Dr.WEB®

Dr.Web Mail Gateway

Максимальное качество фильтрации почтового трафика

Внесен в «Единый реестр российских программ для электронных вычислительных машин и баз данных»

Dr.WEB®
Dr.Web Mail Gateway

Преимущества

- Проверка почтовых сообщений без каких-либо ограничений со стороны почтового сервера, использование технологий анализа сообщений (в том числе Reputation IP Filter), невозможных в случае установки системы анализа трафика на почтовом сервере. Только на уровне почтового шлюза возможны:
  - Активная защита от пассивных и активных атак. Вредоносное письмо можно определить не только по характеру письма, но и по параметрам SMTP-сессии такого письма.
  - Определение подлинности адресов отправителей и получателей.
  - Анализ признаков принадлежности к спаму на основе анализа SMTP-сессии.
  - Защита от замаскированного спама благодаря функции проверки подлинности IP-адреса.
  - Защита от некорректно составленных (malformed) писем путем проверки параметров SMTP-сессии на корректность.
  - Защита от спам-ловушек.
  - Ограничение Open Relays серверов.
  - Экономия интернет-трафика не только за счет ограничения размера вложений, но и за счет возможности анализа писем при их частичном приеме.
- Отсутствие необходимости обучения антиспама.
- Увеличение стабильности работы локальной сети и снижение нагрузки на почтовые серверы и рабочие станции — возможность их нормальной работы в случае увеличения количества вредоносных сообщений.
- Проверка почтового трафика в несколько потоков. Наличие системы динамической оптимизации количества используемых потоков проверки.
- Наличие системы динамической балансировки нагрузки, в том числе при использовании кластера.
- Снижение суммарной стоимости лицензий, необходимых для организации.

Ключевые функции

- Проверка почтовой корреспонденции по протоколам SMTP/LMTP/POP3/POP3S/IMAP4 на наличие спама, вирусов и нежелательной корреспонденции.
- Защита от спам-рассылок.
- Гарантированная доставка сообщений — даже если пользователь недоступен в течение длительного времени и не может получать письма, они не будут удаляться.
- Фильтрация трафика в соответствии с белыми и черными списками адресов.
- Аутентификация отправителей.
- Архивация всех проходящих сообщений.
- Гибкая настройка с помощью правил произвольной сложности — не только для различных пользователей и групп, но и фактически для каждого письма, что позволяет обрабатывать всю входящую и исходящую почту в соответствии с корпоративными стандартами, контролировать соблюдение правил переписки.
- Фильтрация элементов сообщений по ключевым словам, фразам или шаблонам.
- Управление через веб-интерфейс из любой точки мира.
- Модификация обрабатываемых сообщений в соответствии с настройками.
- Автоподпись проверенных почтовых сообщений.
- Статистика, учитывающая все аспекты работы системы.
- Защита работы собственных модулей от сбоев.

Dr.Web Mail Gateway — это:

Соответствие требованиям российского законодательства. Dr.Web Mail Gateway обладает сертификатами соответствия ФСТЭК России и ФСБ России, что позволяет использовать продукт в организациях, требующих повышенного уровня безопасности, в том числе в составе подсистемы антивирусной защиты информационных системах персональных данных (ИСПДн) 1-го уровня защищенности персональных данных, а также систем, содержащих документы с уровнем «Совершенно секретно».

Защита конфиденциальной информации. Продукт позволяет восстанавливать сообщения, случайно удаленные пользователями из своих почтовых ящиков, а также проводить расследования, связанные с утечкой информации.

Открытость. Dr.Web Mail Gateway может интегрироваться в решения других производителей, а благодаря открытому API в него можно добавить новые функциональные возможности.

Лицензирование

Виды лицензий

- По числу защищаемых пользователей.
- Посерверная лицензия — для проверки неограниченного объема трафика на одном сервере, с числом защищаемых пользователей не более 3 000.

Поддерживаемые ОС

- Дистрибутивы Linux, имеющие версию ядра 2.4.x и выше
- FreeBSD версии 6.x и выше для платформы Intel x86 и amd64
- Solaris версии 10 для платформы Intel x86 и amd64

Базовая лицензия компоненты Dr.Web	Дополнительные		
Антивирус	Антиспам	SMTP proxy	Центр управления (лицензируется бесплатно)

Функционал	Управление в ЦУ
Обработка почтовых протоколов POP3/SMTP/IMAP4	✓
Обработка защищенных почтовых протоколов	✓
Возможность установки в качестве Proxy	✓
Возможность использования в режиме прозрачного прокси	✓
Возможность интеграции в почтовые системы	✓
Интеграция с Active Directory/OpenLDAP	✓
Наличие в продукте антивирусного сканера	✓
Антиспам-проверка трафика	✓
Блокировка по типам файлов, в том числе внутри архивов	✓
Антивирусная проверка трафика	✓
Фильтрация по заголовкам с использованием правил	✓
Модификация сообщения согласно правилам	✓
Фильтрация DoS-трафика	✓
Запрет передачи незашифрованных данных	✓
Гарантированная доставка всех почтовых сообщений	✓
Работа с несколькими почтовыми системами с различными настройками	✓
Установка и обновления	
Синхронная и асинхронная обработка сообщений	✓
Установка модулей обработки сообщений в начало и конец очереди обработки	✓
Обновления по требованию	✓
Автоматические обновления	✓
Настройка расписания обновлений	✓
Альтернативные источники обновлений	✓
Обновления из Интернета/локальной сети	✓
Импорт настроек предыдущих версий	✓
Откат настроек	✓
Гибкость при выборе политик информационной безопасности	
Многоуровневая система определения спама (спам / возможно спам)	✓
Отсутствие необходимости обучения антиспама, в том числе через клиентов у пользователей	✓
Проверка имен доменов и IP-адресов отправителей по внешним черным спискам	✓
Проверка на вхождение отправителя в список защищаемых доменов	✓
Проверка доменного имени отправителя, наличия и соответствия DNS A- и MX-записей хостам и IP-адресам отправителя и получателя	✓
Выбор защищаемых адресов	✓
Использование черных и белых списков сетей	✓
Использование черных и белых списков доменов	✓
Списки спам-ловушек	✓

Возможность помещать письма в карантин	✓
Ограничение максимального количества пересылок, числа соединений с одним IP-адресом	✓
Ограничение по максимальному размеру письма	✓
Ограничение по максимальному размеру писем, принятых за одну сессию	✓
Поддержка различных типов доставки сообщений	✓
Запрет изменения тела сообщения	✓
Ограничение по максимальному количеству писем с одного адреса	✓
Ограничение максимального количества соединений	✓
Ограничение времени обработки сообщения и его частей	✓
Проверка заголовков на соответствие спецификации RFC-822	✓
Анализ заголовков и тела по формальным признакам	✓
Авторизация пользователя с помощью имени и пароля, IP-адреса	✓
Создание правил фильтрации	✓
Фильтрация элементов сообщений по ключевым словам, фразам или шаблонам	✓
Фильтрация данных по размеру, типам вложений, имени файла	✓
Настройка дополнительных признаков фильтрации, в том числе для писем, не адресованных получателю, пустых, имеющих ссылки на изображения, содержащих скрипты	✓
Архивирование и регистрация сообщений	✓
Использование внешних баз данных	✓
Возможность помечать и модифицировать письма	✓
Наличие возможности проверки и установки электронно-цифровой подписи, шифрования	✓
Возможность пересылать на определенный адрес или адреса	✓
Выбор действия над сообщением	✓
Обнаружение и удаление вредоносных объектов	
Обнаружение и удаление вредоносных программы любых типов, в том числе внутри сжатых/архивных файлов	✓
Обнаружение неизвестных вирусов	✓
Обнаружение и удаления вирусов, скрытых под неизвестными упаковщиками	✓
Ограничение размера проверяемого файла	✓
Выбор действий для зараженных, подозрительных объектов и объектов другого типа	✓
Выбор защищаемых адресов	✓
Выбор действий для зараженных архивов	✓
Ограничения степени сжатия файла в архиве, размера распакованного файла, подлежащего проверке	✓
Отчеты и статистикиа	
Возможность помещать письма в карантин	✓
Ограничение максимального количества пересылок, числа соединений с одним IP-адресом	✓
Ограничение по максимальному размеру письма	✓
Ограничение по максимальному размеру писем, принятых за одну сессию	✓
Накопление статистики о работе системы	✓

Настройка степени детализации статистики	✓
Возможность регистрации времени события, объекта проверки и типа воздействия	✓
Генерация отчетов	✓
Изменение уровней детализации отчетов	✓
Настройка времени и периодичности отправки отчетов	✓
Оповещение администраторов и пользователей об угрозах различного типа	
Отсылка уведомлений администратору	✓
Использование шаблонов уведомлений	✓
Редактирование шаблонов уведомлений	✓
Использование управляющих писем	✓
Оповещение администраторов и пользователей об угрозах различного типа	
Локализованная версия программы	✓
Руководство по эксплуатации на русском языке	✓
Техническая поддержка на русском языке	✓

ООО «Доктор Веб»

«Доктор Веб» — российский разработчик средств информационной безопасности.
Антивирусные продукты Dr.Web разрабатываются с 1992 года.

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а

Телефон: +7 495 789–45–87 (многоканальный), факс: +7 495 789–45–97

антивирус.рф | www.drweb.ru | www.av-desk.com | http://free.drweb.ru