницу с уведомлением о блокировке от нашего имени).
	• Нет смысла использовать в правилах для Dr.Web ICAPD (этот компонент не обрабатывает SSL, изменение значения переменной никак не влияет на обработку правил).
	Примеры:
	`SET unwrap_ssl = TRUE`
	`set Unwrap_SSL = false`		

`http_templates_dir`	Путь к каталогу, из которого брать шаблон страницы уведомления о блокировке HTTP-запроса или ответа.
	Если путь начинается с `/` — это абсолютный путь, если с любого другого символа, — то это относительный путь. Корнем при этом считается путь из параметра `TemplatesDir`.
	Особенности использования:
	• Имеет смысл только для протокола HTTP(S).
	Примеры:
	`SET http_templates_dir = "/etc/mytemplates"`
	`set http_templates_dir = "templates_for_my_site"`
		Нет	Да

Переменные, используемые в правилах обработки почты

Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)

`header`	Содержимое области заголовков письма.
	
	Особенности использования:
	• Используется для сравнения области заголовков со списком задаваемых шаблонов (используются регулярные выражения).
	• Может быть проверен любой из заголовков, представленных в письме.
	• Сравнение нечувствительно к регистру, допустимо использовать Unicode.
	• Множество значений для проверки значения переменной можно получать из файла.
	
	Примеры:
	`header match ("su..ect: sp.m", "From: sales.*@.*")`
	`Header not match ("Subject: .*купи.*")`
	`header match file("/etc/file")`
		Да	Нет

`body`	Текстовое содержимое тела письма. **Особенности использования:** • Используется для сравнения тела письма со списком задаваемых шаблонов (используются регулярные выражения). • Может быть проверена любая текстовая часть тела письма. • Сравнение нечувствительно к регистру, допустимо использовать Unicode. • Множество значений для проверки значения переменной можно получать из файла.	Да	Нет

Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)

	Примеры:
	`body match ("в.чност[ьи]")`
	`body not match file("/etc/file")`		

`body_part_header`	Заголовки частей тела письма (MIME part).
	Особенности использования:
	• Используется для сравнения заголовков, имеющихся в разделах тела письма, со списком задаваемых шаблонов (используются регулярные выражения).
	• Могут быть проверены заголовки любой части тела письма.
	• Сравнение нечувствительно к регистру, допустимо использовать Unicode.
	• Множество значений для проверки значения переменной можно получать из файла.
	Примеры:
	`body_part_header match ('Content-Disposition: attachment; .*filename="вирус.exe"')`
	`BodyPartHeader not match ("Content-Disposition: attachment; .*")`
	`body_part_header match file("/etc/file")`
		Да	Нет

`attachment_name`	Имена файлов, прикрепленных к письму. **Особенности использования:** • Используется для сравнения имен файлов (*Content-Disposition: attachment*), прикрепленных к письму, со списком задаваемых шаблонов (используются регулярные выражения).	Да	Нет

Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)

	• Сравнение нечувствительно к регистру, допустимо использовать Unicode.
	• Множество значений для проверки значения переменной можно получать из файла.
	Примеры:
	`attachment_name match ("\.ex.$", "\.js$", "^virus.*")`
	`attachment_name not match ("\.txt$", "\.rtf$")`
	`attachment_name not match file("/etc/file")`		

`total_spam_score`	Нормализованная оценка письма, как спама (от 0 до 1), полученная от Dr.Web ASE. Нормализация балльной оценки спама, полученной от Dr.Web ASE, производится по следующим правилам: 1. Число баллов 0 и меньше — 0,0; 2. Число баллов 100 — 0,8; 3. Число баллов 1000 и больше — 1,0. В указанных интервалах нормализованная оценка возрастает. **Особенности использования:** • Переменная числовая, всегда имеет одно значение может использоваться только с условиями типа `lt` и `gt`. • Если Dr.Web ASE не установлен, то проверка писем на спам не производится, и переменную `total_spam_score` нельзя использовать в правилах (попытка проверить истинность условия в правиле будет приводить к ошибке «*Dr.Web ASE не доступен*»).	Да	Нет

Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)
	Пример: `total_spam_score gt 0.32 total_spam_score gt 0.5, total_spam_score lt 0.95`		
`smtp_mail_from`	Адрес отправителя письма, переданный в рамках SMTP-сессии командой `MAIL FROM`. **Особенности использования:** • Используется для сравнения имени отправителя, указанного в рамках SMTP-сессии, со списком задаваемых шаблонов (используются регулярные выражения). • Сравнение нечувствительно к регистру. • Эта переменная не может быть использована в правилах интерфейса *Spamd*: данный протокол не предоставляет информацию об отправителе письма. • Множество значений для проверки значения переменной можно получать из файла. **Примеры:** `smtp_mail_from match ("^john@.*", ".*@domain.com$") smtp_mail_from not match ("^user@domain.com$") smtp_mail_from match file("/etc/file")`	Да	Нет
`smtp_rcpt_to`	Перечень адресов получателей письма, переданный в рамках SMTP-сессии командой `RCPT TO`. **Особенности использования:** • Используется для сравнения имен получателей, указанных в рамках SMTP-сессии, со списком задаваемых шаблонов (используются регулярные выражения).	Да	Нет

Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)

	• Сравнение нечувствительно к регистру.
	• Эта переменная не может быть использована в правилах интерфейса *Spamd*: данный протокол не предоставляет информацию о получателе письма.
	• Если перед `match` указано `all`, то условие с данной переменной будет истинно только в случае совпадения *всех значений из перечня* с указанными шаблонами.
	• Множество значений для проверки значения переменной можно получать из файла.
	Примеры:
	`smtp_rcpt_to match ("^user1@domain.com$", ".*@domain2.com$")`
	`smtp_rcpt_to all match ("^john@.*", ".*@domain.com$")`
	`smtp_rcpt_to match file("/etc/file")`		

`maild_templates_dir`	Путь к каталогу, из которого брать шаблон, используемый для перепаковки почтовых сообщений. Если путь начинается с `/` — это абсолютный путь, если с любого другого символа — то это относительный путь. Корнем при этом считается путь из параметра `TemplatesDir`. **Особенности использования:** • Имеет смысл только для почтовых протоколов (*POP3*, *IMAP*, *SMTP*) и для интерфейсов MTA (*Milter*, *Spamd*, *Rspamd*). **Примеры:** `SET maild_templates_dir = "/etc/my_mail_templates"`	Нет	Да

Переменная	Описание	Может быть использована в	
		условной части	части действия (SET)
	`set MaildTemplatesDir = "templates_for_my_MTA"`		

Категории нежелательных веб-сайтов и угроз

1. Категории нежелательных веб-сайтов (для переменных `sni_category`, `url_category`)

Обозначение	Категория веб-сайтов
InfectionSource	Веб-сайты, содержащие вредоносное ПО («источники распространения угроз»)
NotRecommended	Веб-сайты, используемые для мошенничества («социальной инженерии») и не рекомендованные к посещению
AdultContent	Веб-сайты, содержащие материалы порнографического или эротического содержания, веб-сайты знакомств и т. д.
Violence	Веб-сайты, содержащие призывы к насилию, материалы о различных происшествиях с человеческими жертвами и т. д.
Weapons	Веб-сайты, посвященные оружию и взрывчатым веществам, а также материалы с описанием их изготовления и т. д.
Gambling	Веб-сайты, на которых размещены онлайн-игры на деньги, интернет-казино, аукционы, а также принимающие ставки и т. д.
Drugs	Веб-сайты, пропагандирующие употребление, изготовление или распространение наркотиков и т. д.
ObsceneLanguage	Веб-сайты, на которых содержится нецензурная лексика (в названиях разделов, статьях и пр.)
Chats	Веб-сайты для обмена сообщениями в режиме реального времени
Terrorism	Веб-сайты, содержащие материалы агрессивно-агитационного характера, описания терактов и т. д.
FreeEmail	Веб-сайты, предоставляющие возможность бесплатной регистрации электронного почтового ящика
SocialNetworks	Социальные сети общего характера, деловые, корпоративные и тематические социальные сети, а также тематические веб-сайты знакомств

Обозначение	Категория веб-сайтов
DueToCopyrightNotice	Веб-сайты, ссылки на которые указаны правообладателями некоторого произведения, защищенного авторскими правами (кинофильмы, музыкальные произведения и т. д.)
OnlineGames	Веб-сайты, на которых размещены игры, использующие постоянное соединение с интернетом
Anonymizers	Веб-сайты, позволяющие пользователю скрывать свою личную информацию и предоставляющие доступ к заблокированным веб-сайтам
CryptocurrencyMiningPool	Веб-сайты, предоставляющие доступ к сервисам, объединяющим пользователей с целью добычи (майнинга) криптовалют
Jobs	Веб-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
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, которые можно использовать в условиях правил

Параметры, используемые в правилах компонента Dr.Web ICAPD (указываются с префиксом `ICAPD.`):

Параметр	Описание и пример использования
`Whitelist`	Белый список. Хранит перечень доменов, доступ к которым разрешается, даже если эти домены находятся в базе категорий. **Примеры:** `url_host not in "ICAPD.Whitelist" : Block as BlackList`
`Blacklist`	Черный список. Хранит перечень доменов, доступ к которым запрещен самим пользователем (или администратором). **Примеры:** `url_host in "ICAPD.Blacklist" : Block as BlackList`
`Adlist`	Рекламный список. Хранит перечень регулярных выражений, которые описывают рекламные веб-сайты. Задается самим пользователем (или администратором). **Примеры:** `url match "ICAPD.Adlist" : Block as BlackList`
`BlockCategory`	«Метапараметр»: его значением является список названий категорий веб-ресурсов (*Chats*, *AdultContent* и т. д.), для которых соответствующие параметры `Block*` в секции `[ICAPD.]` установлены в `Yes`. **Примеры:** `url_category in "ICAPD.BlockCategory" : Block as _match`
`BlockThreat`	«Метапараметр»: его значением является список названий типов угроз (*KnownVirus*, *Joke* и т. д.), для которых соответствующие параметры `Block*` в секции `[ICAPD.]` установлены в `Yes`. **Примеры:** `threat_category in "ICAPD.BlockThreat" : BLOCK as _match`

5. Приложение Б. 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/.