

Colleagues,

Thanks to all who replied to the request at the end of this message for information on how you handle spam. A total of 41 institutions are represented in the summary below (some institutions use more than one product). Most institutions responded that they are blocking spam at the perimeter; many provide user control over quarantined mail. Barracuda is the most widely used technology in this sample. Since some of the responses came to me privately, I thought you might find it useful to have a consolidated set of summarized comments.

Barracuda: 18 institutions have implemented or are in the process of implementing; 1 is considering

Tangent's Barracuda-based service: 2

Spam Assassin: 4 (plus 4 additional institutions which have migrated or are migrating to other products)

IronPort: 4

Postini: 2

Sophos PureMessage: 2

Brightmail: 2

Appraver: 1

eSoft Threatwall: 1

GWGuardian: 1

TrendMicro: 1

Symantec AV: 1

CanIt Spamtrap: 1

SpamHaus: 2

PreciseMail: 1

Meridus 100: 1

Undesignated: 3

Summarized responses follow.

1. Barracuda-based service from Tangent (UNC Pembroke)
2. "Appraver" service for faculty/staff account spam/virus filtering. Appraver quarantines mail and sends a daily email to user showing email held. Service doubles as a disaster recovery site for their email. Appraver is too expensive to include students; currently looking at a Barracuda solution for students. (Coast Community College District)
3. Sophos' PureMessage for faculty/staff; quarantined at the gateway. Quarantine digest sent out to faculty/staff twice per day. Manage whitelists/blacklists to supplement built-in controls. (Vancouver Community College)
4. Brightmail and Ironport. Anti-spam filtering at perimeter, with variations: departmentally-managed servers can elect to discard at server, tag and pass,

- bypass perimeter support; manage spam locally. Additional info at <http://www.utexas.edu/computer/spam/> Extensive testing in 2004 determined false positive rate to be negligible. (University of Texas at Austin)
5. Barracuda blocks high-scoring spam at perimeter (Buffalo State College)
 6. eSoft's Threatwall provides spam filtering. Planning to move to "greylisting" 11/13/06. (Moody Bible Institute)
 7. Barracuda in use for 11 months; previously used Spam Assassin (McDaniel College)
 8. GWGuardian from Messaging Architects; spam is quarantined. Currently switching from GroupWise to Exchange. (Samford University)
 9. Product/service not specified. Spam blocked at perimeter; users can receive a report of all deleted or blocked mail. http://www.svsu.edu/its/index.cfm?doc_id=4584 . Block and discard verified spam; block suspected spam. (Saginaw Valley State University)
 10. Barracuda. Blocks spam at the perimeter. (South Dakota Board of Regents)
 11. Barracuda Spam Firewall 300 in use for 6 months. Blocks everything on Spamhaus blacklist. Spam scored over 4 is quarantined for user action; scores from 2.0-4.0 are tagged/passed. (The Lutheran Theological Seminary at Philadelphia)
 12. Barracuda spam firewall blocks at perimeter. Currently blocks over 80% of all inbound mail and marks about 6% of passed email as potential spam. (College of St. Elizabeth)
 13. Barracuda blocks messages at the perimeter at 7.51; quarantines at 6.1; tags at 3.5. All zip files quarantined; a few domains are blocked. Sender is notified if their message is tagged as spam; sender contacts recipient; recipient can contact help desk. Currently block 71%, allow 18%, tag 8%, quarantine 3%. Blocked due to viruses is less than .02%. (Kings College)
 14. Product/vendor not specified. Spam blocked at perimeter. Block domains identified by two blacklist vendors. (Texas Christian University)
 15. Spam Assassin. Default is 5; user can adjust. Mail scored above 5 gets delivered to Spam folders in recipient's mailbox. Due to recent spam increases, now decreasing users' spam folder retention period from 14 to 7 days; no longer backing up the users' spam folders; immediately delete any messages scored above 20. (University of Wisconsin – Milwaukee)

16. Barracuda in use for 2 years. Blocks 80-90% of incoming mail as spam at perimeter. (Middlesex County College)
17. Barracuda blocks spam at perimeter. On 9/29/06, over 1 million messages presented to the Barracuda; only 11% of those were delivered to users' mailboxes. On 10/21/06, Barracuda blocked over 1 million spam messages. (Notre Dame)
18. Barracuda blocks spam at perimeter. Began blocking mail above 7; now blocked at less than 5. At 7, over half the remaining email was still spam. (Binghamton University)
19. TrendMicro spam filtering and Postini's Perimeter Manager service. Blocked at perimeter. Users receive a daily digest listing quarantined mail. They can cause them to be delivered or to view them. Implementation involved complete change of all campus MX records to pass mail through Postini, retirement of Internet facing email relays, working with subdomain owners for enabling subdomain-specific aliases into a user's Postini service, and use of Symantec AV to scan internal email. See <http://it.emory.edu/showdoc.cfm?docid=2641> and <http://it.emory.edu/showdoc.cfm?docid=7710>. (Emory University)
20. Barracuda implemented one year ago; previously used Spam Assassin. (Macalester College)
21. Barracuda (a pair). Spam/virus blocked at perimeter; about 6 out of 7 messages are filtered. User can adjust controls (user can't allow virus infected email in). (Central Wyoming College)
22. Spam Assassin offered as an opt-in service. Provide connect-time filtering (source based) by default; allows users to opt-out.
<https://password.uoregon.edu/spam/>;
<http://cc.uoregon.edu/cnews/spring2006/spamassassin.htm>;
<http://cc.uoregon.edu/cnews/winter2005/darkwing.htm> (University of Oregon)
23. Barracuda. Experience has been that it is mostly plug and play; did have to specifically whitelist a URL link that hotmail was putting into their outgoing mail as advertising, which caused Barracuda to dump emails as spam. Suggest not starting with an excessively high number. (Keene State College)
24. Spam Assassin. Tagging at the perimeter has been less effective recently; have implemented a grey listing strategy. (George Fox University)
25. Barracuda just implemented, due to the fact that Spam Assassin, even with the index set at 3.5, still had massive amounts of spam delivered to the Inbox. Barracuda implemented primarily due to functionality provided each account holder. (University of Arkansas at Little Rock)

26. Sophos PureMessage is the university norm; Graduate School of Business implemented IronPort over the summer. Spam catch rate increased from 50% to as much as 75%. Drop known spam, and quarantine suspected spam. Recommends tiered approach: IP check, SMTP protocol check, content filtering (virus), recipient checking (integration with AD or LDAP to valid recipient). (Stanford University Graduate School of Business)
27. CanIt Spamtrap. Reject mail at the perimeter that exceeds the threshold score; sender receives a "could not deliver" flag. (Ithaca College)
28. Tangent, using Barracuda. (Lawrence Theological University)
29. Brightmail. Spam is blocked at the email server. Daily, recipient receives a summary of blocked emails; user can view, delete, or have it delivered. Automatic deletion in 7 days if not delivered. (Lebanese American University)
30. Ironport. Ironport does not allow individual control, so threshold was set at a point to allow some spam in (false negative) rather than risk catching something by mistake (false positive). Clients can use desktop anti-spam solutions (such as built into Apple Mail) to fine-tune and be more aggressive. Stats show that less than 10% of all email is legitimate. Able to remove a server from the cluster due to the decreased load after Ironport implementation. Internal email is not spam-filtered. (Vassar College)
31. Spam Assassin with individual user control. Users use SquirrelMail to customize their settings. Any spam score of 5-8 are still delivered with subject indicating spam; over 8 is deleted completely or moved to spam folder by choice of user. Over 90% of mail is spam for those who have set up filtering. Looking at routing mail to other service providers to scrub it before it enters the network. All internal emails are whitelisted. Initially found that spam sent to lists was being whitelisted; special rules implemented as a result. (Wesleyan University)
32. Barracuda. In use for 1 ½ years. Initial configuration was undersized. Sits outside the firewall and is first level of defense against spam. Currently, less than 15% of mail reaching the Barracuda is passed on to recipients. Internal mail bypasses Barracuda. Users can adjust parameters to control sensitivity. (Bradley University)
33. Barracuda. Getting some complaints about volume of spam getting through, so sensitivity may be increased. Internal messages are filtered on the Exchange server, since internal systems can get compromised. Exchange server provides secondary spam filtering after Barracuda forwards email from the perimeter. (University of Northwestern Ohio)
34. Barracuda. Filters incoming external email. Seeing increases in spam getting through. Internal email does not get filtered. (Illinois College)

35. Spamhaus XBL/SBL, greylisting. Want to drop connection on the vast majority of spam and viruses before the messages are accepted for processing. Often receiving over 1 m. messages/day; usually less than 20% make it past the acceptance checks; another 5-10% is marked as spam by Bayesian filtering and placed in user spam folders. (York University)
36. Barracuda (pair installed). Filter about 6 out of 7 emails at the perimeter. Have not heard of a false positive. User can adjust filter level for spam but not virus-infected email. (Central Wyoming College)
37. PreciseMail and Product/vendor not specified (blacklist subscription services). Blacklisted mail gets dropped immediately. PreciseMail reviews and scores remaining mail. Scores from 3-22.5 get flagged as spam; user determines how to handle it. If above 22.5, held for two weeks, then deleted. 25% of email is sent through to users. (Central Washington University)
38. Postini. Mail first goes to Postini for filtering. Spam, phish, viruses, kept in individual web-based email boxes for optional action by user. User can designate "allowed senders" and "not-allowed senders." Spam kept for 14 days on Postini site. Little effort required by IT staff other than to provide list of authorized account holders. (Pace University)
39. IronPort. Blocks spam at perimeter. Rarely get a "complaint" that an expected email did not get through, and usually the cause is something other than the anti-spam device. (Southwestern University)
40. Meridus 100 (Bluecat Networks). Spam blocked at perimeter. Both a spam and content filter; uses a Bayesian filter and allows SFD checking, dynamic blacklist checking, virus check and recurrent pattern detection. Bayesian filter set at level 3.0 (scale 5-1) with the action of reject. 96% spam with 0% false positives. While ability exists to quarantine messages and allow user to manage filter level and listings, decided not to implement. (Cincinnati State Technical and Community College)
41. Spam Assassin; currently implementing Barracuda. Up until Oct. 23, 2006, tagged spam in header and passed all email; user decides on filter sensitivity. About 13% of over 1 million messages/day passed through without being classified as spam. Increased spam loads have rendered this an ineffective model; as of 10/23, dropping mail scored at 9 or above on an emergency basis until Barracuda is in production; sensitivity may be ratcheted down (dropping mail scored at 9 or above resulted in only a 9% decrease). (Miami University)