Kaspersky®
Secure Mail
Gateway

Виртуальное устройство безопасности для почтовых серверов

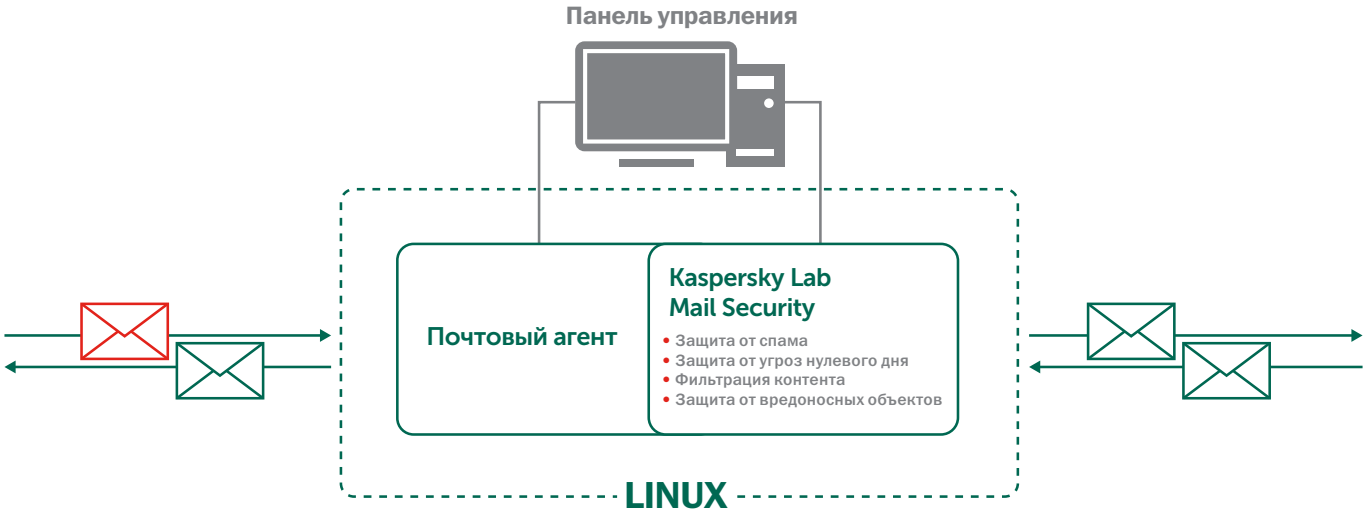
Kaspersky Secure Mail Gateway – это комплексное, интегрированное решение, которое обеспечивает всестороннюю защиту входящего и исходящего почтового трафика от вредоносного ПО, спама, фишинга и атак нулевого дня.

Решение представляет собой виртуальное устройство безопасности, которое может быть интегрировано в почтовую систему в качестве почтового шлюза и поставляется в предустановленном виде вместе с серверной версией операционной системы Linux, решением Kaspersky Secure для Linux Mail Server и почтовым агентом. Продукт крайне просто устанавливается и развертывается: все, что вам нужно сделать, – это настроить решение, используя удобный веб-интерфейс. Для тонкой настройки администраторы имеют возможность управлять решением из командной строки. Kaspersky Secure Mail Gateway предназначен для работы на гипервизоре VMware ESXi.

Почему именно виртуальное устройство?

Снижение затрат на оборудование, простота управления и повышенная отказоустойчивость – вот лишь несколько причин, по которым руководители IT-служб выбирают решения с использованием виртуальных устройств. Kaspersky Secure Mail Gateway уже включает все, что вам необходимо, – это устраняет проблемы программной совместимости, значительно упрощает развертывание и выполнение других сложных задач.

Решение позволяет администраторам управлять всеми аспектами защиты корпоративной почты из единой консоли. Удобство и простота использования продукта позволяют специалистам с небольшим опытом работы в Linux развернуть и эффективно применять мощное решение для защиты почты, в том числе в условиях ограниченных IT-ресурсов компании.



Основные функции

- Единый веб-интерфейс решения позволяет управлять не только защитой почты, но также основными настройками ОС и параметрами почтовой системы.
- Интеграция Kaspersky Security для Linux Mail Server с почтовым агентом позволяет виртуальному устройству функционировать как выделенный почтовый шлюз.
- Простое развертывание и интеграция в существующую почтовую инфраструктуру компании.

Защита от спама

- Сервис принудительного обновления антиспам-баз
- Технология облачной репутационной фильтрации
- Политики для блокирования массовых рассылок

Улучшенная фильтрация почтового трафика

- **Облачная защита от фишинга**: использование облачной базы данных «Лаборатории Касперского» для блокирования сообщений, содержащих ссылки на фишинговые сайты.
- **Фильтрация почтовых вложений** по имени файла, типу, размеру сообщений или в соответствии с набором предустановленных правил или правил, заданных администратором.
- **Помещение в хранилище карантина** зараженных, подозрительных, защищенных паролем и нечитаемых файлов с возможностью настройки уведомлений администратору.
- **Глобальные черные и белые списки**: поддержка правил обработки писем с использованием форматов IPv4, IPv6, шаблонов и регулярных выражений.
- **Создание пользовательских черных и белых списков** отправителей с доступом к собственному карантину через веб-интерфейс.
- **Поддержка технологий аутентификации сообщений** (SPF/DKIM/DMARC) для защиты почтового трафика организаций от спама и других нежелательных сообщений.

Многоуровневая защита от вредоносного ПО

- **Проверка входящего и исходящего SMTP-трафика** на наличие вредоносного ПО с использованием новейшей версии антивирусного ядра «Лаборатории Касперского». Актуальные обновления, поступающие в режиме реального времени напрямую из облачной базы данных «Лаборатории Касперского».
- **Предотвращение атак** с помощью специального модуля защиты от таргетированных атак, в том числе атак с использованием эксплойтов нулевого дня.
- **Фильтр вредоносных URL-адресов**, использующий обновления в режиме реального времени напрямую из облачной базы данных «Лаборатории Касперского»; блокирование сообщений, содержащих ссылки на вредоносные сайты.

Простое, гибкое управление и не только

- **Обработка почтового трафика** на основе правил для групп отправителей и получателей.
- **Поддержка openLDAP и Microsoft Active Directory.** Соединение с LDAP-сервером может быть зашифровано с использованием протокола TLS/SSL.
- **Удобная система уведомлений, отчетов и детализированных журналов**; отчеты в формате PDF по требованию заказчика.
- **Интеграция с Kaspersky Security Center** для осуществления централизованного мониторинга состояния системы защиты.
- **Ролевое разграничение доступа**. Возможность создания роли с ограниченным доступом – для сотрудников, занимающихся поддержкой клиентов.
- **Создание защищенных TLS-соединений** для безопасного обмена почтовыми сообщениями между организациями, а также для управления сертификатами.

www.kaspersky.ru

#ИстиннаяБезопасность

Как приобрести

Kaspersky Secure Mail Gateway можно приобрести в составе следующих продуктов:

- Kaspersky Total Security для бизнеса
- Kaspersky Security для почтовых серверов