Dr.WEB®
с 1992 года

Фильтрация почтового трафика при использовании компанией внешних почтовых сервисов

Фильтрация почтового трафика при использовании компанией внешних почтовых сервисов

Достаточно часто встречаются случаи, когда в компании наряду с корпоративной почтой используется внешний почтовый сервис (gmail.com, mail.ru, yandex.ru и др.). Бывает и так, что компания полностью отказывается от использования своего почтового сервиса, переходя на аренду почты.

При этом в обоих случаях бывает, что безопасность внешней почты не контролируется никак. Например, пользователи получают и отправляют почтовые сообщения с личных устройств и компьютеров, на которых не установлены средства защиты, в результате чего злоумышленники могут начать внедрение в компанию именно с таких незащищенных машин.

Сделать это они могут, перехватив почтовый канал благодаря ошибкам в настройке или имеющимся уязвимостям, либо еще проще — подготовив вредоносную программу, не распознаваемую антивирусом почтового сервиса.

Если компания хочет быть уверена, что с адресов ее сотрудников ее клиентам или партнерам не уйдет спам или троянец, то защищаться нужно. Даже тогда, когда собственного почтового сервера нет. Вариантов защиты почты может быть два. Можно установить каждому сотруднику на каждое его устройство антивирус. Как показывает практика, это почти нереально. Или можно пропускать почтовый трафик через так называемый почтовый шлюз — специальный антивирус, пропускающий через себя почтовый трафик всей компании. Для этого мы рекомендуем использовать Dr.Web для почтовых серверов Unix, настроенный на проверку так называемого транзитного трафика.

Напомним также, что компании, защищающие данные граждан России, обязаны использовать сертифицированные антивирусные продукты. Также сертифицированные продукты должны использоваться для защиты ГИС, систем обработки сведений, содержащих гостайну, объектов КИИ. Dr.Web для почтовых серверов Unix сертифицирован по требованиям ФСТЭК России и ФСБ России, а также иных организаций и может быть использован для защиты персональных данных, конфиденциальной и секретной информации.

Возможности Dr.Web для почтовых серверов Unix позволяют организовать антивирусную и антиспам-проверку почтовой корреспонденции компонентом Dr.Web Firewall для Linux. В случае использования этого компонента, осуществляющего прозрачный перехват почтового трафика, все данные проверяются с помощью другого компонента Dr.Web для почтовых серверов Unix — сетевого монитора SpIDer Gate.

Для настройки Dr.Web Firewall для Linux может использоваться как специальная утилита управления Dr.Web Ctl, так и веб-интерфейс управления Dr.Web для почтовых серверов UNIX.

Чтобы настроить режим «прозрачного» прокси, измените значение ряда параметров, находящихся в конфигурационном файле, в секции настроек Dr.Web Firewall для Linux (секция [LinuxFirewall]):

Параметр	Требуемое значение
InspectSmtp	▪ On, если требуется перехватывать данные, передаваемые по протоколу SMTP (*передача данных между MUA и MTA или между MTA и MTA*). ▪ Off, если не требуется перехватывать данные, передаваемые по протоколу SMTP.
InspectPop3	▪ On, если требуется перехватывать данные, передаваемые по протоколу POP3 (*передача данных между MUA и MDA*). ▪ Off, если не требуется перехватывать данные, передаваемые по протоколу POP3.
InspectImap	▪ On, если требуется перехватывать данные, передаваемые по протоколу IMAP (*передача данных между MUA и MDA*). ▪ Off, если не требуется перехватывать данные, передаваемые по протоколу IMAP.
AutoconfigureIptables	Yes
AutoconfigureRouting	Yes
LocalDeliveryMark	Auto
ClientPacketsMark	Auto
ServerPacketsMark	Auto
TproxyListenAddress	127.0.0.1:0 *Если для работы Dr.Web Firewall для Linux используется особый IP-адрес или порт, укажите их здесь.*
OutputDivertEnable	▪ Yes, если требуется перехватывать исходящие соединения (т. е. соединения, инициированные на данном узле, — например, соединения инициированные MTA). ▪ No, если не требуется перехватывать исходящие соединения.
OutputDivertNfqueueNumber	Auto

Параметр	Требуемое значение
OutputDivertConnectTransparently	No
InputDivertEnable	▪ Yes, если требуется перехватывать входящие соединения (т. е. соединения, инициированные на удаленном узле, серверной стороной которых является приложение, работающее на данном узле, например MTA). ▪ No, если не требуется перехватывать входящие соединения.
InputDivertNfqueueNumber	Auto
InputDivertConnectTransparently	Yes

Чтобы обеспечить встраивание Dr.Web для почтовых серверов UNIX в каналы передачи электронной почты, использующие безопасное соединение SSL/TLS, дополнительно необходимо:

- Включить проверку трафика, передаваемого через SSL/TLS, установив значение соответствующего параметра и выполнив команду:

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

  Рекомендуется использовать команду cfset утилиты **drweb-ctl** *или веб-интерфейс управления, т. к. в этом случае также будут автоматически изменены правила проверки, зависящие от данного параметра.*
- Экспортировать сертификат, который будет использован Dr.Web для почтовых серверов UNIX для встраивания в защищенные каналы SSL/TLS, выполнив команду (необходимо указать имя файла, в который будет сохранен сертификат в формате PEM):

  $ **drweb-ctl** certificate > <*cert_name*>.pem
- Добавить полученный сертификат в системный перечень доверенных сертификатов и, возможно, прописать его в качестве доверенного у клиентов и сервера электронной почты.

После внесения изменений в настройки следует перезапустить Dr.Web для почтовых серверов UNIX (используйте команду **drweb-ctl** reload).

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

- Утилитой управления из командной строки Dr.Web Ctl (используйте команды **drweb-ctl** cfshow и **drweb-ctl** cfset).
- Веб-интерфейсом управления Dr.Web для почтовых серверов UNIX (по умолчанию доступ через браузер по адресу https://127.0.0.1:4443).

Подробная пошаговая инструкция по настройке Dr.Web для почтовых серверов Unix изложена в документации по продукту.

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Все права на технологии Dr.Web принадлежат компании «Доктор Веб». «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ, имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки, которые расположены в России.

Компания «Доктор Веб» — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. Свой выбор в пользу продуктов Dr.Web сделали Государственная Дума Федерального Собрания РФ, ЦИК России, Минобороны России, Верховный Суд РФ, Совет Федерации Федерального Собрания РФ, Центральный банк Российской Федерации, многие другие государственные учреждения и крупнейшие компании.

Вот только некоторые клиенты Dr.Web: https://customers.drweb.com.

Dr.Web внесен в «Единый реестр российских программ для электронных вычислительных машин и баз данных» **Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.**

Использование отечественного антивирусного ПО Dr.Web обеспечивает нашим клиентам защиту от рисков, связанных с изменением международной обстановки, таких как отказ в использовании, продлении, поставке или получении обновлений, а также от угроз, созданных для целенаправленных атак на предприятия и граждан России.

Со знаком качества

«Доктор Веб» имеет сертификаты, позволяющие использовать ПО Dr.Web в организациях с повышенными требованиями к уровню безопасности.

Dr.Web сертифицирован на отсутствие недекларированных возможностей – по 2 уровню контроля, на соответствие требованиям документа «Требования к средствам антивирусной защиты», утв. приказом ФСТЭК России № 28 от 20.03.2012 г., на соответствие требованиям ФСБ России к антивирусным средствам.

Продукты Dr.Web применяются для защиты информации, содержащейся в различных информационных системах, в том числе информации ограниченного доступа (государственная тайна, персональные данные и т. д.).

Использование ПО Dr.Web позволяет обеспечить надлежащее выполнение требований норм законодательства РФ о применении мер для защиты:

– информации с ограниченным доступом (государственная тайна, персональные данные и т. д.);

– отдельных категорий граждан от информации, причиняющей вред.

Сертификаты ФСТЭК России	**Сертификаты Минобороны России**	**Сертификаты ФСБ России**	**Все сертификаты и товарные знаки**

Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Тел.: +7 495 789–45–87 (многоканальный)
Факс: +7 495 789–45–97

https://антивирус.рф | https://www.drweb.ru | https://curenet.drweb.ru | https://free.drweb.ru