

Layered Defense Solution to Fight Spam Using GroupWise and 3rd Party Solutions

Everybody knows that spam is costing companies money. The problem is that these companies do not understand the scale to which this spam is affecting their bottom line. Most spam calculators (www.cmsconnect.com) estimate that spam will cost a company of 100 employees about \$20,000 per year.

Recently, a small financial firm in Alabama put in place a layered defense model to decrease spam and viruses. They found that this model decreased spam by 99.889% and viruses by 100%. This article will delineate the model that they used through need analysis, implementation of components and cost and maintenance.

Need Analysis

Before Greg Cook, IT Director of Cook and Co., spent any money on any anti-spam product, he wanted to make sure that the product, in which he invested his money, was going to be one that fulfilled every need that his company had. He developed three requirements that the anti-spam system had to meet.

The first requirement was that it could be operated in-house. Cook and Co. wanted to be able to monitor the email without having to use the services of a third party. Most companies prefer this for reasons of security, confidentiality and liability. Along these same lines, Cook and Co. wanted a model that did not require the services of a full time email administrator. Instead, they wanted something that could be managed and maintained with minimal effort.

The second requirement was that any solution(s) implemented should fight both spam and viruses. In some cases, viruses can be more damaging to businesses than spam. Cook also placed high priority on insuring that legitimate email would pass and flow through the system without being inadvertently lost or blocked.

The final requirement was that the cost must be reasonable, relative to anticipated volume of legitimate email and within budget. To justify this need, Cook decided that he would calculate the cost per legitimate email based on the cost of the new anti-spam solution.

Implementation of Components

After processing their needs, Cook and Co. proceeded to implement a layered defense anti-spam solution. They felt that the following components best met their needs as described above.

The first line of defense started with a dual processor, dual/mirrored hard drives, and public and private NIC's. This equipment provided the foundation Cook needed to support the other software that he would use. He chose Novell 6.0 for the OS and GroupWise 6.5 for the email software. Novell GroupWise has long been the industry standard for providing security and reliability, thus fulfilling that need of Cook and Co. Additionally, using Novell greatly reduced exposure to viruses since most viruses are targeted towards Microsoft products. The GroupWise Internet Agent (GWIA) allows administrators to use real time blacklists (RBL's) and in-house black lists to effectively block spam. Cook found that the GWIA, with the RBL's and in-house black lists, blocked 4,204 junk emails of the 8,049 that the company received in a day. This represented a 52% reduction in traffic on the network. Moreover, the GroupWise software allows users to prevent dictionary spam, messages addressed to non-existent users, to pass through the GWIA. This stopped an additional 3,159 messages for Cook and Co., reducing the total workload on the server by 91%.

After passing through the first line of defense, 686 messages were scanned and reviewed by the second line of defense. This line was anchored by the McAfee Netsheild for NetWare v. 4.6 anti-virus protection for the email server and McAfee Enterprise 7.0 for the workstations. The McAfee software allows companies to have an automatically updated list of viruses every 30 seconds providing maximal protection. The 686 messages were intercepted by the Windows 2000 workstations which were running Guinevere 2.15, SpamAssassin 2.63 and the McAfee anti-virus software. The Guinevere software deleted or stripped harmful attachments, filtered email for offensive subject matter and deferred attachments too large for prime time network activity. Guinevere passed the contaminated email on to SpamAssassin and McAfee to effectively remove it before it could cause any damage. Of the 686 messages that made it to the second line of defense, only 94 survived. Of the 592 that were stopped, 189 scored high enough as spam to be deleted immediately and 394 scored a high enough probability for spam that they were archived and never delivered to the end user. Finally, 3 were automatically forwarded to SpamCop for reporting and 6 were identified as viruses by Guinevere and McAfee. After passing through the second line of defense, only 1.17% of the messages still existed.

The last line of defense occurred at the GroupWise Message Transfer Agent (MTA) on the email server. The MTA is protected by GWAVA 3.0, and McAfee 4.6 for NetWare. GWAVA scans the messages for spam and viruses and then gives virus infected

emails to McAfee to scan and delete. Of the 94 that were scanned by GWAVA at the MTA, 1 was identified as a virus and deleted, and 8 were identified by GWAVA as potential spam. These 8 were reviewed by an administrator and 2 were released to the end users. After the third line of defense, 99.989% of the messages had been removed due to their contamination as spam or virus and 87 were delivered to the end users.

Prior to upgrading to GroupWise 6.5 and implementing the RBL blocks, Cook's Guinevere and SpamAssassin workstation was processing as much email in one day, as it does today in an entire month! These programs he used in the three pronged defense are all extremely fast and efficient. A legitimate incoming message will hit the user's desktop notifier in well under 20 seconds.

Cost and Maintenance

Cook figured that the total initial cost was \$7,575.00 broken down in the following table.

Layered Defense Model- Cost Analysis

Product	Cost
First Line of Defense	
Dual processor, dual/mirrored hard drives, and public and private NIC's	\$2,500.00
Novell 6.0 and GroupWise 6.5	\$2,000.00
Second Line of Defense	
McAfee NetShield and McAfee Enterprise 7.0	\$800.00
Windows 2000 workstation	\$800.00
Guinevere 2.15	\$500.00
SpamAssassin	FREE
Third Line of Defense	
GWAVA 3.0	\$975.00
Total Initial Cost	\$7,575.00

Cook determined that the system would require maintenance at \$1000.00 annually for 3 years. With this cost added in, he determined that the annual cost of the layered defense model would be \$3,525. He also calculated that in one year he would receive around 31,755 messages (87 messages/day x 365 days/year). Dividing the cost, \$3,525, by the volume, 31,755 messages, he determined that the cost per message was \$0.11.

The additional cost for daily maintenance on the system is minimal. The system usually requires 15 minutes of maintenance each day. This involves scanning the 8 emails that GWAVA pulls out of the MTA. Cook is able to complete the maintenance each morning before work.

Conclusion

Cook figures that running email costs him about \$300 per month. He states that the money he spends on spam protection returns much more in terms of decreased client response time and employee efficiency.

This anti-spam model offers unprecedented results in security, reliability and cost. The layered defense anti-spam model decreases traffic on the server, avoids destructive spam and viruses, and avoids unnecessary costs associated with email maintenance. This anti-spam defense model provides a structure under which you can be sure that your system will be secure from spam.

This is only one example of the many that have found that they have saved tremendously because of the qualities offered by GroupWise and its partners. If you would like to see the full article and breakdown of the layered defense model from Cook and Co., please visit <http://www.cookco.us/spam.htm>.

www.GWAVA.com