Enhanced Messaging Security: Slicing Spam and Other Threats At The Network Edge

Overview The volume and sophistication of attacks that threaten business email networks and systems are growing at exponential rates. This growth curve poses significant problems for IT and security groups trying to manage these threats.

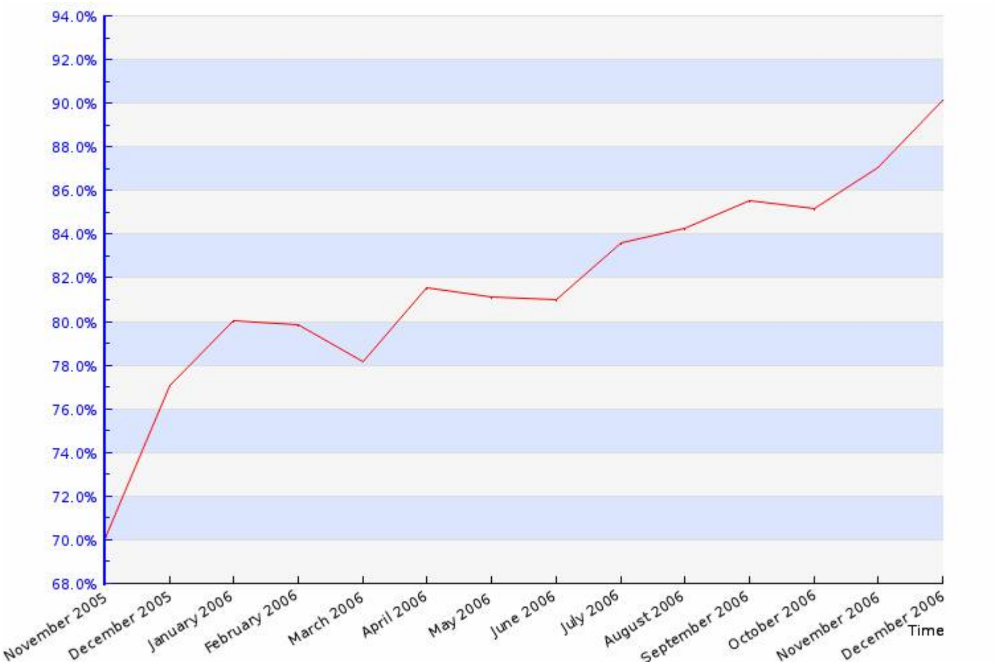
In this white paper, you'll learn about:

- The current types of email threats
- Why the exponential growth in email volume poses significant challenges for the corporate network infrastructure
- How adding a messaging security layer at the network edge addresses these challenges, and significantly scales and strengthens an overall messaging security solution.

Challenge According to recent studies, the current volume of email sent worldwide is now over 75 billion messages per day. By 2008, this number is expected to rise to a volume of 100 billion per day or more. This exponential increase in message volume has the capability to overwhelm corporate email systems. About 85% of all email worldwide is "unwanted," a percentage that has been growing steadily over time. Unwanted email includes spam, viruses, malware, Trojans, denial-of-service, and phishing attacks. Even more troublesome is that the volume of total unwanted email is *doubling* every 6-9 months.

Spam Volumes Are Out of Control

% of Worldwide Email That Is Spam



Threats to corporate email security can be grouped into four primary categories:

Spam
Spam is broadly defined as any message that is unsolicited and unwanted, or “junk mail.” Most spam messages attempt to sell products or services; a large percentage of these messages are pornographic or otherwise offensive.

Phishing
Phishing is a scam in which fraudsters "fish" for personal information by pretending to be a legitimate company. These attempts often claim that your account is in jeopardy and ask you to validate, confirm or update information such as credit card numbers.

Viruses
Viruses come in many forms. Some are intended merely to cause a nuisance and block network traffic temporarily, while others, such as Trojans, are designed to steal vital information and relay it to an external server controlled by the hacker who created the virus.

Zombies
Zombies are the newest threat to enterprise network security. A zombie PC is one that has been taken over by a remote hacker through the use of Trojans, which are files that appear to be legitimate but instead are viruses that hijack a PC and use it to send spam, viruses, DoS attacks and phishing scams. These zombie machines are networked and used in conjunction with each other to send thousands of messages each, often targeting specific entities.

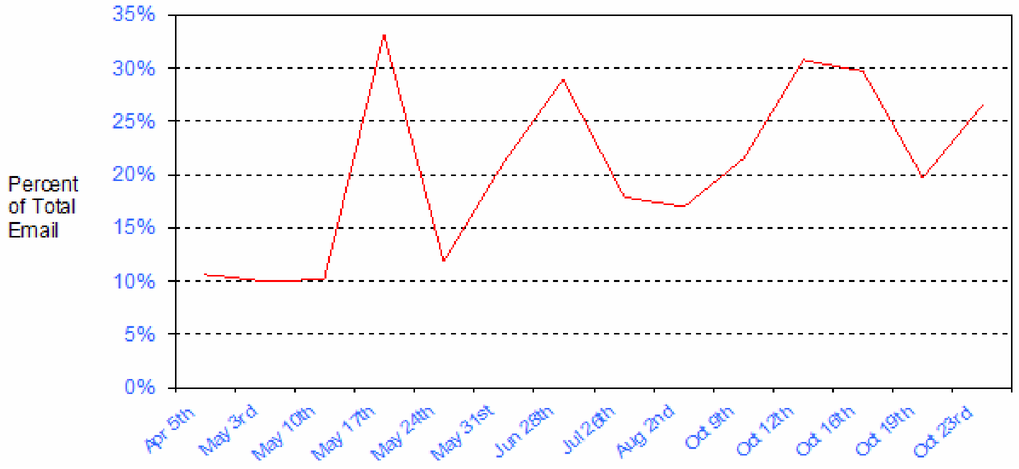
While each of these categories poses a unique threat to email security, many attacks combine several elements to exploit multiple vulnerabilities simultaneously.

Detecting Spam
Unwanted email is becoming more difficult to detect, mainly because attackers are professionals with the budget and technical prowess to develop spam, phishing attacks, viruses and zombies that can get through existing filters. Gone are the days of lone hackers working late at night. Many of these hackers run teams of engineers with very sophisticated equipment and technology.

Professional hacking teams typically have all the same security software that corporations do, and will constantly test their strategies to see if they can outsmart the filters. One example of this is *hash busting text*, where spammers will have their zombie networks send out emails that are each unique and cannot be recognized with a hash. Another example is the increasing use of image-based spam, where all the text is in image format, and even the images can be made to vary uniquely (more hash busting). This makes it very difficult to detect email based solely on the content of the email.

The net result is that the reputation of the sender is becoming more and more important as a way to detect unwanted email. Legitimate senders with good reputations will rarely send spam, and if their systems are ever compromised by a zombie, their reputation score will almost immediately reflect that and their emails can be flagged as unwanted until their systems and corresponding score returns to normal.

Hard-to-detect Image Spam is Growing – A Six Month Window, 2006



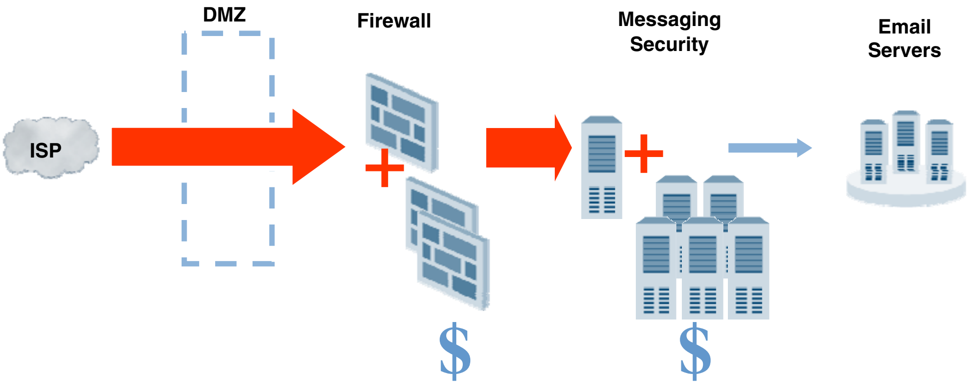
The Corporate Messaging Security Challenge
Every message that crosses the corporate gateway uses valuable bandwidth, which is already in short supply in most organizations. IT departments are being forced to add additional mail security gateways and mail servers to their infrastructure as the volume of mail outstrips the capacity of their existing machines.

Considering that the inbound mail volume at many companies is doubling every three to four months, mainly due to bad emails, it's easy to see that IT departments have a significant challenge on their hands trying to purchase, test, and install the components of their rapidly growing email infrastructure.

IT departments are forced to manage these increasingly complex infrastructures, requiring valuable man-hours. In addition, administrators must learn the intricacies of several different programs and control ever-expanding racks full of servers – an expensive proposition for many organizations.

Reactive Approach….

- Ask for more budget
- Add more bandwidth
- Add more Firewall capacity
- Add more Messaging Security capacity



Simply adding hardware is a reactive approach. Considering the growth rate of inbound email, to double or triple hardware and infrastructure costs every 6-9 months is simply not in the budget. To take a more proactive approach, many administrators are starting to use products or services that look at the sender's reputation. By doing so, they hope to eliminate bad email at the connection (network or TCP/IP) level. While the intent is laudable, the issues with many of these reputation services are numerous.

By deploying an email gateway MTA such as Sendmail, Postfix or any of a number of other alternatives, administrators attempt to cut down the number of messages passing through. Unfortunately, each of these solutions requires additional levels of security in order to accurately and effectively reduce message volume to a tolerable level. For example, to cut down on spam volume, a Sendmail environment may rely on Spam Assassin to reduce spam, Panda Perimeter Scan for anti-virus protection, and several other products to address other individual threats.

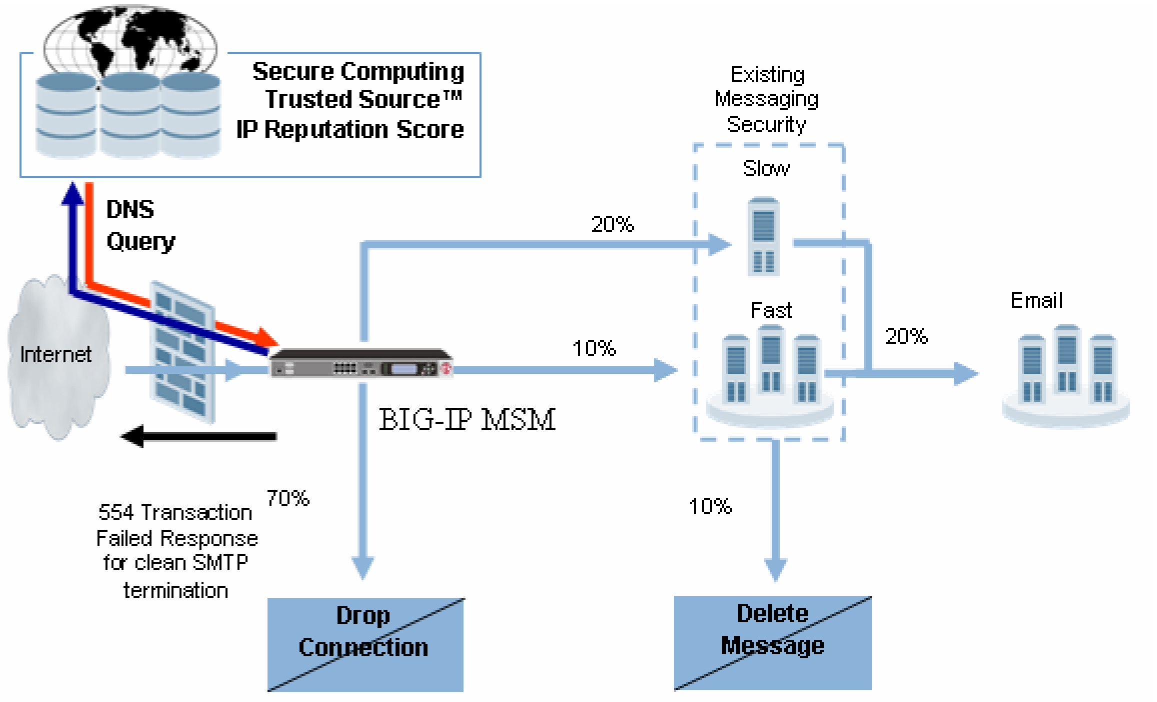
The obvious weakness in this approach is that each of these products is designed as a stand-alone application; few, if any, are designed to interact with applications from other vendors, leaving a gaping hole in the correlative intelligence-gathering process necessary for effective overall security. Each message content filter is forced to download the message data from the previous gateway, eating up valuable bandwidth. In addition, each application loaded onto a box requires additional processing power (rackspace, power, admin effort), and must query multiple outside sources to obtain up-to-date information each time a sender tries to connect to the network.

Solution A Better Approach

Rather than trying to add more hardware and multiple new layers to the infrastructure, consider another approach. A typical (simplified) messaging architecture involves email traversing the network edge, followed by the email security gateway, and finally the email server. The intelligence in these email security gateway products employ multiple techniques, including anti-virus scanning, deep content inspection, filtering for keywords and heuristics, and custom rules. More recently, the notion of a sender's reputation as a key factor in categorizing and managing inbound email has emerged as a critical step in the process. To handle the email volume, as well as for high availability and redundancy, most organizations virtualize multiple security gateways and mail servers behind an application delivery networking controller such as BIG-IP® Local Traffic Manager (LTM). Rather than continuing to add secure gateway hardware to this infrastructure to handle growing email volumes, a better approach would be to add security intelligence at the network edge, cutting down the email that passes on to the email security gateways and servers for further inspection and processing.

F5's BIG-IP Message Security Module

F5's Message Security Module (MSM) on BIG-IP LTM is a network-edge solution which adds security intelligence to manage and filter inbound email traffic by considering the sender's reputation when making traffic management decisions. MSM leverages TrustedSource™, Secure Computing's revolutionary reputation system, for information about every sender that attempts to connect to the protected enterprise's mail servers. TrustedSource is the first and only reputation system to combine traffic data, whitelists, blacklists, and outbreak detection with the unparalleled strength of Secure Computing's global customer network of more than 1600 customers in 40 countries, including over one-third of the Fortune 500. It is also the only reputation system available that is able to provide numerical scoring for every IP address across the Internet (approximately 4.2 billion.)



When BIG-IP receives an SMTP connection request, it will hold the response to the sender until the sender's reputation is checked against TrustedSource. An administrator has incredible flexibility in determining what to do with the email based on that reputation, including partitioning email traffic between various pools of email gateways and servers for "fast-tracking" known *good senders*, redirecting senders with questionable reputations, and immediately dropping known *bad sender* connections with an error code telling them not to retry the connection, as it will only lead to another rejection.

By filtering out known spam senders with MSM, administrators can eliminate up to 70% of their email volume right at the network edge. This significantly cuts down on the bandwidth and expanding hardware costs required to deal with the remaining 30% of email passed onto existing security gateways and mail servers, and helps maximize existing messaging security solutions already in place. Note also that adding an edge device before or after the traffic manager or load balancing device can complicate mail traffic flow and requires additional resources to ensure the high availability that is already built into the BIG-IP system.

Benefits of Implementing BIG-IP MSM

BIG-IP MSM adds value to corporate email security efforts in several areas:

- **Decreased load on the network, security devices and messaging servers** – By identifying and blocking known "bad" IP addresses, MSM can reduce the intake of messages into the network by up to 70%. This is critical in handling the constantly increasing load of mail.
- **Infrastructure growth control** – By significantly decreasing the load on mail servers, MSM allows organizations to handle the additional mail volume, often without the expense of adding expensive mail gateways or servers.
- **Increased effectiveness** – If a known spammer tries to use a new technique to evade detection, MSM will still recognize the origin of the message, causing it to be blocked. Email security solutions that do not employ IP-based reputation will be unable to maintain their effectiveness against new threats.

Conclusion

The load and risk imposed on your network by unwanted email is growing. It's not just annoying your employees and burdening your IT staff, but its dangerous as well. Historical single-layer deep inspection architectures for dealing with high volumes of spam are no longer adequate. A new architecture is needed that enables you to scale easily, avoid ongoing large investments in messaging security technology, and quickly ease the burden on your messaging systems. F5 MSM is a unique product that can solve all of these problems and is built on the trusted and widely deployed BIG-IP system and TMOS platform.

About F5

F5 Networks is the global leader in Application Delivery Networking. F5 provides solutions that make applications secure, fast and available for everyone, helping organizations get the most out of their investment. By adding intelligence and manageability into the network to offload applications, F5 optimizes applications and allows them to work faster and consume fewer resources. F5's extensible architecture intelligently integrates application optimization, protects the application and the network, and delivers application reliability—all on one universal platform. Over 10,000 organizations and service providers worldwide trust F5 to keep their applications running. The company is headquartered in Seattle, Washington with offices worldwide. For more information, go to www.f5.com.