

Решения для борьбы со спамом на предприятии

Продукты второго поколения для защиты электронной почты



Сью Тиббеттс



Фильтры спама принимают располагать на серверах Internet-провайдеров, на шлюзах сети предприятия (например, на DMZ-сервере), на почтовых серверах и настольных компьютерах. Эти подходы, особенно если они объединены в многоуровневом решении, эффективно уменьшают число непрошенных по-

сланий в почтовых Ящиках пользователей. Ко с увеличением объема спама замедляется обработка сообщений на почтовом сервере и возникает необходимость в дополнительных хранилищах сообщений, отмеченных как потенциальный спам. Поэтому многие компании заменяют программные решения для борьбы со спамом первого поколения специализированными устройства-

Таблица Решения для борьбы со спамом на предприятии						
Компания	Продукт	Цена в долларах	Совместимость с версиями Exchange	Подозрительные сообщения блокируются, удаляются, направляются в сборный почтовый ящик или карантин	Заранее подготовленные правила для спама	
Специализированные устройства						
Barracuda Networks http://www.barracuda.com	Barracuda Spam Firewall 200	От 1399	Все SMTP-совместимые почтовые серверы	Да	Да	
	Barracuda Spam Firewall 300	От 1399	Все SMTP-совместимые почтовые серверы	Да	Да	
	Barracuda Spam Firewall 400	От 3999	Все SMTP-совместимые почтовые серверы	Да	Да	
IronPort Systems http://www.ironport.com	IronPort C-Series Email Security Appliance	От 2639 (с поддержкой и обновлениями)	Все SMTP-совместимые почтовые серверы	Да	Да	
Secure Computing, Inc http://www.securecomputing.com	IronMail Messaging Gateway Security	От 5995	Все SMTP-совместимые почтовые серверы	Блокирует спам до поступления на почтовый сервер; не передает потенциальный спам в сборный почтовый ящик или в карантин	Да	
SurfControl http://www.surfcontrol.com	RiskFilter	Цена договорная	Все SMTP-совместимые почтовые серверы	Да	Да	
Symantec http://www.symantec.com	Symantec Mail Security 8200 Series	3065 для 100 пользователей (вместе с поддержкой и обновлениями)	Все SMTP-совместимые почтовые серверы	Да	Да	
Vircom http://www.vircom.com	ModusGate	5000 для 50 пользователей	Все SMTP-совместимые почтовые серверы	Не направляет спам в сборный почтовый ящик	Да	
WatchGuard Technologies http://www.watchguard.com	spamBlocker	От 450	Все SMTP-совместимые почтовые серверы	Функцию карантина планируется реализовать в будущих версиях	Да	

ми или возлагают задачи фильтрации спама на хост-службы независимых поставщиков. Данный обзор поможет оценить возможности устройств фильтрации спама и хост-служб и выбрать технологии, обеспечивающие самую надежную защиту электронной почты.

Покупка специализированного устройства

Специализированные устройства представляют собой автономные устройства с собственными операционными системами и предназначены именно для фильтрации спама. Их можно установить во входной точке сети или перед почтовым сервером. Многие устройства поставляются с заранее настроенными правилами, политиками и списками (например, черными списками, белыми списками, собственными списками поставщика) и готовы к рабо-

те без дополнительной настройки. Большинство устройств располагает интерфейсом пользователя на базе Web, с помощью которого можно централизованно и дистанционно управлять политиками электронной почты, отыскивать и извлекать сообщения из карантина, а также готовить отчеты в реальном времени и по данным журналов.

Большинство поставщиков устройств ежедневно обновляют правила, чтобы эффективно отражать новые угрозы. Некоторые поставщики предоставляют возможность бесплатного обновления в течение года после покупки устройства; другие предлагают службу обновления по подписке за дополнительную плату. Преимущество устройств с отсутствием пользовательских лицензий. Компания приобретает устройство, которое обслуживает некоторое количество пользователей электрон-

Обновление службы	Обновление правил в реальном времени	Фильтры на национальных языках	Настраиваемые политики	Байесова фильтрация	Карантин для отдельных пользователей	Настраиваемые фильтры	Инструментарий для анализа содержимого сообщений
Да	Да	Да	Да	Да	Нет	Да	Да
Да	Да	Да	Да	Да	Да	Да	Да
Да	Да	Да	Да	Да	Да	Да	Да
Да	Да	Да	Да	Нет (используется IronPort Threat Operations Center)	Да	Да	Да
Да	Да	Да	Да	Да	Да	Да	Да
Да	Да	Да	Да	Можно настроить для анализа, аналогичного Байесову	Да	Да	Да
Да	Да	Да	Да	Да	Да	Да	Расширение, предоставляемое по подписке
Да	Да	Да	Да	Да	Да	Да	Да
Да	Да	Да	Да	Нет; используется технология обнаружения повторяющихся комбинаций	Функция будет реализована в будущей версии	Да	Да

ной почты или усредненное число входящих и исходящих почтовых сообщений в день. В целом, компании с более чем сотней пользователей более выгодно купить специализированное устройство.

Использование хост-службы

• хост-службы фильтруют сообщения электронной почты, прежде чем те попадут на почтовый сервер компании. Благодаря хост-службе сокращается нагрузка на ресурсы сервера, не требуется покупать дополнительные аппаратные средства или программы, а потенциальный спам хранится на сайте поставщика. Обычно поставщики службы быстро реагируют на новые формы спама.

Крупные компании часто выбирают хост-службы из-за дополнительных функций электронной почты, таких как фильтрация и шифрование исходящих сообщений, а также применение политик, но хост-службы могут пригодиться и малым предприятиям с числом сотрудников не более ста, а также компаниям, в которых нет штатного администратора системы обработки почты. Стоимость хост-службы часто определяется числом

пользователей электронной почты: чем больше пользователей, тем выше стоимость службы.

Многие поставщики служб предоставляют дополнительные услуги, в том числе автоматическое восстановление после аварии и возможность передать функции отказавшего узла исправному, архивирование сообщений в автономном хранилище (ради соответствия законодательным актам и бесперебойной работы компании), обеспечение избыточности данных, защиты системы мгновенного обмена сообщениями (IM) и фильтрации исходящего трафика. Наличие одной или нескольких дополнительных услуг может отразиться на стоимости службы.

Критерии выбора

Основные требования к системе защиты от спама с исчерпывающий план обслуживания или легко устанавливаемое специализированное устройство, которые гарантируют надежное блокирование спама (по меньшей мере, 97%) и минимум выбраковки полезных сообщений. При анализе хост-служб советую обратить внимание на время бесперебой-

Таблица

Решения для борьбы со спамом на предприятии (окончание)

Компания	Продукт	Цена в долларах	Совместимость с версиями Exchange	Подозрительные сообщения блокируются, удаляются, направляются в сборный почтовый ящик или карантин	Заранее подготовленные правила для спама
Службы					
AppRiver http://www.appriver.com	SecureTide	Цена договорная	Все SMTP-совместимые почтовые серверы	Да	Да
Clearswift http://www.clearswift.com	MIMESweeper for Exchange 5.2	13 000 для 1000 пользователей	Все SMTP-совместимые почтовые серверы	Да	Да
MessageLabs http://www.messagelabs.com	MessageLabs Email Protect	От 2 долл. в месяц для одного пользователя	Все SMTP-совместимые почтовые серверы	Да	Да
Postini http://www.postini.com	Postini Perimeter Manager Enterprise	43 000 за 2 года для 1000 пользователей (вместе с консультациями и обслуживанием)	Все SMTP-совместимые почтовые серверы	Да	Да
St. Bernard http://www.stbernard.com	Singlefin Security Services	От 2,95 долл. в месяц для одного пользователя	Все SMTP-совместимые почтовые серверы	Да	Да
Symantec http://www.symantec.com	Symantec Hosted Mail Security	2 долл. в месяц для одного пользователя	Все SMTP-совместимые почтовые серверы	Да	Да


Примечание редактора. Некоторые поставщики сообщили, что у них нет продуктов, точно соответствующих требованиям обзора, или не предоставили информацию о своих продуктах.

ной работы, гарантированное соглашение об уровне обслуживания (SLA), и задержку сообщений. Важно, чтобы хост-служба помещала сообщения в очередь в случае отказа сети компании или линии связи. Кроме того, устройство или служба должны поддерживать почтовые серверы предприятия, быть совместимыми с LDAP и работать с несколькими доменами. Чем больше механизмов защиты (от вирусов, имитации соединений, Зшпионов и фишинга) и технологий фильтрации реализовано в службе или устройстве, тем лучше.

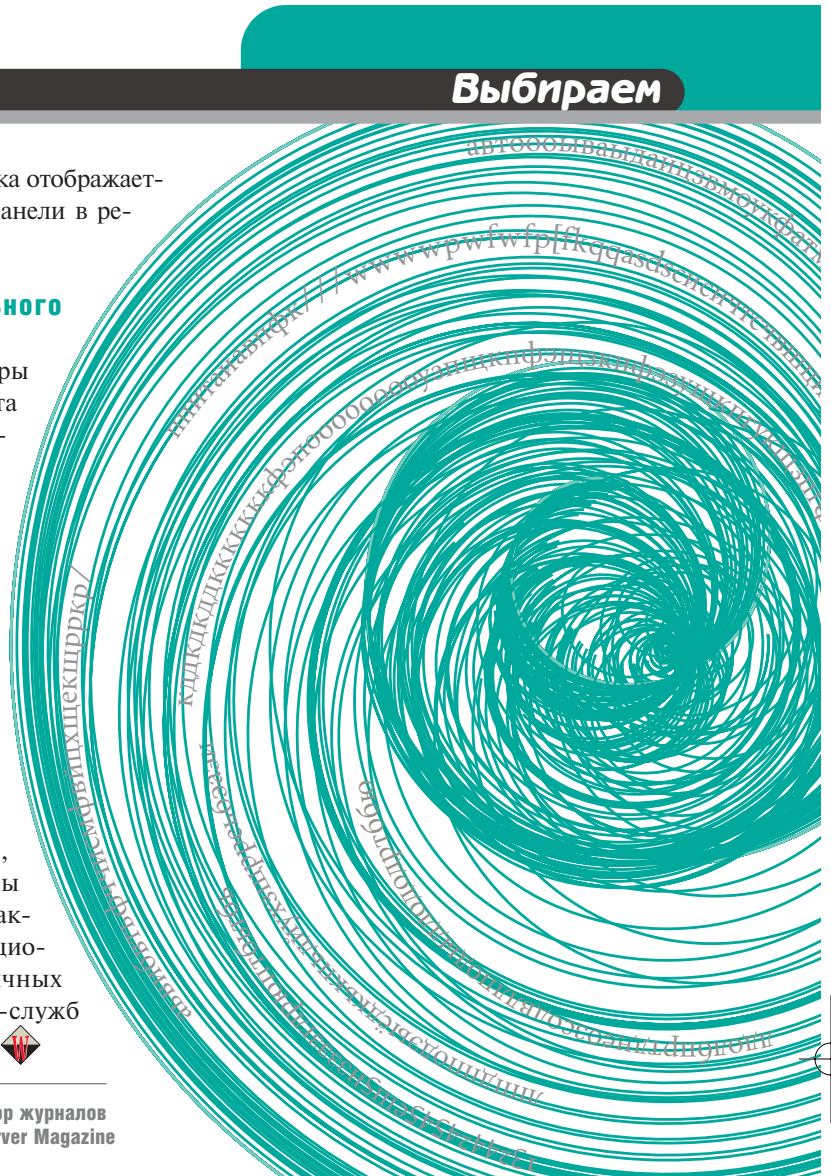
Для эффективной борьбы со спамом предпочтительны продукты и службы с Web-интерфейсом (многоязыковым для пользователей в разных странах), которые обеспечивают дистанционный мониторинг и доступ к отправленным в карантин, заблокированным и удаленным нежелательным сообщениям; управление политиками (в частности, настройкой политик для различных доменов, групп пользователей и отдельных пользователей), правилами и списками; администрирование учетных записей пользователей; подготовку отчетов (в некоторых

продуктах статистика отображается на приборной панели в реальном времени).

Выбор оптимального решения

Ключевые факторы выбора с простота использования, надежность фильтрации, масштабируемость, ценовая структура, обслуживание потребителей и помощь в развертывании или установке, а также другие функции или услуги, которые могут пригодиться в будущем. В таблице приведены сравнительные характеристики и функциональность различных устройств и хост-служб фильтрации спама. 

Сью Тиббеттс — редактор журналов Windows IT Pro и SQL Server Magazine



Обновление службы	Обновление правил в реальном времени	Фильтры на национальных языках	Настраиваемые политики	Байесова фильтрация	Карантин для отдельных пользователей	Настраиваемые фильтры	Инструментарий для анализа содержимого сообщений
Да	Да	Да	Да	Да	Да	Да	Да
Да	Да	Да	Да	Нет, используется SpamLogic	Да	Да	Да
Да	Да	Да	Да	Да	Да	Да	Да
Да	Да	Нет	Да	Да	Да	Да	Да
Да	Да	Да	Да	Да	Да	Да	Да
Да	Да	Да	Да	Да	Да	Да	Да