Dr.WEB

Enterprise Security Suite

Управление Dr.Web для Интернет-шлюзов UNIX

Dr.Web Enterprise Security Suite. Управление Dr.Web для Интернет-шлюзов UNIX
Версия 10.0
Руководство администратора
15.11.2016

«Доктор Веб», Центральный офис в России

125040

Россия, Москва

3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: http://www.drweb.com/

Телефон: +7 (495) 789-45-87

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

«Доктор Веб»

«Доктор Веб» – российский разработчик средств информационной безопасности.

«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

Глава 1. Введение 5
1.2. Назначение документа 5
1.3. Условные обозначения и сокращения 6
Глава 2. Dr.Web Enterprise Security Suite 8
2.1. О продукте 8
2.2. Защита станций сети 9
Глава 3. Dr.Web для Интернет-шлюзов UNIX 11
3.1. Компоненты Dr.Web для Интернет-шлюзов UNIX 11
3.2. Настройка Dr.Web для Интернет-шлюзов UNIX 13
3.2.1. Настройки Dr.Web ICAPD 14
3.2.2. Ведение журнала 14
3.2.3. Антивирус 15
3.2.4. Прокси 17
3.2.5. Фильтрация 18
3.2.6. Прочие 21
3.2.7. Уведомления 22
Приложение A. Правила фильтрации 23
Параметры запросов 24
Логические выражения 25
Макросы 27
Правила доступа 28
Настройка прокси-сервера 30
Приложение B. Техническая поддержка 32

Глава 1. Введение

1.2. 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 для Интернет-шлюзов UNIX и особенности централизованного управления данным ПО.

Для получения дополнительной информации обращайтесь к следующим руководствам:

- **Руководство пользователя** антивирусного решения Dr.Web для Интернет-шлюзов UNIX 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» https://download.drweb.ru/doc/.

1.3. Условные обозначения и сокращения

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.
`C:\Windows\`	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:

- DNS – система доменных имен (Domain Name System),
- FQDN – полностью определенное имя домена (Fully Qualified Domain Name),
- FTP – протокол передачи файлов (File Transfer Protocol),
- 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 адаптации Интернет-контента (Internet Content Adaptation Protocol),
- IP – протокол Интернета (Internet Protocol),
- MIME – многоцелевые расширения Интернет и почты (Multipurpose Internet Mail Extensions),
- SSL – уровни защищенных сокетов (Secure Socket Layers),

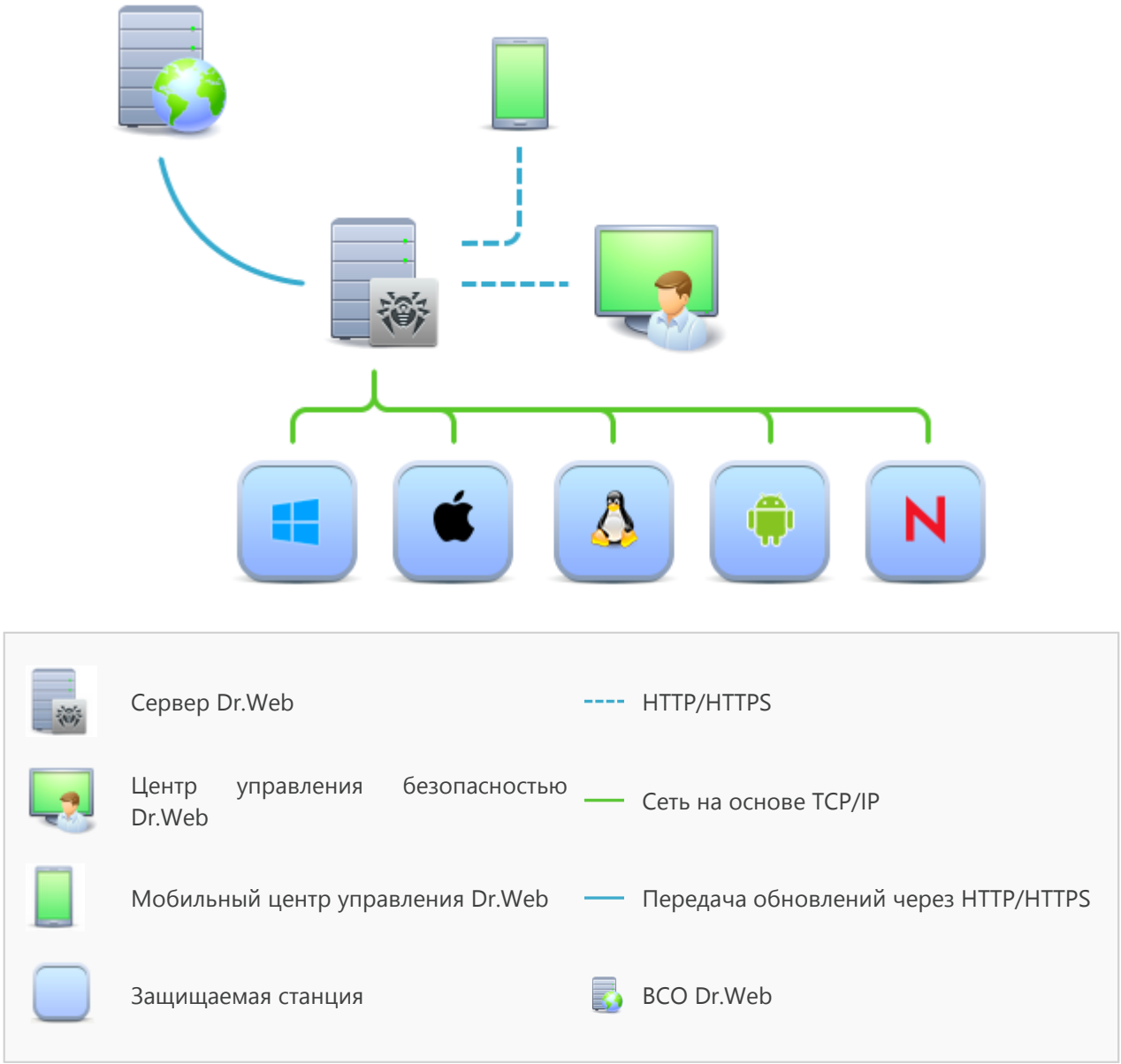
- TCP – протокол управления передачи (Transmission Control Protocol),
- TLS – защищенный транспортный уровень (Transport Layer Security),
- URL – единообразный локатор ресурса (Uniform Resource Locator),
- ВСО – Всемирная Система Обновлений Dr.Web,
- ЛВС – Локальная Вычислительная Сеть,
- ОС – Операционная Система,
- ПО – Программное Обеспечение.

Глава 2. Dr.Web Enterprise Security Suite

2.1. О продукте

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*.



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 станций сети

Защита рабочих станций осуществляется антивирусными пакетами Dr.Web, разработанными для соответствующих операционных систем.

Защищаемый компьютер с установленным антивирусным пакетом, в соответствии с его функциями в антивирусной сети, именуется *рабочей станцией* антивирусной сети. Необходимо помнить, что по своим функциям в локальной сети такой компьютер может быть как рабочей станцией или мобильным устройством, так и сервером 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 между станцией и Сервером осуществляется по протоколу, используемому в локальной сети (TCP/IP версии 4 или 6).

Установка

Локальная установка осуществляется на компьютере пользователя непосредственно. Может производится как администратором, так и пользователем.

Подробное описание процедур установки антивирусных пакетов на рабочие станции приведено в **Руководстве по установке**.

Управление

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

- Централизованная настройка антивирусного пакета на рабочих станциях при помощи Центра управления безопасностью.

  При этом администратор может как запретить, так и оставить возможность пользователю самостоятельно изменять настройки антивирусного пакета на станции.
- Настройка расписания антивирусных проверок и других заданий, выполняемых на станции.
- Получение статистики сканирования и прочей информации о работе антивирусных компонентов и о состоянии станции.

- Запуск и останов антивирусного сканирования и т.п. (в зависимости от функциональных возможностей антивирусного пакета, установленного на станции).

Обновление

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

В случае временного отключения рабочей станции от антивирусной сети, антивирусный пакет на станции использует локальную копию настроек, антивирусная защита на рабочей станции сохраняет свою функциональность (в течение срока, не превышающего срок действия пользовательской лицензии), но обновление ПО не производится. Если для станции разрешено функционирование в *Мобильном режиме*, при потере связи с Сервером будет доступно обновление вирусных баз непосредственно с серверов ВСО Dr.Web.

Принцип работы станций в мобильном режиме описан в **Руководстве администратора**.

Глава 3. Dr.Web для Интернет-шлюзов UNIX

В настоящем документе рассматриваются аспекты настройки компонентов, входящих в продукт Dr.Web для Интернет-шлюзов UNIX, предназначенный для работы в ОС **GNU/Linux**, **FreeBSD**, **Solaris** (**Solaris** – только для платформ Intel x86). Руководство адресовано лицу, отвечающему за антивирусную безопасность и настройку сетей, называемому в данном руководстве «Администратором».

Проблема защиты Интернет-шлюзов в UNIX-системах имеет следующие аспекты:

1. Проверка всего входящего FTP- и HTTP-трафика на наличие вирусов, их диагностика и обезвреживание. При этом вирусы могут быть (и в большинстве случаев являются) отнюдь не специфичными для UNIX-систем. Через Интернет распространяются обычные Windows-вирусы, в том числе и макровирусы для **Microsoft Word**, **Excel** и других офисных приложений.
2. Фильтрация доступа к HTML-ресурсам как по MIME-типу и размеру, так и по имени узла.
3. Ограничение доступа к интернет-ресурсам благодаря использованию обновляемых тематических черных списков.

Программный комплекс Dr.Web для Интернет-шлюзов UNIX выполняет все перечисленные функции.

3.1. Компоненты Dr.Web для Интернет-шлюзов UNIX

Для защиты интернет-шлюзов UNIX-систем предоставляются следующие антивирусные компоненты:

Dr.Web ICAPD

Центральный компонент программного комплекса Dr.Web для Интернет-шлюзов UNIX. Позволяет интегрировать его с приложениями, использующими протокол ICAP (как правило, это защищаемый прокси-сервер HTTP/FTP, использующийся для доступа рабочих станций, включенных в ЛВС, к Интернету).

Консольный сканер Dr.Web Scanner (настройки доступны только на станции)

Служит для обнаружения и лечения вирусов на локальной машине, в том числе и в каталогах общего доступа.

Резидентный компонент Dr.Web Daemon (настройки доступны только на станции)

Используется компонентом Dr.Web ICAPD для проверки файлов и, при возможности, обезвреживания угроз.

Карантин

Используется для изоляции вредоносных и подозрительных объектов в специальном каталоге.

Описание работы с Карантином через Центр управления приведено в **Руководстве администратора**.

Dr.Web ICAPD (**drweb-icapd**) позволяет интегрировать все компоненты программного комплекса Dr.Web для Интернет-шлюзов UNIX с приложениями, использующими протокол ICAP. На данный момент поддержка протокола ICAP включена в прокси-серверы **Squid** и **SafeSquid**. Dr.Web ICAPD соединяет прокси-сервер, поддерживающий протокол ICAP, с Dr.Web Daemon (**drweb-daemon**) для проверки всего входящего FTP- и HTTP-трафика на наличие вирусов. Кроме того, он позволяет фильтровать доступ к HTML-ресурсам как по MIME-типу и размеру соответствующих файлов, так и по имени узла. Также с его помощью можно ограничивать доступ к страницам благодаря использованию как обновляемых списков категорий интернет-ресурсов, так и черных и белых списков, определенных пользователем (администратором комплекса).

Принципы работы:

1. Клиент выполняет запрос некоторого ресурса (HTTP-запрос `GET`).
2. Прокси-сервер запрашивает у Dr.Web ICAPD по протоколу ICAP возможность обращения к указанному серверу.
3. Если доступ к указанному серверу не должен быть заблокирован (сервер находится в пользовательском белом списке, не находится в пользовательском черном списке, не находится в блокируемых категориях веб-сайтов или если для запроса сработали разрешающие доступ правила), то Dr.Web ICAPD разрешает прокси-серверу выполнить HTTP-запрос. В противном случае Dr.Web ICAPD предписывает прокси-серверу вернуть клиенту сгенерированную Dr.Web ICAPD HTML-страницу с уведомлением о блокировке ресурса.
4. Если доступ к удаленному серверу был разрешен, то прокси-сервер получает от него ответ, который по протоколу ICAP передает Dr.Web ICAPD на антивирусную проверку.
5. Если пользователь добавил удаленный сервер в белый список, полученный контент не проверяется и Dr.Web ICAPD предписывает прокси-серверу передать контент клиенту. В противном случае, Dr.Web ICAPD проверяет выполнение правил контент-фильтрации, и, если для контента выполняется действие scan, отправляет полученный файл на проверку сканирующему демону Dr.Web Daemon.
6. По результатам проверки к запрашиваемому контенту применяется одно из следующих действий:
   a) `pass` – Dr.Web ICAPD разрешает прокси-серверу вернуть запрошенный контент клиенту;
   b) `report` – Dr.Web ICAPD предписывает прокси-серверу вернуть клиенту сгенерированную HTML-страницу с уведомлением об отклонении запрошенного файла;
   c) `move` – Dr.Web ICAPD помещает исходный файл в Карантин и предписывает прокси-серверу вернуть клиенту сгенерированную HTML-страницу с уведомлением о помещении запрошенного файла в Карантин;

d) `truncate` – Dr.Web ICAPD предписывает прокси-серверу вернуть клиенту пустой файл.

Эти же действия (за исключением перемещения в Карантин) могут быть указаны и в самих правилах контент-фильтрации. Таким образом, можно разрешить компоненту Dr.Web ICAPD пропускать без проверки, или наоборот, безусловно отвергать данные некоторых типов (например, потоковое видео). Для этого требуется, чтобы был активизирован и корректно настроен режим *ICAP preview*.

Настройка прокси-серверов **Squid** и **SafeSquid** для работы с Dr.Web ICAPD описана в Руководстве Администратора по продукту Dr.Web для Интернет-шлюзов UNIX.

3.2. Настройка Dr.Web для Интернет-шлюзов UNIX

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 ОС семейства UNIX (**Linux**, **Solaris** или **FreeBSD**) или группы, содержащей такие станции.
3. В открывшемся управляющем меню в разделе **Конфигурация**, в одном из подразделов **UNIX**: **Linux**, **Solaris** или **FreeBSD** выберите компонент Dr.Web ICAPD.
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.

3.2.1. Настройки Dr.Web ICAPD

Раздел **Dr.Web ICAPD** содержит следующие настройки функционирования Dr.Web для Интернет-шлюзов UNIX:

- Ведение журнала – настройки ведения файла журнала событий на защищаемом сервере.
- Антивирус – настройки проверки на вирусы файлов, загружаемых из сети Интернет.
- Прокси – настройки связи с защищаемым прокси-сервером HTTP (например, **Squid**).
- Фильтрация – настройка условий блокировки доступа к веб-сайтам и фильтрации данных, загружаемых из Интернета.
- Прочие – дополнительные настройки.
- Уведомления – настройки отправки уведомлений администратору.

3.2.2. Ведение журнала

В данном разделе вы можете управлять следующими параметрами ведения локального журнала Dr.Web для Интернет-шлюзов UNIX на защищаемой станции:

- **Файл журнала** – определяет имя файла, в который сохраняются сообщения журнала. Если указано значение syslog, то журнал сохраняется системным сервисом syslog (при этом необходимо задать значения настроек **Подсистема syslog** и **Приоритет syslog**).
- **Подсистема syslog** – определяет метку записи сообщений от Dr.Web ICAPD при использовании системного сервиса `syslog` (если значение syslog указано в поле **Файл журнала**).
- **Приоритет syslog** – определяет уровень важности, присваиваемый системным сервисом **`syslog`** сообщениям от Dr.Web ICAPD (если значение syslog указано в поле **Файл журнала**).

- **Уровень журнала** – определяет уровень подробности сообщений, отправляемых в журнал. Представляет собой число, являющееся суммой произвольной комбинации следующих значений:

  0 – выводить информацию об ошибках и обнаруженных вирусах;

  1 – выводить информацию уровня Info: о проверенных чистых файлах и прочую служебную информацию;

  2 – выводить общие сообщения;

  4 – выводить сообщения о результатах разбора фрагментов данных (chunks of data);

  8 – выводить расширенные сообщения по фрагментам данных;

  16 – выводить протокол работы синтаксического анализатора;

  32 – выводить прочие отладочные сообщения.

  Например, если требуется выводить в журнал общие сообщения (2), сообщения синтаксического анализатора (16) и информацию об ошибках и обнаруженных вирусах (0), то значение образуется следующим образом: 0 + 2 + 16 = 18.

  Максимально подробный вывод информации, включающий вывод всех данных, включается, таким образом, если указано 63. Обратите внимание, что если указано –1, то это означает отключение вывода информации в журнал.

- **Максимальный размер журнала** – определяет максимальный допустимый размер файла журнала. При каждом запуске Dr.Web ICAPD осуществляется проверка размера файла журнала. Если размер превышает заданное значение, то журнал будет перезаписан заново. Задайте значение 0, чтобы не проверять размер файла журнала при старте.

3.2.3. Антивирус

В данном разделе вы можете управлять параметрами антивирусной зашиты, которые Dr.Web для Интернет-шлюзов UNIX будет применять при проверке интернет-соединений.

Действия

Определяет перечень событий, на которые будет реагировать Dr.Web ICAPD, и действия, которые следует применять к файлам при возникновении этих событий. Под файлом здесь понимается порция данных, отправленных пользователем на сервер (например, файл или поля формы, отправленные запросом POST) или данные, поступившие в ответ от сервера, (например, ответ на запрос пользователя GET).

В качестве событий, на которые может реагировать Dr.Web ICAPD, доступны следующие:

- **Неизлечимые** – к обнаруженной угрозе не удалось применить действие **Лечить**.
- **Подозрительные** – проверенный файл отмечен как подозрительный.
- **Зараженные** – в проверенном файле обнаружен известный вирус.
- **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 программы** – в проверенном файле обнаружена потенциально опасная программа.
- **Программы взлома** – в проверенном файле обнаружена программа взлома.
- **Непроверенные архивы** – проверенный файл представляет собой не проверяемый архив (например, защищенный паролем или размер которого превышает максимально допустимый для распаковки).
- **Ошибка Демона Dr.Web Daemon** – при попытке проверки файла произошла ошибка Демона Dr.Web Daemon.
- **Пропускаемые файлы** – файл не может быть проверен демоном Dr.Web Daemon (защищенный паролем или испорченный архив, символическая ссылка, файл нестандартного формата и т.п.).
- **Лицензионные ограничения** – файл не может быть проверен вследствие ошибки лицензии на станции (например, истек срок действия лицензии).

Для этих событий доступны следующие действия:

- **Сообщать** – вместо файла вернуть пользователю HTML-страницу с сообщением об обнаруженной угрозе.
- **Перемещать в карантин** – переместить файл в Карантин и вернуть пользователю HTML-страницу с сообщением о перемещении обнаруженной угрозы в Карантин.
- **Отсечь** – вернуть пользователю запрошенный файл с удаленным внутренним содержимым.
- **Игнорировать** – вернуть пользователю запрошенный файл.
- **Лечить** – выполнить лечение обнаруженной угрозы и вернуть пользователю вылеченный файл (если лечение невозможно, применить к файлу действие, указанное в поле **Неизлечимые**).

> Не все типы действий доступны для всех типов событий. Например, действие **Лечить** доступно только для события **Зараженные**.

Карантин

Определяет параметры доступа к Карантину на защищаемой станции, хранящему изолированные файлы с угрозами.

- **Каталог карантина** – путь к каталогу Карантина с изолированными файлами на станции.
- **Права доступа файлов в карантине** – маска прав доступа к файлам, перемещенным в Карантин. Маска задается в стандартной для UNIX-систем форме из трех цифр.

Дополнительно

Определяет дополнительные параметры проверки.

- **Сокеты для связи с демоном Dr.Web Daemon** – список путей локальных сокетов на станции, через которые Dr.Web ICAPD взаимодействует с компонентом проверки файлов – демоном Dr.Web Daemon. Для проверки файлов должно быть указано не менее одного сокета. Адреса в списке разделяются запятыми.

  Примеры: `inet:3000@localhost`, `local:%var_dir/.daemon`, `pid:/usr/local/drweb/run/drwebd.pid`

  Если вы используете Dr.Web Daemon, запущенный на удаленной (по отношению к защищаемой станции) машине, флажок **Локальное сканирование** должен быть сброшен. Когда первым в списке стоит адрес сокета или PID-файла Dr.Web Daemon, обеспечивающего локальное сканирование, то при невозможности установить соединение по этому адресу, режим локального сканирования принудительно отключается. Если список пуст, то Dr.Web ICAPD работает без подключения к Dr.Web Daemon, и проверка на вирусы не производится.
- **Эвристический анализатор** – определяет, следует ли использовать эвристический анализатор для поиска неизвестных угроз. Объекты, обнаруженные эвристическим анализатором помечаются как подозрительные.
- **Локальное сканирование** – включает и выключает режим локального сканирования. Если флажок установлен, Dr.Web Daemon сканирует файлы в локальном режиме; при этом компоненту передаются только пути к файлам. В противном случае ему будет передаваться содержимое файлов. Локальное сканирование может использоваться только в том случае, если Dr.Web Daemon расположен на той же машине, на которой работает Dr.Web ICAPD.

3.2.4. Прокси

В данном разделе вы можете настроить связь Dr.Web ICAPD с защищаемым им прокси-сервером HTTP (таким, как **Squid**):

- **Номер порта** – номер порта, который прослушивается Dr.Web ICAPD в ожидании подключений от прокси-сервера. Обратите внимание: значение параметра должно совпадать со значением соответствующего параметра, заданного для HTTP прокси-сервера.
- **Имя узла** – IP-адрес или имя узла, на котором установлен Dr.Web ICAPD. Обратите внимание: значение параметра должно совпадать со значением соответствующего параметра, заданного для HTTP прокси-сервера.
- **Поддерживать соединения** – не разрывать установленные соединения с прокси-сервером при ожидании поступления запросов.
- **Режим предпросмотра** – использование режима предпросмотра *ICAP preview*. Если прокси-сервер некорректно работает с режимом предпросмотра, можно отключить эту возможность (снять флаг).
- **Разрешенные клиенты** – список путей к текстовым файлов через запятую. Заданные файлы содержат IP-адреса и/или имена узлов, с которых прокси-серверам разрешен доступ к Dr.Web ICAPD через ICAP протокол. Если список пуст или в указанных файлах не задано ни одного адреса, то Dr.Web ICAPD принимает соединения от всех узлов сети.

3.2.5. Фильтрация

В данном разделе вы можете настроить список правил, используемых Dr.Web ICAPD для блокировки веб-страниц, посещаемых пользователями, а также определить правила применения блокировки и проверки файлов в зависимости от их типа.

Содержание

Определяет параметры блокировки доступа к веб-сайтам различных категорий а также содержит перечни используемых черных и белых списков доступа.

Блокировка доступа к веб-сайтам различных категорий

Флажки **Блокировать** (**Блокировать сайты для взрослых** и т.д.) позволяют включить или отключить блокировку доступа пользователей к сайтам соответствующих категорий. Если блокировка включена, при попытке доступа пользователь получит от сервера в ответ HTML-страницу с уведомлением о заблокированном доступе к сайту.

Обратите внимание, что один и тот же веб-сайт может входить в различные категории. В этом случае доступ к нему будет блокироваться, если он входит хотя бы в одну из блокируемых категорий. Если требуется разрешить доступ к такому веб-сайту, нужно отключить блокировку всех категорий, к которым он относится. Кроме того, вы можете создать правила для разрешения доступа к веб-сайтам из блокируемых категорий в зависимости от условий.

Управление черными и белыми списками

Dr.Web ICAPD поддерживает списки доступа, представляющие собой наборы адресов веб-ресурсов, доступ к которым может быть разрешен или запрещен. Помимо списков категорий, которые поставляются вместе с Dr.Web ICAPD и автоматически пополняются компанией «Доктор Веб», администратор может также создать произвольное количество пользовательских списков.

Вы можете задавать не только черные, но и белые списки. Пользовательские черные списки запрещают доступ, а белые списки разрешают доступ к веб-сайтам.

Доступны два вида пользовательских белых списков:

- *Доверенный список*. Для всего контента узлов сети, находящихся в этом списке, антивирусная проверка не производится.
- *Разрешающий список*. Разрешается доступ к узлам сети, находящимся в этом списке, даже если они находятся в блокируемых категориях, но не в пользовательском черном списке.

Обратите внимание на следующие особенности пользовательских списков:

- Если некоторый узел сети находится в доверенном списке, то доступ к нему регулируется как обычно – проверкой на нахождение в блокируемых категориях с учетом правил, а также в черном пользовательском списке.
- Если некоторый узел сети находится в черном списке, то доступ к нему блокируется безусловно, т.е. нельзя создать переопределяющего правила, разрешающего доступ к этому узлу. Кроме того, этот список имеет приоритет над разрешающим белым списком, т.е. если один и тот же узел сети указан в пользовательском черном списке и в разрешающем белом, то доступ к нему будет блокирован.

Параметры:

- **Каталог dws-файлов** – путь к каталогу на защищаемой станции, в котором хранятся файлы категорий интернет-ресурсов, поставляемых вместе с Dr.Web ICAPD.
- **Белые списки для фильтрации по содержимому** – пользовательский белый список с разрешенными узлами. Содержит список путей к текстовым файлам на защищаемой станции, разделенных запятыми. Заданные файлы содержат список узлов, контент которых не будет проверяться на соответствие с черным списком. Тем не менее, передаваемый контент будет проверяться на вирусы. Настройка необходима для предоставления доступа к веб-сайтам, которые заблокированы настройками черного списка.
- **Файлы черных списков** – пользовательский черный список. Содержит список путей к текстовым файлам на защищаемой станции, разделенных запятыми. В заданных файлах перечислены узлы сети, доступ к веб-сайтам на которых запрещается.
- **Файлы белых списков** – пользовательский белый список с доверенными узлами. Содержит список путей к текстовым файлам на защищаемой станции, разделенных запятыми. Заданные файлы содержат список узлов, контент которых не будет отправляться на антивирусную проверку. Тем не менее, передаваемый контент будет проверяться на соответствие с черным списком. Обратите внимание, что этот параметр лишь отключает антивирусную проверку файлов, поступающих от узлов, но не разрешает доступ к самим узлам.

Фильтрация по MIME

Эта секция содержит единственное многострочное поле-редактор **Правила фильтрации MIME**, в котором вы можете задать правила определения, файлы какого типа и размера будут отправляться на антивирусную проверку.

Этот текст всегда начинается со строки `MimeStart`, заканчивается строкой `MimeEnd` и содержит правила фильтрации файлов, по одному на строку.

Для использования данной возможности необходимо, чтобы прокси-сервер поддерживал режим *ICAP preview*. Кроме того, убедитесь, что установлен флажок **Режим предпросмотра** на странице Прокси.

Для правил фильтрации используется следующий синтаксис (элементы выражения разделяются пробелами):

```
<MIME-тип> <действие1> <размер> <действие2>
```

где

- <*MIME-тип*> - MIME-тип файла, например:
  - `*` – файл любого типа;
  - `application` – исполняемые и архивированные файлы, документы в формате PDF, MS Word и др.;
  - `audio` – аудиофайлы (`mp3`, `wav`, `wma` и др.);
  - `image` – изображения (`gif`, `jpg`, `png`, `svg` и др.);
  - `message` – сообщения между веб-серверами и клиентами;
  - `multipart` – контейнеры (почтовые файлы, запакованные файлы);
  - `text` – текст или исходный код (`html`, `xml`, `css` и др.);
  - `video` – видеофайлы (`mpeg-1`, `mp4`, `wma`);
  - `model` – файлы трехмерных моделей.

  При необходимости может быть указано как целое семейство MIME, так и конкретный тип (например: `video` – любые видеофайлы, а `video/mpeg` – видео типа MPEG).

  Для объекта всегда применяется правило, заданное для MIME-типа, наиболее близкого MIME-типу объекта. Таким образом, правило для MIME-типа `"*"`, подходящее любому типу, применяется, только если не имеется правил с более близким классом типов MIME.
- <*действие1*> – наименование действия (`scan`, `pass`, `reject`), которое следует выполнить в случае, если размер объекта данного MIME-типа не превосходит размер, указанный в поле <*размер*>.
- <*размер*> – пороговый размер. Если размер объекта данного MIME-типа не будет превосходить пороговый, то к нему применится действие <*действие1*>, иначе к нему будет применено действие <*действие2*>.
- <*действие2*> – наименование действия (`scan`, `pass`, `reject`), которое следует выполнить в случае, если размер объекта превосходит указанный <*размер*>.

  Если в качестве размера указать ключевое слово **`all`**, то это означает, что первое действие (<*действие1*>) будет применяться ко всем объектам данного MIME-типа, вне зависимости от их размера. В этом случае <*действие2*> не указывается.

Допускаются следующие значения действий:

- `scan` – отправить файл на антивирусное сканирование;
- `pass` – пропустить файл к пользователю без проверки;
- `reject` – заблокировать файл и вернуть другой объект. Обратите внимание, что это действие должно указываться с дополнительным ключом, определяющим, какие данные возвращаются пользователю:

- `-report` – вернуть пользователю вместо запрошенного файла HTML-уведомление о блокировке;
- `-trunc` – вернуть пользователю запрошенный файл, усеченный до нулевой длины (пустой файл).

Обратите внимание, что без уточняющего ключа действие `reject` указывать нельзя.

Порядок следования правил в секции не имеет значения.

Определения

Эта секция содержит единственное многострочное поле-редактор **Определения**, в котором вы можете задать собственные макросы, используемые в переопределяющих правилах доступа к веб-сайтам. Макросы задаются в секции `[def]`.

Правила

Эта секция содержит единственное многострочное поле-редактор **Правила разрешения/блокировки**, в котором вы можете задать собственные правила разрешения и/или запрещения доступа к веб-сайтам. Правила задаются в секции `[match]`.

Подробную информацию о макросах и правилах переопределения см. в Приложении А.

3.2.6. Прочие

В данном разделе вы можете задать прочие (вспомогательные) параметры работы Dr.Web ICAPD:

- **Шаблоны** – путь к каталогу на защищаемой станции, в котором расположены шаблоны, используемые для генерации HTML-страниц, возвращаемых пользователю при блокировке вредоносных файлов и доступа к интернет-ресурсам.
- **PID-файл** – путь к PID-файлу Dr.Web ICAPD с информацией о PID, сокете UNIX или номере порта (в зависимости от того, что используется при взаимодействии), которая сохраняется при запуске Dr.Web ICAPD.
- **Максимальный размер блока памяти** – максимальный размер блока памяти, который Dr.Web ICAPD пытается выделить за один раз. При достаточном количестве оперативной памяти значение данного параметра можно увеличить для повышения производительности.
- **Время ожидания** – максимальное время в секундах, в течение которого сокеты, открытые Dr.Web ICAPD, могут находиться в режиме ожидания. При получении/отправке хотя бы одного байта через сокет, счетчик ожидания обнуляется. Если указано значение 0, время ожидания не ограничивается. Этот параметр оказывает влияние на соединение Dr.Web ICAPD не только с HTTP-прокси, но и с Dr.Web Daemon.

- **Пользователь** – пользователь, с правами которого работает Dr.Web ICAPD.
- **Кэш** – путь к каталогу, в котором создаются и хранятся временные файлы Dr.Web ICAPD.

3.2.7. Уведомления

В данном разделе вы можете задать параметры работы Dr.Web ICAPD с уведомлениями для системного администратора о любых инцидентах на защищаемых станциях (обнаружение угрозы, запрет доступа к веб-странице и т.п.):

- **Адрес администратора** – почтовый адрес администратора для отправки уведомлений.
- **Отправлять уведомления** – следует ли посылать администратору уведомления при попытках загрузки вредоносных объектов.
- **Отправить уведомления о блокировке тематическими списками** – следует ли посылать администратору уведомления при попытках загрузки страниц, заблокированных с помощью тематических черных списков.
- **Команда отправления почты** – команда `shell`, выполняемая для отправления почтовых уведомлений администратору. Параметр `%s` в указанной команде заменяется на **Адрес администратора**.
- **Отправлять статистику** – отправлять статистику об обнаруженных вирусных инцидентах в Центр управления.
- **Ожидание перед повторной отправкой** – промежуток времени в секундах, в течение которого администратору не высылаются уведомления об одном и том же инциденте (повторные попытки открытия страницы, запрещенной к посещению, или загрузки инфицированного файла). Если указано значение 0, то уведомление высылается при каждом блокировании страницы.

Приложение А. Правила фильтрации

Существует возможность задавать индивидуальные настройки доступа к интернет-ресурсам. Такое переопределение параметров осуществляется с помощью специальных правил.

В текущей версии Dr.Web для Интернет-шлюзов UNIX можно переопределять следующие параметры:

- `BlockAdult` – блокировка доступа к веб-сайтам для взрослых;
- `BlockViolence` – блокировка доступа к веб-сайтам, посвященным насилию: содержащим фото и видео материалы автомобильных аварий, авиакатастроф, стихийных бедствий и т.п.;
- `BlockWeapon` – блокировка доступа к веб-сайтам, посвященным оружию: содержащим тексты, фотографии и видеоматериалы оружия (от холодного оружия до оружия массового поражения) и информацию о производстве взрывчатых веществ;
- `BlockGamble` – блокировка доступа к веб-сайтам, посвященным азартным играм: интернет-казино, игровым и букмекерским веб-сайтам;
- `BlockDrugs` – блокировка доступа к веб-сайтам, посвященным наркотикам: содержащим информацию о производстве, распространении и использовании наркотических веществ;
- `BlockObscenity` – блокировка доступа к веб-сайтам, содержащим нецензурную лексику;
- `BlockChats` – блокировка доступа к чатам;
- `BlockTerrorism` – блокировка доступа к веб-сайтам, посвященным терроризму: содержащим подробные описания террористических актов, производства взрывчатых веществ и материалы террористической пропаганды;
- `BlockEmail` – блокировка доступа к веб-сайтам, предоставляющим бесплатные почтовые услуги;
- `BlockSocialNetwork` – блокировка доступа к социальным сетям: сайтам знакомств, бизнес-сайтам социальных сетей, корпоративным социальным сетям и т.п.;
- `BlockMalwareLinks` – блокировка доступа к веб-сайтам, содержащим вредоносные программы;
- `BlockAll` – блокировка доступа ко всем веб-сайтам.

Правила доступа задаются в секции **Правила** на странице Фильтрация; макросы, используемые в правилах, задаются в секции **Определения** на той же странице.

Порядок определения актуального значения параметров доступа к веб-сайтам с учетом правил:

1. Dr.Web ICAPD определяет, относится ли веб-ресурс к какой-либо из известных категорий.
2. Если соответствующий URL найден в перечне категорий (например, в списке сайтов, посвященных терроризму), то Dr.Web ICAPD определяет режим доступа к веб-сайтам данной категории. В Центре управления данные настройки задаются соответствующими

флагами (в приведенном примере, **Блокировать сайты, посвященные терроризму**) на странице **Фильтрация**.

3. Сначала поиск значения соответствующего параметра осуществляется в секции **Правила** по следующему алгоритму:
   - вычисляется значение выражения оператора `if` для значений переменных запроса,
   - если оно истинно, то осуществляется поиск требуемого параметра в соответствующем блоке конфигурации,
   - если такой параметр найден, то возвращается его значение и поиск завершается,
   - если параметр не найден, либо если переменная не удовлетворяет критериям, заданным конкретным выражением оператора `if`, то осуществляется переход к следующему оператору `if`.
4. Если в секции **Правила** ни одно из правил не может быть применено к данному запросу, либо не содержит необходимого параметра, возвращается глобальное значение этого параметра (или значение по умолчанию).

Поиск значения параметра осуществляется до первого совпадения, и, соответственно, возвращается первое найденное значение (из блоков конфигурации тех операторов `if`, выражения в которых имеют значение `true`).

Один и тот же ресурс может одновременно входить в различные категории и черный список пользователя. В этом случае доступ к нему будет блокироваться, если он входит хотя бы в один из активных черных списков. Если требуется разрешить доступ к такому ресурсу, нужно отключить все категории, к которым он относится, и исключить его из пользовательских черных списков.

Однако, чтобы в этом случае заодно не разрешить доступ к остальным запрещенным ресурсам этих категорий, крайне рекомендуется включать в разрешающее условие как проверку на URL ресурса, к которому разрешается доступ, так и проверку свойств клиента (таких, как IP-адрес), которому этот доступ предоставляется.

Обратите внимание, что если ресурс включен в пользовательский черный список, то разрешить доступ к нему при помощи разрешающего условия невозможно.

Параметры запросов

Каждый запрос, направляемый от клиента прокси-серверу, имеет ряд уникальных параметров. Эти параметры можно использовать в правилах:

Имя параметра	Тип параметра	Описание
`request_url`	строка (string)	URL запроса
`request_username`	строка (string)	Имя пользователя, под которым он авторизовался на прокси-сервере.

Имя параметра	Тип параметра	Описание
		Оно берется из заголовка `X-Client-Username`, а если этот заголовок отсутствует, то значение параметра берется равным пустой строке.
`request_ip`	IP-адрес с маской сети (CIDR)	IP-адрес пользователя, от которого пришел запрос на прокси-сервер. Он берется из заголовка `X-Client-IP`, а если такой заголовок отсутствует, то параметр принимает значение `undefined`.
`system_time`	время (time)	Текущее системное время (часы и минуты).

Для использования параметров `request_ip` и `request_username` нужно обеспечить соответствующую настройку прокси-сервера HTTP (см. пример настройки **Squid**).

Логические выражения

Логические выражения – это операции сравнения и вызова макросов, объединенные логическими операторами `&&` («логическое И», «AND»), `||` («логическое ИЛИ», «OR»), `!` («логическое отрицание», «NOT»). Для группировки операций и изменения их приоритета могут использоваться скобки.

Логические операции задаются только при помощи операторов `&&`, `||` и `!`. Обозначения `AND`, `OR` и `NOT` не используются.

Синтаксис логических выражений `BOOL_EXPR`:

```
macro_name() | COMPARE |
(BOOL_EXPR) | !BOOL_EXPR |
BOOL_EXPR && BOOL_EXPR |
BOOL_EXPR || BOOL_EXPR
```

Где `macro_name()` – вызов макроса с именем `macro_name`, а `COMPARE` – одна из перечисленных ниже операций сравнения. Используемый макрос должен быть определен заранее в секции **Определения**.

Используемые обозначения при определении операций сравнения `COMPARE`:

Обозначение	Комментарий

`string_var`
 	
`cidr_var`
 	
`time_var`
	Параметр соответствующего типа (`STRING`, `CIDR` или `TIME`)

Обозначение	Комментарий
TIME	Строка в формате "ЧЧ:ММ" или "Ч:ММ" (часы, минуты), в кавычках
STRING	Произвольная строка в кавычках
REGEX	Регулярное выражение формата *POSIX extended*, в кавычках
FILE_NAME	Путь к файлу, в кавычках
CIDR	IPv4-адрес в кавычках (возможно, с префиксом сети, указанным через слеш). Если префикс сети не указан, то подразумевается /32. Пустая строка "" означает специальное значение undefined

Поддерживаемые операции сравнения для переменных типа string:

Операция	Комментарий
string_var == STRING	Переменная совпадает со строкой
string_var != STRING	Переменная не совпадает со строкой
string_var ~ REGEX	Переменная содержит подстроку, которая проверяется на совпадение с регулярным выражением (используется метод *search*)
string_var == file:FILE_NAME	Переменная совпадает хотя бы с одной строкой из указанного файла
string_var ~ file:FILE_NAME	Переменная соответствует хотя бы одному регулярному выражению из указанного файла

Операции == и ~ для строк регистронезависимы.

Поддерживаемые операции сравнения для переменных типа cidr:

Операция	Комментарий
cidr_var <<= CIDR	IP-адрес входит в сеть указанного диапазона
cidr_var <<= file:FILE_NAME	IP-адрес входит хотя бы в одну из сетей, перечисленных в указанном файле

Если для операции <<= оба аргумента имеют значение undefined, то результатом операции считается true. Если же только один из аргументов имеет значение undefined, то результат этой операции – false.

Поддерживаемые операции сравнения для переменных типа `time`:

Операция	Комментарий

`time_var > TIME`
`time_var >= TIME`
`time_var < TIME`
`time_var <= TIME`
	Сравнение времени

Каждая операция сравнения имеет определенный приоритет относительно других операций. В порядке убывания приоритета операции сравнения распределяются следующим образом:

1. `!` («логическое НЕ», «NOT»)
2. `<` («меньше»), `<=` («меньше или равно»), `>` («больше»), `>=` («больше или равно»)
3. `==` («совпадает»), `!=` («не совпадает»), `~` («соответствует»), `<<=` («входит в группу»)
4. `&&` («логическое И», «AND»)
5. `||` («логическое ИЛИ», «OR»)

Операции, перечисленные в одной строке, имеют одинаковый приоритет и вычисляются слева направо.

Для некоторых операций возможно чтение массива значений из файла (с указанием префикса `file:`). Строки, начинающиеся с символов «`#`» или «`;`», а также пустые строки пропускаются при чтении значений.

Содержимое файла `file:FILE_NAME` читается при обработке конфигурационного файла. Соответственно, при изменении содержимого файла со значениями или пути к нему необходимо перечитать конфигурацию Dr.Web ICAPD, например, послав ему сигнал `SIGHUP`.

Макросы

Макросы можно использовать в любых логических выражениях, но каждый макрос должен быть определен перед использованием. Макросы определяются в секции **Определения** раздела **Фильтрация**. Объявление макросов должно предваряться строкой `[def]`.

Синтаксис определения макроса:

```
macro_name = { BOOL_EXPR }
```

Где `BOOL_EXPR` – логическое выражение.

Все макросы возвращают логическое значение, аргументы не поддерживаются. По сути, макрос – это просто сокращенная запись логического выражения.

Пример:

Определяем макросы `is_localhost` и `local_ip`: данные макросы будут иметь значение `true`, если запрос пришел с одного из указанных IP-адресов или с одного из IP-адресов, перечисленных в файле.

```
[def]
is_localhost = { request_ip <<= "127.0.0.0/8" }

local_ip = {
     request_ip <<= "127.0.0.0/8"
     || request_ip <<= "192.168.0.0/16"
     || request_ip <<= "172.16.0.0/12"
     || request_ip <<= file:"/tmp/icapd/other_local_ips.txt"
}
```

Определяем макрос `worktime()`: он будет иметь значение `true`, если текущее системное время попало в промежуток от 9:30 до 13:00 и от 14:00 до 18:15.

```
[def]
worktime = {
 (system_time>="9:30" && system_time<="13:00")
 ||
 (system_time>="14:00" && system_time<"18:15")
}
```

Правила доступа

Правила доступа определяются в секции **Правила** раздела **Фильтрация**. Объявление правил должно предваряться строкой `[match]`.

При задании правил используются специальные операторы `if`.

Синтаксис оператора `if`:

```
if BOOL_EXPR {
     блок_конфигурации
}
```

Где `BOOL_EXPR` – логическое выражение, а `блок_конфигурации` – список параметров, которым присвоены новые значения, отличные от глобальных значений, указанных на странице **Фильтрация** (раздел **Содержание**).

Примеры

Если требуется заблокировать доступ к интернет-ресурсам из списков **Adult** и **Email** в рабочее время для пользователей из локальной сети, а также для пользователей с определенного IP-адреса, то можно использовать следующее правило:

```
[match]
if (local_ip() ||
    request_ip <<= "87.249.57.20") &&
    worktime()
{
  BlockAdult = yes
  BlockEmail = yes
}
```

Если требуется заблокировать доступ к интернет-ресурсам из списка **Terrorism** в ночное время (с 23:00 до 8:00) для пользователей с определенных IP-адресов, то можно задать следующее правило:

```
[match]
if (request_ip <<= "93.185.182.46" ||
    request_ip <<= "195.98.93.66") &&
    (system_time>="23:00" ||
    system_time<="8:00")
{
  BlockTerrorism = yes
}
```

Чтобы запретить пользователю `"edx"` доступ к сети Интернет в нерабочее время:

```
[match]
if request_username=="edx" && !worktime()
{
  BlockAll = yes
}
```

Обратите внимание, что макросы `local_ip()` и `worktime()`, используемые в примерах, должны быть предварительно определены.

Чтобы запретить доступ к конкретному интернет-ресурсу всем пользователям, чьи имена удовлетворяют регулярному выражению `"vasya.*"`, либо удовлетворяют любому из регулярных выражений, перечисленных в файле, либо совпадают с одной из строк в файле, используйте следующее правило:

```
[match]
if (request_username ~ "vasya.*" ||
 request_username ~ file:"/tmp/icapd/users_re_block.txt"
 || request_username == file:"/tmp/icapd/users_block.txt")
 && (request_url == "http://example.com/mega_music.mp3")
```

```
{
  BlockAll = yes
}
```

Обратите внимание, что установка в правиле `BlockAll` в `No` не означает, что в результате срабатывания условия будет обеспечен беспрепятственный доступ к запрошенному ресурсу. В этом случае доступ к ресурсу разрешается, если он попадает в пользовательский белый разрешающий список или не попадает в активные черные списки (как в блокируемые категории, так и в пользовательский черный список). Управление блокировкой категорий, а также пользовательскими черными и белыми списками производится на странице **Фильтрация**.

В случае если в обычном режиме доступ к ресурсам из некоторых тематических списков запрещен, но нужно разрешить доступ к некоторому ресурсу, следует создать соответствующее разрешающее правило.

Например, пусть требуется разрешить посещать ресурс `socialnetwork.com` пользователям, IP-адреса которых принадлежат подсети `192.168.1.1/32`, не смотря на то, что он относится к блокируемым тематическим спискам **SocialNetworks** и **Chats**:

```
if (request_ip <<= "192.168.1.1/32") && (request_url ~
"socialnetwork.com")
{
  BlockSocialNetwork = no
  BlockChats = no
}
```

Данное правило разрешает доступ к ресурсам, находящимся в тематических списках **SocialNetworks** и **Chats**, только в том случае, если:

- IP-адрес запросившего доступ клиента относится к подсети `192.168.1.1/32`;
- URL, запрошенный клиентом, содержит подстроку `socialnetwork.com`.

Во всех остальных случаях применяются глобальные настройки блокировки, указанные на странице **Фильтрация** (раздел **Содержание**). Обратите внимание, что если ресурс принадлежит более чем одному списку, то чтобы обеспечить к нему доступ, следует отключить блокировку для всех категорий, которым он принадлежит.

Настройка прокси-сервера

Для получения возможности использовать переменные `request_username` и `request_ip` необходима дополнительная настройка прокси-сервера **Squid**. Для этого требуется отредактировать его конфигурационный файл (обычно это файл `/usr/local/squid/etc/squid.conf`).

Если нижеприведенные строки уже есть в конфигурационном файле, то нужно раскомментировать их и исправить значения по умолчанию в случае необходимости. В противном случае нужно добавить данные настройки в конец файла.

Для использования переменной request_ip:

```
# request_ip
icap_send_client_ip on
```

Для использования переменной request_username:

```
# request_username
icap_send_client_username on
icap_client_username_header X-Client-Username
icap_client_username_encode off
```

Приложение В. 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:

- ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.ru/doc/;
- прочитайте раздел часто задаваемых вопросов по адресу http://support.drweb.ru/show_faq/;
- посетите форумы компании «Доктор Веб» по адресу http://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»:

- заполните веб-форму в соответствующей секции раздела http://support.drweb.ru/;
- напишите электронное письмо по адресу support@drweb.com;
- 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 http://company.drweb.ru/contacts/offices/.