International Journal of Engineering & Technology, 7 (2.4) (2018) 147-150

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

IPV4 and IPV6 based hybrid approach for spam and virus detection

Swati Hira [1, 2], Samir Ajani [1, 2], Pratibha Kokardikar [1, 2], Shubhangi Neware [1, 2]

[1] Department of Computer Science & Engineering, Information Technology
[2] Ramdeobaba College of Engineering and Management, Nagpur, India
**Corresponding author E-mail: hiras@rknec.edu*

Abstract

The proposed email setup consist of multiple mail servers distributed at two levels to achieve desirable email access performance. It is a well-established fact that 99% of the emails received over internet are either spam or contained viruses and such emails can be dropped at the first entry point of the Network. Thus, the first level in the proposed architecture has been taken as an email gateway which is equipped with antivirus and anti-spam software. Spam assassion is an open source freeware software for filtering of the spam emails. Perl based spamassassion id to CPU and Memory hungry for heavily loaded server thus this new arrangement would then overcome the Problem of slow Email access for users by detaching spamassassion from email repository servers. The second level of the servers with email repositories for users all the email servers used in this implementation would be Linux X86 servers. Virtualization technique presents a software interface to virtual machines that is similar but not identical to that of the underlying hardware. First level is implemented in Virtual machine. So as to provide scalability, portability, migration and vendor independent.

Keywords: *Spam; Virus; Internet Protocol; Multilayer Filtering.*

1. Introduction

As computing becomes pervasive, people increasingly rely over the Internet. Now, the Internet is a preferred source to access online services such as E-mail services, e-banking, e-government, etc. User mails require a strong security mechanism from viruses and spam detection [1, 2]. Security is a major issue in internet based E-mail access service system. There are various internet threats which affect the security system of internet and increase risk for receiving bulk mail resources over highly secured network. Most of the spam and virus detection system relies on single layer filtering.

Single-layer filtering is the traditional security process that requires antivirus and anti-spam software installation on server. Single layer filtering is vulnerable to detect spam because it requires lot of time to process mails on single server. For applications that require greater security, it may be advisable to implement more complex systems, such as multi-level anti spam, antivirus email setup [3]. In a two-level filtering system, incoming mails are processed at first level for filtering and scanning and processed mails are then forwarded to the second level mail server. The management of antivirus, anti spam and its supporting software complexities are handled by the centralized server configurations. Keeping the email-setup secure and containing clean mails in user's inbox, while receiving mails from different domains, over Internet is a challenging task. The challenges start from filtering useful mails from all received mails which are received at first level (server level) to reduce the processing time of the second server, across the Internet is the most simplified way and without posing any potential threat to the networked resources.

This paper has addressed the security issues involved in the email-setup of the organization accessible from the Internet. It allows users to access their mails present in their respective inboxes which are guarantees to contain monthly urgent emails. The above discussion underlines the need for Multilevel Email-setup for highly trusted network. To do so in the present work an Email-setup that is both secure and highly usable has been designed using multiple levels. An email setup has been designed using multilevel scheme using Virtual Machines for better resource utilization and LDAP Server for managing information's [4].

Fig. 1 shows the spam detection process of proposed system.

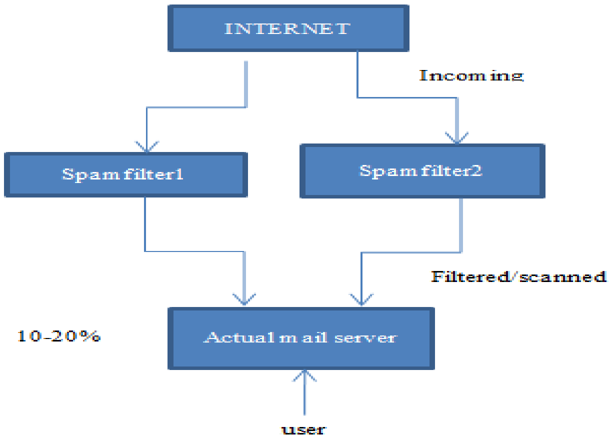

Fig. 1: Spam Detection Process of Proposed System.

2. Existing system architecture

It would not be a secure way for most of the email setup to simply use antivirus and anti spam software for spam and virus detection

[5]. The existing system works only on single level. Current system has Load Distribution on single level which makes accessing of useful mail difficult from bulk mails

All the processing on mails as scanning ,filtering and mail accessing done on same level .The system addressed the problem of Load balancing and low throughput. Hence we need to provide different access levels for secure accessing of mail services. Current system architecture is shown Fig 2.

3. Proposed system architecture

Fig. 3 shows the proposed system architecture. On first level Virtual Machines has been created with following components: Mail gateway (Qmail 1.03), antivirus (Clam AV) and anti spam (Spam Assassin) installed on first Virtual Machine. On the second level Actual Mail Server setup has been created.

Both levels have been implemented using Centos 5.5 as Operating System. The developed setup will be used to access the spam and virus free emails over the Internet. The first level of email setup detects and filters out 80% spam and virus effected mails. The second level of mail server which acts as user end email server receives clean mails from the first level. All implementations have been done using open source tools. This proposed system provides following solutions:

3.1. Trusted email setup

Strong security relies by filtering and scanning mails on multi-level. Clamav, Spam Assassin, Qmail 1.03 and supporting packages are uses as the level of filtering and scanning, which provides multilevel trusted Email setup for highly secured network.

3.2. Managing anti-spam

Spam Assassin uses as the first level of filtering/scanning, which supports pyzor, razor, DCC, Bayesian filtering and provides security against spam mails for managing the identity of the users of a secure mails.

3.3. Managing anti-virus

The Use of Clam AV mechanism to enhance the security of mails from virus

3.4. Secure e-mail service

The RRCAT web mail services will be accessible over internet in simplified and secure manner.

3.5. Security against spam and virus

70-80% spam and virus effected mails are detected, so the user receives almost clean mails.

3.6. Secure data storage

A LDAP directory acts as the authoritative data store for all identity information as well as the configuration information for the identity management system itself.

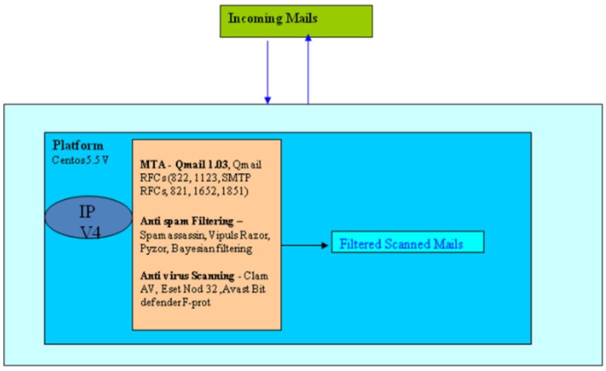
Incoming Mails
Platform
Centos5.5 V
IP V4
MTA - Qmail 1.03, Qmail RFCs(822, 1123, SMTP RFCs, 821, 1652, 1851)
Anti spam Filtering – Spamassassin, Vipuls Razor, Pyzor, Bayesian filtering
Anti virus Scanning - Clam AV, Eset Nod 32 ,Avast Bit defender F-prot
Filtered Scanned Mails

Fig. 2: Spam and Virus Detection Using Single Level Architecture.

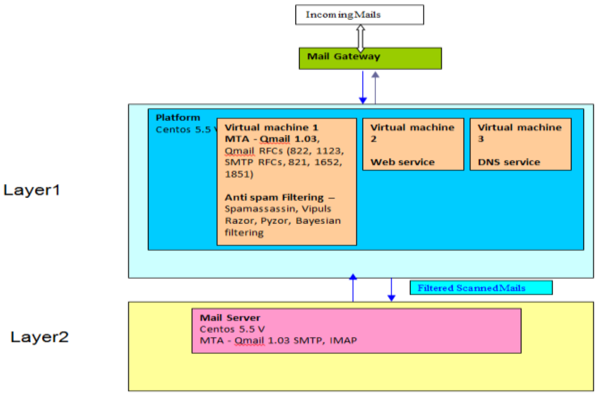

Fig 3: Spam and Virus Detection Using Multi-Layer Architecture.

4. Expected outcomes

The result of this paper is a Multilevel, Anti spam, Anti Virus and Email setup with IPV4 and IPV6 support. This system also provides necessary scripts and interfaces for successful creation of Virtual Machine with support for IPV4 and IPV6 protocols using Para virtualization tools [6]. This setup uses well proven and tested open source technologies for achieving multilevel filtering/scanning of emails thus providing necessary control of allowing only clean emails to reach the users. Results are shown in below figures on daily and monthly basis. Fig. 4(a) and 4 (b) shows result on single layer system. Fig. 5-7 shows result on multiple layer system for daily and monthly received data. Fig 5(a)-5(b) and Fig 6(a)-6(b) shows the result on layer1 using different spam filter as spamfilter1 and spamfilter2. Fig.7(a)-(b), shows the result at layer2 or the finally received data by user. From results we can observed that we are getting more number of spam mails in single layer system while in multiple layer system less spam mails are received because the mails are already filtered at layer1. In other terms in previous system all types of mail (Spam/Virus/Clean) are received by user in their inbox while in proposed system user received almost clean mail received.

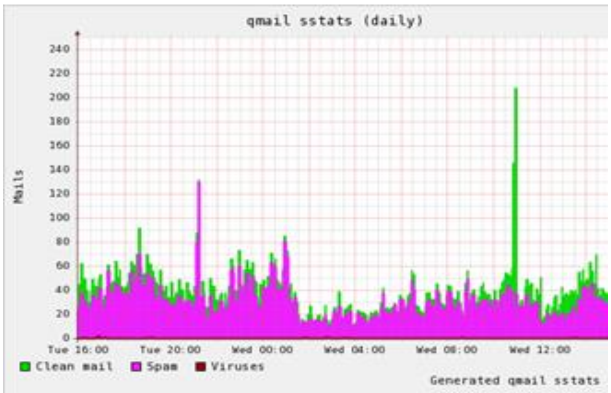

Fig. 4: (A) Spam and Virus Detection Graph for Previous System (Daily).

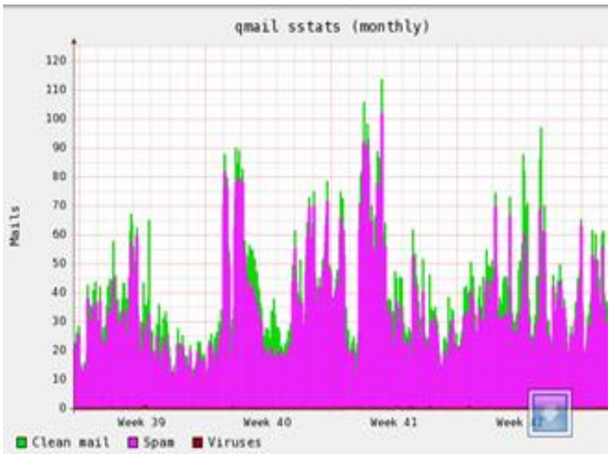

Fig. 4: (B) Spam and Virus Detection Graph for Previous System (Monthly).

5. Proposed system results

5.1. Spam filter 1

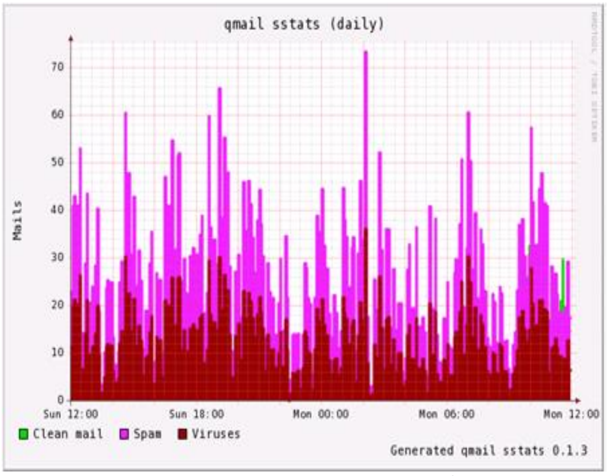

Fig. 5 :(A) Spam and Virus Detection on Spamfilter1 (Daily).

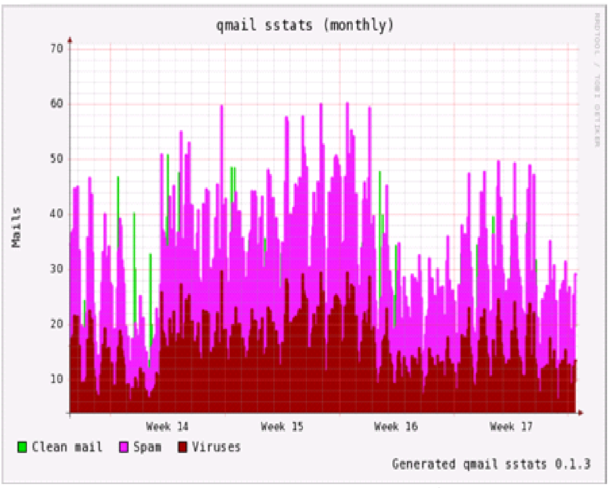

Fig. 5 :(B) Spam and Virus Detection on Spamfilter1 (Monthly).

5.2. Spam filter 2

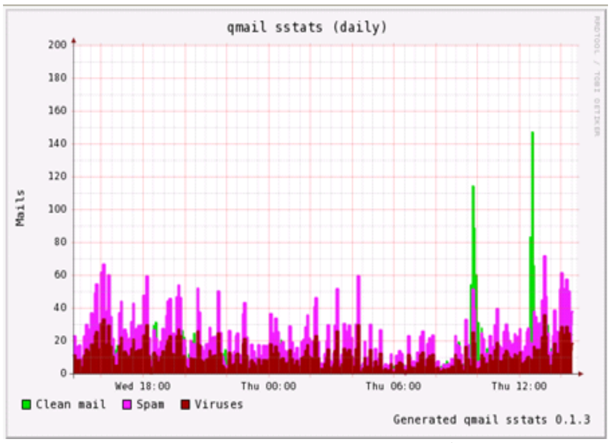

Fig. 6: (A) Spam and Virus Detection on Spamfilter2 (Daily).

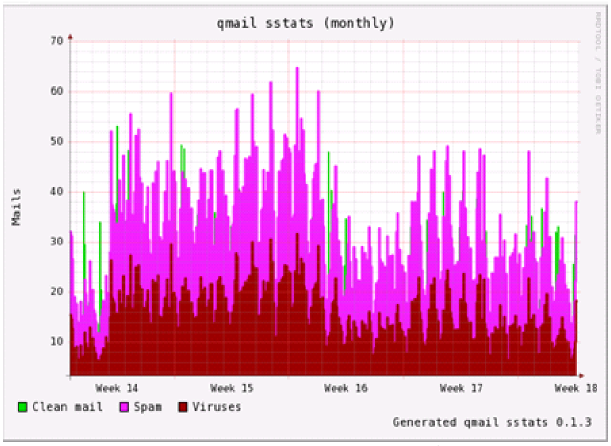

Fig. 6: (B) Spam and Virus Detection on Spamfilter2 (Monthly).

5.3. Actual server

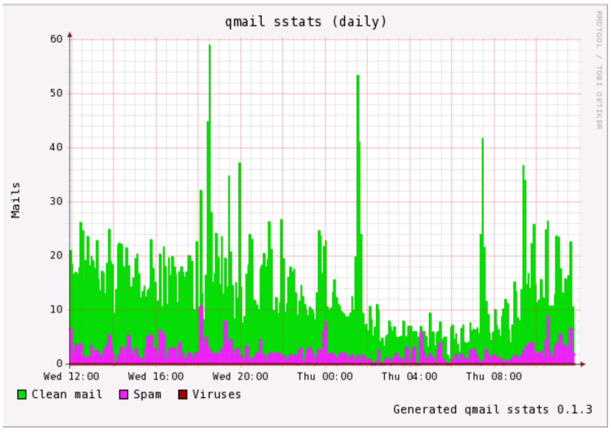

Fig. 7: (A) Spam and Virus Detection on Actual Server (Daily).

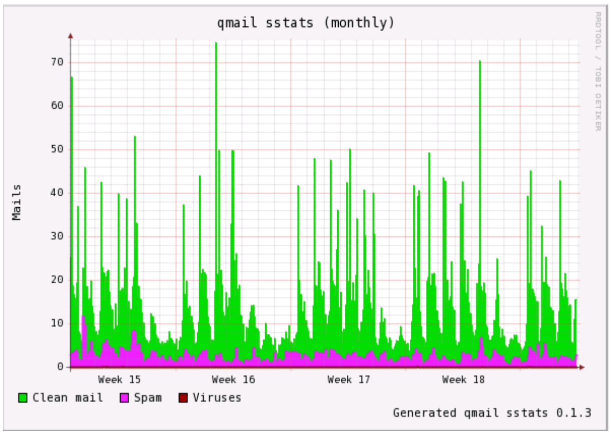

Fig. 7: (b) Spam and virus detection on actual server (monthly).

6. Conclusion

In this paper, High throughput multilevel Anti spam and Antivirus email setup with IPV4 and IPV6 support has been designed and developed. Server virtualization has been used for the development of first layer of Anti spam filtering and Antivirus scanning, to achieve optimum usage of hardware resources. The Analysis of incoming mails, spam mails and virus infected mails shows that more than 72% spam and virus mails are processed at the first layer. Hence actual user end mail server receives only clean mails at second layer which improves the performance of the mail server. It resulted in improved server response time to the user of mail servers. IPV6 implementation has also been incorporated in the setup to adhere the future generation protocol. The setup is developed using the open source software which are readily available on internet.

References

[1] Hassan Najadat, Ismail Hmeidi, ”Web Spam Detection Using Machine Learning in Specific Domain Features”, Department of Computer Information Systems Jordan University of Science and Technology , Referenced in 2008.

[2] Minoru Sasaki,”Spam Detection Using Text Clustering” Department of Computer and Information Sciences, Ibaraki University, Hitachi, Ibaraki, Japan, Referenced in 2005.

[3] Ye Wang, Hussein Abdel-Wahab,” A Multilayser approach of anomaly Detection for Email Systems”. Dept of Computer Science, Old Dominion University 2006.

[4] Debora jean byrne,Austin TX (US),Chetan Ram Murthy,New York,”Light Weight Directory Access Protocol(LDAP) Directory server cache mechanism and method”, Referenced on Feb 2002.

[5] BrysonP.Gordan,CampbellCA(US),”Comprehensive anti-spam system, method, and computer program product for filtering unwanted email messages.”,Referenced on May 2004.

[6] Peter Kosik, Patrik Ostrihon and Reza Rajabiun, “IPV6 and Spam”, MIT Spam Conference, Referenced in 2009.