Gateway Antivirus Implementation using Open Source along with Performance Testing and Improvement Analysis

Hiren V Mer[1], Sheetal Mehta[2]

[1]Parul institute of Engineering & Technology,
Limda, vadodara, India
hiren_com@yahoo.co.in

[2]Parul institute of Engineering & Technology,
Limda, vadodara, India
prof.sheetal.mehta@gmail.com

Abstract: ***The project includes implementation of gateway antivirus with open source methodologies along with benchmark testing and performance improvement. The gateway antivirus solution implementation would include antivirus protection at HTTP, FTP, SMTP & POP3 protocols at the gateway level. Benchmark testing with various attack scenarios would be included along with performance analysis for the improvement of gateway level antivirus solutions in various deployment scenarios.***

Keywords: HTTP Proxy; semi-proxy**.** Anti-Virus Based File Scanning, File Trickling

1. Introduction

With the development of the Internet, more and more information all over the world is abounding in the internet, while more and more problems of the security of information system are emerging. Particularly in recent years, computer virus is no longer restricted to the transmission of traditional Storage medium but expanded its reach around the globe directly through the network. Now compute specialists all over the world are working on ways of virus protection and some reach a conclusion that anti-virus gateway is one of the most effective means to cut off the transmission of virus. At present, there are two main anti-virus gateways: common HTTP anti-virus gateway and transparent proxy HTTP anti-virus gateway. Common mode has an advantage of high performance, but somewhat lacks in functionality; transparent proxy mode has an advantage of powerful function, but it is advantages couldn't be ignored in the performance. In order to meet requirements of performance and function, this paper presents a new solution of semi-proxy, which can be a better solution for satisfying requirement of performance in anti-virus gateway without sacrificing functionality.

2. The factors of performance of file based antivirus scanning

The AV engine of traditional file based virus scanning starts to scan only after a complete file has been received. Before the scanning, the gateway AV equipment has to pause packet forwarding, and to cache the received packets. After the scanning is finished, the gateway AV equipment will send out the cached file. If a large file is being transmitted, this method will lead to significant performance degradation and large transmission delay. Because the data packets have been blocked and therefore-not forwarded before the termination of AV scanning, the receiver has to wait a long time, and this can cause connection timeout very easily. In addition, the data caching process is limited by the capacity of storage media. When the number of concurrent connections is increased, the number of files to be cached becomes larger and larger, and finally all the storage capacity is consumed and it will be impossible to further cache data and establish any new connection for a request of AV inspection.

From the above discussion, in order to improve the performance of file based virus scanning, the first and most important problem to be solved is the connection timeout caused by data blocking, and in the meanwhile, it is necessary to optimize the data caching algorithm, so that the data blocking can be mitigated under the condition of finite storage capacity, and therefore more and more connections will be allowed. Software development is achieved through a collection of activities that lead to the building of a software product. Software development is traditionally divided into various phases, which we describe briefly in the following sections. For small projects, the phases are carried out in the order shown; for larger projects, the phases are interleaved or even applied repetitively with gradually increasing refinement.

3. Requirements for Gateway Antivirus

1) The low rate transmission and the high rate transmission of file trickling must not affect the processing of concurrent connections done by the main process of data processing. In another word, during the transmission of the file, the main process should be able to parse and process the data on other connections in order to avoid communication blocking.

2) When multiple files are scanned for viruses, the AV engine should be able to send multiple files by using trickling method.

3) When multiple files are transmitted at full rate, the AV engine should balance the opportunity of sending each file, in order to avoid a long waiting state for any connection, at the same time to limit its transmission rate, and not to affect data communication on other connections.

4) Before the AV result is available, the AV engine should not send out the whole file by using the method of "file trickling".

5) When the connection experiences an anomaly or when a virus is found, the AV engine should stop sending the file immediately.

4. Technical challenges

Here we are checking the file for FTP,SMTP and POP3.FTP protocol is when send the file to the other node then gateway antivirus check the file which we send through FTP. SMTP and POP3 protocol is also used for this gateway antivirus and we can make it secure.

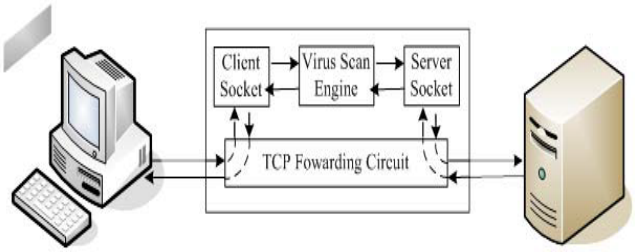

Figure 1: http antivirus proxy

this is same for the FTP,SMTP and POP3.In the world there are commercial software's ate used for the file scanning/virus scanning so here we used open source for the file scanning and virus scanning.

4.1 Specification

Gateway Antivirus Features and Benefits:

Easy-to-use, signature-based Gateway AV provides an additional layer of security designed to identify and block viruses, worms, spyware and other blended threats attempting to enter your network through e-mail.
1) Protection at the gateway. Scans e-mail traffic at the gateway to block viruses, worms, and spyware before they can enter your network and execute their dangerous payload.
2) User-definable actions. Lets you define the action to be taken when viruses are identified, including: allow, block, and lock.
3) Locks infected attachments. Prevent execution of malicious payloads at the desktop.
4) **Non-stop protection**. Signatures are updated without interruption, so you never have to leave your network exposed.
5) Continuously updated database. Include thousands of virus signatures, with WildList and zoo viruses, for far reaching coverage. Schedule signature updates at regular intervals for continuous and timely protection.
6) Robust de-compression support. Scans within a large number of compression types including ZIP, RAR 2.0, TAR, GZIP, ARC, and MS CAB to provide solid and efficient protection.

4.2 Testing

Viruses, worms, and Trojans are stopped at the gateway:

1) Scans all major protocols, including HTTP, HTTPS, FTP, TCP, UDP, SMTP, and POP3 to block all types of malware.
2) Email traffic is scanned at the gateway to stop threats before they gain access to your servers and execute their dangerous payloads.
3) Suspect email can be flagged to go into quarantine, where administrator can restrict access or allow users to review quarantined files through automatic email alerts.
4) Provides safer web browsing by preventing the download and execution of malicious code.

Highly effective scanning

1) Incorporates highly rated scanning engine from industry-leader AVG Technologies.
2) Signature database can be configured to check for updates hourly, ensuring timely, far-reaching coverage.
3) Dynamic heuristic analysis uses code emulation to identify polymorphic viruses and dangerous code that signatures can't catch.
4) Compressed and encoded files are decompressed for inspection, with wide compression support including .zip, .gzip, .tar, .jar, .rar, .chm, .lha, .pdf, XML/HTML container, OLE container (Microsoft Office documents),.cab, .arj, .ace, .bz2 (Bzip), .swf.
5) Buffered scanning process ensures optimum performance for in-line HTTP scanning.

Cost-effective virus scanning

1) Provide network-wide protection for all users configured behind your WatchGuard XTM firewall with a single Gateway AV subscription.
2) Purchase Gateway AV bundled with our suite of powerful security subscriptions for even greater savings.

5. Conclusion and Future work

In this Gateway antivirus we can check the file using gateway. When we send email then file is scan by the gateway. If we send file to other node then it will also scan the file to send to destination. Here the all the antivirus is commercial it will not freeware. Here we made the gateway antivirus using open source so we can scan file for HTTP, FTP, SMTP and POP3.

References

[1] C.K. Bai, "New Scanning Technologies of Gateway Virus," Network & Information, China, vol.23, pp. 94-96, 2008.

[2] Jianping Cui: A Further Study on Banker's Algorithm, Science and Technology Information (Academic Research), No. 17, 2007.
[3] ZHAO Yan, CHEN Guang-xing: Implementation and Improvement of Banker Algorithm by C Language, Journal of Tonghua Normal College, Vol.29, No.2, 2008
[4] China, vol.25, pp. 155-156, 2005, B.Y. Lin and S.Q. Wang, "Research of Virus Filter Gateway Based on HTTP and Proxy" Computer Engineering and Applications.
[5] M.G. Tan, B.S Wang, and J.Y. Zhang, "Research and Implementation on the capturing technique of TCP transparent proxy,"Microcomputer Information, China, vol.24, pp. 35-36, 2008.
[6] S.M. Shan, H.C. Lu, and Z.Y. Liu, "File sharing service monitoring technique based on protocol analysis in application layer," Journal of Dalian University of Technology, China, vol.18, pp.26-27, 2007
[7] http://support.gateway.com/s/tutorials/Tu_844825.shtml

Author Profile

Hiren V Mer received the B.E .in from GEC Modasa in 2008 and Pursuing M.E degrees in Computer Science Engineering from Parul Institute of Engineering & Technology in 2011-2013.