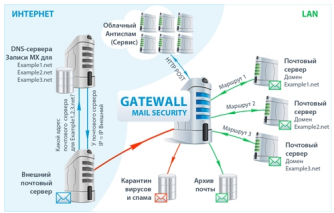
GateWall Mail Security для Exchange Server/SMTP/Lotus – это решение для **защиты корпоративной почты**
от вирусов, фишинга, спама и прочих вредоносных сообщений, позволяющее также предотвращать утечки
конфиденциальной информации
. Продукт обеспечивает
архивацию сообщений
, предоставляет возможность
мониторинга почты
, поддерживает
синхронизацию по IMAP
с MS Exchange 2003 и Lotus Domino, а также может работать с любыми другими почтовыми серверами.

Благодаря модульной структуре GateWall Mail Security обладает крайне высокой производительностью и отказоустойчивостью. «Облачные» модули фильтрации вирусов и спама, обеспечивают фильтрацию спама и защиту от вирусов с крайне быстрым временем реакции на новые угрозы (Zero-Hour Protection) и практически нулевым ложным срабатыванием.



Защита от утечек персональных данных и иной конфиденциальной информации

GateWall Mail Security оснащен модулем защиты от потери данных (иначе DLP - Data Loss Protection), предотвращающим утечки конфиденциальной или другой нежелательной информации, а также проникновение ее извне.

В зависимости от настроек система позволяет Блокировать, Задерживать сообщения, или Оповещать инженера безопасности об отсылке подозрительного письма. DLP-модуль позволяет определять все зашифрованные сообщения и определять, какие действия должны к ним применяться.

В GateWall Mail Security используется три типа фильтрации: Регулярные выражения (Regexp), Сравнение документов (Docmatch) и Лемматизатор (Lemmatizer). Каждый из них посредством разных способов поиска информации в теле, теме, вложениях и других частях письма, исследует почтовые сообщения на наличие в них определенных ключевых слов или фраз и проводит сравнение передаваемых данных с образцами конфиденциальной информации.

Преимущества облачного решения

При использовании Entensys Zero-Hour не требуется установки громоздкого приложения, затрачивающего для нормальной работы значительную часть ресурсов сервера. Быстродействие облачного антивируса, встроенного в Gatewall Mail Security, зависит лишь от загруженности внешнего канала, т. е от скорости подключения к сети Интернет.

Раннее обнаружение вирусов

Современные вирусы, черви и трояны используют различные слабости антивирусных технологий: основной проблемой является время, необходимое для создания сигнатур или эвристики. Entensys Zero-Hour™ обеспечивает самое раннее обнаружение новых эпидемий.

Entensys постоянно мониторит Интернет и выявляет массовые вспышки вирусных эпидемий, как только они появляются. Использование сотен серверов (honeypots) по всему миру позволяет распознавать как спам, так и вирусы. Решение Entensys Zero-Hour

не основано только лишь на применении сигнатур, как во многих других антивирусах.

Entensys Zero-Hour обеспечивает проактивное обнаружения вирусов, которое позволяет начинать борьбу с новым вирусом до того момента, как он поразит миллионы компьютеров.

Фильтрация по содержимому письма

"Облачный" антиспам отфильтровывает письма, основываясь на анализе их содержания и эвристике. Технология Entensys позволяет анализировать спам-сообщения на любых языках, а также графические сообщения. Центр обнаружения спама выявляет спамерские атаки в любой точке мира.

Низкий уровень ложных срабатываний

Одним из важных достоинств "облачного" антиспама является крайне низкий уровень ложного срабатывания - менее, чем одно на 1,5 миллиона сообщений. При этом уровень детекции спама составляет более 97%. Традиционный метод блокировки спама на основе черных списков IP и DNS обладает несравненно более высоким уровнем ложного срабатывания. Объяснить это можно тем, что в черные списки часто попадают нормальные пользователи. Достаточно того, чтобы какой-либо компьютер из локальной сети был скомпрометирован и использовался для рассылки спама.

Клиент отправляет "облачному" сервису UID письма, который позволяет определить, является ли почтовое сообщение спамом. Решение блокирует не IP-адрес, домен или электронный адрес, а конкретное письмо или атаку спама.

Таким образом "облачный" антиспам может использоваться в организациях, в которых ошибочное удаление писем может приводить к потере клиентов или другим проблемам.

Дополнительные методы защиты от спама

В обработке входящих сообщений в GateWall Mail Security фильтрация выполняется в несколько этапов - по соединениям, по адресу источника, по адресу назначения и по содержанию. В дополнению к "облачному" антиспаму, не требующему настройки со стороны пользователя, GateWall Mail Security поддерживает следующие дополнительные методы фильтрации:

- на основе DNS (DNSBL, RHSBL, Backscatter, MX, SPF, SURBL);
- на основе распределенной антиспам системы ("облачный" антиспам);
- на основе статистики (собственная реализация фильтрации Байеса).

Кроме этого решение поддерживает контроль SMTP протокола (контроль правильности команд в соответствии с RFC), ограничивает максимальный размер письма, максимальное количество получателей и т.п.

Интеграция с IMAP

В решении от Entensys реализована интеграция с IMAP-сервером MS Exchange или Lotus Domino. Интеграция предоставляет возможность создания общей папки IMAP на удаленном почтовом сервере и обработку сообщений в этих папках.

Архивирование сообщений

В продукте реализовано копирование входящих сообщений. Копирование выполняется до антиспам и антивирусной фильтрации. В настройках архивирования можно выбрать направление (только входящие, только исходящие или оба), а также указать адреса

исключений.

Загрузчик почты

В GateWall Mail Security имеется возможность загружать почту с любых POP3-аккаунтов и распределять полученную почту по ящикам пользователей. Поддерживается загрузка с ящиков, на которые приходит почта для одного пользователя, а также сбор почты с ящика для многих пользователей, так называемые мультибоксы (multibox). Данная функция удобна для сбора личной и корпоративной почты с бесплатных ящиков (например, @mail.ru, @yandex.ru) и с других внешних серверов.

Мониторинг и статистика

GateWall Mail Security предоставляет информацию обо всех сообщениях, обработанных сервером решения. Мониторинг сообщений в GateWall Mail Security позволяет выполнять фильтрацию по дате, по статусу обработки (доставлено/заблокировано), по адресу источника или назначения, выполнять принудительную отправку сообщений, заблокированных как спам, а также создавать списки исключений.

Прочее

Продукт поддерживает посылку автоматических ответов, настройку правил по обработке почты. В решении реализована возможность менять приоритет обработки почтовых сообщений, управление сервисами доступно в веб-консоли, а в истории сообщений можно выбирать произвольный диапазон дат.

В GateWall Mail Security реализована система правил по работе с вложенными в почтовое сообщение файлами. Например, можно запретить открытие исполняемых файлов, тем самым, обезопасив систему от заражения троянами.