

Защита почтового трафика абонентов xSP от вирусов и спама

Описание решения

Москва 2008

Содержание

1	Маркетинговый анализ необходимости предоставления услуги	3
2	Описание предлагаемого продукта для антивирусной защиты почтового трафика и фильтрации спама	3
3	Техническая схема предоставления услуг	5
4	Коммерческая схема сотрудничества	6
5	Заключение	6

1 Маркетинговый анализ необходимости предоставления услуги

В настоящий момент на рынке ISP наблюдается устойчивая тенденция: предложение провайдерами своим абонентам широкой линейки сервисов в дополнение к базовой услуге доступа в Интернет. Сервисную услугу по предоставлению почтовых ящиков для абонентов можно рассматривать как одну из наиболее популярных в пакетах услуг, предлагаемых своим клиентам провайдерами.

При организации подобной услуги, защита предоставляемых почтовых ящиков как от вирусов, так и от спама является обязательной – незащищенный почтовый ящик резко снижает свою привлекательность для абонента.

Предоставление абонентам почтовых ящиков с установленными для них антивирусной защитой и фильтрацией спама и управляемыми самим провайдером, выгодно как провайдерам, так и абонентам. Провайдер при этом получает:

- Более защищенную от вирусов абонентскую сеть, снижение объемов вирусного трафика, уменьшение вероятности массовых атак с участием абонентов провайдера, решение проблем с зараженными компьютерами при подключении новых абонентов, снижения ущерба от простоя оборудования в результате вирусных атак.
- Дополнительное конкурентное преимущество (при этом важно, чтобы предлагаемое решение было популярно на рынке и имело высокий уровень детектирования вирусов и фильтрации спама).

Абонентам провайдера так же выгодно пользоваться подобным сервисом, поскольку они получают возможность безопасной работы в интернете.

Особенную актуальность данное решение имеет для провайдеров, предлагающих хостинг-услуги, поскольку предоставление клиенту одного или нескольких почтовых ящиков является фактически де-факто стандартом для пакетов хостинг-услуг.

2 Описание предлагаемого продукта для антивирусной защиты почтового трафика и фильтрации спама

Для антивирусной защиты почтового трафика и фильтрации спама в рамках предлагаемого решения могут быть использованы базовые приложения «Лаборатории Касперского» – Kaspersky Security Mail Gateway 5.6 или «связка» двух приложений Антивирус Касперского 5.6 для Linux Mail Servers и Kaspersky Anti-Spam 3.0.

Антивирус Касперского 5.6 для Linux Mail Server (далее называемый также Антивирус) обеспечивает антивирусную защиту почтового трафика и файловых систем серверов, работающих под управлением операционных систем Linux или FreeBSD и использующих почтовые системы sendmail, postfix, qmail или exim.

Приложение позволяет:

- Проверять входящие и исходящие почтовые сообщения на наличие угроз.

Антивирусная проверка почтового трафика и фильтрация спама для xSP

- Обнаруживать зараженные, подозрительные, защищенные паролем и недоступные для проверки объекты.
- Обезвреживать обнаруженные в файлах и почтовых сообщениях угрозы. Лечить зараженные объекты.
- Сохранять резервные копии сообщений перед их антивирусной обработкой и фильтрацией; восстанавливать сообщения из резервных копий.
- Обработать почтовые сообщения согласно правилам, заданным для групп отправителей и получателей.
- Выполнять фильтрацию почтовых сообщений по имени, типу и размеру вложений.
- Уведомлять отправителя, получателей и администратора об обнаружении сообщений, содержащих зараженные, подозрительные, защищенные паролем и недоступные для проверки объекты.
- Формировать статистику и отчеты о результатах работы.
- Обновлять базы антивируса с серверов обновлений «Лаборатории Касперского» по расписанию и по требованию.
- Настраивать параметры и управлять работой приложения как локально (стандартными средствами операционной системы с помощью параметров командной строки, сигналов и модификацией конфигурационного файла приложения), так и удаленно через веб-интерфейс.

Kaspersky Anti-Spam 3.0 (далее называемый также Антиспам) является программным комплексом, который осуществляет фильтрацию электронной почты с целью защиты пользователей почтовой системы от нежелательных массовых рассылок – спама.

На основании правил, заданных администратором, приложение обрабатывает сообщение, а именно: доставляет получателю в неизменном виде, блокирует, генерирует сообщение о невозможности приема письма, добавляет или изменяет заголовок, и выполняет другие действия, заданные администратором. Каждое почтовое сообщение проверяется на присутствие в нем признаков, характерных для нежелательных массовых рассылок.

Во-первых, проверяются различные параметры письма (фильтрация по формальным признакам):

- адреса отправителя и получателя (из envelope), размер письма, а также различные заголовки письма (включая заголовки From и To);
- адреса отправителя письма (e-mail и / или IP-адрес) с помощью «черных» и «белых» списков, наличие IP-адреса отправителя в выбранном списке сервисов DNS-based Real-Time Black List (DNSBL);
- наличие DNS-записи о сервере-отправителе (reverse DNS lookup);
- IP-адрес отправителя на соответствие списку разрешенных адресов для домена с помощью технологии Sender Policy Framework (SPF);
- адреса и ссылки на сайты, присутствующие в тексте письма проверяются с помощью сервиса Spam URI Realtime Blocklists (SURBL);

Во-вторых, используется контентная фильтрация, т. е. анализируется содержание самого письма (включая заголовок Subject) и файлов вложений. При этом применяются лингвистические алгоритмы, основанные на сравнении с письмами-образцами и на поиске характерных терминов (слов и словосочетаний).

Также Kaspersky Anti-Spam проводит проверку графических вложений, сравнивая их с сигнатурами известных спам-сообщений. Результаты этого сравнения также учитываются при принятии решения о принадлежности письма к спаму.

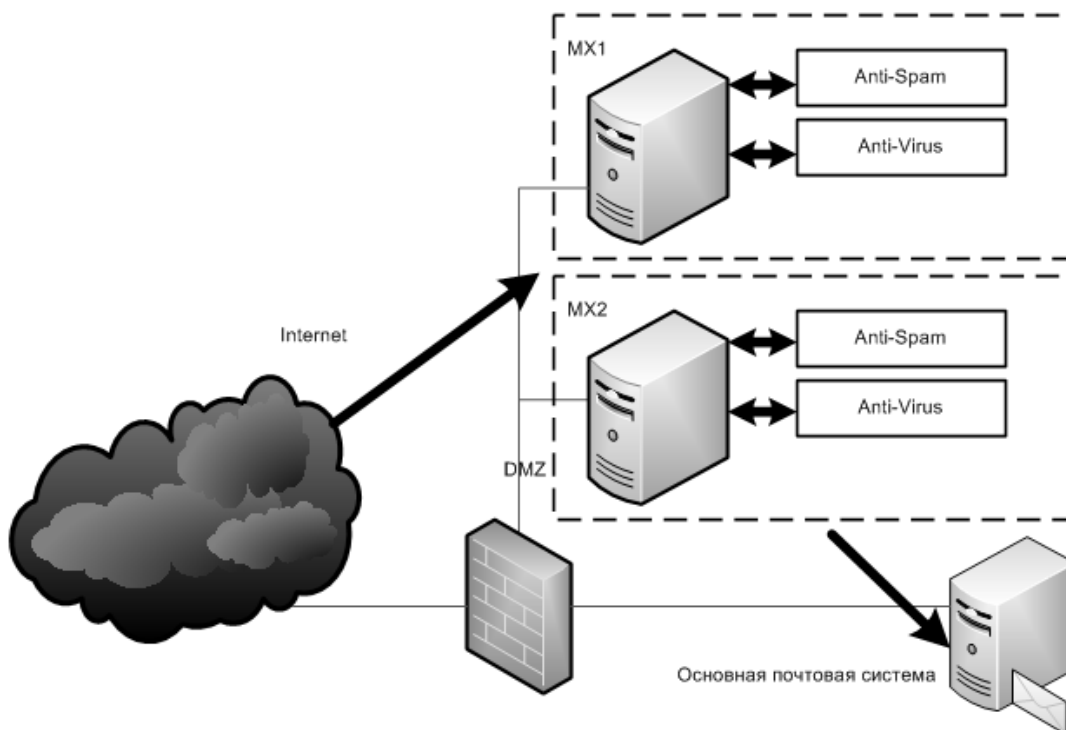
Приложение Kaspersky Mail Gateway 5.6 включает в себя как антивирусный фильтр, так и антиспам-ядро, по возможностям аналогичные предыдущим приложениям. Подробнее о нем см. ниже.

Решения «Лаборатории Касперского» обладают уникальным набором функций и возможностей, что позволяет достигать высокого уровня защиты пользователей.

3 Техническая схема предоставления услуг

Основные схемы развертывания

Конкретная схема развертывания Антивируса Касперского для проверки абонентского веб-трафика зависит как от логической структуры сети провайдера, так и от нагрузки на прокси-серверы, при помощи которых осуществляется предоставление услуг доступа в Интернет.



При типичной схеме развертывания, антивирусное ПО и ПО для фильтрации спама устанавливаются на существующие или специально выделенные почтовые сервера на базе sendmail, postfix, qmail или exim (рекомендуется postfix или exim), работающие под управлением операционных систем Linux или FreeBSD. Использование выделенных серверов – почтовых релейов для антивирусной проверки почтового трафика и фильтрации спама обязательно в том случае, если почтовые сервера провайдера построены с использованием других почтовых систем или ОС, и рекомендуется в остальных случаях. Это дает возможность гибко и оперативно изменять логические потоки прохождения почты и проводить регламентные работы на почтовых релейах. Из тех же соображений рекомендуется использование минимум двух почтовых серверов с установленным антивирусом и антиспамом, даже если требования по нагрузочной способности (см. ниже) позволяют обойтись только одним физическим сервером.

Другой возможной конфигурацией развертывания является установка антивирусного ПО и антиспама (или, например, только антиспама) на выделенном сервере без почтовой системы и передача на проверку почтовых сообщений с имеющихся почтовых серверов по

выделенному для этой цели сетевому интерфейсу. Эта схема применяется в том случае, когда по каким-то причинам невозможна установка почтовых релейов, удовлетворяющих описанным выше требованиям.

Антивирусная проверка и фильтрация спама являются довольно сложными алгоритмическими задачами. При расчете потребности в вычислительных ресурсах для антивирусной проверки почтового трафика и фильтрации спама, можно исходить из следующих приближений: один сервер 2x Intel Xeon CPU (4 Core) 3 GHz, 4GB RAM для потока не более 1 млн почтовых сообщений и не более 8GB почтового трафика в сутки, включая все поступившие спам-сообщения. При установке приложений на сервера с существующей почтовой системой при расчете загрузки и требуемого количества серверов необходимо применять это приближения с учетом загрузки самого почтового сервера без установленных и работающих антивируса и антиспама.

Для приложения Kaspersky Mail Gateway схема развертывания выглядит аналогичным образом. Это приложение может заменить «связку» почтовый релей – Антиспам – Антивирус. В отличие от двух вышеописанных приложений, для его работы на почтовом реле не требуется работающей почтовой системы (postfix, exim и проч.), в которую производится интеграция – приложение само представляет собой полноценный почтовый маршрутизатор, после постинсталляционной настройки готовый к ретрансляции почтовых сообщений с включенной фильтрацией вирусов и детектированием признаков спама. Это решение может быть интересно организациям и компаниям, которые только переходят на платформу Linux или FreeBSD и не имеют сотрудников, хорошо знакомых с особенностями настройки почтовых систем postfix, exim и т.п.

4 Коммерческая схема сотрудничества

После проведения технических консультаций и определения применимости решения для антивирусной проверки почтового трафика абонентов и фильтрации спам сообщений, «Лаборатория Касперского» готова предоставить временные лицензии для тестового внедрения и использования на срок 1 месяц.

Стоимость последующего использования лицензий рассчитывается исходя из объема среднесуточного проверяемого почтового трафика абонентов.

Оплата права использования производится единовременно на годовой период. Договор на передачу прав использования может заключаться с любым Авторизованным партнером «Лаборатории Касперского»

5 Заключение

«Лаборатория Касперского» обладает значительным опытом сотрудничества с операторами связи и располагает необходимыми конкурентоспособными и эффективными технологиями для внедрения решений по защите абонентов операторов связи.

По всем вопросам, связанным с данным предложением вы можете обращаться по следующим контактам:

Тел: +7(495) 797 8700, 645 7939, 956 7000 Факс: +7(495) 797 8700

E-mail: sales@kaspersky.com