

IMail Server



Using IMail Server as a Anti-spam Gateway

Abstract

As the amount of unsolicited commercial email, or spam, arriving in business users' inboxes continues to mount, organizations are looking for effective, low-cost ways to address the problem. Many organizations using groupware products – such as Microsoft Exchange® or IBM Lotus Notes® - have found that their email solutions require expensive and complicated add-ons to block spam, and often provide disappointing results.

A cost effective solution is to place a gateway between the Internet and the internal groupware server. IMail Server has over 20 different methods to identify and stop spam. By using IMail server as a gateway, organizations benefit from off-loading the pre-processing and identification of spam to another computer, intercepting resource-sapping spam before it reaches internal systems and users.

IPSWITCH™

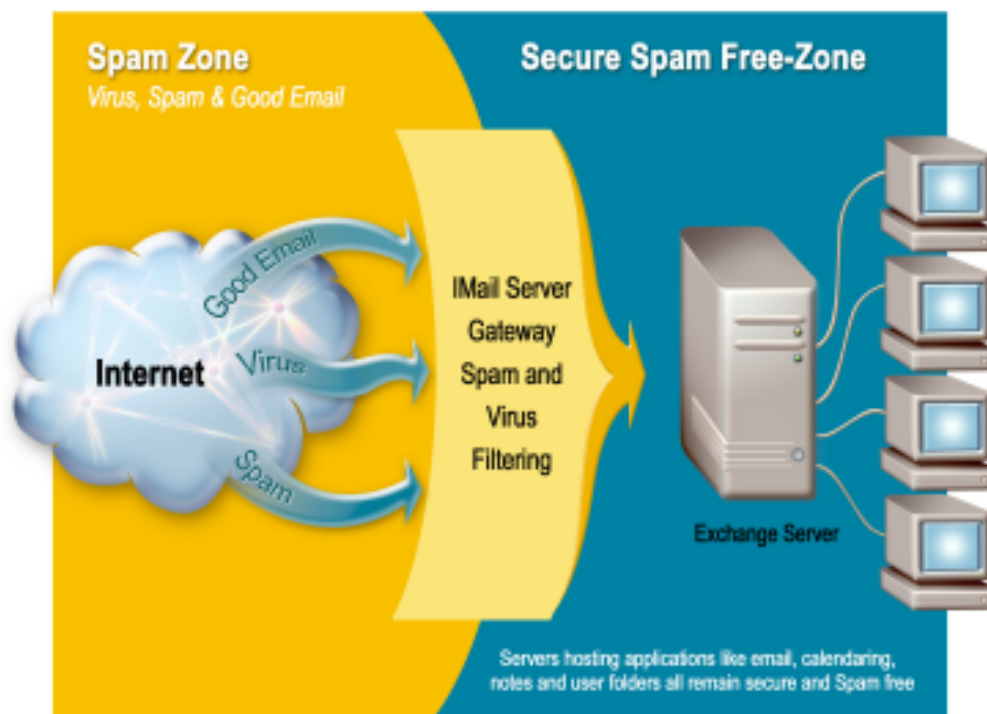
The Problem – Spam in the Enterprise

The negative impact of spam on business is well documented and readily corroborated by virtually every organization that uses email. Dealing with spam is a frustrating and productivity-draining activity for end users. Osterman Research (www.ostermanresearch.com) estimates that spam can cost \$1,400 per user per year in lost productivity. In addition, spam consumes computing resources and can present legal issues for companies that do not take steps to block offensive material from reaching employees. The problem is growing worse. IDC estimates 1.96 trillion spam messages will be sent worldwide in 2003, increasing to 2.28 trillion in 2004¹.

Organizations that rely on a groupware product – such as Microsoft Exchange® or IBM Lotus Notes® – for email are finding that they must install add-ons to block spam. This approach has several drawbacks. Groupware products are often seen as complicated to configure – sometimes requiring a full-time, trained and certified administrator. Installing an add-on only compounds the complexity of the system, and calls for more detailed knowledge of the product. Add-ons can also be costly; even for relatively small organizations client access licenses (CALs) for anti-spam add-ons may easily cost thousands of dollars per year. Lastly, add-ons frequently offer few anti-spam features and do a less-than-effective job against increasingly sophisticated spammers. A simple rules based phrase filter that can search headers, subject and body is easily defeated by today’s spamming techniques.

An Effective Solution – Use an Anti-Spam Gateway

Using an anti-spam email gateway to fight spam offers several significant advantages over groupware add-ons. An email gateway is inserted between the Internet and the groupware server as in Figure 1.



¹ See the IDC study “Worldwide Email Usage Forecast, 2002-2006: Know What's Coming Your Way” at <http://www.idc.com/getdoc.jsp?containerId=27975>

One significant advantage of this approach is improved performance of the groupware server. By offloading the processor-intensive content scanning functions to an email gateway, organizations can free up resources on the groupware server. Groupware servers tend to have fairly substantial system requirements, and system resources on these servers are further taxed by add-ons. Pre-processing spam with an email gateway provides anti-spam functionality without any performance degradation on the server. In fact, an email gateway that blocks spam before it reaches the groupware server can improve performance, enabling organizations to support more users on existing groupware server hardware.

In general, the closer spam gets to the end-user, the more costly it is to the organization. Spam that reaches the end-user has already incurred costs as it passed through the IT infrastructure, and will now cost even more as the end user processes it. Although an anti-spam add-on may block some of the spam from reaching users, valuable system resources are still burdened – including storage space, and the associated costs of system backups. In contrast, the email gateway keeps spam as far as possible from the end-user, while still keeping the functionality in house and most easily managed.

Another key advantage of this approach is affordability. Gateways can cost a fraction of groupware add-ons, particularly for organizations with more than one hundred email users. And although scanning email content does require processing power, compared to groupware servers, an email gateway can be run on less advanced and much less expensive hardware. In addition, because a well-designed gateway is easy to install and configure, this approach can also reduce costs by minimizing administrative overhead.

An email gateway can also improve security, because it complies with the principle of least privilege. Certainly email must be accepted from the outside world, but often Internet access to groupware functions like calendaring and scheduling is not required. With an email gateway only the gateway system is exposed; the groupware server and the sensitive information it holds are insulated from the Internet.

Benefits Of Using IMail Server as an Email Gateway

Organizations that use Ipswitch's IMail Server as a gateway gain all of the advantages of email gateways – including ease of use, affordability, and security. But IMail Server also offers more than 20 different mechanisms to identify and block unwanted email, providing companies with the technology needed to accurately identify spam and combat the ever more elaborate techniques employed by spammers.

Ease of Use

IMail Server is designed with ease of installation and maintenance as a top priority. Many administrators – even those with little experience – are able to install IMail Server and have it up and running in 20 minutes or less. Once installed, IMail Server maintenance is facilitated by features such as remote administration and built-in monitoring, notification, and restart. With no user limits, IMail Small Business and IMail Professional simplify licensing as well. Because there is no client access license, an organization may continue to add groupware users without worrying about exceeding some arbitrary user count.

Affordability

From a pure cost standpoint, IMail Server is an attractive anti-spam solution for most organizations. At \$695, IMail Small Business is typically a small fraction of a company's groupware and messaging budget. A full year of upgrades – including the latest anti-spam technologies -- and telephone technical support is an additional

\$249. Assuming an average cost of \$9 per user for a groupware add-on anti-spam solution, Figure 2 illustrates the cost savings offered by IMail Server as the number of users increases.

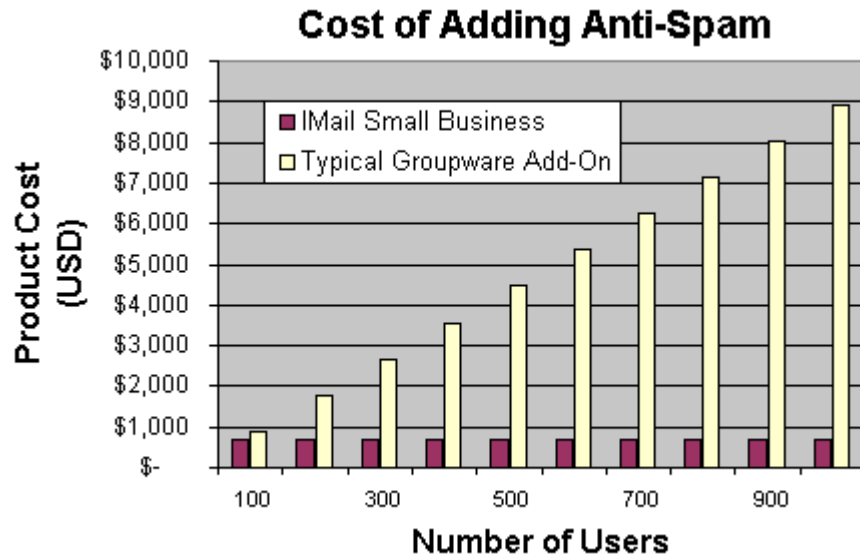


Figure 2: IMail Small Business provides anti-spam functionality at a flat cost

The additional hardware costs of running IMail Server as a gateway on a separate machine are minimal. The system requirements for 10,000 users or less are modest -- an Intel Pentium II based system running at 300MHz, with 256 MB of RAM. Many organizations can re-purpose a decommissioned machine to serve as an IMail Server host at a minimum of cost.

Security

Serving as an email gateway, IMail Server offers multiple security features that protect organizations in a variety of ways. Many of IMail Server's anti-spam measures inherently provide added security, including the ability to block mail from selected IP addresses or domains, authenticating users before allowing them to send mail through the server, and allowing relays only for local users or users on local hosts. IMail Server can also be configured to limit the number of recipients per outgoing message to help prevent spamming from an organization's own users, set maximum outbound message size to enforce service level agreements and usage policies, and scan outbound mail to prevent obscene or confidential material from being sent. With the addition of IMail Anti-virus, an IMail Server gateway can also detect and eliminate viruses before they reach an organization's groupware server. IMail Anti-virus is fully integrated with IMail Server and powered by Symantec™ technology. The anti-virus engine and virus definitions are updated automatically, without requiring individual services or the server to be restarted.

Advanced Spam Detection

IMail Server provides over 20 different techniques to identify and block unwanted email. These techniques employ both content filtering – including Bayesian statistical filters and advanced HTML filtering – and connection filtering – including the use of real-time blackhole lists.

- **Bayesian Statistical Filters** use probability to determine if incoming mail is spam or not. Each email message is analyzed based on how frequently the words it contains appear in valid email compared to spam. When spam slips through, or when valid email is falsely identified as spam, a user or administrator can report the issue back to IMail Server to help the filter “learn” over time. No set of anti-spam rules will work for every company. Through continuous learning these filters become customized for a particular organization as they increase in accuracy and effectiveness.
- **Advanced HTML Filtering** scans HTML-formatted email messages for characteristics common to spam. For example, most spam contains a call to action to visit a Web site; if the URL for that Web site is on a blacklist the email is blocked. HTML filtering also removes HTML tags prior to the statistical analysis of the words in the message. This defeats a common spam technique of embedding comments or invalid tags to intentionally confuse statistical filters – such as “Get Ri<!-- comment -->ch Quick!”.
- **Real-Time Blackhole Lists (RBLs)** are third-party services that maintain lists of domain names and IP addresses of known spammers. They also may simply categorize domain names and IP addresses by geographical region, allowing organizations to block email from regions where they do not regularly do business.

To minimize false positives, organizations can configure IMail Server to use white lists; allowing any email from trusted email or IP addresses to pass through. In addition, IMail Server can be easily configured to use a combination of these techniques to improve its ability to accurately identify spam. For example, an organization may require email message to fail three or more anti-spam tests before it is identified as spam. IMail Server is also fully configurable to meet the specific needs of any organization – phrase lists can be tailored, over time statistical filters learn what an organization’s definition of spam is, and the organization chooses which tests to use to identify spam.

A Cost-effective Anti-Spam Solution

The business problems caused by spam are growing more acute as the ranks of spammers swell. Organizations are looking for economical, but effective ways to eliminate spam and its costs – reduced productivity, burdened IT resources, and end-user frustration. Groupware add-ons can be expensive, complicated, and even ineffective against more sophisticated spammers. By using IMail Server as an email gateway, organizations garner the benefits of advanced anti-spam functionality, simplified administration, and added security, often at a fraction of the cost of a groupware add-on solution.

For more information on IMail Server, including a comprehensive list of IMail Server’s anti-spam features, visit: <http://visit.ipswitch.com/info-icemail>.

About Ipswitch:

Founded in 1991, Ipswitch, Inc. develops easy-to-use, affordable, software products that extend mission-critical IT resources for businesses and improve efficiency for consumers.

Its product family includes WS_FTP Pro, the world’s most popular FTP client; WS_FTP Server with 128-bit SSL encryption, the first industrial-strength, full-featured FTP server for Windows NT/2000/XP; WhatsUp Gold, a leading network mapping, monitoring, notification and reporting tool; IMail Server, a leading Internet messaging server with 53 million users; IMail Anti-Virus, an add-on product powered by Symantec’s CarrierScan™ and fully integrated with IMail Server; and Ipswitch Instant Messaging, a secure Instant Messaging solution specifically designed for businesses.