TrustLayer™ Mail

100% Malware-Free E-mail: A Guaranteed Approach

PANDA SECURITY | *One step ahead.*

100% Malware-Free E-mail: A Guaranteed Approach

Panda Security's Mail Filtering Managed Service Guarantees Clean E-mail

Table of Contents

Table of Contents 2

Battling the Increase in Malware and Spam 3

The Mail Server – A Critical Vulnerability 3

- Denial of Service (DoS) Attacks 4
- Directory Harvest Attacks (DHA) 4
- Phishing 4
- Spyware 5

Levels of Protection for the Mail Service 5

Achieving Network Security through Managed Services 5

Panda TrustLayer Mail Managed Service 6

- How It Works 6
- Benefits of Using TrustLayer Mail 8

Conclusion 9

PANDA SECURITY | *One step ahead.*

Battling the Increase in Malware and Spam

IT managers are working hard to combat the increasing volume of malware attacks on their enterprises. These attacks are also becoming progressively more sophisticated. As a result, the risks of them causing damage to the business are greater than ever before.
The majority of threats that reach a company do so through the mail server. There are several reasons for this trend:

- The enterprise's mail service is the most frequently used communication channel across the Internet
- An e-mail is easy to access and manipulate
- The SMTP mail protocol is simple and can be emulated by any Internet user
- Many confidential company communications are still transmitted using e-mail
- Firewall-type corporate security devices do not filter SMTP traffic which reaches e-mail servers
- Mail directories often include highly sensitive corporate information, such as organizational charts, key functions, directories with strategic information, etc.
- The mail service is a channel for mass infection, via worms and Trojans that replicate in each target, using infected computers and reading mail lists in the host computer.

E-mail has become an indispensable tool in business management and even in personal relations, all but replacing traditional means of communication. But as with any widely implemented tool, it is susceptible to being used deliberately in ways that are detrimental to the users of the mail service.

One such negative use of e-mail services is spam. Mass mailing has proven to be a powerful, low-cost marketing tool. Spammers are able to get very quick returns, receiving payment for the number of mails that they send across the Internet. This has caused an avalanche in the development of this type of mail, reaching exorbitant figures in some countries. According to the Messaging Anti-Abuse Working Group (MAAWG), 82-87% of all incoming e-mail is currently categorized as spam or "abusive e-mail".[1]

Spam is a nuisance at a personal level, as it has to be handled (opened, read, deleted) and clearly has a huge financial impact, due to the costs of processing large volumes of useless mail by the company. All of the time used by employees (users, IT administrators, etc.), as well as the use of server and communication resources, represent significant costs to the enterprise.

In addition to increased costs, spam slows down communication systems. When the mail server is forced to process large volumes of junk e-mail, it is clearly detrimental to its ability to process useful mail. Unfortunately, spam is growing in frequency every year, with an increasing number of spammers generating ever more junk mail. This means there is a growing need for tools that can effectively filter and eliminate this type of mail.

The Mail Server – A Critical Vulnerability

E-mail traffic is based on the SMTP protocol, which offers little or no reliable safeguards when it comes to exchanging information over the Internet between two nodes. In addition, it is a protocol that is easily emulated, and it is possible to generate SMTP traffic for exchanging information across the protocol from an Internet node (a simple PC) without the intention to send mail but rather to saturate a server.

Corporate firewalls cannot block mail traffic, since e-mail is a fundamental source of the company's communication. For this reason, spammers know it is the ideal channel for sending all types of viruses

1 http://www.maawg.org/about/MAAWG20072Q_Metrics_Report.pdf

and malware (spyware, hoaxes, phishing, etc.) to the unsuspecting enterprise. The following sections will examine some of the attack scenarios that could be clearly detrimental to users of a mail service.

Denial of Service (DoS) Attacks

An attack on a mail server can involve massive sending of connection requests to the server. This means that large communication volumes are generated (frequently from different sources) without even an e-mail being sent. The server can respond in several different ways:

- Option A: Not respond to communication requests aimed at mail addresses not registered in the mail server
- Option B: Respond with an error message to the sender
- Option C: Return a message that the server is busy

If the mail server takes Option A, it is applying a policy that will apply to malicious mail, but also to potentially useful mail in which the sender has, for example, made an error on typing the address. It is therefore not advisable to configure the server in this way.

Option B means that for each time the SMTP protocol is started, the e-mail server will be interrogated for an address and it will answer the requesting node as to whether or not it exists in the domain. This is the most common way in which mail servers work today, as it offers a reasonable degree of certainty about the reception of the message.

Option C occurs in special circumstances, either because the mail server is saturated or because it has been adopted as a tactic to respond to an identified attack. The objective of DoS attacks is clear: slow down the e-mail server, and, if possible, render it inoperative with the corresponding financial consequences.

Directory Harvest Attacks (DHA)

DHA is a technique used by hackers to capture the mail directories of the targeted organization. They do this with software that generates random e-mail addresses, using feasible combinations (common names, positions, department names, etc.).

By mass-mailing to these types of addresses and using a trial and error technique, hackers can capture not just e-mail addresses, but also sensitive information such as organizational structure, drives with restricted information, etc. The consequences that this could have are easy to imagine, and could even rise to expensive legal liability on the part of the targeted company if negligence in data-processing procedures can be proven.

Phishing

This term describes how malicious users pass themselves off as someone else (normally a company) in order to obtain confidential information from the recipient of the 'phishing e-mail'. Typically phishers send e-mails that appear to come from a bank or financial institution and under some pretext or other, ask the recipient for confidential information, such as account access codes. Spoofing of the third-party Web page (which victims are led to through a link in the e-mail) is sometimes highly accurate. This deceitful practice has a high level of success, with often devastating financial consequences.

Spyware

Spyware is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent. Spyware provides another form of obtaining confidential information from the recipient of e-mail, by sending files which when they run, drop resident Trojans on computers to log and then send certain information about the user when they access certain Web pages.

Levels of Protection for the Mail Service

Mail security can be provided at several different network levels:

- **Mail security on the PC**. This is not an effective solution from an administrative point of view for eliminating spam or combating denial of service or directory attacks. In fact, all attacks would occur as described in the previous sections of this paper, unless the mail server is protected. Moreover, spam filtering may not effectively meet the criteria of 'high rejection of spam and few false positives' and is at users' discretion.
- **Security in the Mail Server**. All unwanted mail traffic passes through the network to reach the e-mail server, meaning that there is already a processing overload on other network devices. Awareness of attack types and origins is limited to the experience of the client's network administrator. Moreover, the mail server is burdened with additional workloads.
- **Security at the Gateway Level**. The same arguments as in the case above apply. But the situation is a little bit better as the gateway is nearer to the perimeter than the mail server.
- **Security through Specific Hardware in the Network Perimeter.** This method does not resolve the overload in the communication resources, as spam uses the client's communication lines. It does, however, eliminate the processing load on the network.
- **Network Security through Managed Services**. This method provides an effective solution to all of the previous problems:
  - Spam is eliminated outside of the client's network, without using their resources
  - DHAs or denial of service attacks cannot target the mail server
  - It does not place an additional processing load on the client's network devices
  - It does not require investment in additional hardware
  - It includes updated information at the network level to rapidly reach and respond to new network attacks

Achieving Network Security through Managed Services

The most reliable solution for achieving network and mail security is by leveraging a managed service. In this model, security measures are applied through a mail filter system in a node outside of the client's network. To do this, all traffic from the client's mail domain is redirected to the filter system by modifying the MX[2] file in the client's domain name system (DNS). From that point on, mail addressed to the client's domain is first sent to the managed services provider's filter system. This system processes and scans all mail with one or more antivirus and anti-spam engines, and, optionally, filters the content following criteria based on words, file types, or image types.

2 MX is short for "mail exchange" record, an entry in a domain name database that identifies the mail server that is responsible for handling e-mails for that domain name.

Mail classified as spam can then be treated according to different policies. In a managed service environment, the client's domain administrator can establish his or her own policies or delegate this filtering configuration decision to the managed service provider.

A managed service also offers greater defense against denial of service and directory attacks. The experts managing the filter system will detect anomalous behavior in domain traffic and can take countermeasures to fight against these attacks. For example, in the event of a DoS attack, the filter system can slow down the response to this address, nullifying the attack by increasing response times, and therefore the waiting time in the node carrying out the attack. This slowdown could block any type of response to certain addresses.

With a managed network service, large quantities of information can be quickly gathered about security attacks. This observatory-type strategy provides a clear advantage when it comes to the early detection of new threats. For example, a new phishing e-mail may start to spread on the Internet purporting to be from an online bank and asking recipients to enter their account details. This sender's address is false and the Web page that the victim is redirected to appears to be that of the bank. A managed service will detect this new threat more rapidly and can employ security measures to ensure that no clients' domains are affected.

Panda TrustLayer Mail Managed Service

Panda TrustLayer Mail is a managed mail filter security service that guarantees clean, secure e-mail delivery. TrustLayer Mail provides four main functions: anti-malware, anti-spam, content filtering, and mail continuity:

- **Anti-Malware Protection** – Using the most advanced preventive protection technologies, TrustLayer Mail detects all types of known and unknown malware content in e-mail. TrustLayer Mail doesn't just scan and remove viruses, it also blocks and eliminates all types of dangerous files from entering the network such as worms, Trojans, dialers, hacking tools, hoaxes, security risks, and phishing scans. It detects both known viruses (through its signature engine) and new threats by incorporating the latest proactive technologies and direct handling of suspicious files by PandaLabs. This commitment is backed by an SLA guaranteeing that users will only receive e-mail that is 100% free from malware.
- **Anti-Spam Protection** – The Panda TrustLayer Mail Service combines several anti-spam engines to achieve detection ratios over 98.5%, ensuring end users don't receive spam.
- **Content Filtering** – Lets clients define and enforce company security policies by establishing what attachments can be received and which should be blocked.
- **Mail Continuity** – Panda TrustLayer Mail prevents possible network failures from affecting business continuity. In the event of the failure of clients' servers or networks, mail will still be accessible for several days.

How It Works

Mail filtering takes place while messages are in transit on the Internet – before they can enter clients' networks. TrustLayer Mail scans and takes action according to the criteria defined for each mailbox. If the mail is clean, it will be immediately sent to the recipient. If suspicious behavior or a conflict with established policies is detected, the system will act accordingly – deleting the message or storing it in quarantine. The quarantine feature allows suspicious or invalid messages to be securely stored, and if necessary, viewed away from clients' systems and prevents junk mail from saturating communication servers and other IT resources.

PandaLabs transmits – in real-time – the identifiers of all new threats on the Internet, so systems are constantly being updated. In addition, **every five minutes the system checks for new virus signature files along with new anti-spam rules that include new detection methods**. Once received, they are distributed across the cluster transparently to users.

This fully customizable service provides 24x7 technical support and is driven by leading-edge technologies, such as Panda Security's TruPrevent technology and advanced heuristic scanning for detecting unknown threats. The service also includes rapid analysis and support from PandaLabs, one of the most prestigious laboratories in the IT security sector.

TrustLayer Mail delivers:

- **Maximum Data Security and Confidentiality** – TrustLayer Mail employs the most rigorous measures to guarantee the security and confidentiality of clients' data and information. Mail scanning is performed with strict confidentiality, in line with ISO/17799 security policies, applying to both data management and physical security. It monitors both inbound and outbound mail to prevent inappropriate or confidential material from entering or leaving the company.
- **Straightforward Interface** – Domain administrators and mailbox users have access to Web consoles with a series of configuration options depending on their corresponding permissions. This console is highly intuitive and a user guide is available for any queries.
- **Customizable Definitions** – TrustLayer Mail allows a high level of customization without detracting from its simplicity. Security policies can be established for user accounts, even allowing end users (if they have permissions) to configure their own spam white lists and blacklists.
- **Quarantine Management** – TrustLayer Mail stores all spam or messages that could contain viruses in its own quarantine. This ensures that the end clients' servers are not saturated by spam, saving resources and storage capacity. Messages carrying viruses are stored in the system's quarantine for up to 30 days. However, known mass-mailing worms that spoof the sender's identity are deleted directly, although a record is kept in the log for statistical purposes. After the predetermined time in the quarantine, the message is automatically deleted. Attachments suspected of containing a virus and do not match known identifiers are sent to PandaLabs for detailed analyses. PandaLabs will take action (either releasing it or confirming that it is infected) usually with in less than four hours.
- **Continuous Information about Threats** – The service allows end clients to review the quarantine and receive a range of reports through the secure Web interface. These reports are customizable and provide continuous information about the mail traffic situation and any attacks that occur.

Panda TrustLayer Mail service does not require initial investments in hardware technology, clients do not have to install complex and costly software, and it involves no maintenance costs. To use the system, clients only need to redirect their mail server to Panda's filter system through a simple DNS redirection. The service is then available to clients within 24-hours.

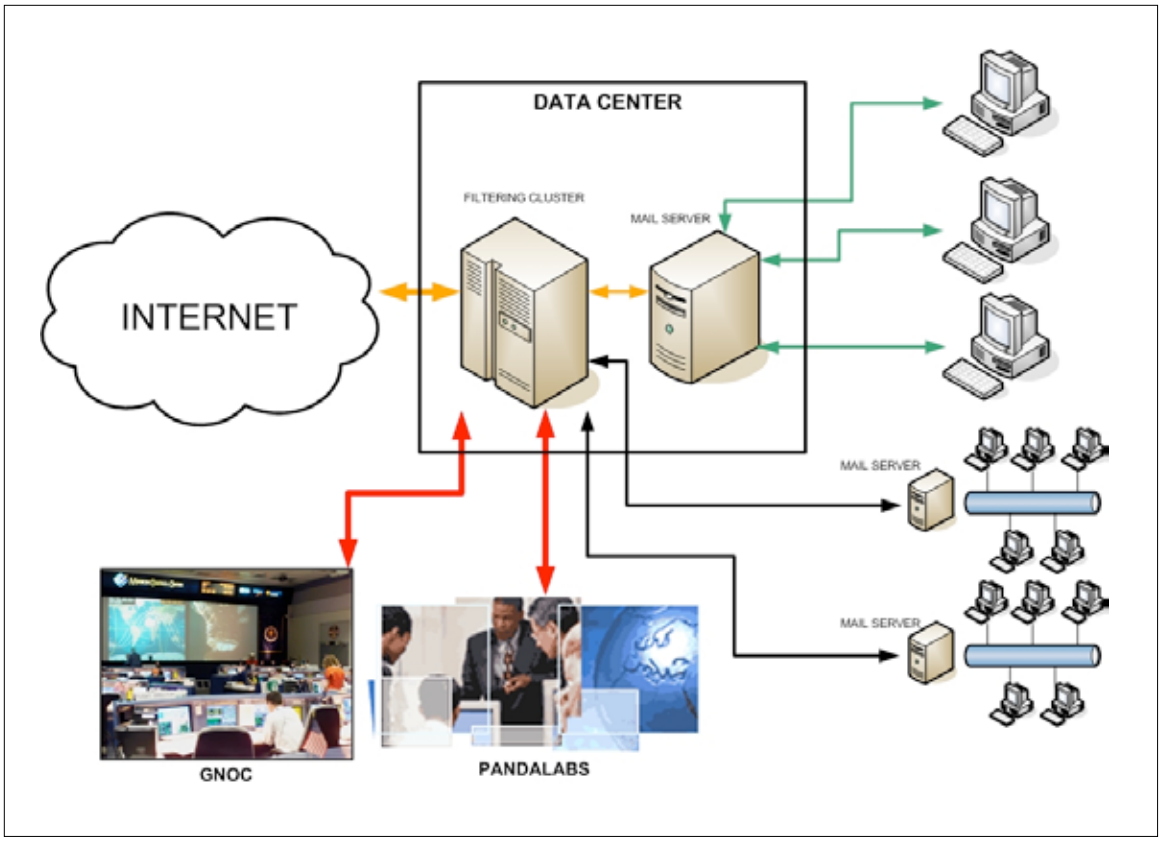

Figure 1. Panda Security TrustLayer Mail Service filters all mail before sending it on to recipients or quarantining suspect e-mails.

Benefits of Using TrustLayer Mail

TrustLayer Mail provides users with an optimal cost-to-quality ratio by having constantly manned systems and reduced inbound traffic. By virtue of being a managed service, it offers maximum protection, since malware is increasingly complex and fast-changing. The solution delivers advantages only available through an external mail-cleaning system – benefits not possible with traditional mail server software or dedicated gateway devices.

Additional benefits include:

- **Reduces Costs in Resource Usage** – By blocking unwanted mail before it enters the corporate network, TrustLayer Mail reduces the use of enterprise bandwidth and storage capacity.
- **Reduces Personnel Costs** – As it is managed and maintained remotely, it reduces the need for mail service management, including traveling to branch offices.
- **Eliminates Costs of Dedicated Hardware and Software** – It eliminates the need for hardware or software dedicated to protecting the company's e-mail.
- **Increases Employee Productivity** – By removing junk mail, it prevents time lost reading and deleting annoying and unproductive messages.
- **Provides a Predictable Investment** – Clients only pay for the number of active mailboxes they have. The service is easily scalable to the number of mailboxes needed by any company.
- **Business Continuity Protection** – Mail is protected even in the event of crashes of company servers.

- **Information Protection** – TrustLayer Mail provides unsurpassed information protection by using the very latest technologies for combating viruses, spam, and any other types of attacks that could compromise corporate data.

Through its use of Panda Security's TruPrevent protective technology and individual analysis of suspicious e-mails by PandaLabs, TrustLayer Mail service is able to offer a 100% virus-free guarantee SLA. The system architecture offers load-balancing and redundancy, and is designed to offer maximum availability backed by 24x7 support – to ensure an uninterrupted, clean e-mail delivery service.

Conclusion

Spam and malware attacks are becoming increasingly sophisticated and targeted to specific objectives; therefore the risk of them causing extensive damage is greater than ever. The best technique for combating these threats is through a managed network service, given the high level of specialization that a third-party service provider can offer. Managed security systems for mail filtering are now the most effective and cost-effective methods for companies whose IT resources could be compromised by the threats transmitted via e-mail.

TrustLayer Mail Service provides the industry's most advanced security methodology for today's enterprises. It acts outside the client's network using redundant platforms and preventive detection systems that can resist attack and isolate new threats – even before they have been identified. It is an effective method because it does not require investment in specific systems, it reduces investments in communication infrastructure, and is offered at a predictable cost to the client.

With Panda Security's team of security experts managing mail protection, availability, and confidentiality – clients can redirect their valuable resources to focus on the enterprise's core business activities.

For more information on Panda TrustLayer Mail Managed Service, please visit www.pandasecurity.com.