Всегда впереди идущий игрок против спама - Barracuda Spam & Virus Firewall.

На сегодняшний день порог допустимого спама превысил более 90 процентов писем от реально легитимной почты. Огромное количество бесполезных сообщений наносит очевидный вред получателям, постоянно необходимо просматривать совсем ненужные письма, при этом тратить время и силы. Для борьбы от спама используют системы автоматической фильтрации входящих и исходящих писем. Решение Barracuda Spam & Virus Firewall - это комплексный механизм защиты от спама, вирусов и другого вредоносного контента, распространяемого по электронной почте. Благодаря возможности обработки до 10 миллионов почтовых сообщений в день, Barracuda Spam & Virus Firewall способен обеспечить безопасную работу большого количества активных пользователей крупных компаний.

Доступна настройка сканирования входящей или исходящей почты, и при этом можно установить для каждого пользователя свой карантин, который управляется администратором и пользователем, что при этом можно полностью обучить данное устройство на фильтрацию спама.

В отличие от программных решений, Barracuda Spam & Virus Firewall уменьшает загрузку почтового сервера, освобождая его от антивирусной и антиспам фильтрации. При получении почты через Barracuda Spam Firewall, происходит сканирование на 12 уровнях включая:

- anti-spam,
- anti-virus,
- anti-spoofing,
- anti-phishing,
- anti-spyware,
- denial of service, rate controls,
- IP analysis,
- аутентификация отправителя,
- проверка получателя,
- virus scanning,
- ручная политика,
- fingerprint analysis (анализ по "отпечаткам пальцев"),
- intent analysis (URL фильтрация в письме),
- image analysis, анализ по Байесу,
- spam scoring, что позволяют создать защиту не только от спама, а и защиту от уязвимости почтовых серверов, также от процессов, несущих в себе потенциальную угрозу для корпоративной информации.

Централизованная настройка уровня защиты от спама (регулируемая шкала действий с почтой, которая проходит через устройство, где можно назначить по оценки писем, когда их нужно блокировать, помечать, или изолировать в карантин).

Обновления (Barracuda Energize Updates) в on-line режиме устанавливаются автоматически, а команда инженеров постоянно работает для разработки наиболее эффективных методов борьбы с постоянно меняющимися видами спама и вредоносного кода. Эти системы гарантируют организациям, что вся исходящая почта легитимная и не содержит вирусов.

Специалисты компаний провели исследование особенностей украинско-российского сегмента мирового виртуального пространства. Полученные результаты легли в основу проекта адаптации продукта и создания универсального решения по защите корпоративных пользователей от спама и вредоносного контента, распространяемого по почте (вирусы, spyware, phishing и многое другое).

Данное устройство является аппаратным решением с централизованным простым управлением, интуитивно понятным веб-интерфейсом, легко интегриться в инфраструктуру сети, соответствует цене-качеству. Не лицензируясь по рабочим местам, а на устройство, Barracuda Spam & Virus Firewall предлагает наиболее приемлемую по цене фильтрацию почтового трафика.

Решение обеспечивает функциональность и простоту использования для всех категорий бизнеса. Его запуск и настройка не требуют дополнительной установки или модификации существующего ПО почтовых серверов заказчика, и могут быть выполнены в кратчайшие сроки.

В данное устройство заложено также еще следующее возможности:

- Списки блокировки и разрешения IP-адресов
- Локализация Web-интерфейса администрирования
- Настройка входящей или исходящей почты (только по отдельности)
- Поддержка TLS/SSL
- Установки карантина и спама для каждого из пользователей
- Поиск в Exchange и LDAP и улучшение их работы
- Операционная система Barracuda Spam&Virus Firewall: (GNU / Linux)
- Двойная антивирусная защита

Двойная антивирусная защита Barracuda Spam&Virus Firewall имеет на борту ядро от Barracuda и Clam AV.

Главная цель второго движка Clam AntiVirus — интеграция с серверами электронной почты для проверки файлов, прикреплённых к сообщениям. В пакет входит масштабируемый многопоточный демон clamd, управляемый из командной строки сканер clamscan, а также модуль обновления сигнатур по Интернету freshclam.

Возможности антивирусных ядер:

- возможность использования с большинством почтовых серверов;
- сканер в виде библиотеки Си;
- сканирование файлов и почты «на лету»;
- определение свыше 499 000 вирусов, червей, троянов, сообщений фишинга;
- анализ сжатых файлов RAR (2.0, 3.0), Zip, Gzip, Bzip2, MS OLE2, MS Cabinet, MS CHM (сжатый HTML) и MS SZDD;
- поддержка сканирования mbox, Maildir и «сырых» почтовых файлов;
- анализ файлов формата Portable Executable, упакованных UPX, FSG или Petite.

Почта, содержащая новый вирус или упреждающие оповещение спама (virus or spam outbreaks), могут быть блокированы в реальном времени, при этом Barracuda Spam Firewall посылает вирусные варианты центральной базе на обследования. Barracuda Central - ежедневно принимает спам, вирусные представления и интернет запросы от больше чем 85 000 клиентов во всем мире, которая работает в реальном времени, и больше чем 1,5 биллиона писем в мире проверяется ежедневно базой Barracuda Central.

Вдобавок всех перечисленных функций, предназначенных для борьбы со спамом, особенно интересен принцип анализа по Байесу, что дает возможность самообучаться в процессе анализа корреспонденции. Данная технология отличается использованием байесовских принципов для распознавания спама по образу, моделирование которого происходит благодаря анализу самого спама.

Однако простота применения байесовских принципов обманчива, так как отнесение письма к спаму производится по сложным алгоритмам выявления общих элементов в реальных посланиях. Таким образом, чем большее количество спама подверглось анализу, тем лучше работает фильтр. Кроме того, метод Байеса обладает автокоррекцией, поскольку в случае изменения структуры писем фильтр изменяется автоматически.

При обучении антиспам-фильтра по методу Байеса для каждого встреченного в письмах слова высчитывается и сохраняется его «вес» — вероятность того, что письмо с этим словом является спамом.

Отнесение письма к «спаму» или к обычной корреспонденции производится по тому, превышает ли его «вес» некую планку, заданную пользователем (обычно берут 60-80%). После принятия решения по письму в базе данных обновляются «веса» для вошедших в него слов.

Компания Barracuda рекомендует два способа настройки устройства для фильтрации входящей почты. В первом случае, описанном ниже, вы просто ставите устройство за корпоративным брандмауэром в той же самой сети, в которой находится ваш почтовый сервер.

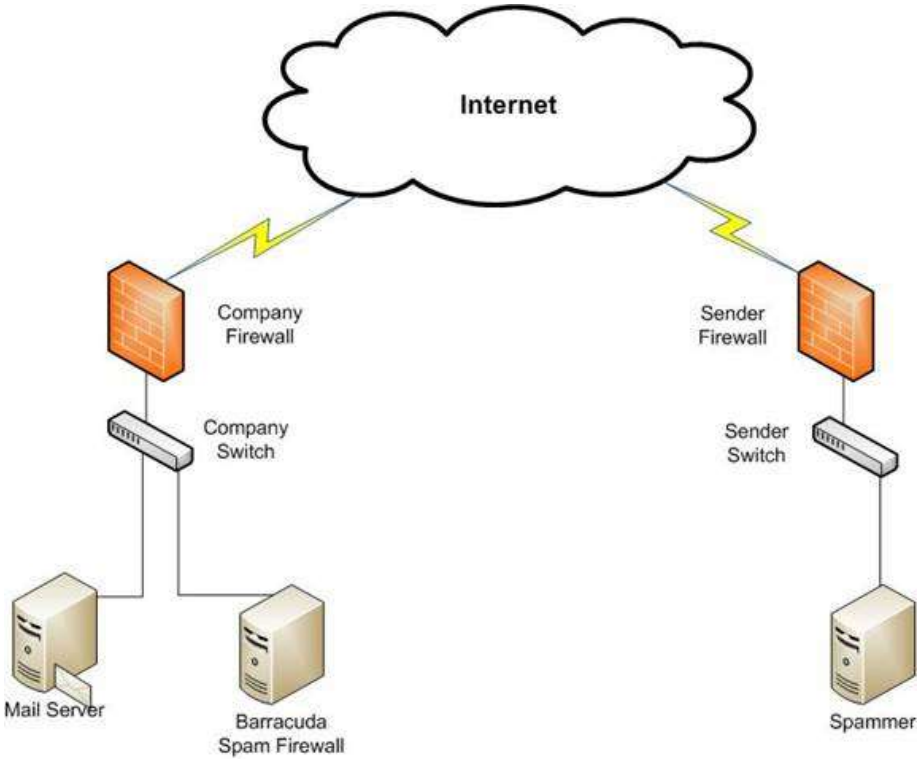

Рисунок 1

Как показано на рисунке, вам просто нужно переадресовывать SMTP-трафик на IP-адрес устройства. Далее, вы переадресовываете все отфильтрованные сообщения на почтовый сервер.

Рисунок 2 показывает размещение устройства в DMZ для усиления безопасности и отделения устройства как от внутренней, так и от внешней сети.

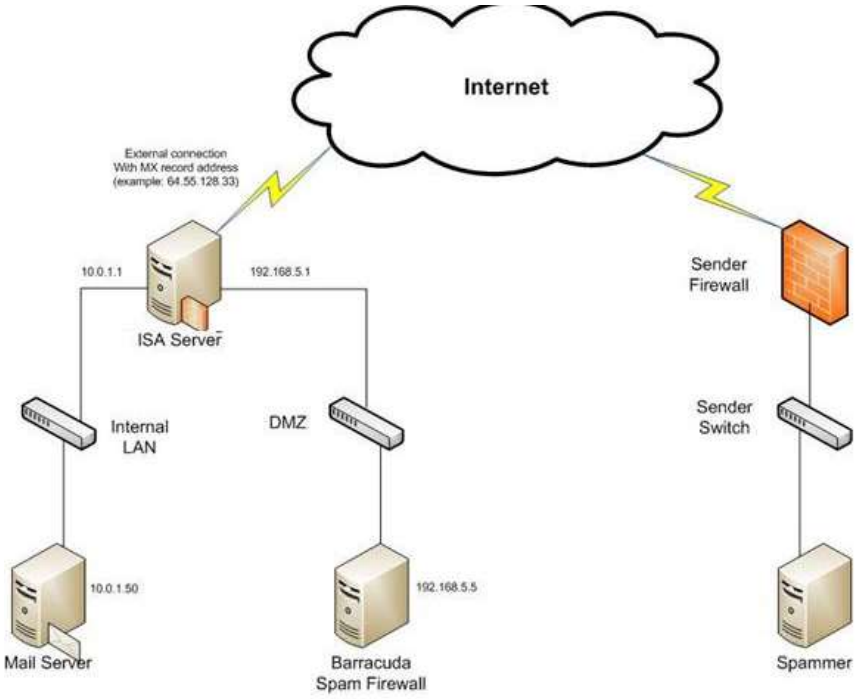

Рисунок 2

Помещение устройства в DMZ похоже на размещение там web-сервера. Основная разница заключается в том, какие порты мы откроем на устройстве, сервере ISA/TMG (или аналог) и в нашей внутренней сети, а также в том, как мы будем публиковать устройство для внешнего мира.

Автор статьи: Сергей Бартко, инженер-консультант Barracuda, Softprom

e-mail: barracuda@softrom.com
www.softprom.com