

IMail Server



Twenty Ways to Stop Spam with IMail Server

Abstract

Spammers are getting smarter. Senders of unsolicited commercial email, or spam, are using increasingly sophisticated techniques and technologies in attempt to ensure their messages reach as many recipients as possible. Not only are there more spammers today, but they are employing a wider array of tactics than ever before. To protect end-users from the productivity-sapping effects of spam, organizations must stay one step ahead. IMail Server from Ipswitch employs more than twenty different ways for detecting and blocking spam, including advanced techniques such as Bayesian statistical filtering, URL domain black lists, and HTML tag filtering (numbers 14, 16 and 17 below). IMail Server provides organizations with the ability to combine multiple techniques to accurately identify and stop spam. With this capability, even spammers who devise a workaround for one or more anti-spam strategies still stand little chance of getting their unwanted messages past IMail Server.

Fighting Spam Requires Advanced Techniques

Spammers – businesses and individuals that send unsolicited commercial email – have proven to be both determined and technologically savvy. Despite miniscule response rates and the ire of email users everywhere, the number of people sending spam continues to grow. IDC estimates 2.28 trillion spam messages will be sent worldwide in 2004, up from 1.96 trillion in 2003.¹ And, despite concerted efforts of businesses to block spam, it continues to sap productivity and drain resources. Spammers are leveraging technology not only to increase the number of messages they send, but also to thwart some of the rudimentary anti-spam approaches that are now in place at some businesses. Simply filtering on phrases such as “Get Rich Quick!” is no longer reliable, as many spammers now use HTML formatting tags to break up the message, disguising it from filters while leaving it readable to end users. Studies conducted by Ipswitch have shown that the effectiveness of individual anti-spam techniques vary from month to month.

Spam can rapidly progress from an annoyance to a serious business problem. At the Lexington Convention and Visitors' Bureau in Kentucky, for example, a legacy mail system was being flooded by up to 200,000 spam messages on some weekends. The situation deteriorated quickly, and employees had problems sending and receiving legitimate mail.²

A multi-layered approach -- which combines a broad set of techniques to turn spam's own objectives, characteristics, and defenses against itself – is the most effective way to fight spam today. Ipswitch's IMail Server uses more than 20 different strategies at multiple levels (see Figure 1) – including connection filtering, SMTP filtering, content filtering and delivery/processing rules – to stop spam. By combining a variety of techniques, businesses can use IMail Server to create an exceptionally effective anti-spam barrier that is custom tailored to the particular needs of the organization.

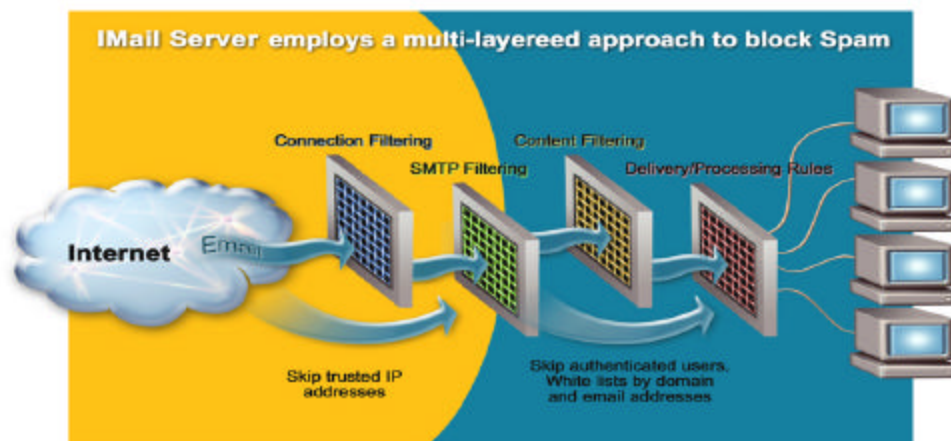


Figure 1: IMail Server employs a multi-layered approach to block spam

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

² http://success.ipswitch.com/success_stories/stories/imail_server

Connection Filtering

Because spammers do not want to be caught, they work very hard to remain anonymous and avoid being traced. The more anonymously they can send email, the more likely it is that they will be able to continue using the same systems and services they are using without threat of interruption. Connection filtering detects many of the methods that spammers use to avoid being traced and also includes mechanisms for blocking spam that comes from known spam senders. Since connection filtering occurs as the sending mail server contacts IMail Server, it is the earliest possible opportunity to block spam, and as such, is also very effective. Connection filtering techniques identify spam by checking characteristics of the sending server and information presented by the sending server before it begins to transfer mail.

1. Domain Name System (DNS) Black Lists (BL) – DNS BLs are databases of known spammers. These databases contain a list of IP addresses that are known to send spam. They also contain IP addresses that have open mail relays, because these systems are frequently used to relay spam. IMail Server can check one or more of these lists each time an email server establishes a connection. If the IP address of the connecting server is on the RBL, then IMail Server will flag any incoming mail from that server as spam.
2. Trusted DNS Black Lists - *Trusted* DNS BLs are lists that administrators deem to be very accurate. Whereas a match on a regular DNS BL might require additional indicators to identify a message as spam, any email received from a system on a trusted list is deleted immediately.
-  3. Verify MAIL FROM - The "MAIL FROM" address provided during the SMTP conversation is verified for each incoming message to ensure that the user is a valid user at the specified domain. If the user or server does not exist, the message is identified as spam.
4. Verify HELO/EHLO domain - The HELO/EHLO domain passed during the SMTP conversation is used to perform a DNS query. IMail Server verifies that the domain specified has an "A" record or an "MX" record. In addition, IMail Server will not accept mail from clients that do not begin the SMTP conversation with "HELO" or "EHLO".
5. Reverse lookup - The IP address of the sending email server is used to perform a reverse DNS lookup to determine the domain name. If the domain has a valid PTR record, the message is accepted. This test does not compare the returned PTR record domain name with the HELO/ELHO domain name; it only tests for the existence of a PTR record. IP addresses without PTR records are usually either dial-up or spoofed, both of which are common indicators of spam. Because some legitimate mail servers do not have a reverse DNS entry, Ipswitch recommends that this test be used in conjunction with the other connection filtering tests to minimize false positives.

SMTP Filtering

SMTP is an open protocol that was designed more for practicality than for privacy. Spammers often take advantage of SMTP's openness to enhance their ability to get more spam through to more people. After two mail servers establish a connection with each other, they initiate a dialog in which the sending mail server tells the receiving server who the next email message is from,

and to whom it is being sent. During this SMTP (Simple Mail Transfer Protocol) exchange, IMail Server employs SMTP filtering rules to stop spam before it is received into the organization's mail system. SMTP filtering is similar to connection filtering but it relies more heavily on the information provided by the sending server, rather than the TCP/IP connection information.

6. Prevent remote mail to local groups – IMail Server can restrict sending email to group aliases to only email sent from the IMail Server computer.
7. Check valid sender – IMail Server will verify the format used in the MAIL FROM field. The email address provided must be in the format of user@host. Some spammers attempt to mask their identity by providing invalid FROM or REPLY-TO information.
8. Disable VRFY command – When this option is disabled, IMail Server will not respond to the SMTP VRFY command. This command is often used by spammers in “dictionary attacks” when they are attempting to harvest or validate email addresses.
9. Wildcard domain kill list – IMail Server will reject all email if the message's sender matches a domain name on the SMTP kill list. Support for wildcards enables administrators to use patterns such as “@*domain.com” to catch any domain ending in “domain.com”, including “@smtp.domain.com”, “@foo.domain.com” or simply “@domain.com”.
10. Email address kill lists – IMail Server will reject all email from senders on its SMTP kill list.
11. Max recipients per message – IMail Server can limit the number of recipients allowed for each message. Spammers often will send one message to hundreds of email addresses at a single organization, but IMail Server can disallow any messages addressed to more recipients than a user-defined threshold.
12. Delay between recipients – With this option, IMail Server will insert a delay between accepting each recipient of an email message. Some spam software transmits all of the recipients without waiting for a response between each email address. However, a standards-based email client will always wait for each email address to be accepted before continuing. By delaying between recipients, IMail Server limits spam while legitimate messages are largely unaffected. This technique also slows down spammers who will often give up in hopes of finding a faster spam conduit.
13. Refuse NULL sender – This feature allows IMail Server to reject incoming email with a NULL sender field. Note that enabling this feature is not in accordance with Internet-standard RFCs (Request For Comment) and will prevent IMail Server from accepting bounced messages from many email servers. Ipswitch recommends that this feature be enabled only after all of the consequences have been considered.

Content Filtering

Because the goal of all spam is essentially the same – selling or promoting a product or service – a great deal of spam content shares common characteristics. Certain words and phrases such as “Silk ties” or “Eliminate debt” appear with such frequency in spam that they can be used as excellent indicators of unwanted email. Other characteristics are also reliable spam identifiers, such as the call to action – “Find out how, click here” – or even the ubiquitous removal notification -- “If you want to be removed from our mailing lists...”. Content filtering turns the spammers' need to promote and sell against them by analyzing the words, phrases, structure and URLs contained within an email message to separate spam from legitimate email. Aware that many businesses have implemented some level of message scanning, spammers have started

obscuring their phrases using HTML formatting tricks. To be effective, content filtering must be able to sift through HTML to find the telltale signs of spam.



14. Bayesian statistical filtering– Some words simply appear more frequently in spam. With Bayesian statistical filtering, the words in an incoming email message are evaluated based on the frequency that they appear in spam and non-spam email. A probability is then calculated on the likelihood of the email being spam. The statistical filters can be updated with an organization’s own sample of good and bad messages to improve the accuracy of the filter. One particularly effective way of helping the filter “learn” is to update it with any spam that it failed to identify on its first pass. Very quickly the filter will be able to improve its ability to accurately identify what constitutes spam for a particular business. Ipswitch periodically updates the default filter with new samples of good and bad email provided from a variety of sources such as spam traps, internal email, customers and partners.

15. Phrase filtering – IMail Server searches through the body of the message for specific phrases. As with the Bayesian statistical filters, Ipswitch continually updates the default filter with the latest phrases being used by spammers. In addition, the phrase filters are fully customizable, because phrases that clearly indicate spam for one business are entirely reasonable for another. For example, while a pet supply business would likely recognize all email containing “Viagra” as spam, a doctor’s office may not.



16. URL domain black list – IMail Server searches through the body of the message for specific URLs that have been cultivated from a large sample of spam. This is a very effective way to identify spam since all spam has some call to action that typically urges the user to visit a web site or other online resource. Ipswitch regularly updates this list of URLs to ensure that it stays current.

17. HTML tag filtering - IMail Server can look for and filter out specific HTML attributes commonly found in spam. Spammers often use HTML formatting in an attempt to circumvent statistical and phrase filtering. For example, spammers may place an HTML comment in the middle of a word, such as: VIA<!--comment here-->GRA. This causes a single word, in this case VIAGRA, to appear as two words (VIA and GRA) to the filtering software, but as a single word to the email recipient. Often, the comments themselves contain neutral words that spammers intentionally use to throw off statistical filters. Without HTML tag filtering, a statistical filter would not catch this, because it cannot distinguish HTML tags from other text. It would merely look for the words VIA and GRA in the organizations list of words frequently found in spam. IMail Server’s HTML parser will extract the comments from the text, so that it can be examined effectively by statistical filtering. It is also possible to consider comments as spam indicators regardless of the text, if needed. In addition to embedded comments, nested tables, invalid tags and image tags are all used by spammers to disguise messages.



embedded comments - An HTML comment which is invisible when the HTML is rendered in a browser or in email.

nested tables – A nested table is one table contained within another table



invalid tags - An invalid tag is a tag that does not adhere to HTML 4.0 standards

image tags – An image tag includes a graphic in the email message.

In addition to these attempts to defeat filtering, spammers also use HTML in a number of other ways. These approaches can also be used to help identify and block spam.

script tags – A script tag directs the email client to run some form of script, typically JavaScript. Spammers often use this as a way to display text after the statistical and phrase filters have scanned the message.

mailto hyperlinks – A mailto hyperlink is a link that, when clicked, will create a new outgoing message.



deceptive URLs - Spammers sometimes encode URLs to conceal the hostname or IP addresses from a content filter. The following are examples of deceptive URLs:

http:// 3232235887/domainname.htm

http:// 0xC0A8016F /domainname.htm

http:// 0300.0250.001.0157/domainname.htm

http:// 3232235887@3232235887/o%62s%63ur%65%2e%68t%6d

hyperlinks – Spammers often include links in their messages as a call to action to visit a website. This may be accompanied by a tag calling an image or graphic. Note that many valid email messages contain links, so care should be taken when enabling this option.

Delivery/Processing Rules

Delivery and processing rules provide an easy way to combine multiple conditions and create advanced scenarios to identify spam.

18. Boolean inbound rules – Inbound rules can search through the header, from, sender, to, subject and body looking for specific words, phrases or patterns. Inbound rules can combine multiple conditions using AND/OR logic, and can be based on the pass/fail status of other anti-spam tests. Inbound rules can move messages to a submailbox, forward the message to another email address, delete the message, send a copy to another email address or bounce the message. For example, an organization may create a rule that applies the following logic: if the subject of the message contains “employment opportunity” AND the recipient is not the human resources department, then forward a copy of the message to the human resources director.
19. Boolean outbound rules – Outbound rules provide the same functionality as inbound rules, but are applied as messages are *sent out from* an organization. Outbound rules can allow the message through, send the message and copy the message to another email address, delete the message, redirect the message or bounce the message. This capability can be helpful in ensuring that no system or person within the organization is sending spam or unknowingly relaying spam.

Educating End Users

One of the most effective ways to stop spam is to educate end users. Informed users are less likely to fall into common traps that spammers use to acquire email addresses and sustain their business. Ensuring that everyone is aware of a few basic rules makes the spammers' job more difficult, reduces inbound spam, and may even help curtail spamming as a practice.

20. User precautions:

- *Never* buy any product or service as a result of a spam message. Spammers only send spam because it is profitable. The closer the response rate drops to zero, the less spam there will be.
- Do not use a valid email address when posting to news groups' list servers, chat rooms or bulletin boards. If giving an email address is absolutely required, disguise it by removing the symbols. For example, instead of jsmith@abc.com use "jsmith at abc dot com", which is much less likely to be automatically detected by email address harvesting software.
- Do not reply in any way to spam. Once you reply, the spammer will know your email address is valid and will share it with other spammers. This includes requesting to be removed from their lists, replying via email, telephone, fax or clicking on links within the message.
- Do not use your business email address online unless you trust the organization collecting it and you know how it will be used. Instead, use a disposable account on one of the free email services for situations where you are unsure of how your information will be used.
- If possible, turn off your email client's ability to preview messages or disable outbound HTTP for the mail client. Many spam messages have links in them that report back to a Web server as soon as you view the message.
- Forward spam to the IT department. IT staff will then be able to modify filters to catch similar messages in the future. Try to keep the message headers intact, as this will help the IT department track down the source of the message.

ASSESSING YOUR SPAM RISK

What you do online and where you provide your email address dramatically effects the likelihood of making it onto a spammer's list















LOW	HIGH
 <p>Provide Email Address to a Known Vendor Make sure you read their privacy policy.</p>	
 <p>Provide Email Address in a Web Guest book Many spammers use programs called 'bots' that monitor web sites and harvest email addresses.</p>	
 <p>Post Email Address to a Newsgroup Disguise your email address: for example spamtrap 'at' ipswitch dot com instead of spamtrap @ipswitch.com</p>	
 <p>Use Email Address in a Chat Room Many spammers use programs called 'bots' that monitor chat rooms and harvest email addresses.</p>	
 <p>Opening Spam Spam can include links back to the spammer's server verifying your email address.</p>	
 <p>Reply to Spam Most of the time the reply address is fake, if it is not, you will be confirmed as a "good" email address.</p>	
 <p>Buy Spam Product The main reason most spam is sent is to make money which means people have to purchase a product or service.</p>	

Figure 2: Educating end users about online behavior that encourage spam is an effective way to reduce it

Preventing False Positives

All anti-spam methods have the potential to occasionally flag a valid message as spam. IMail Server provides a number of features to help prevent these false positives, while maximizing the amount of spam that is blocked:

- Skip authenticated users – IMail Server can allow all email from authenticated users (users that provided a username and password during the SMTP transaction) to bypass the content filters. This is useful in many corporate environments where all users on the system are trusted to not send out spam. Service provider users' intentions are not as clear and even email from authenticated users on the server may need to be scanned for spam.
- White lists by domain – All email from a specific domain will bypass the content filters.
- White lists by email address – Messages from a specific email address will bypass the content filters.
- Trusted IP addresses – Messages from a specific IP address will bypass content and connection filtering.

Cost-effective Messaging with Effective Anti-Spam Technology

Organizations must combat the increasingly devious methods of spammers with advanced techniques and technology. Whereas many anti-spam solutions employ one -- or at most a handful -- of different techniques, IMail Server provides a broad range of advanced technologies that can be combined to effectively defeat the advanced techniques of today's spammers. By using IMail Server, businesses can minimize spam and its costs – reduced productivity, burdened IT resources, and end-user frustration – with an easy-to-administer, secure and cost-effective messaging solution. For more information on IMail Server visit http://www.ipswitch.com/Products/IMail_Server/.

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 60 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.