IronPort™

GET THE MESSAGE?

Best Practices in Email Marketing

Email marketing has proven its value, delivering higher customer responses at 1/20th of the cost of traditional direct marketing channels. As a result most major marketers have embraced some type of email marketing, ranging from simple email newsletters to highly sophisticated CRM systems that target messages and promotions to specific users. But the dramatic advantages of email marketing have also created new challenges for companies trying to communicate with customers via email. A shadowy industry of "spammers" has sprung up to attempt to leverage the power of email marketing by sending unsolicited and often offensive messages to massive Internet audiences. IronPort Systems estimates that as much as 60% of all email traffic is unsolicited spam. As a result ISPs, Corporations and Universities are deploying increasingly aggressive spam-filters. Since spammers are constantly evolving their messages to look like legitimate messages, these spam filters are blocking as much as 30% of the outgoing mail of a legitimate email marketer.

> ***"Mail that is sorted into bulk folders often remains unopened. Seventy six percent rarely or never read emails in this folder."***
>
> —DoubleClick 2002 Consumer Email Survey,
> October, 2002

BULK MAIL JAIL

The problem of legitimate commercial email getting caught in spam filters is insidious. It is widespread, difficult to measure, and is likely to remain an ongoing issue over time.

> ***"Mail that is sorted into bulk folders often remains unopened. Seventy six percent rarely or never read emails in this folder."***
>
> —DoubleClick 2002 Consumer Email Survey, October, 2002

Blocking spam is a cat-and-mouse game. ISPs and corporations will deploy new filtering techniques constantly. As fast as they do, there are intelligent humans sending spam who detect that their messages are getting blocked, and they create and send new permutations until they detect their messages getting through. This "arms race" seems to have no near-term end. As ISPs and Corporations are deploying powerful content filters with highly sophisticated rules derived from genetic research, spammers are beginning to put their messages into images, which cannot be read by content filters. As a result of this arms race, ISPs are constantly changing the "rules" and legitimate email marketing messages that were delivered today could be blocked tomorrow.

> ***"E-Mail Marketers' Worst Nightmare: AOL 8.0"***
>
> —New York Post, October 22, 2002

The problem is exacerbated by the fact that if an ISP or corporation determines a message is spam, it typically doesn't notify the sender; it just labels the message as spam and shunts it into a bulk mail folder, in effect deleting it. Spammers set up elaborate networks of mailboxes at ISPs to monitor their delivery rates. Few corporate marketers have resources to implement this type of labor-intensive system thus most corporations are unaware that their messages aren't getting through.

TRIP WIRES

The mechanisms that ISPs and Corporations use vary widely and change over time. However, there are some fundamentals that are guaranteed to cause problems every time. These "trip wires" are outlined below:

1. **No reverse DNS —** A sender of mail must ensure that their reverse DNS is properly configured. When the sending mail server connects to a receiver, the receiver will typically do a reverse look-up on the sender's IP address and get a PTR record (the fully qualified domain of the sending server). Diligent MTAs will perform a double-DNS lookup and verify that the PTR record and the DNS A record match. The ISP may then compare the domain name of the PTR record, the DNS A record, the envelope mail from and the SMTP HELO command. If any of these do not match the ISP may assume it is an attempted forgery and mark the message as spam.

2. **Bad bounce management —** Connections from servers whose recipient lists consistently generate a high bounce failure rate. (i.e. when over 10% of a sender's mailing list is destined for users that do not exist) may be blocked. ISP's may also reject connections from senders who are unable to accept return messages at the MAIL FROM (also known as envelope sender or return path) and FROM/REPLY TO addresses

3. **Too many connections —** If a sender of mail opens too many connections at one time or does not properly spread connections across multiple receiving gateways the ISP will often assume the incoming messages are a spam flood and will block.

4. **Too many messages per connection —** If a sender attempts to deliver too many messages per connection the receiving ISP will often begin blocking.

If the sender's IP addresses show up on at least one of the commonly used public blacklists then many ISPs and corporations will block all incoming mail. A sender can get added to these blacklists for a number of reasons including an improperly configured "open" relay or proxy server that allows others to relay mail through their network, high complaint rates from end users or a number of other reasons.

BREAKING THROUGH

IronPort Systems has developed a family of high performance messaging gateway appliances that have built-in intelligence to address the mechanics of spam filters and increase delivery rates. These intelligent features operate as follows:

1. **DNS check —** IronPort offers a DNS check to its customers. By including the address dsncheck@ironport.com into the sender's database, IronPort will continually test the senders reverse DNS configuration including a double DNS lookup. If there is a problem a message will be sent to the IronPort appliance, which will alert the system administrator. The IronPort customer engineering team can also provide technical documentation on proper DNS configuration.

2. **Global unsubscribe —** Global Unsubscribe complements a company's ongoing list management practices by ensuring certain email addresses are excluded from all outbound campaigns. For example, some organizations may want to globally unsubscribe role account addresses such as postmaster@ or support@, which do not ordinarily appear in legitimate mailings. IronPort's MXCheck can also poll the MAIL FROM or FROM/REPLY TO domains periodically to ensure they are listening on port 25 and are ready to accept mail.

3. **"Good Neighbor Algorithm" —** The IronPort A-Series appliances have a built-in "Good Neighbor Algorithm" that automatically manages connections with receiving ISPs. The IronPort appliance will begin opening multiple connections per receiving domain, spread across all of the receiver's servers in accordance with the receivers MX preferences. The IronPort appliance will keep opening connections until it senses that the aggregate data rate being sent to that domain has flattened out, at which point it gracefully backs off and stops opening new connections. In addition, the IronPort appliance has a manual over-ride for the maximum number of connections for a given domain. This gives the sender the ability to hard limit the maximum number of connections opened to any specified domain.

4. **Message groups —** The IronPort A-Series groups messages bound for a common domain and maintains a separate queue for each receiving domain. It will send multiple messages per connection, with a configurable limit on the max number of messages per connection. Users can also configure bounce retry intervals per destination, providing the administrator maximum flexibility in dealing with individual ISPs.

5. **Automatic alerts —** IronPort customers receive automatic alerts if any of their bonded IP addresses show up on any one of 10 public blacklists.

BEST PRACTICE: SEGMENTING TRAFFIC BY IP

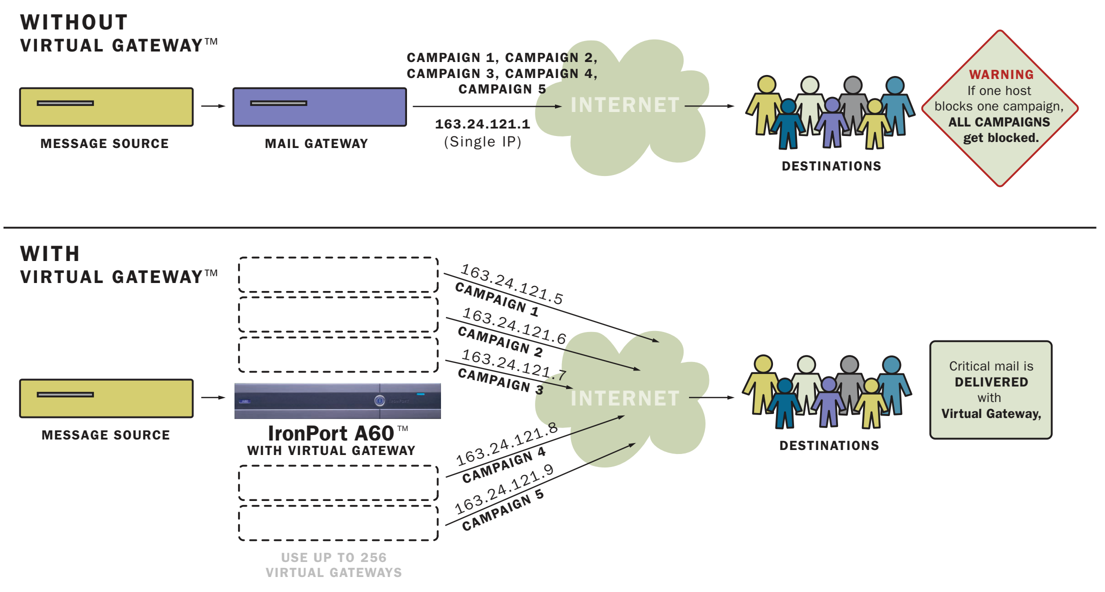
The four networking techniques discussed above can help minimize issues with receiving ISPs, however, experience has shown that even the most carefully managed commercial email program can still run in to problems that lead to blacklisting or blocking. To minimize this, sophisticated marketers have begun the practice of putting certain classes of traffic on specific IP addresses. The largest service providers now put each of their customers on unique IPs, and often provide them with different IP addresses for different campaigns.

Best Practices in Email Marketing

Within any large corporation there are distinctly different classes of traffic ranging from Employee emails, to customer service messages, transaction confirmations, customer retention programs, and new customer acquisition programs. The first and most basic step is to separate commercial emails from employee emails. This is best implemented by using a separate gateway with separate IP addresses and domain names for each type of mail. Too many IT departments have felt the pain when marketing drops a large bulk mailing into the corporate gateway, plugging the corporate queues and getting corporate mail rejected at multiple ISPs.

> ***"If you want to deliver mail to AOL, you need to segment your traffic by IP."***
>
> — Joe Barrett, SVP of System Operations,
> AOL at SpamJam Conference 2003

The next level of sophistication is to begin to separate the different classes of commercial traffic. The transaction confirmations get one IP address, the customer service messages get another, the email marketing gets yet another, as illustrated below. This acts like "water tight compartments" limiting problems only to the class of traffic that caused them. Many customers will set up multiple IP addresses for marketing – known good lists are run on one trusted IP, unknown or new lists are run on a different IP.



The IronPort solution offers a simple and powerful way to segment traffic. As campaigns are created in the marketing automation software, the IronPort appliance can be configured to filter all incoming mail and identify different campaigns based on encoded strings in the message header. The IronPort appliance has a unique feature called Virtual Gateway that will assign each campaign its own unique IP address. This type of segmenting yields the most robust and reliable delivery of commercial email.

Best Practices in Email Marketing

TRUSTE/BONDED SENDERS GET DELIVERED

In addition to the networking techniques and architecture discussed above, IronPort has developed a program to help identify legitimate senders of mail called Bonded Sender.™ Under the supervision of non-profit Internet Privacy group TRUSTe, Bonded Sender represents the "Good Housekeeping seal of approval" for email senders. Bonded Senders agree to adhere to a high set of standards for email delivery and "put their money where their mouth is" by placing a financial bond that ensures the legitimacy of their traffic. If users complain beyond a certain rate (i.e. 1 complaint per million messages), the sender agrees to pay a fine of $10 per complaint. In exchange for their participation in the program, Bonded Senders get preferred delivered at thousands of ISP's, companies and universities. This simple market based mechanism is meant to have little or no cost to a legitimate sender, but would be prohibitive for a spammer.

Once a sender is accepted into the Bonded Sender Program, the sender selects some or all of their IP addresses to bond. Many corporations will choose to bond the corporate mail, transaction and customer service mail, and marketing programs aimed at existing customers. New mailing lists or unknown campaigns are run on a separate non-bonded IP. IronPort's Virtual Gateway technology makes this segmentation possible.

The largest ISPs have sophisticated abuse departments that deal with deliverability issues. Best practices have shown that any company doing large-scale email marketing is well served to establish a direct dialog with these ISPs. Since many of these ISPs are IronPort customers, IronPort can facilitate introductions to the right organizations within these large entities.

One of the most difficult parts of managing receiver relations comes from the fact that the receivers that fall outside of the 5 largest ISPs don't have abuse teams or contacts or procedures. The Bonded Sender Program is targeted at the large universe of receivers beyond the big 3 that make up as much as 60% of the deliveries for many email marketers. The Bonded Sender Program currently reaches a remarkable 8,000 ISPs, Universities and Corporations. These receivers access the Bonded Sender list of IP addresses using a DNS query, and route mail from Bonded Senders around any content filters, avoiding any potential false positives. Bonded Sender processes more than 200 million messages per day, and has been growing at more than 30% per month.

SUMMARY

The power and promise of email marketing has lead to challenges that are a by-product of the explosion in spam. However, with tools and technology from companies like IronPort, legitimate senders of mail will have little difficulty getting through and will be able to harness this incredibly powerful new channel for customer communication.

IRONPORT™

IronPort Systems, Inc.
1100 Grundy Lane, Suite 100
San Bruno, California 94066
tel 650.989.6500 **fax** 650.989.6543
email info@ironport.com
www.ironport.com

THE IRONPORT STORY

IronPort Systems is focused on one goal: to revolutionize Internet Messaging. We have developed a family of products called Messaging Gateway™ appliances that offer breakthrough performance, unprecedented ease of use, and reduced total cost of ownership. The IronPort team has done it before: our technology stems from experience at Hotmail, eGroups, ListBot, and Yahoo!