



Symantec TurnTide™
AntiSpam Router:
Fighting Spam
with a Multi-Layered
Architectural Approach

Symantec TurnTide™ AntiSpam Router: Fighting Spam with a Multi-Layered Architectural Approach

Contents

Executive summary	3
The spam threat	4
The cost of spam	5
The 'hidden' cost of spam	5
The problem will only increase	6
Spam defense 101	6
A new perspective on spam defense	7
A multi-layered architecture for spam defense	9
The value of a perimeter defense in practice	11
Symantec TurnTide AntiSpam Router as a Perimeter Defense	12
Conclusion	13
References	13

Symantec TurnTide™ AntiSpam Router: Fighting Spam with a Multi-Layered Architectural Approach

Executive summary

Spam has exploded from an annoyance to an economic and security risk that threatens the viability of email as a communications medium. Recent surveys have shown that up to 80% of all email is now composed of spam. From an economic perspective, spam cost U.S. businesses some \$10 billion last year, and this number is growing. The undercounted and underreported productivity costs may even be higher. Furthermore, spam has become a major vector for the transmission of viruses, worms and other malicious code.

By now, most organizations have adopted an antispam strategy. Unfortunately, many organizations are using an overly simplistic approach to a complex security and economic problem, by placing all of their defenses in a single layer of defense, such as mailbox or server filtering. Just like the Maginot Line of the early 20th century, these single lines of defense are about to be (and in some cases already are) overloaded by the increasing onslaught of spam traffic. No single product is foolproof at defending an organization from all threats, and any single point of failure will compromise the security of the organization as a whole. Applying the same defense at multiple places, such as filtering at both the server and the inbox layers, is like having two locked gates – both of which can be opened by the same key. Organizations should employ multiple methodologies that require the spammer to use multiple methods to attempt to sidetrack the defense. Moreover, defenses should be employed that attack the problem effectively from both the security and economic perspectives.

The security principle of “defense in depth” can be applied to provide an effective security and economic deterrent to the ever increasing volume of spam. The key to reducing the risks associated with spam in today’s environment is to deploy a multi-layered approach to defend the organization – significantly reducing spam volume while keeping false positives (and expenses) low. These defenses are deployed in three layers:

- **The Mailbox Zone** – where individualized filtering and blacklisting predominate
- **The Server Zone** – where SMTP servers are protected via filters or appliances
- **The Network Zone** – where an entire network is protected via a perimeter defense

Symantec TurnTide™ AntiSpam Router: Fighting Spam with a Multi-Layered Architectural Approach

The defense of the Network Zone is a new and emerging trend that shows enormous promise as both a perimeter security defense as well as an effective economic defense. It also provides a complementary layer of defense, adding strength to the innermost two layers with a unique approach. Deploying a perimeter defense in the Network Zone provides a new opportunity to:

- Control the explosive growth of spam volume, often freezing volume related costs
- Physically keep spam from ever entering a protected network
- Actually fight the spammer's economic model
- Increase the scalability and effectiveness of filtering solutions in the other two zones
- Extend control to outbound as well as inbound spam

The Symantec TurnTide AntiSpam Router is the first in an emerging class of solutions designed to provide perimeter defense in the Network Zone, and has been proven to provide a maximum level of protection combined with a unique ability to reduce and control the cost of spam.

This white paper describes the nature of the spam problem and provides a tutorial on the effectiveness of a multi-layered architectural approach in the fight against spam.

The spam threat

The problem posed by spam has evolved from an annoyance to email users to a global problem that threatens the usefulness of email as a 21st century communications tool.

In fact, clients of the influential Gartner Group report that up to 80% of all incoming email is spam¹. Different organizations may experience different levels of spam, but clearly there is no denying that what began as a trickle of unsolicited messages has turned into a flood of IT resource and security problems, robbing organizations of communications bandwidth, productivity, and money.

The spam threat has become so severe that a recent cover story of InfoWorld² reads:

"Email is broken. Attempts to fix it have failed. Spam keeps clogging inboxes. Viruses keep slipping through. The situation is now critical. It may not be salvageable."

With leading industry publications making such dire predictions, is it any wonder that the spam problem has leaped to the forefront of the concerns of IT managers? A recent survey conducted by TechRepublic³ showed that 65% of the IT managers surveyed considered spam management to be among the top three priorities for their organizations today.

Symantec TurnTide™ AntiSpam Router: Fighting Spam with a Multi-Layered Architectural Approach

The cost of spam

The increasing volume of spam brings with it a huge cost to the legitimate businesses that bear the brunt of the costs of spam volumes. According to Ferris Research, spam cost businesses in the U.S. alone more than \$10 billion in 2003⁴.

With every spam message received and processed, IT organizations incur costs. These costs are largely in the following areas:

- **Network Bandwidth** – Every spam email message, whether it is blocked from email servers or not, consumes network bandwidth.
- **Server Capacity** – An organization's email servers must process messages as they are received. If spam filtering software is used, this software also consumes CPU cycles.
- **Storage Capacity** – Spam messages accepted into the email network must be stored (and potentially archived).
- **Spam Defense** – If an antispam solution is in place, it must be licensed and must use the network and processing resources of the organization.
- **Administrative Costs** – IT administrators support corporate email. As spam increases the inbound email volume, administrative costs increase accordingly.

In addition to its drain on the IT budget, spam has also become a major vector for viruses and all sorts of malicious code entering an organization. According to the META group, some 80% of all virus incidents are initiated by Internet-delivered email⁵.

Spam does damage in other areas as well. Due to the high volume of pornographic and offensive content in spam, organizations are increasingly exposed to the threat of “hostile work environment” lawsuits and other legal and regulatory headaches.

There are other problems related to spam that result in many costs and exposures to an organization such as ‘phishing’ attacks, directory harvesting attacks, denial-of-service attacks and more.

The ‘hidden’ cost of spam

A huge and mostly hidden cost of spam is the lost productivity due to email users sorting through their email to separate the legitimate email from the spam. The aforementioned report from Ferris Research⁴ estimates that these costs make up 42% of the overall cost of spam and more importantly, due to its nature, these costs are invisible to IT organizations.

Symantec TurnTide™ AntiSpam Router:
Fighting Spam with a Multi-Layered Architectural Approach

The problem will only increase

The Radicati Group estimates that the flood of worldwide spam volume will reach 35 billion messages in 2004, and may increase to 142 billion messages by 2008, if nothing succeeds in turning the tide⁶. In addition to the increase in overall message volume, spammers are increasingly resorting to graphically intensive html-formatted and even multimedia messages in an attempt to increase their response rate. In doing so, they are greatly increasing the average size of individual spam messages, worsening the issue of spam.

Spam defense 101

As you would expect, few IT organizations are taking this assault lightly. A number of tools have emerged to help fight spam. These antispam tools take a number of forms and are deployed in a number of ways, but like any other tool, they can be graded according to their effectiveness and accuracy. With regard to spam defense, these terms have specific meaning:

- **Effectiveness** – Refers to the percentage of actual spam that is detected and acted upon. 90% effectiveness means that 9 out of 10 spam messages are detected and blocked or quarantined.
- **Accuracy** – Refers to the rate of false positives. A false positive is a legitimate message that is mistaken for spam. Accuracy is related to effectiveness in that antispam methods with high effectiveness tend to have a high false positive rate. False positives can be very expensive (for example: blocked purchase orders, meeting invitations, etc.) and are to be avoided if at all possible.

The table below is by no means complete, but is a representative sample of spam defense weapons available to the IT administrator.

Method	Summary	Effectiveness	False Positives?	Drawbacks/Comments
Blacklists	List of IP addresses, domain names, SMTP addresses from which an email server will not accept mail.	Low - Medium	Yes	<ul style="list-style-type: none"> • High false positive rate due to inadvertent listing of mixed senders • Address spoofing rampant • Must keep current; maintenance can be costly
Filtering	Messages are analyzed using various methods to determine their likelihood of being spam. Spam messages are then rejected or quarantined.	Low - High	Yes	<ul style="list-style-type: none"> • Spammers constantly trying to outwit filters • Doesn't scale well under high volume • Quarantine costs can be high • Combinations are most effective
Challenge Response	New senders are asked questions that presumably only a human can answer, often involving recognition of images.	Medium - High	No, but a high "abandon rate"	<ul style="list-style-type: none"> • Generate additional volume in challenges to legitimate traffic • Legitimate senders often abandon the process
Certifying Marks	Cryptographic keys or special text must accompany legitimate messages.	Medium - High	No, but a high "abandon rate"	<ul style="list-style-type: none"> • Legitimate senders are often not a part of the program • "Unmarked" messages must still be filtered

Symantec TurnTide™ AntiSpam Router: Fighting Spam with a Multi-Layered Architectural Approach

Early efforts centered on blacklists. While blacklists may still be an effective component of spam defense, they are no longer effective as a sole means of defense. Challenge/Response and Certifying Marks represent an emerging area which may or may not reach the critical mass of adoption that will be required to attain their full potential. The most prevalent antispam tool today uses filtering, often combined with some of the other methods. This approach can be quite effective (upwards of 90%) in keeping spam out of the end user's mailbox. However, the resources required to achieve this effectiveness scales in proportion to the amount of spam that is sent into the network. If the resources are not increased to meet the incoming volume, server and network capacity will be overloaded, resulting in lengthy email delays and the potential loss of legitimate email.

Filters are effective, but they are not without cost. From a resource perspective, the more spam is entering the network, the more filtering power is required to identify and block the spam. Since the risk of false positives is unacceptable to most organizations, suspected spam must be quarantined and examined for potential delivery. All of this incurs costs to an organization, which increases as the volume of spam increases.

There are scalability concerns with this strategy as well. The spammers are engaged in a constant game of cat and mouse with filter makers. As soon as a new filtering approach is used, spammers immediately try to defeat it. Some have theorized that the existence of filters is the very cause of the spam explosion. The logic of brute force leads spammers to conclude that if 90% of their messages are blocked, the easiest response is to send ten times as many messages in order to reach their quota of "marks".

A new perspective on spam defense

The oft-quoted Chinese general Sun Tzu offers the advice that to succeed in battle you must first know your enemy. Therefore, any new approach to stopping spam begins with an answer to the question "Why do spammers spam?". When famed bank robber Willie Sutton was asked a similar question, "Why do you rob banks?" his answer was short and to the point: "Because that's where the money is". Spammers spam because "that's where the money is". On a business level, the economics of spam are compelling: the initial capital outlay is low and most of the operating costs are borne by the victims.

Symantec TurnTide™ AntiSpam Router: Fighting Spam with a Multi-Layered Architectural Approach

Compare the spam model to the long-established legitimate direct mail advertising industry. Direct mail pieces are relatively expensive to design, print and package. Bulk mailing costs in the U.S. are currently between \$0.16-0.25 per piece. Postage alone on a 5 million piece mailing could easily approach a million dollars, plus production costs. With direct mail response rates between 1% and 2% (1-2 responses per 100 mailings), the direct mailer needs a pretty high margin to survive, and therefore chooses their prospects carefully.

The spammer, on the other hand, can start his or her operation with an investment of under \$200 in software and domain hosting fees. A recent (spam-promoted) offer provides a list of over 230 million email addresses for less than \$100 (incidentally, there are far cheaper ways by which spammers obtain email addresses). Let's assume a given spammer has made their initial investment and is selling an item that yields a meager \$10 per item profit. Given this, response rates that would bankrupt a direct mailer generate sizeable profits for the spammer:

Response Rate	Spammer's Profit
1 in 1,000	\$2,000,000
1 in 10,000	\$200,000
1 in 100,000	\$20,000
1 in 1,000,000	\$2,000

With an economic model like this, the explosive growth in spam should be no surprise. The alarming part of this model is the spammer's profit equation of: *More Messages Sent = More Profit*. Since the economic victims (ISPs and IT organizations) of this process bear the costs of the spammers operation, the victim's (IT/ISP) side of the equation becomes: *More Messages Received = More Costs*. The spammer is clearly in control of the economics of spam.

As such, it becomes important to think of spam as a security problem; more specifically, as a deliberate theft of the victim's resources. An IT organization is no longer just keeping annoying ads out of end-user mailboxes. They are defending their organization from a massive, well-coordinated theft of resources attack; an attack that grows in volume and intensity with each passing day.

Symantec TurnTide™ AntiSpam Router: Fighting Spam with a Multi-Layered Architectural Approach

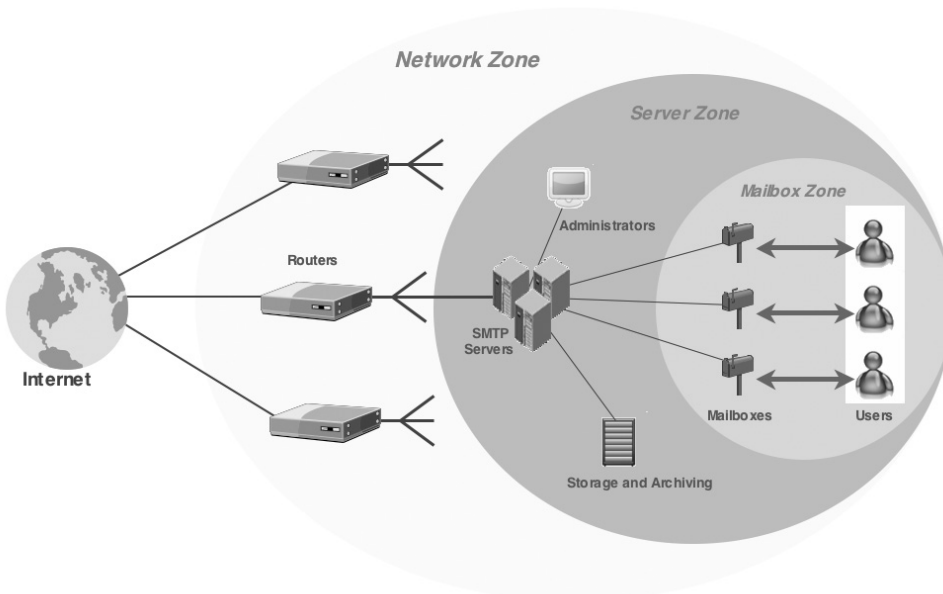
A multi-layered architecture for spam defense

Military historians often criticize generals for “always preparing to fight the last war”. Similarly, today’s war on spam simply cannot be fought exclusively with yesterday’s technology.

Defending mailboxes and SMTP servers is no longer enough. Spammers will simply increase the volume and overwhelm the defenders, drowning them in a sea of red ink. Preventing the theft of an organization’s valuable resources must begin at the outermost perimeter of the network, and then layer inward in multiple lines of defense to be truly effective in changing the economic equations that drive spam. The keys to winning the economic battle with spam are reducing spam volume while keeping false positives low.

The 2nd century Roman Emperor Hadrian is often credited with the concept of “perimeter defense”. This concept is often applied in modern times, for both military and computer network security – but has been noticeably absent in the battle against spam.

Imagine an organization’s email infrastructure as having three layers or zones. In the innermost zone, which we will call the Mailbox Zone, end users interact with their mailboxes, primarily using POP3 and IMAP4, as well as proprietary protocols. Just beyond this layer lies the Server Zone, the home of an organizations email servers, handling both inbound and outbound mail, usually via SMTP. At the perimeter is the Network Zone, the land of routers, bridges and switches handling all of the networks packet traffic, including the email traffic. An effective multi-layered defense strategy includes defenders in two, or possibly all three zones.



Symantec TurnTide™ AntiSpam Router: Fighting Spam with a Multi-Layered Architectural Approach

In the Mailbox Zone, the focus of defense is on keeping spam out of an individual's inbox. Numerous products sold as add-ons to Microsoft Outlook, for example, are used as individual means of defense. While these tools can be highly personalized and individually effective, they offer no organization-wide protection and provide little defense from the economic consequences of spam. They are also inefficient for the growing population of mobile, wireless users.

In the Server Zone, a layer of defense is applied across all mailboxes. Add-on products for Microsoft Exchange and Lotus Notes are found here as well as gateway MTA's and appliances that sit in front of multiple email servers. These defenders are generally quite effective and offer organization-wide protection. However, as spam grows in intensity, more defenders are required to maintain effectiveness, resulting in increased defense budgets.

In both the Mailbox and Server zones, filtering approaches are the technology of choice due to their high effectiveness. But these defenders must grow to match inbound volume. These defenses do little or nothing to reduce costs in the Network Zone – they fail to prevent the theft of the IT resources needed to receive process, filter and quarantine each message resulting in administrative and storage costs increasing with spam volume.

The key to an economic defense strategy is to deploy a defender at the perimeter of the enterprise, in the Network Zone, to hold the volume constant as spam volume from the Internet continually increases. Symantec TurnTide AntiSpam Router has introduced the first in a new class of antispam products – the AntiSpam Router (ASR). Using TCP traffic shaping at the TCP protocol level, Symantec TurnTide AntiSpam Router manages the quality of service that each email sender is given, based on how likely it is that they are sending spam. Legitimate senders get excellent quality of service and their mail flows quickly, while spammers are given very poor quality of service and their mail is slowed to a trickle. Spammers have no way to force mail into the protected Server Zone, so that spam backs up on the sending servers. This provides an economically effective defense.

Using a defense at the TCP traffic level in the Network Zone provides a perfect complement to the SMTP layer defense deployed in the inner layers. The best multi-layered defenses complement each other by using multiple methodologies to complicate any attempts to attack. For example, using message filtering at multiple layers is much like surrounding yourself with two locked gates, both of which can be opened by the same key – there are multiple defenses, but they can both be defeated in the same way. Spammers' attempts to bypass filters may still be defeated or slowed at the TCP level, and vice-versa, providing efficient economic defense and eliminating a potential single point of failure.

Symantec TurnTide™ AntiSpam Router: Fighting Spam with a Multi-Layered Architectural Approach

The value of a perimeter defense in practice

Most, if not all, organizations have applied some form of defense in the Mailbox and/or Server Zone(s) by this point. It is typical of these solutions to claim effectiveness of 98% or more with a false positive rate of about one tenth of 1% (even these claims are often dubious). Let's use these numbers to construct a simple model. If we assume that a typical solution achieves the aforementioned effectiveness and accuracy, and that a moderately sized organization sees 1 million incoming messages per day, this yields an infrastructure that:

- Must be capable of processing 1 million messages per day (including bandwidth, storage and quarantine)
- Actually delivers 20,000 spam messages per day to user mailboxes
- Generates 1000 false positives every day (hopefully dealt with through quarantine and not rejection)!

Now let's add a perimeter defense that uses a technique such as TCP traffic shaping, which does not reject individual messages, and offers an extremely conservative effectiveness rate of 90%. This yields an infrastructure that:

- Must be capable of processing 100 thousand messages per day (including bandwidth, storage and quarantine)
- Delivers 2,000 spam messages per day to user mailboxes
- Generates less than 10 false positives per day (a much smaller quarantine)

Not only are the results more impressive on the surface, but the greatly reduced inbound volume allows for greater "tuning" at the innermost layers, meaning that our hypothetical organization would likely see even better results than this model suggests initially. The cost savings in the areas of processing, bandwidth, storage, quarantine and administration generally more than cover the costs of the perimeter defense. Organizations that are required to archive inbound communications see a dramatic decrease in the cost and complexity of archiving. The extra security provided by the perimeter defense also pays for itself through peace of mind for the organization's security staff.

Symantec TurnTide™ AntiSpam Router: Fighting Spam with a Multi-Layered Architectural Approach

Symantec TurnTide AntiSpam Router as a Perimeter Defense

Spam filters analyze individual messages and use the results to separate spam from legitimate email. Symantec TurnTide AntiSpam Router focuses on pinpointing the true source of each email and analyzing that source's behavior over time. Then Symantec TurnTide AntiSpam Router limits the bandwidth and resources that spamming sources can use, dialing down the flow of email from them to a rate of as little as a handful of messages per hour. While filters relieve the symptoms of spam, Symantec TurnTide AntiSpam Router addresses the cause.

Symantec TurnTide AntiSpam Router uses the proven technique of TCP/IP traffic shaping to control the rate at which network packets can be sent from the spammer's servers. By doing so, it relieves enterprise mail servers from the burden of scalability against the spammers' volume. This not only lightens the load of downstream email servers, but has an upstream effect of impacting the economic model of the spammer making protected networks economically unattractive. In fact, many "spam cannons" have been coded to abandon attacks to networks that offer the spammer poor throughput. Additionally, since traffic is "shaped" and not blocked, the classic false positive scenario is avoided, so the worst that can happen is that legitimate email caught in a spam storm may take a little while longer to reach its destination – and these occurrences are quite rare.

This technique needs to be applied at the network level. Several products exist that limit traffic at the SMTP level. Unfortunately, research shows that up to 90% of the costs have already been incurred by this point. Additionally, SMTP servers are such that tricks and protocol violations may be employed to attempt to bypass these filters. By acting at the TCP/IP level, Symantec TurnTide AntiSpam Router prevents even these attacks – packets sent by spammers that try to evade TurnTide's TCP/IP traffic shaping would violate the TCP/IP protocol and would not reach their destination anyway.

The Symantec TurnTide AntiSpam Router provides a unique and effective perimeter defense, and provides a solution that:

- Controls the explosive volume of spam
- Reduces false positives
- Actually fights the spammer's economic model
- Can actually increase the scalability and effectiveness of filtering solutions
- Can be extended to control outbound spam as well as inbound

Symantec TurnTide™ AntiSpam Router: Fighting Spam with a Multi-Layered Architectural Approach

Conclusion

A multi-layered architectural approach is the key to success in the war on spam. The Symantec TurnTide AntiSpam Router is the first real-world proven solution designed to provide an effective perimeter defense in an multitiered antispam strategy.

References

- 1 Gartner Report: “Enterprise Spam Filtering: Overview”, April 2004
- 2 InfoWorld, April 19, 2004 Issue 16.
- 3 TechRepublic White Paper “The Enterprise Challenge: Spam Management”
- 4 Ferris Research Report: “Spam Control Problems and Opportunities”, Jan 2003
- 5 META White Paper: “Spam, Viruses and Content Compliance”, August 2003
- 6 Reuters/USA Today: April 12, 2004 and CIOL IT Unlimited April 12, 2004

About Symantec

Symantec is the global leader in information security providing a broad range of software, appliances and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure. Symantec's Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions. Headquartered in Cupertino, California, Symantec has operations in 35 countries. More information is available at www.symantec.com.

Symantec has worldwide operations in 35 countries. For specific country offices and contact numbers please visit our Web site. For product information in the U.S., call toll-free 1 800 745 6054

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
1 408 517 8000
1 800 721 3934
www.symantec.com

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Other brands and products are trademarks of their respective holder/s. Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. NO WARRANTY. The technical information is being delivered to you as-is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice. Copyright © 2004 Symantec Corporation. All rights reserved.
10/04 10326368