INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

HYBRID CLOUD-BASED FIREWALL SYSTEM PERFORMANCE AND RELIABILITY

HEMANGI DHANANJAY BHOIR[1], NILIMA M. DONGRE[2]

1. ME Student: Department of Information Technology, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, India.
2. Ass. Prof, Department of Information Technology, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, India.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: Firewalls are the first defense line for the networking services and applications as it protects the network by blocking unwanted traffic based on filtering policies. We are focusing on the hybrid firewall which is actually combination of on-premise firewall and off-premise firewall as we need to combine the benefits of both the firewall. In hybrid based firewall selection of right firewall (on-premise or off -premise) at right time will improves the performance and reliability of the entire system. This decision can be taken by the load balancing component of hybrid based firewall with the help of optimal scheduling algorithm. Round Robin algorithm and least session algorithm are two algorithms for load balancing which are compared with different parameter to make decision for the better one.

Keywords: Network Security; Hybrid Firewall; Load Balancing; Least Session Algorithm; Round Robin Algorithm

Corresponding Author: MS. HEMANGI DHANANJAY BHOIR

Access Online On:

www.ijpret.com

How to Cite This Article:

Hemangi Dhananjay Bhoir, IJPRET, 2016; Volume 4 (9): 401-410

PAPER-QR CODE

INTRODUCTION

A firewall works as a barrier, or a shield, between your PC and cyber space. When you are connected to the Internet, you are constantly sending and receiving information in small units called packets. The firewall filters these packets to see if they meet certain criteria set by a series of rules, and thereafter blocks or allows the data. This way, hackers cannot get inside and steal information such as bank account numbers and passwords from you. Most firewalls, like the one built into Windows XP, will alert you about suspicious incoming traffic. Anyone trying to gain access to your PC will hit the firewall first. The firewall detects the attack, and gives you a warning about it. In the evolution of firewall they are mainly categorized into three types such as Packet Filter, Stateful Inspection and Application Firewall [1].

Packet Filter: It is oldest and most basic firewall which examines for suspicious packets at either network layer or transport layer and delivers legitimate packets with good performance. Advantages: It gives high throughput and has low overhead. It is cheaper to buy. Disadvantage: Security level is not as expected i.e. it is less secure.

Stateful Inspection: It has capability to provide application level filtering even though it operates at the transport layer. Advantage: It traces the state of connection and discard packets which deviates from its identified states. Disadvantage: It requires vast resources and Complexity level is high.

Application Firewall: It is working as a communication application or proxy agent between two hosts to avoid direct connection between them which results in better security. Advantage: Application gateways/proxies do not allow a direct connection to be made between endpoints. They actually break the client/server model. Disadvantage: Some attackers can work at lower layer to build successful attack. Addition of proxy will consume a more resources.

Nowadays internet is essential part in business running. To keep track on business from top level to lowest in the hierarchy internet plays very important role. Some businesses are completely working online. As use of internet increased the attackers also increased to exploit system therefore it become necessity to secure network from them. To filter the network traffic and detects malicious packets companies uses firewall. Firewall at company requires deployment and maintenance cost as well as it requires regular updation to keep it up to date. But the firewall itself is not secure from the employees of the company specially network administrator who set the policies for the firewall.

In order to reduce firewall management and deployment costs and also to be secure from the threat of the employee to attack on firewall policy, businesses outsource their firewalls to Cloud Providers, as part of their Software as a Service (SaaS) and utility Computing provided by the Cloud [3], [4]. Cloud based firewall or virtual firewall running in a virtualized environment and provide packet filtering and monitoring service for businesses. This model saves money for businesses from management, deployment, and upgrading perspectives.

On premise or Physical firewalls are limited by the hardware capacity and it requires considerable financial cost. Off premise or Virtual firewalls are not limited by resources but they can be affected by the attacks from the outside of the virtualized domain which makes them to compromising its reliability. Hence new architecture is presented which combines physical firewall and cloud firewall together in order to utilize the benefits from both.

The remainder of this paper is organized as follows. Section II presents Literature review. Section III briefly addresses the issues in current systems and how it can be overcome. Section IV reports comparison of Round Robin algorithm and Least Session algorithm and then analysis of it, and Finally, Section V concludes the topic.

LITERATURE SURVEY

Firewalls are the most popular network-based security devices and have been widely deployed since the early days of computer networks. They are designed to permit or deny network traffic based on a firewall policy that specifies what types of packets should be allowed from/into the protected network [2].

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction [10].

It provides the scalable IT resources such as application and services as well as the infrastructure on which they operate, over the internet, on pay-per-use basis to adjust capacity quickly and easily. It helps to accommodate changes in demand and help any organization in avoiding the capital cost of software and hardware [9].

Firewalls are comes in two modes. First, Hypervisor Mode: This is run inside a virtual machine as a virtual firewall. Therefore, it monitors only local packets. Second, Bridged Mode: This is acts itself as a virtual machine as it placed between different network nodes. It allocates resources on demand but creates problem when migration of virtual machine is demand [1].

Motivation to Cloud Based Firewall:

Firewalls impose significant cost for most businesses especially smaller ones. As Internet traffic increases rapidly, the traditional firewalls needs to analyze a huge traffic against security policies thus firewall processing becomes the network bottleneck [3].

Businesses required appointing network admin for firewall deployment, maintenance and monitoring and also needs to provide training and invest for research on new emerging firewall technologies [3]. Businesses also have threat of the employee to change security policy for sake of money from competitors.

To overcome the threat of employee to attack on firewall policy at organization end we use the concept of cloud based firewall [3]. This model saves money for businesses from management, deployment, and upgrading perspectives.

Motivation to Hybrid Firewall

Physical firewalls has limited resources and it also requires additional cost of deploying firewall. Virtual firewalls are good as they are extensible in terms of resources and protected against threat of employees to change firewall policies. However, virtual firewalls can collapse if there is attacks from the outside of the virtualized environment. Hence, proposed architecture consists of both physical and virtual approaches together.

HYBRID FIREWALL

Hybrid firewall makes the use of large resources available on cloud to satisfy the need of physical firewall in terms of computational power with nominal cost. The proposed architecture consists of two parts i.e. Physical part and virtual part which makes it hybrid. In this physical firewall do the traditional work at company but it is powered by the virtual firewall which is nothing but the virtual machine which contains firewall program to detect malicious activities and performs other activities such as monitoring and reporting. A company agrees to purchase a security service offered by the Cloud Provider, this service comes as an additional resource that complements existing ones. The main idea of the proposed technique is to allow the physical firewall to do its operation of monitoring, reporting and analysis but when physical firewall overloaded network traffic is redirected to the virtual firewall for inspection.

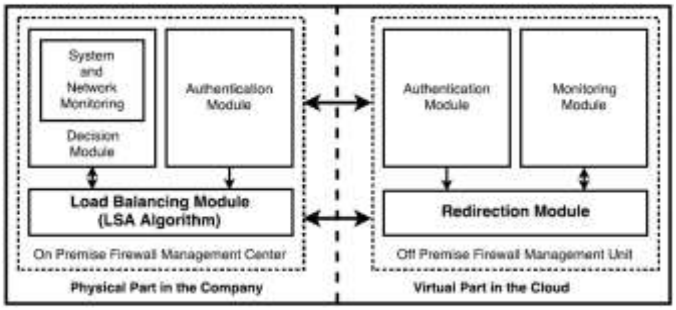

System and Network Monitoring
Decision Module
Authentication Module
Load Balancing Module (LSA Algorithm)
On Premise Firewall Management Center
Physical Part in the Company
Authentication Module
Monitoring Module
Redirection Module
Off Premise Firewall Management Unit
Virtual Part in the Cloud

Figure 1. Hybrid Firewall Architecture

On Premise Firewall Management Center

On premise firewall management center is located at the company office and it contains physical part of firewall. On Premise Firewall Management Center which is illustrated in Fig. 1 is a management tool that helps us to provide greater performance and efficient management. It has three modules: authentication, decision and load balancing. [1]

Authentication module: Authentication module is need to establish trust relationship between On premise and Off premise firewall. To do this, two steps are followed. First, Authentication based on signed certification and Second, Secure tunnel establishment between on premise and off premise firewall. The authentication module can use MS-CHAPv2, CHAP, MS-CHAP, , SIP Digest, PAP and other common EAP methods.

Decision Module: This module plays an essential role on on premise firewall management center. Decision module makes decision about when the traffic to be directed to off premise firewall to avoid exceeesive load on on premise firewall and when to stop using off premise firewall as traffic decreases. To take appropriate decision, this module need to deals with the system and network monitoring modules which keeps track of local ability information. Based on the information given by system and network monitoring module decision module can detect if the firewall is overloaded or not. If it is overloaded then the decision is made to redirect a amount of input traffic to the off premise firewall for analyzing. If on premise firewall is not overloaded, then it can continues its monitoring and analysing activity. For now, the percentage of redirected traffic is defined by the network administrator of the company. Additional information about virtual machine in off premise firewall is also sent to decision module to make decision about use additional virtual machines on off premise firewall.

Load Balancing Module: Load balancing module follows the instuction given by decision module. Its first job is to set up a shared traffic. This requires to apply certain rule specified by the decision module. Its work includes specifying port, suitable protocol and IP address. To operate, this module has to get network information from authenticate virtual machine on which virtual firewall runs and query from decision module to take action. However, to be more optimal use of efficient load balancing algorithm for sharing the incoming traffic is essential.

Off Premise Firewall Management Unit

Off premise firewall consist of large number virtual machines on which firewall application runs and required resources are provided by cloud using Infrastructure-as-a-Service (IaasS) Model. Every virual machine which runs the firewall application is responsible for carefully analyzing the network trafic redirected from the on premise firewall center and transfer the ligitimate packets to Local Area Network (LAN) of the company. To manage the firewall at virtual machine on cloud; it is equipped with the Off premise Firewall Management Unit as showed in Fig. 1. To communicate with on premise firewall and its operation it comprises of Authentication, Monitoring and Redirection Module.

Authentication Module: It does the similar functionality as that of physical firewall authentication module at company premise.

Monitoring Module: Off premise monitoring module moniters the virtual system parameters and network. It performs monitoring function and send alert to on premise decision module when any of the virtual firewall overloaded.

Redirection Module: Redirection module redirects the legitimate packets back to the ccorporate Local Area Network (LAN) after analysing by the virtual firewall. It is also responsible for receiving packets only from the on premise firewall and must discard packets from unknown source.

Load Balancing in Hybrid Firewall

In order to achieve a high throughput by optimal resource utilization load balaning method distribute workload to multiple computers. Load balancing manages the load by distributing client requests across multiple servers but only distribution cannot solve the overhead problem. Consider a scenario in which limited number of servers providing service to a large number of clients in such a cases server can become overloaded and degrade its performance. Load balancing is a concept which forworded a client request to the best suited server to handle and to prevent bottleneck. There are many different kinds of load balancing algorithms available, which can be categorized mainly into two approaches such as Static and Dynamic [5].

Round Robin algorithm

Round Robin algorithm is one type of static load balancing algorithms. In static load balancing processors are known in advance or at the beginning of the execution and it does not depend on current state of the system. Static load balancing schemes uses a prior knowledge of the system [6] Advantage: static load balancing is to decrease the overall execution time of a synchronous program while minimizing the communication delays. Disadvantage: Static load balancing is suitable for stable and homogeneous environment.

In working all processes are equally distributed among available processors irrespective of their process time. Hence, at certain point small size processes executes early and makes processor idle but large size processes takes times and overload the processor. This algorithm is mostly used in web servers where HTTP requests are of similar nature and distributed equally. [7]

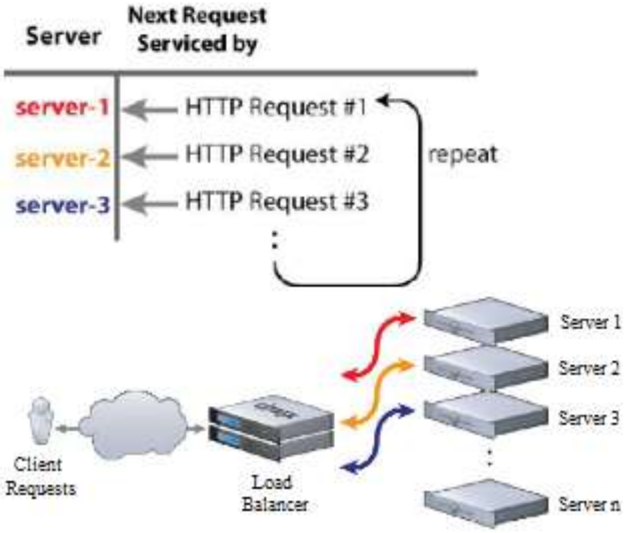
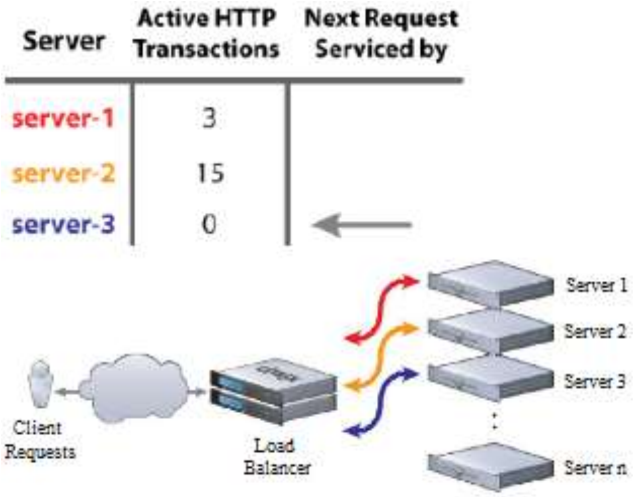


Figure 2 Round Robin Algorithm[11]

Least Session Algorithm

Least Session Algorithm (LSA) is a dynamic load balancing algorithm, unlike Round Robin algorithm decisions in dynamic load balancing are based on the current state of the system, no prior knowledge is needed. Advantage: If certain node fails will not collapse the entire system. It will slightly degrades the performance of the system. These algorithms are more resilient than static algorithms because they can easily adapt to alteration and provide better results in heterogeneous as well as dynamic environments.



Server	Active HTTP Transactions	Next Request Serviced by
server-1	3	
server-2	15	
server-3	0	←

Figure 3 Least Session algorithm[12]

Least Session algorithm is based on least connection mechanism which is a part of dynamic scheduling algorithm. It needs to count the number of connections for each server dynamically to estimate the load. The load balancer records the connection number of each server. In this case Load Balancer allocates the load to the server whose having least connection. The number of connection increases when a new connection is dispatched to it, and decreases the number when connection finishes or timeout happens. [8]

COMPARATIVE ANALYSIS

Comparison

Table 1. COMPARISON OF GA BASED, DECOY BASED AND ANT BASED CYBER DEFENSE

Parameter	Hybrid Firewall using RR	Hybrid Firewall using LSA
Approach	Static	Dynamic
Nature	Prior Knowledge Base is required about each node statistics.	Run Time Statistics of each node are monitored to adopt to changing load requirement.
Usage	Used in Homogeneous Environment	Used in Heterogeneous Environment
Performance	Less	More
Reliability	Less Reliable	More Reliable
Adaptability	Not Adaptive	More Adaptive
Resource Utilization	Lesser Resource Utilization	Better Resource Utilization
Response Time	Shorter Response Time	Higher Response Time
Processor Thrashing	Free from Processor Thrashing	Substantial Processor Thrashing

Analysis

Above discussed methods in table 4.1 shows the different Load balancing in Hybrid Based Firewall. Load balancing is totally dependent upon the situation in which workload is assigned in execution time. We have seen Static load balancing approach is stable as compared to dynamic load balancing as no information regarding present workload state is passed among processors. As per the reliability is concern Least Session Algorithm is always better than that of Round Robin Algorithm because processes lies on the one host can be transferred to another host if failure occurs; moreover Round Robin method just tries to assign task to processor in order to achieve minimum response time ignoring the fact that this task assignment can result in to a situation in which some processor finish their work early and sit ideal due to lack of work but the Least Session method takes care of assigning the load in such a way that no processors should sit ideal.

CONCLUSION

Hybrid Based Firewall is a new evolution which combines benefits from both; physical firewall as well as virtual firewall that increases the computational power of physical firewall with low financial cost and using the vast resources offered by the cloud. In order to increase effectiveness of hybrid architecture we use Least Session algorithm that shows significant improvement in computing power, System and Network performances of Hybrid based firewalling.

REFERENCES

1. Guenane, F., Boujezza, H., Nogueira, M., Pujolle G., "An architecture to manage performance and reliability on hybrid cloud-based firewalling", Network Operations and Management Symposium (NOMS), 2014 IEEE, Pages 1-5, 5-9 May 2014
2. Qi Duan and Al-Shaer E., "Traffic-aware dynamic firewall policy management: techniques and applications", Communications Magazine, IEEE (Volume:51 , Issue: 7), Pages 73-79, July 2013
3. Amir R. Khakpour, Alex X. Liu, "First Step Toward Cloud-Based Firewalling", 2012 31st International Symposium on Reliable Distributed Systems, 2012
4. Hamid Mcheick, Ziad Rajih Mohammed and Abbass Lakiss, "Evaluation of Load Balance Algorithms", Software Engineering Research, Management and Applications (SERA), 2011 9th International Conference on, Pages 104-109, 10-12 Aug. 2011
5. Akshay Daryapurkar, Mrs. V.M. Deshmukh, "Efficient Load Balancing Algorithm in Cloud Environment", International Journal Of Computer Science And Applications , Vol. 6, No.2, Apr 2013

6. Alok singh, Vikas Kumar Tiwari, Dr. Bhupesh Gour, "A Survey on Load Balancing in Cloud Computing Using Soft Computing Technique's", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 9, September 2014

7. Sonika Matele, Navneet Singh,Dr.K.James Mathai, "A Study of Load Balancing Issue Among Multifarious Issues of Cloud Computing Environment", International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), 2013

8. Soumya Ray and Ajanta De Sarkar, "Execution analysis of load balancing algorithms in cloud computing environment", International Journal on Cloud Computing: Services and Architecture (IJCCSA),Vol.2, No.5, October 2012

9. R.W. Lucky, "Cloud computing", IEEE Journal of Spectrum, Vol. 46, No. 5, May 2009, Pages 27-45

10. Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing" NIST Special Publication 800-145, September 2011.

11. Craig Ellrod, "Load Balancing – Round Robin", http://blogs.citrix.com/2010/09/03/load-balancing-round-robin/, September 3, 2010.

12. Craig Ellrod, "Load Balancing – Least Response Time", http://blogs.citrix.com/2010/09/03/load-balancing-least-response-time/, September 3, 2010