International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

|| Volume 9, Issue 4, April 2020 ||

Virtual Private Cloud Firewall Using Six Sigma

Prof.Sharda Chhabria[1], AniketShukla[2], SahilSingh[3], Dnyaneshwar Ade[4], Nikhil Kotkar[5], Yuvraj Karayat[6]

Assistant Professor, Department of Computer Engineering, G H Raisoni Academy Of Engineering And Technology, Nagpur, India[1]

UG Students, Department of Computer Engineering, G H Raisoni Academy Of Engineering And Technology, Nagpur, India[2,3,4,5,6]

ABSTRACT: Cloud computing is highly scalable technology, it is an on-demand configurable pool of resources and one among the latest topics in the information sector. The paper presents a Cloud Computing infrastructure, where like various other cloud providers in the world a cloud is created that is virtual and private for all the users those who are using the cloud. The infrastructure presented offers the cloud where the clients can have full access to everything without internet. This infrastructure can be used by a single organization or a group of different organizations. Whatever be the case either a group of organization using it or different organizations are using it, in both the cases the cloud is able to provide the isolation between the users. The security of users' data is provided by a firewall on the cloud whose acces is given to only administrator. The administrator can be dynamic, it can be changed and it is connected to the cloud through wireless medium

KEYWORDS : Area-efficient, Low cost, More Secure, Easy to Access.

I. INTRODUCTION

Cloud computing in recent years have became the great centre of attraction for the IT hubs, big companies and firms, it is also going through day by day enhancements in it, and also the introduction of more and more technical elements is taking place.The popularity gained by cloud computing is due to the extend of services provided by it. That invloves various useful services that were there in the market before but cloud computing has come up with some different ways of those services, like storage or we can say infinite storage because the cloud computing services are highly scalable.This also provides the user with great computing power and some really good resources which can cost an individual good money if he is going to buy them for their use only.The best thing is that the user need to pay for those services for whom he has opted for.Cloud computing let the users feel like all the services whether it be storage or other computing resources all are present at his disposal.So, overall cloud computing has brought an absolutely new way of accessing and handling the things.

A private cloud is owned by a particular organization so the question comes "is there any need of firewall in cloud which is already private?" the answer should be "yes" .It's a good idea to setup a basic firewall for the VPC. However, the bulk of network security should be handled via security groups rather than the network filters. In many organizations there are group of people who used to work on different projects but the resources they require from the company side are present at the common point that is the private cloud of the company. So in these cases there should be the bit of isolation between there processed data here the firewall plays a vital role.

II.SECURITY ISSUES FOR CLOUD COMPUTING

Cloud computing model has gained a great popularity since its introduction. It not only provides great services but it also provide huge information about security enhancements and risks reductions in the model. IaaS is the great strength provider for the complete cloud infrastructure it acts at the bottom layer, it provides some of the most powerful functionalities of a complete cloud.IaaS has the capabilty to support multiple virtual machines, IaaS also provides a platform where the hackers have to get large number of attacking instances to launch attacks.These challenges are never ending for any old or upcoming technologies in the market.In the field of cloud computing, the hackers by using some external means can hit to the database and can steal the data that is highly confidential for a client using the

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

|| Volume 9, Issue 4, April 2020 ||

cloud.There are possibilities that hacker not only intend to steal the data but also to sabotage the data and hamper the softwares.These challenges have a start but not an end.So to tackle such situations various security models have to be made and deployed effectively.

Traditional security: One of the very common sort of security issue is traditional security.When an attacker tries to enter the computers connected through a network and eventually be the part of the network and later on attack the complete cloud infrastructure and compromise the security.The attacker once entered the network can easily take down the all security models and mechanisms.The attcker can even get to the administartion end in worst case scenario.

Availability:It is kind of security concern where mainly the center is attacked for carrying for the attack.The center is taken down and then the important applications are attacked.Some of the crucial process that only resides on center only get compromised.These are the crucial processes that are directly controlled by the centre.Once the center is down the required loophole is made for the hacekrs.

External agent controllingthe data:The data which a client is putting is upon the cloud is really confidential and the client can not afford to loose that data at nay cost.For this reason the cloud provider should be someone who is absolutelyreliable.When the client wants to stop taking the services from the cloud provider then the cloud provider should be able to delete all the data of that client and give assurance to the client for the same.All these things involves lots of risks and various other factors that can put a client into trouble.So before paying and before being the client of a particular cloud provider.The complete cloud infrastructure is handled by any third party.All the data all the applications are somewhat under the third party control.This also becomes the responsibilty of the cloud providers to safeguard the data.

III.VPN AND FIREWALL,THE PILLARS OF SECURITY FOR CLOUD COMPUTING

The cloud computing infrastructure mainly aims to provide some basic opearations even in any worst case.Even if the attack has taken place the basic operations like safe and secure delivery of the data to and from the cloud should be possible for sometime,so the the client's data can be transferred to some safer infrastructure and stored safely.The issues of security are solved upto great extent by the VPN and FIREWALL. VPN is a great asset for cloud computing ,it uses various techniques and the most important of them are standard encryption algorithms and it makes sure that the data is secured.

SCENARIOS OF NETWORK ESTABLISHMENT

In the process of network establishment and network simulation the mandatory element is OPNET simulator.OPNET simulator is a very well known simulator in the field of cloud computing, it has also been used in various researches till now. In the simulation processes basically , two servers represents are deployed and they act as two departments. Over here in this process the major role of VPN and FIREWALL comes up, their impact is measured by checking how robust the network has become and also by the throughput.

Listed below are some Parameters used in scenarios are:

Two servers: For the representation of the two departments the two servers are needed.So the two servers (PPP Server) are used.

Firewall: There has also been used the firewall (ethernet2_slip8_firewall) which has the role tomonitor and check the every access request.

Setiing Up VPN: The VPN can solve the great deal of problems if configured and deployed properly.If the VPN tunnel is established then it only let the specified clients to pass through the tunnel and get access of the required applications from the server.

NETWORK SETUP FOR VPC(VIRTUAL PRIVATE CLOUD):

The cloud infrastructure provide various kinds of facilities for all domain works.VPC it is the cloud which is virtual and is used by one single organization only.It is the virtual form of the physical network.It used to make all the data centers,

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

|| Volume 9, Issue 4, April 2020 ||

resources and servers into an virtual environment. It provides the connectivity for your computer, or any other device connected.

DETAILS OF VPC SPECIFICATIONS:

To setup an VPC, one should be fully aware about the type of VPC going to be deployed.Any VPC network that is setup, it is associated with various routes only.VPC can form only that particular set of routes. There are not only routes but also various firewall rules.The important thing about the VPC is that they are setup at one zone but thy are not only in association with that zone only.It provides the clients with great services all the time.To fullfil this purpose the subnets are used.Once the VPC is setup various resources can be put on it.All these resources collectively form the VPC and they can communicate with each other by uing IPV4 addressess.
Amidst all these the network should be able to secure the network administration and that is possible by using cloud identity access and management.
Most of the times the VPC is owned by a single organization only, but sometimes one VPC is used by two companies which are working on somewhat similar project.So in this case only the few of the members are given the authorization and they can create the resources that use subnets of the shared VPC network.There is also an intresting concept of VPC peering with the help of which two PCs can be connected.
.

IV.DEVELOPMENT

GNS3:In the earlier stages of the cloud computing the developers and cloud computing experts faced many problems.They were not able to test the functionality of the cloud which they have preapred ,they were not able to check networks whether working properly or not.For every experiment they have to buy new and expensive network devuces.This approach was also not so feasible, because every experiment required some different specifications of devices.

GNS3 was introduces by Jeremy Grossmann.It was great tool that gave relief to the cloud computing experts.GNS3 stands for Graphical Network Simulator.With the help of this software the experts are able to emulate networks.GNS3 is not the only software that has made the virtuality and emulation possible,there are various softwares like Vmware or Virtual PC that are extensively used and are used to emulate so many operating systems like Windows,XP professional or Ubuntu Linux in a virtual environment.These softwares has made it possible to run ubuntu Linux in a virtual environment on clients computer.But in the field of networking the GNS3 is primarily used.In GNS3 there is an element called Dynamips which are core programs of the GNS3 due to which the IOS emulation is possible.

There are so many additional developers also involved in creating GNS3 and there names are David Ruiz, Romain Lamaison, Aurélien Levesque, and Xavier Alt. Dynamips was developed by Christophe Fillot. Dynagen’s primary developer was Greg Anuzelli.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

|| Volume 9, Issue 4, April 2020 ||

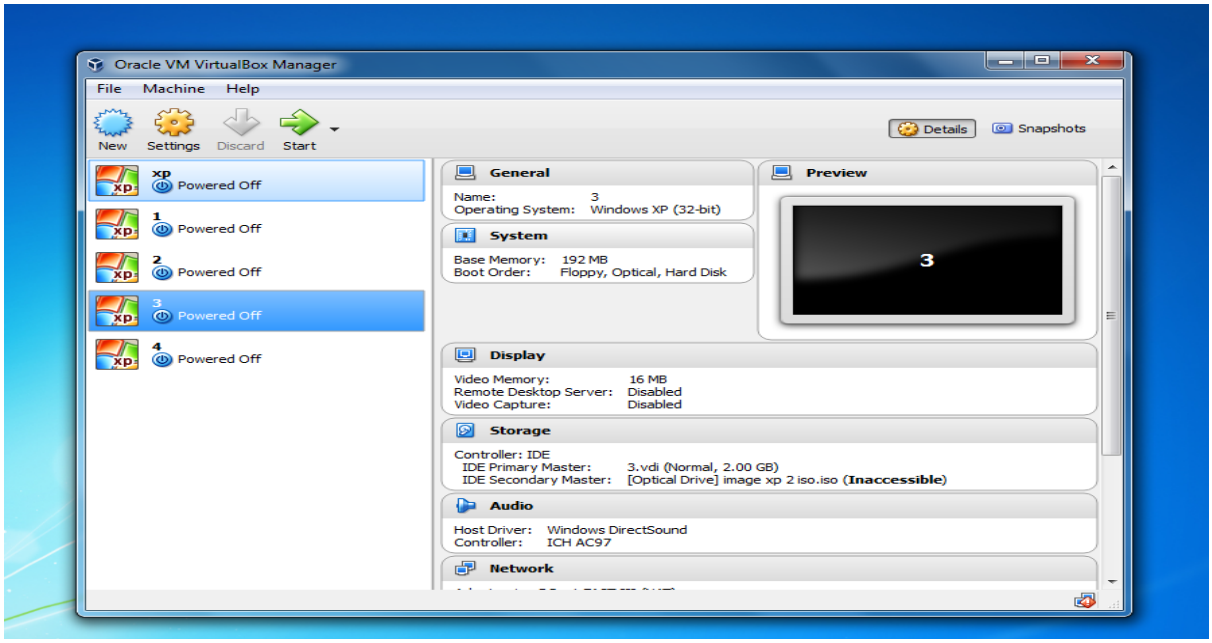

Fig3: Virtual Box is installed and various clients are created on it then they are connected to GNS3 environment. **Clonning Process**:**Cloning** is the method of producing identical genes through different procedures.

Created the cloud on one Computer. Its not like actual cloud that we know about, that has got the infinite storage and lots of resources on it. It would be practically impossible to build a Computing as a Service platform in a simple laptop or a PC.Once the cloud is created the server is installed over it, various dummy websites is created and uploaded on server.The computer on which the cloud is made ,two devices are used with it ,SXT and POE. SXT at cloud side is configured as **Server/AP.**The users which were already created using virtual box their complete configuration is done on the computerwhich is used for making cloud.One user from those many created is brought out in physical world and presented in the form of Computer, which is capable of using all the services provided by the cloud.This user is also connected through same set of those two devices SXT and POE.SXT at user side is configured as **Client/CPE**.All the administrative rights are given to the admin only.The admin has got the access of all the cloud services, as well it can also limit the access power of any user of cloud.Connected the admin to cloud in the setup.Admin got the control over cloud and is able to see all the users and their ip addresses also on the screen.Finally the user which was brought into real world was able to access the web site on cloud.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

|| Volume 9, Issue 4, April 2020 ||

V.CONCLUSION

The cloud is created in the physical world and the server is installed into it with the help of virtual box.The virtual box is installed on the cloud only.The full functioning firewall is deployed over cloud that is controlled by the admin which can be connected to the cloud and can be disconnected to manage the load.One of the user among many created is realized and it is given a desktop to operate the things.The user can only access the things for which he/she is authorized.Any misconduct created by any user will be alarmed to admin.The admin can take the required actions.Similarly other users can also be taken out in the real world from the virtual world.

REFERENCES

[1] Ala Al Qahtani (Department of computer Science and Engineering) King Saud University, Saudi Arabia, "Impact of VPN's and Firewalls on Public Cloud Performance", [December 2017].

[2] Rajesh Kumar Chakrabarti (Dept. of Computer Science Engineering) Shri Vaishnav Institute of Technology & Science Indore (M.P.), India, "The architectural framework for public cloud security", [May 2014].

[3] Amir R. Khakpour Alex X. LiuDepartment of (Computer Science and Engineering)Michigan State University, " First Step Toward Cloud-Based Firewalling", (IJACSA) International Journal of Advanced Computer Science and Applications, [January 2012]

[4] Caner ILinc, Todd Booth, and Karl Andersson Pervasive and Mobile Computing Laboratory Lulea University of Technology,"WallDroid: Cloud Assisted Virtualized Application Specific Firewalls for the Android OS", IEEE 3rd International Conference on Cloud Computing, [2012].

[5] Wen-Hwa Liao Department of Information Management Tatung University Taipei, Taiwan," A Dynamic VPN Architecture for Private Cloud Computing ",[March 2011].