

InfoWorld

November 17 2003 ■ ISSUE 45

GET TECHNOLOGY RIGHT

SPAM SHOOTOUT

Five anti-spam solutions for enterprise networks face our live spam challenge

BY LOGAN G. HARBAUGH

AS ANYONE WITH an e-mail inbox knows, the spam problem isn't going away. According to a major anti-spam vendor, spam has increased from 8 percent of all e-mail traffic in 2001 to 50 percent in July 2003. Other estimates show that figure as high as 70 percent of all traffic. Two classes of products can help slay spam in the enterprise environment: gateways and services. Both allow you to block spam for all network users at a single, centrally managed point before it hits your mail server.

For this review, I looked at two services and three gateway products. Services filter spam before it arrives at your network, reducing the volume of traffic on your Internet connection. Services also typically offer multiple datacenters for redundancy, high volume, and fast response. Setup requires merely changing the MX (mail exchange) record for your domain. But a service is not under a local administrator's control, so if the service goes down, mail may not get through.

Gateways are harder for spammers to circumvent by sending e-mail to the real mail server's IP address; they offer local control of the anti-spam technology; and they allow mail to continue to arrive if the anti-spam gateway goes down. But a gateway gives the local administrator yet another system to maintain, and the total traffic through your Internet connection remains the same because spam isn't filtered until it reaches your network.

The five products I tested: Brightmail Anti-Spam Enterprise Edition Version 5.1, Front-Bridge TrueProtect E-mail Security Suite, Postini Perimeter Manager Enterprise Edition, Proofpoint Protection Server 1.2.1, and SpamAssassin 2.44, an open source spam filter included with Red Hat Linux 9.

In contrast to the commercial products, SpamAssassin represents an older, first-generation anti-spam solution, and its age showed in my tests. It filtered only 62 percent of spam, whereas the other products produced great results, blocking 90 percent to 96 percent of all the spam they encountered with few, if any, legitimate messages blocked.

Differentiating between spam and legitimate messages can be difficult. Newsletters, press releases, and other marketing materials from companies you have a relationship with can be very similar to spam in content. These all present challenges to the filters. The e-mail I used for testing was real e-mail containing many messages that stressed the filters.

I looked at two categories of mail incorrectly identified as spam: false positives that were not critical, such as newsletters and marketing

For all five commercial products, even noncritical false positives such as newsletters were few.



information; and false positives that were critical, such as personal e-mail from colleagues. Each product was tested with a different stream of mail, so the number of messages received varied, but all received enough messages to assess their capabilities.

The critical issue is not that the filter may have misidentified a few e-mails, but how easily those messages can be found and added to a whitelist so that future e-mails from the same source are not stopped. All the products except Brightmail and

SpamAssassin allow end-users to add senders to the domain whitelist themselves. Brightmail allows users to forward misidentified e-mails to the administrator, who can choose to add the sender to the whitelist. SpamAssassin allows only the administrator to add to the whitelist, with no direct access for users.

All the products allow the administrator to blacklist known spammers and choose among a variety of responses to messages identified as spam — adding an identifier to the subject line, adding a message header, deleting the message, or quarantining it. Delegation of specific administrative functions is possible with all the products except SpamAssassin, although the granularity of delegation varies among the four. Spam settings can be set by enterprise (multiple domains) or domain, and Postini also allows individual groups or users within a domain to have different rules.

And all the products but SpamAssassin use dynamic updates to keep up with the evolving technologies spammers use to circumvent less sophisticated filters. The default update cycle may be every few minutes or once per week, depending on the product. Keeping the filters up to date requires a subscription or maintenance fee.

Finally, in addition to stopping spam, all four commercial products provide content-filtering features, allowing the administrator to block incoming or outgoing e-mail that contains proprietary data, audio or video files, executables, sexually explicit words, or racial slurs. They also pro-

vide protection against DoS attacks and directory harvesting attacks.

In my testing, the performance of the newer products was more than acceptable in every case. Per-user, per-year pricing should not be an obstacle, even for the most expensive product. Choosing the right product will depend on your network topology, your philosophy regarding outsourcing, requirements for administrative control and reporting, traffic loads, and your operating system and mail server platform.

Postini Perimeter Manager

Postini's anti-spam service processes about 150 million messages per day. Although it started as a service for ISPs, it has recently moved into the enterprise space and provides a broad, sophisticated array of services. It is the only product I tested that includes anti-virus scanning in the base price.

Setting up the service is simple, requiring the same MX record change as FrontBridge's service. Adding users is automated and very easy — each user receives a message the first time that spam is blocked from their account, letting them know how to access quarantined e-mail and retrieve, delete, or whitelist mail. All administrative tasks can be accomplished through the Postini Web site, and management tasks can be delegated in a very

Postini's response to spam is unusually flexible, and can be set by individual, group, or domain.



granular manner. Managing multiple domains is easy. Reporting is flexible in the criteria reported, but long-term tracking is not available in the standard corporate edition — only daily and weekly reports are made available.

Response to spam is unusually flexible, and can be set by individual, group, or domain. Administrators can allow users to add senders to the whitelist, retrieve messages from quarantine, and even change filter settings — or they can lock

things down so that end-users can do nothing without an administrator. The spam filters have separate settings from lenient to strict for a variety of categories, including bulk e-mail, special offers, get-rich-quick messages, and adult content.

The Standard Edition includes spam filtering, inbound server monitoring, connection management, delivery management, detailed reporting, inbound attachment management, inbound virus blocking, and inbound content manage-

ment. The Enterprise Edition adds outbound server monitoring, outbound virus blocking, outbound attachment management, outbound content management, and disaster-recovery service. It can also check outbound e-mail for policy violations concerning language, recipients, and attachments.

Postini is very flexible and feature-rich, and it caught nearly 94 percent of spam in my tests, edged out only by Brightmail and Proofpoint. It lagged slightly in avoiding false positives, but the differences here could easily be overcome by whitelist tuning.

Tools of the Anti-Spam Trade

Anti-spam solutions differ in the techniques they use to block spam and in the amount of flexibility and control they provide to admins and end-users. While Brightmail had the edge in our performance test, Postini provided the most granular management capabilities.

| | SERVICE OR GATEWAY | BLACKLIST | WHITELIST | WHITELIST ADMINISTRATION | SIGNATURES | HEURISTICS | BAYESIAN ANALYSIS | PROPRIETARY METHODS | AUTOMATIC UPDATES OF FILTER CRITERIA | END-USER ACCESS TO QUARANTINED E-MAIL | ANTI-VIRUS |
|--------------|--------------------|-----------|-----------|--------------------------|------------|------------|-------------------|---------------------|--------------------------------------|---------------------------------------|------------|
| Brightmail | Gateway | Yes | Yes | Admin only | Yes | Yes | No | Yes | Yes | Spam folder | Optional |
| FrontBridge | Service | Yes | Yes | Admin or end-user | Yes | Yes | No | Yes | Yes | Web | Optional |
| Postini | Service | Yes | Yes | Admin or end-user | No | Yes | No | Yes | Yes | Web | Yes |
| Proofpoint | Gateway | Yes | Yes | Admin or end-user | No | Yes | Yes | Yes | Yes | Web | Optional |
| SpamAssassin | Gateway | Yes | Yes | Admin only | No | Yes | Optional | No | Optional | None | No |

1. Postini's reports are limited to the current day or week.

2. SpamAssassin doesn't provide formal reports, but information can be obtained from log files.

Brightmail Anti-Spam Enterprise Edition 5.1

Brightmail brightmail.com

VERY GOOD 8.4

| | |
|---------------------|---|
| Manageability (25%) | 8 |
| Accuracy (25%) | 9 |
| Ease of use (20%) | 8 |
| Setup (20%) | 8 |
| Value (10%) | 9 |

COST: Yearly subscription: \$1,499 for 50 users, \$5,999 for 500, \$35,000 for 5,000

PLATFORMS: Linux, Solaris, Windows

BOTTOM LINE: Brightmail's gateway solution includes a spam folder agent for Microsoft Exchange and IBM/Lotus Domino, allows Outlook users to provide "spam" or "not spam" feedback with a click, and provides good reporting. However, administration is relatively inflexible; end-users cannot whitelist senders directly. Nevertheless, Brightmail proved the most accurate in filtering spam (96 percent). Excellent support and a large user base mean that Brightmail should continue to have high accuracy in the future.

FrontBridge TrueProtect E-mail Security Suite

FrontBridge frontbridge.com

VERY GOOD 8.5

| | |
|---------------------|---|
| Manageability (25%) | 8 |
| Accuracy (25%) | 9 |
| Ease of use (20%) | 8 |
| Setup (20%) | 9 |
| Value (10%) | 8 |

COST: Yearly subscription: \$1,350 for 50 users, \$9,000 for 500, \$75,000 for 5,000

PLATFORM: Service

BOTTOM LINE: The FrontBridge service blocked 90 percent of spam in our tests, with few false positives. Adding users is virtually automatic, end-users can easily recover quarantined messages and whitelist senders, and reporting is excellent, however real-time information is unavailable due to delays of up to six hours. FrontBridge also offers a good array of additional services, including mail policy enforcement and disaster recovery. A new alliance with Sprint and a research facility make this a good bet into the future.

Postini Perimeter Manager Enterprise Edition

Postini postini.com

EXCELLENT 8.7

| | |
|---------------------|---|
| Manageability (25%) | 9 |
| Accuracy (25%) | 9 |
| Ease of use (20%) | 9 |
| Setup (20%) | 9 |
| Value (10%) | 8 |

COST: Yearly subscription: \$1,350 for 50 users, \$10,000 for 500, \$68,750 for 5,000

PLATFORM: Service

BOTTOM LINE: Postini offers highly accurate spam filtering, a rich and flexible feature set, and granular administration, allowing anti-spam settings to be tightened or loosened to different types of e-mail, and policies to be tailored to individual users, groups, and domains. The service is easy to use for both admins and end-users, who can be allowed to perform admin tasks or locked out altogether. Postini was the only product tested to include anti-virus scanning in the base price.

Proofpoint Protection Server 1.2.1

Proofpoint proofpoint.com

VERY GOOD 8.3

| | |
|---------------------|---|
| Manageability (25%) | 8 |
| Accuracy (25%) | 9 |
| Ease of use (20%) | 8 |
| Setup (20%) | 8 |
| Value (10%) | 8 |

COST: Yearly subscription: \$1,000 for 50 users, \$10,000 for 500, \$54,049 for 5,000

PLATFORMS: Red Hat Linux 8 or 9, Solaris

BOTTOM LINE: Proofpoint is more demanding technically to install and configure, but the company's superb tech support makes this a nonissue. Spam filtering is highly accurate, and a flexible classification system allows administrators to configure different responses to spam depending on spam likelihood. End-users can easily recover quarantined messages and add senders to whitelists, and reporting features are excellent. But delegation of administrative tasks is not as detailed or granular as with Postini.

SpamAssassin 2.44

SpamAssassin Open Source spamassassin.org

GOOD 6.0

| | |
|---------------------|---|
| Manageability (25%) | 7 |
| Accuracy (25%) | 5 |
| Ease of use (20%) | 6 |
| Setup (20%) | 6 |
| Value (10%) | 6 |

COST: Free

PLATFORMS: BSD, Linux, Solaris, Windows

BOTTOM LINE: The SpamAssassin software is free, and plenty of add-ons are available on the Internet, but this gateway is much more difficult to install and keep up-to-date than commercial alternatives. Complex setup, scanty documentation, on-going requirement for research and tuning, and the lack of tech support make this a poor choice for most companies. Unless you have more staff than money, spend the \$10 to \$20 per user, per year for one of the commercial gateways or services.