ISSN:0975-9646

Enhancing Firewall for Serving the Distributed Security Requirements for Cloud

[1]Yamini Bangur, [2] Vijendra Mandraha

Department of Computer Science & Engineering
SVITS College, Indore (M.P), India

Abstract: **Cloud computing is a recent technology used for providing the scalable and on demand computation as a service to the end user. The service used here is measurable and represents the fault tolerance behaviour. Cloud mainly serves the scalable users demands of resources and their security based on certain characteristics of distributed environment by which the controlling and managing burdensome are reduced form the service users. Along with cloud applications exponential growth the vulnerability of security breaches is also raising. This is because cloud involves defined interaction with SLA based policies for the resource and service usages. If someone violates these rules the protection level of system gets compromised. Traditional security of the system is handled by the firewall. They are made for a static and fixed environment having limited policies and interactions. But is cloud environments the scenarios are changed totally and hence the behaviour of firewall might also get adaptive as per the need of distributed computing. This paper aims to provide and effective firewall which could handle dynamic security requirements, provides better access control for various processes and users with minimum processing time and high detection rates. At the initial stages of work, the direction seems to provide benefits over the traditional systems.**

***keywords* - :** Cloud computing, Security, Distributed Firewall, Resource Optimization, Filtering Rues, Detection Rates, CVSS, Entropy;

I. INTRODUCTION

cloud computing is the recent are of work in the industry and research domains due to the extreme possibilities and its openness. It provides centralized control over all the resources with defined policies and their quantitative assessments. It offers various computation resources as a service to the end user. Resource can be of hardware of software type whose capacity and power can be distributed among different processes. All its needs an effective console for analysing the behaviour of all the services. There are some problems associated with the traditional computing related to their reliability, scalability, fault tolerance, measurability and security. Among them, the security is the one area which requires high emphasis on the guiding rules developed by the policy makers and resource users.

Cloud is a well managed group of resources whose capacity and power is merged or distributed to satisfy the end users needs. Here the resource service used by the cloud provider is transparent to the application developed in cloud. It serves the remote access with satisfying the rules of capacity, availability and partition logics. Here the task could be of any size and cloud processes it in near optimal time. Thus such a massive processing requires dynamic handling of the heterogeneous resources at different locations. Now once the resources serve the processing parameters then, the issues of verifying their processes and the types of user utilizing these computations is remains to be solved. Cloud resources are provided as a service on an as needed basis. The cloud itself typically includes large numbers of commodity-grade servers, harnessed to deliver highly scalable and reliable on-demand services. The amount of resources provided in the cloud system for the users is increased when they need more and decrease when they need less.

The system must have a check against the users, their behaviour, systems authenticity, intermediate communication handling, unauthorized access, and attack prevention [1]. Previously they are provided using traditional firewalls. These firewalls are not used directly for cloud because of their different service architecture. Because the cloud provides scalability of resources, handles dynamic user demands, provides everything guided by the defined service level agreements (SLA's) etc. The cloud based systems can guarantee the data security and the user does not have to look over the protection parameters. So the cloud computing must ensure the security of data stored in the cloud system. Today's, there are many companies which provides the cloud platforms such as Amazon, VMware, EMC Google, IBM and Microsoft [2].

As the data stored on cloud storages are having some cost attributes and value to them. Thus it is of keen importance to the attacker to get in control for that data. Once the data is lost by the provider against the malicious activities, trust over the system gets crashes and affects the organizations financial decisions. The system must be protected more carefully than the traditional system. The company must have confidence in the cloud computing if they want to store the private data in the cloud system. Governance and security are crucial to computing on the cloud, whether the cloud system is in firewall or not. This work takes these issues and proceeds towards developing a novel system of distributed firewall for dynamic security handling in cloud computing.

II. BACKGROUND

Cloud computing is an trusted third party based service methodology which maps the users demand and resource availability. Among the various features offered by the cloud environment as a service security is having the widest range of options and applicability. It is key behind each and every operations of cloud computing. Traditional security solutions can't be able to provide protection level as demanded by the cloud consumer or provider. It has no boundaries and thus the limited of fixed security control is lacking the depth protection. Some of the security problems associated with cloud are: access authentication, data security, privacy, platform stability and controlled operations. The cloud running over the internet or the private cloud, both is facing the similar issues. Thus majorly the security is taken as biggest concern for safe cloud operations.

Some of the previously recognized security problems are attacks vulnerabilities, hacking operations, malicious activities detection etc [3]. For making a better place to communicate over the cloud it requires some modification and a focused security as a service over it. One of the essential elements in network and information system security, firewalls has been widely deployed in defending suspicious traffic and unauthorized access to Internet-based enterprises. Sitting on the border between a private network and the public Internet, a firewall examines all incoming and outgoing packets based on security rules. Firewall are the well known protection system against these threats but their working level is limited with fixed set of operations and their static level. They only deal with the similar pattern of security breaches occurring over the system. Whenever there is certain change the systems definition needs to be revised along with all security mapping to the all logical places where it is applied. Hackers and malicious intruder may hack into cloud accounts and steal sensitive data stored in cloud systems. The data and business application are stored in the cloud center and the cloud system must protect the resource carefully.

Also developing the security as a service model requires adoption of virtualization, service oriented architecture and utility computing. Over the Internet and it includes the applications, platform and services. If the systems meet the failure, fast recovery of the resource also is a problem. The cloud systems hide the details of service implementation technology and the management. The user can't control the progress of deal with the data and the user can't make sure the data security by themselves. The data resource storage and operation and network transform also deals with the cloud system. The key data resource data and privacy are very import for the user.

Protection Required in Cloud [4, 5]

- Fine grained access control
- Security audit can be used for regular monitoring and SLA verifications
- Policy guided data and application migrations
- Integrity Verifications using HMAC and MD5 based approaches
- Confidentiality Assurance using standard cryptosystems
- Guaranteed Availability and Fault Tolerance
- Privacy Protection
- Privilege Control

The user does not know what network are transmitting the data because the flexibility and scalability of cloud systems. The user can't make sure data privacy operated by the cloud in a confidential way. The cloud system can deploy the cloud centre in different area and the data can be stored in different cloud nodes. The different area has different laws so the security management can meet the low risk. Cloud computing service must be improved in legal protection.

How Firewall Works

Firewall implements security using the defined security policies which provides filtering rules for the data transitions on the cloud network. The data which satisfies the security requirements of the organization if allowed to travels in the network and rest of the packets are blocked. The process of configuring a firewall is tedious and error prone. The policy management is quite complicated task because of their dynamically changing thousands of the rules. They rules are conflicting in nature and might overlap somewhere which defining them in the system. Cloud requires open access to all the services for fats control over the data. Along with that it must satisfies the security requirements. Thus it needs to be modified in such way which satisfies all the characteristics of the cloud so that security service can be developed. On the other hand, due to the complex nature of policy anomalies, system administrators are often faced with a more challenging problem in resolving anomalies, in particular, resolving policy conflicts. An intuitive means for a system administrator to resolve policy conflicts is to remove all conflicts by modifying the conflicting rules. Thus the cloud based firewall must be configured so as to support the distributed processing environment and handles the conflicts of policy rules and still effectively detects the anomalies coming along with the rule formations.

III. Literature Survey

During the last few decades providing security to the networked solution is changes abruptly. Now with the rapid development of cloud based environment the security control is getting more complex. Among them the firewall handling in distributed environment is quite a tedious job. This section covers some of that implementation and suggestions applying towards making the distributed firewall an effective concept.

The paper [6] focuses on the cloud computing security problems and their impacts on the application development and migrations. It analyses the cloud security breaches against the various applications and their working scenarios. The data stored in the cloud system can meet the problem of stolen and modified unlawfully. All it aims is towards making the high data availability, privacy and reliability over the trusted third party based systems. While serving its goals there is various mechanisms such as authentication, access control, encryption, privacy preserving, digital certificates etc. It includes network access control and directory level security control. The cloud computing provider must make variety of measures to protect the security in order to effectively solve these problems.

The paper [7] detects the unintended security breaches such as data leakages and access control using the updated firewall framework named as FAME. The effectiveness of the firewall is totally depends upon the type of policy and rules configured for accurate and timely detection. All the anomalies must be correctly classifies and removed out of the system. It represents an innovative policy anomaly management framework for firewalls, adopting a rule-based segmentation technique to identify policy anomalies and derive effective anomaly resolutions. The system is developed in tow levels. The upper level is the visualization layer, which visualizes the results of policy anomaly analysis to system administrators. Two visualization interfaces, policy conflict viewer and policy redundancy viewer, are designed to manage policy conflicts and redundancies, respectively. The lower level of the architecture provides underlying functionalities addressed in policy anomaly management framework and relevant resources including rule information, strategy repository, network asset information, and vulnerability information.

The paper [8] controls the cloud security using the predefined set of notarized rules known as service level agreements (SLA's). All it aims towards assessing the risk associated with the system in a near real time. The security is the most primary construct for the cloud because it depends on the system and user who is adopting the cloud solutions. High reliability and cloud security is assured using the physical technical controls such as firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) or Network Access Control (NAC) products that ensure access control continue to be critical components of the security architecture. However there are certain changes is going on with all the approaches used in traditional computation. Analysing the benefits of these approaches, it shows that the cloud is satisfying te all security requirements and hence serve the complete security solutions.

In the paper [9] a specific project is studied and a solution is presented which relates with the direction of our work. Mainly its servers the traffic analysis, distribution and diversion towards a cloud firewall using a tool named AMRES (Academic Network of Serbia) network. Although some of the methods can be only used with the Cisco equipment, other methods can be used with equipment of any manufacturer or open-source solutions that are relaying on proxy functionality in order to forward the web traffic. Ironport firewall devices are providing a set of filtering features. But the two most important that are used in AMRES are:

- ➢ Filtering based on web categories
- ➢ Antimalware filtering using Webroot scanner

The solution give the above approach is highly scalable and easy to deploy. It provides equal distribution of web traffic hence the load on the system is also gets reduced.

The proposal given with the paper [10] is an decentralized firewall concept used for cloud computing. It is having a small group of user and provider which shares the data between each other. Here the decentralized approach will leads towards distribution of copies of data which raises the problem of handling the multiple copies of the similar data. Thus there is some modification suggested by the system which increase the detection accuracy and decrease the load on the system. Some of the other presented approaches shad also given with the paper.

The paper [11] is a white paper which presents a tool named SteelApp application firewall. It is an scalable solution provides the high level of protections wing the custom third party frameworks. It can be used to apply business rules to your online traffic, inspecting and blocking attacks such as SQL injection and cross-site scripting (XSS), while filtering outgoing traffic to mask credit card data, and help compliance with PCI-DSS and HIPAA by filtering of outgoing data. Establishing a comprehensive patch management system is important, but in practice this approach can prove very difficult and costly. Typical web applications are built on open source components by third-party developers who rely on open web frameworks. While you get interoperability and a shorter development time, it comes at the expense of complex patch management to solve security vulnerabilities. The software consists of three scalable components: Enforcer, Decider and Administration Interface. The solution given by the approach is providing better results with distributed management interface can be used to protect both types of deployment, or even in a shared services environment.

IV. Problem Statement

Cloud is an outsourced environment where the trusted third party lets the overall control on the services and the user's data. They are cloud service providers which control the complete resources and their respective SLA for the users concerning and fulfilling the needs of security against the requirements. Cloud uses some of the traditional mechanism in its own way. Mainly the aims is towards making the confidentiality, availability and integrity over the system. The unauthorized access and malicious activities planted for the system gets blocked by the comprehensive efforts of all of the approaches. Firewall plays a vital role is serving the goal of the security against the various types of the attacks. The firewall aims towards analysing the traffic coming or going to the system. Thus the analysis totally depends upon the filter rule which directs the allowable and not allowed data and control packets.

In case of cloud environment the traffic is diverted for single application through various distributed location and the data accesses over that location are performed simultaneously. This parallel and distributed access makes the firewall operations very complex against their detection parameters and filtering rules. Implementing the centralized console based firewall operations is a very complex operation. Also the cloud firewall must checks the various VM instances executing over the network for malicious traffic detection and removal.

Thus, the distributed firewall must look over the traffic; apply their priority and queuing rules, evaluates the risk associated with vulnerable operations, generates the timely alerts and protect the system against the known and unknown types of attacks.

V. PROPOSED WORK

Developing the solution of above detected problems will be made feasible using the dynamic security controls and filtering rules. The resource allocation policies respect to their service will also be continuously changing and hence the behaviour of the firewall will also be discrete. The VM monitoring and the instance analysis must also be performed over here. This work suggests a novel distributed firewall for the cloud computing which satisfies all the requirements of the user and service provider. The work handles the resource request, maintains the service list mapped with that resources and arrange the in the priorities of the risk associated with them. Along with the basic characteristics of firewall it satisfies the reliability and scalability phenomenon. It resolves the conflicts associated with the traffic and precedence analysis with effective anomaly detection and allows the authentic packets to flow between the servers and VM instances.

The proposed distributed firewall phenomenon will detects and removes the malicious traffic from the network. The filtering rules are also dynamic in nature. There are some situations where the traditional approach drops the actual normal traffic and allows the malicious packets. Thus the false detection rate must also be in keen observation and aims towards reducing the false detection ratio. The approach suggested is segmentation based approach which checks each segments against the filtering rules and try to gains the fine grained access of services for the users. Based on this technique, a network packet space defined by a firewall policy can be divided into a set of disjoint packet space segments.

Based on the various mechanisms for improving the segmentation, verification, risk analysis and filtering the suggested approach will definitely outperforms the results of the traditional approaches. A grid based visualization approach is introduced to represent policy anomaly diagnosis information in an intuitive way, enabling an efficient anomaly management.

In addition to that the work had also suggested and console based centralized operations for the firewall irrespective of the nature or locations of the data. To evaluate the practicality of the suggested tool, set of extensive experiments is designed with real-life firewall policies.

Description

The approach starts with the initiation of the communication request between the user and cloud service providers or admin. The system detects the presence of malicious traffic after recoding the communication or analysing the traffic flowing though the network. Thus the network entity will starts capturing the data of each and every communication and information exchanges. The generated data is matched against the rules used for defining the normal and malicious packets. These rules are defined over a server named as policy server. This policy server is having its own centrally controlled the rules or definition repository. This repository is continuously updated by the new definitions and filtering rules. This policy server wills serves as the classification rule holder and work as a part of the proposed distributed firewall. Now the firewall module analyses the traffic, the content, and packets formats, data associated with the packets, malicious behaviour and inspection.

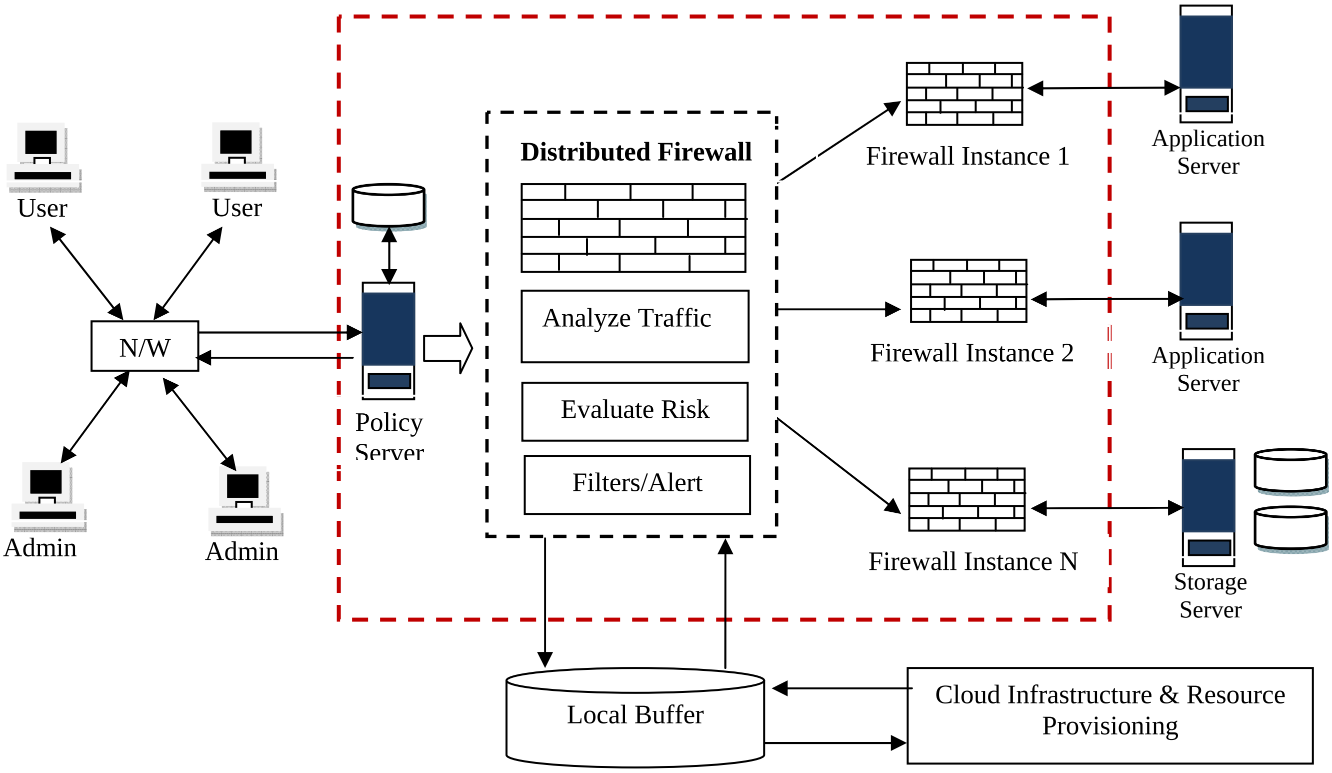

FIGURE 1: ENHANCED DISTRIBUTED FIREWALL FOR CLOUD

Now, once the statics is generated they can be filtering out form the traffic. Here the segregation is performed in different classes according to the traffic characteristics. The operations with the distributed firewall is having an additional buffer which holds the repetitive instructions, rules and packets which are highly vulnerable for similar type of requests.

As cloud is an service based environment, thus the above mention operation will be also implemented using a service model. This service of distributed firewall will be supported by the clouds infrastructure and the resources are provisioned accordingly. It provides the scalability and reliability for the distributed firewall. Once the things are checked and verified then only the VM instance s are allowed to communicate with their respective services. Now during the access there are situation where all of a sudden a VM starts malfunctioning then, it could also be controlled by the system because a continuous monitoring on the VM instances, resources, service operations and the network traffic is performed which detects the change in behaviour even during the mid of the operations.

Here the attack detection is a standout amongst the most noticeable zones of work. The Firewall is the most known methods for discovering the unauthorized access to the framework and obstructs the vindictive traffic. Actualizing firewall for cloud experience different system arranged difficulties, for example, load balancing, scheduling, and traffic difference, filtering, controlling the rate of lending, instance management, attack detection. In the wake of considering the different examination articles, there is some instrument which determines these issues.

Apart from the above mentioned goals and objective fulfilled there are so many other interrelated work which is one during the implementation of proof of concepts and hence the remaining flaws in the approaches can be sorted out at that time.

APPLICATION AREA

(i) Dynamic web security
(ii) Web services monitoring
(iii) Web performance logger
(iv) Cloud based web computing
(v) Blogging
(vi) Social networking
(vii) Transaction Systems
(viii) Online services marketing

VI. EVALUATION PARAMETERS

As the work is totally based on detecting the malicious traffic correctly, thus the factors should also exhibit the same nature. Thus the false positive rate detection must be reduced along with that the detection accuracy must be increased. The risk associated with the malicious traffic based operations must be having high vulnerability, thus the assessment can be performed here. Thus, the suggested work will adopt some quantitative assessment factors which interpret the correctness of the results.

(a) CVSS Factor

Thus, the work selects the Common Vulnerability Scoring System (CVSS) as an underlying security metrics for risk evaluation. Two major factors, exploitability of vulnerability (reflecting the likelihood of exploitation) and severity of vulnerability (representing the potential damage of exploitation), are utilized to evaluate the risk level of a network system. Beside those two factors, another important factor in determining the criticality of an identified security problem is asset importance value. Since the CVSS base score can cover both exploitability of vulnerability and severity of vulnerability factors, we incorporate the CVSS base score and asset importance value to compute the risk value vulnerability as follows:

Risk Value= (CVSS Base Score) X (Importance Value)

(b) Entropy Factor

The Entropy calculation is used for calculating the amount of traffic. Sometimes the intruder may impose DDOS attack/flooding attack. So the system which is implementing more traffic needs to be tracked. The monitoring process can be done to calculate the behavioural distance. Abnormal behaviour of the client is frequently reported to the administrator. Also the countermeasures are selected to perform which include traffic redirection, port blocking, network reconfiguration, updates the filtering rules, Deep packet inspection, and Virtual Machine isolation. Later with the work, more generic formulas can be representing with the implementation proof**.**

(c) Classification Accuracy

It is the third and the most important factor intended specifically for the effective detection of the malicious traffic. Here the factors aim towards improving the detection accuracy by reducing the incorrect detections.

ACKNOWLEDGMENT

The authors wish to thanks Dr.Anand Rajavat and Prof.Vijendra Mandraha for their support in this work.

VII. CONCLUSION

Cloud computing is having wide variety of service which is attracting the user. Once the users gets on to the cloud it is provider's responsibility to serve the users security requirements and protects its data against the malicious releases. Thus cloud implements the firewall in a different way. As the cloud is totally a distributed environment thus then nature of the firewall is also be the same. But developing the distributed firewall is having so many associated problems such as latency, bandwidth, load, network, access control, authentication etc. Among them this paper presents the distributed firewall against the VM instances executing at different remote locations. Thus, a new directional work had been started for practically achieving the new firewall strategies for cloud. It also aims toward achieving the provisioning and rules generation for the distributed nature firewall. At the initial level of work the approach providing effective results.

REFERENCES

[1] Steven M. Bellovin, “Distributed Firewalls”, in Research at SMB Corp, 1999

[2] Daniel Wan, “Distributed Firewall”, GIAC Paper, SANS Institute, 2002

[3] Hiral B.Patel, Ravi S.Patel and Jayesh A.Patel, “Approach of Data Security in Local Network using Distributed Firewalls”, in IJP2PTT, ISSN: 2249-2615, Vol:1, Issue:3, 2011

[4] Harleen Kaur, Omid Mahdi Ebadati E and M. Afshar Alam, “Implementation of Portion Approach in Distributed Firewall Application for Network Security Framework”, in IJCSI International Journal of Computer Science Issues, ISSN (Online): 1694-0814, Vol. 8, Issue 6, No 2, November 2011

[5] “Security Guidance for Critical Area of Focus in Cloud Computing”, By Cloud Security Alliance, 2011

[6] Wentao Liu, “Research on Cloud Computing Security Problem and Strategy”, in IEEE Transactions, ISSN: 978-1-4577-1415-3/12, 2012

[7] Hongxin Hu and Gail-Joon Ahn, “Detecting and Resolving Firewall Policy Anomalies”, in IEEE Transaction on Dependable And Secure Computing, ISSN: 1545-5971/12, doi: 10.1109/TDSC.2012.20, Vol. 9, No. 3, May 2012

[8] Todd Steiner and Hamed Khiabani, “An Introduction To Securing a Cloud Environment”, GIAC Paper, SANS Institute, 2012

[9] Ivan Ivanovic, “Distribution of web traffic toward the centralized cloud firewall system”, in Belgrade University Computer Centre, University of Belgrade, Belgrade, Serbia, 2013

[10] Hao Zhuang, “Cost-efficient Resource Allocation for Decentralized Clouds”, in EDIC Research Proposal, 2009

[11] “Riverbed SteelApp Application Firewall :Securing Cloud Computing Applications With A Distributed Web Application Firewall”, White Paper by RiverBed Corp.2013

[12] Meng Liu, Wanchun Dou, Shui Yu & Zhensheng Zhang, “A Decentralized Cloud Firewall Framework with Resources Provisioning Cost Optimization”, in IEEE Transaction on Parallel and Distributed Systems, ISSN: 1045-9219, doi: 10.1109/TPDS.2014.2314672, 2014