Performance Evaluation of Dynamic Routing Protocols using Firewall and VPN_Firewall under Cloud Computing

Kimmy
Computer Science Department
CT Institute of Engineering, Management and Technology Jalandhar, India

Shivani Khurana
Computer Science Department
CT Institute of Engineering, Management and Technology Jalandhar, India

ABSTRACT
Cloud Computing is buzzword in market now days. It has been developed to reduce the overall expenses as it provides the on demand services at any time on pay-per-use pattern. Internet is the medium for deploying cloud computing services for users to access the required application and services .It allows the users to access the services which are actually not reside in their own data centers. It provides an efficient and very flexible way for the services, applications to meet business needs. Its infrastructure consist three layers- IAAS, PAAS and SAAS. Cloud computing deploy its services through:- Private, Public and Hybrid Cloud. As the Cloud Computing is still on its initial stage of development and can say in its growing phase, so it suffers from various threats, attacks and vulnerabilities that sometime prevent the user, customers from trusting on it. User's sensitive data resides on Cloud, but due to its lack of security control the confidential data of the clients are comes under the risk of malicious activities or the unauthorized access from illegal users. So it needs an efficient method for ensuring security. In this paper it is recommend to use of Firewalls and VPN_Firewall (virtual private network) in cloud networks for its security. There is a performance evaluation of OSPF, IGRP and EIGRP protocols under two scenarios- with Firewall, and VPN_Firewall.

Keywords
Firewall, VPN, EIGRP, OSPF, IGRP, Cloud Computing.

1.INTRODUCTION
The traditional Computing uses hardware, software and storage resources to getting the desired computational services whereas Cloud Computing has separating the number of applications, services from the underlined hardware and from resources (Networks, Servers, Storage) users, customers are no longer bother to purchase the Hardware, Software, Storages. They have to pay on the consumption basis only [1]. Architecture of Cloud Computing includes – Infrastructure as a service which provides the virtual infrastructure for users to deploy their services. Platform as a service provides the platforms or environments for deploying the application and services and with Software as a service you can access the software online on your desktops without any installation. Before starting the journey to cloud the customers, organizations must keep in mind the various attacks, threats and vulnerabilities which can intrude their confidential data [11]. Cloud Computing Technology is not trustworthy as it can easily effect by the threats and attacks, the data can be loss and misused by unauthorized access. In order to create awareness and to protect the users of cloud from malicious activities there must be an powerful and trustworthy security policies, measures or techniques which can protect or secure the user's data on Cloud. In this paper Firewall and Virtual Private Networks are discussed for the purpose of Security in Cloud Computing. This paper uses three services Database, Remote login and FTP. This paper evaluates the performance of dynamic routing protocols using Firewall, VPN_firewall and discuss some security support services, threats and vulnerabilities of Cloud Computing and also propose a model with two scenario.

1.1 Firewalls
Firewall is a parameter –based an security options. The firewalls just protect and facilitate the networks and by stopping unwanted activities. Firewalls provides an authorization that assures only a specified user who have access right can access the services and applications such as FTP, Web browsing, Remote login [12]. Basically firewall is a specially designed router that sits between the site and the network. Firewall working is to forward all the packets from one network to the other network and filter them according to the requirement [4]. They filter and forward the packets whose addresses are characterize in table. It has additional functionality of encryption for more security. In Cloud Computing if there is an installation of firewalls then it provides number of options for providing security like- can block the attacks, can restrict unauthorized, unauthenticated access to the particular type of service and all. Firewall packet filtering done at network layer of OSI reference model.

1.2 Virtual Private Network
A VPN (Virtual Private Network) provides capability to create a secure network across a public network like Internet through the use of Encryption, IP Tunneling or encapsulation to connect remote sites, networks and users together. VPN provides security and established level of trust over the Public Internet [5]. So VPN plays an important role to provide security in Private Cloud. There are two methods to set up the VPNs - in first method VPNs are installed between network firewalls and the encrypted routers to perform the encrypting and decrypting of the traffic and not require any software on systems. In second method, it needs a VPN server, VPN client and also requires special software. VPN_Firewall makes a tunnel to pass the data in encrypted form or encapsulation form that is securely from it. VPN tunnel using tunneling protocols like L2F, PPTP and L2TP.These protocols generates the encapsulated packet. As PPTP uses RSA algorithm for data encryption and L2TP used 3DES algorithm for data encryption and also uses MD5 for check the integrity of the data.

1.3 Dynamic Routing Protocol
It contains the distance vector routing, link state routing and hybrid routing protocols.

1.3.1 Eigrp
Enhanced Interior Routing Protocol is an enhanced and more powerful version of IGRP. EIGRP is a Cisco proprietary protocol. It can also load balance up to 6 equal/unequal cost links. Dual algorithm works behind EIGRP protocol. Its metric uses Bandwidth, Load, Delay and MTU. Its costs to

determine the best and shortest path is (10^7/Bandwidth * delay/100) * 256. EIGRP uses the concept of A.S (Autonomous system) having range of 1-65535 which is a collection of routers which are managed by a common administration policies [3]. Eigrp is the best protocol among all routing protocols like OSPF, IGRP and RIP. So this paper recommends the Eigrp protocol to be configured in two models given below.

1.3.2 OSPF

Open Shortest Path First Protocol uses the Dijkstra algorithm for its working. It is an open standard protocol can be used by all and also known by the name of shortest path first algorithm. Its metric to determine the best and shortest path is 10^8/bandwidth. It can also perform load balancing up to six equal cost link [2]. In OSPF there is no limitation of size of the network. The concept of areas used in OSPF which means a group of routers comes under a single administration. There is also an election for selecting DR and BDR on broadcast and non-broadcast multi-access networks.

1.3.3 IGRP

Interior Gateway Routing Protocol has been developed by Cisco for large networks. It also counts maximum hops for finding shortest distance. This protocol developed to overcome the problems faced by RIP. IGRP has maximum hop count of 255 and also can performs unequal cost load balancing.

2 THREATS OF CLOUD

While cloud computing services are available and accessible 24*7 through any internet browsing. As it is mostly used technology today but instead of this it also have some threats [8].

2.1 Abuse and nefarious use of Cloud

As the cloud providers provide the various services to their users including unlimited bandwidth, storage capacity and sometimes they offer free trial periods which give an opportunity to the attackers or hackers to waste the bandwidth, storage and access the Cloud for malicious activities.

2.2 Insecure Interfaces and APIs

For accessing the cloud services, users need some software interfaces and API's .So these software interfaces and APIs should be secured properly as they play an important part in communication between Cloud server and Cloud clients.

2.3 Malicious Insider

The malicious insiders are not trustworthy employees at the Cloud provider's end or user's end who can steal the valuable, confidential data by easily cracking passwords, cryptographic keys and files. So the employee's hiring procedures and their granting access, authorization, authentication must be strong enough so that they cannot perform these kinds of activities.

2.4 Virtualized Technology

As the Cloud is all about virtualization, so the customer's data, information and their applications are residing on virtual machines on the servers. As these virtual machines are managed, secure control by the hypervisor because new instance that is guest operating system used in virtual machines are installed on a hypervisor and this hypervisor works as a middleware between virtual machines and the hardware. That's why hypervisors are the main target of the hackers or attackers for performing malicious activities [6].

2.5 Data loss or leakage

The data can be loss due to number of reasons like operational failure, data failures, natural disasters, hardware and communication medium failures and inconsistent use of encryption keys will leads to destruction of confidential data.

3. VULNERABILITIES OF CLOUD

There are number of vulnerabilities that must be considered whenever any organization move their confidential data to a cloud storage. These vulnerabilities are given below [10].

3.1 Data protection and portability

Cloud provider provides services to the clients on the contract basis but whenever the contract tenure terminates and customers don't want to continue then what will happen to the confidential data of customers will it misused or deleted by the provider ? and if the Cloud provider just went out of the business due to any reason then again will the sensitive data of client move to another provider? Will that provider trustable or not?

3.2 Vendor lock In

The customers who taking services from Cloud provider they have to depends upon that particular provider for their services and products. The customers cannot migrate their data and codes to the other cloud provider easily because it is very expensive task in Cloud Computing. So customers are just stuck in their only Cloud provider and it is also called vendor lock in problem which also called as interoperability and portability challenge in Cloud Computing. This problem rises due to the lack of standards.

3.3 Internet dependency

Cloud Computing use the Internet as a medium for providing its services. So this technology totally depends upon the Internet but whenever Internet goes down or slow, then this technology not able to provide its services successfully. So it is totally depends upon the Internet for its services to deploy. As some of Asian, African or other countries which are undeveloped cannot take the full advantage of Cloud Computing technology because they are not receiving the proper bandwidth and speed of Internet services.

3.4 Reliability and Availability of services

If we talk about reliability and availability then Cloud Computing is not an appropriate technology for example in 2008 Amazon S3 that is Amazon Simple Storage Service went down for a long time which is not affordable for the businesses and organizations which causes data loss, network and communication failure and data misuse, so it will stop reaching the services to the legitimate users.

3.5 Session riding and hijacking

The session hijacking refers to hijack the valid session key to get an unauthorized access for the services and information residing on the system and can misuse or destroy the sensitive data of the users. In session riding, the hackers can send the malicious codes, commands to the web pages, applications, web sites, e-mails and some tricky links to the users so that they can visit the specially crafted web sites with fraud and get infected by the malicious activities [9].

4. SIMULATOR USED (OPNET)

OPNET IT Guru Tool is used for implementing the comparison without Firewall, with Firewall and VPN Firewall. OPNET is a GUI (Graphical User Interface) based tool which is easy to use as it has in-built protocols, algorithms, models and networks. Its results are can be plotted in excel spreadsheets. In this paper we used two scenarios which uses application config, profile config, ethernet4_slip_gtwy routers, ip32_Cloud, ppp_servers and ppp_wkstn.

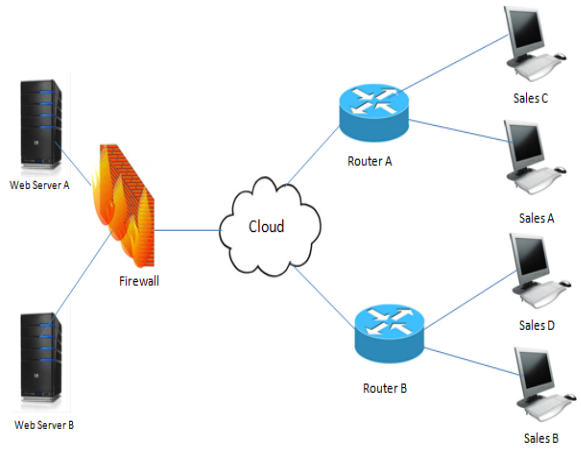

Fig 1: Network with Firewall

In this figure a Firewall router is used to deny some access. In this scenario the database and the remote login services are denied in Firewall configuration so that the sales client A, B, C,D are not able to access the database of the Cloud's server or they can't access the remote login of Cloud servers from the client data centers [7]. But in this network database and remote login is denied by all clients as if some trustable organizations want to access even they can't able to get the services. So this is the limitation of firewall scenario that it will filter or block the required services for all users.

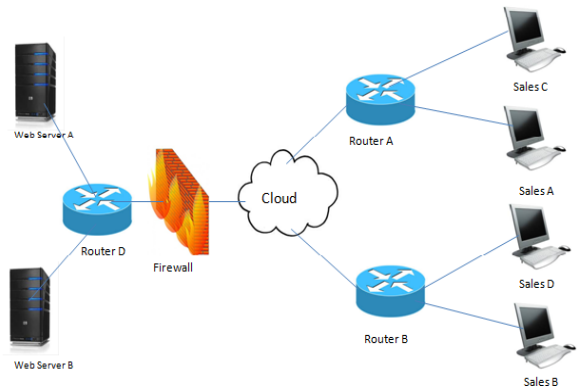

Fig 2: Network with VPN_Firewall

In this figure a VPN Firewall is installed which uses the concept of IP tunneling the tunnel is generated from router A to router D in this scenario .As we want that sales clients A and C can access the database and remote login, that's why there is a need of IP tunneling to encapsulate the packets [6]. Now in this scenario sales client D and B can't access the database and the remote login access, because there is no tunnel between router B to router D. So difference between the only Firewall and VPN Firewall is Firewall block or filter the services for all users, but VPN Firewall can block some required users or allow some required users also [7].

5. RESULTS AND DISCUSSIONS

There is a comparison with firewall network and VPN firewall. Results are taken under the FTP, DB Query and Remote login services under IGRP, OSPF and EIGRP protocol and the following results will evaluate that which protocol gives better result and under which scenario.

Case1. Performance evaluation of IGRP, OSPF and EIGRP in terms of point to point link utilization, point-to-point queuing delay, router CPU utilization , server CPU utilization , server load and FTP traffic sent, client DB traffic sent and remote login traffic sent under VPN_Firewall scenario.

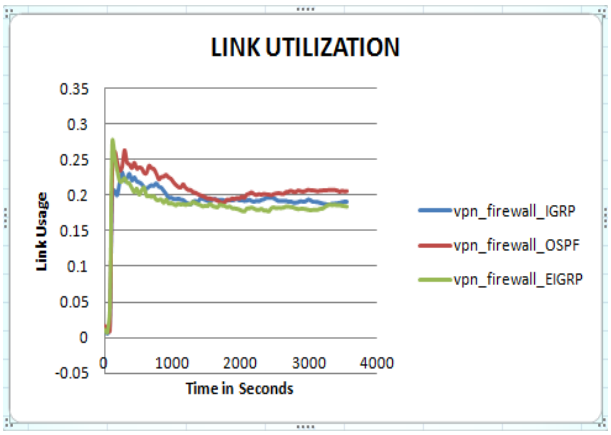

Fig 3: Point to point link utilization for a VPN_Firewall.

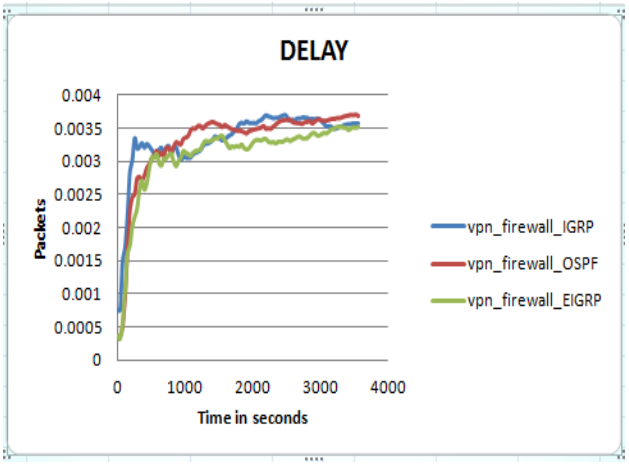

Fig 4: Point to point link queing delay for a VPN_Firewall.

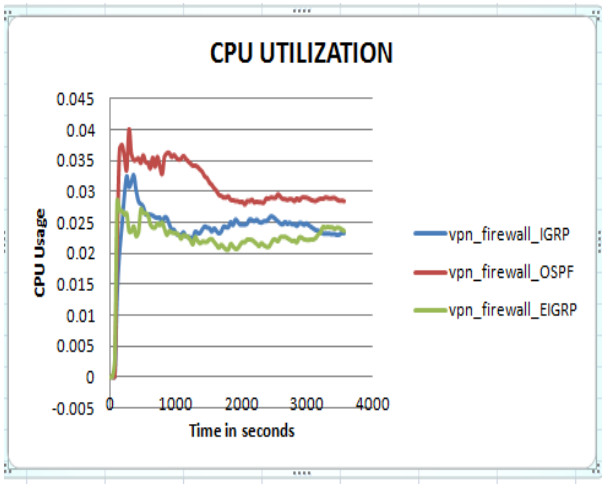

Fig 5: Server cpu utilization for a VPN_Firewall.

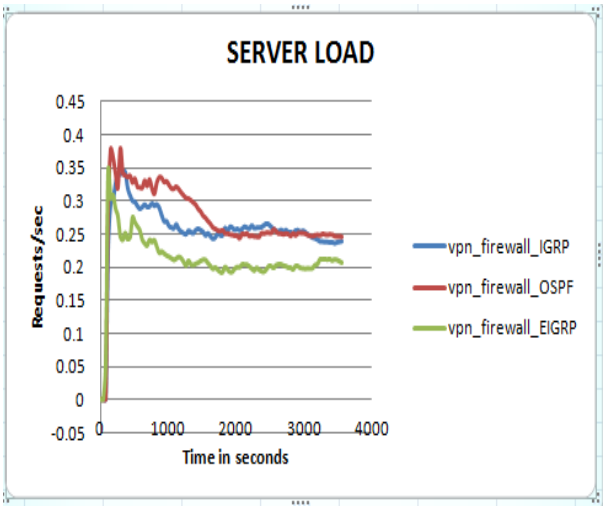

Fig 6: Server performance load for a VPN_Firewall.

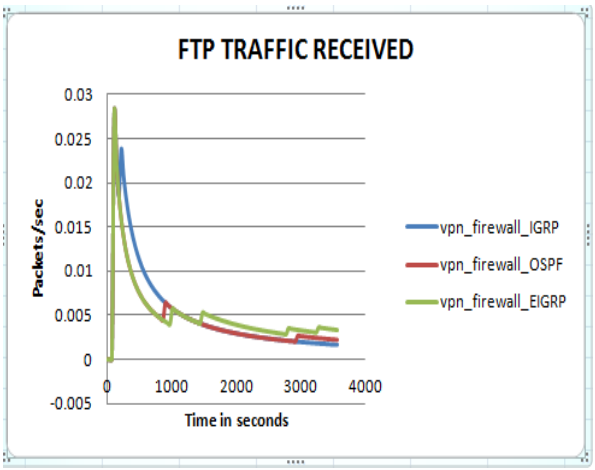

Fig7: Ftp traffic sent for a VPN_Firewall

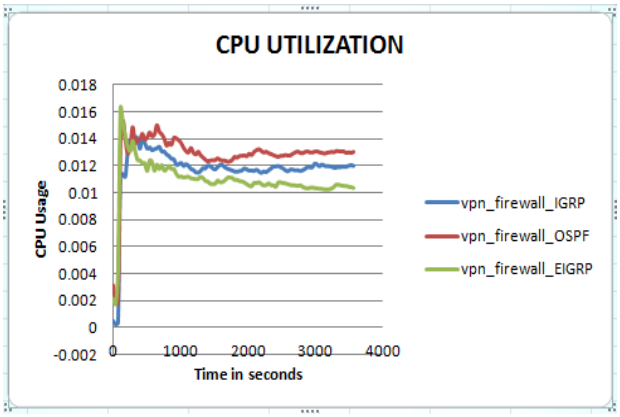

Fig 8: Router CPU utilization for a VPN_Firewall.

Case2. Performance evaluation of IGRP, OSPF and EIGRP in terms of point to point link utilization, point-to-point queuing delay, router CPU utilization , server CPU utilization , server load and FTP traffic sent, client DB traffic sent and remote login traffic sent under Firewall scenario.

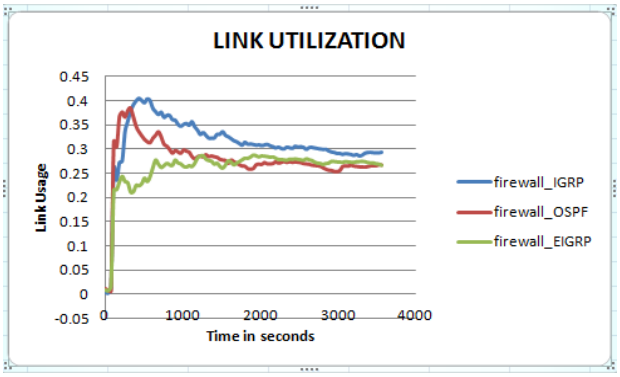

Fig 9: Point to point link utilization for a Firewall scenario.

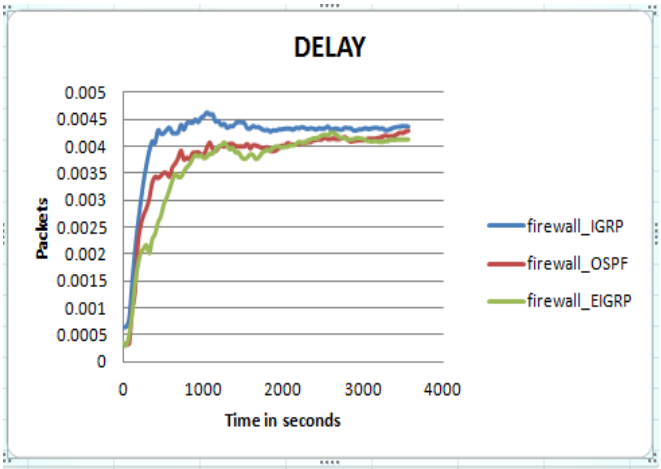

Fig 10: Point to point link queing delay for a Firewall scenario.

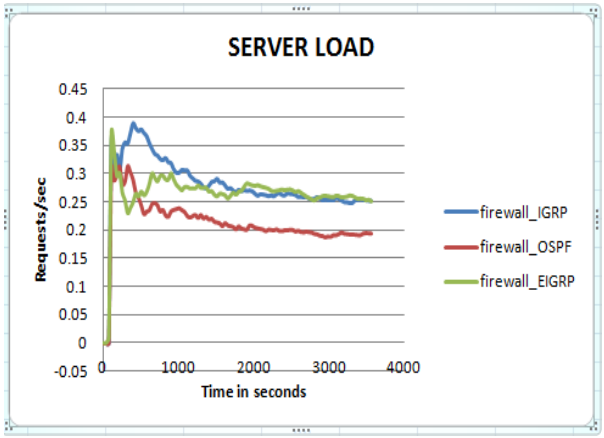

Fig 11: Server performance load for a Firewall scenario.

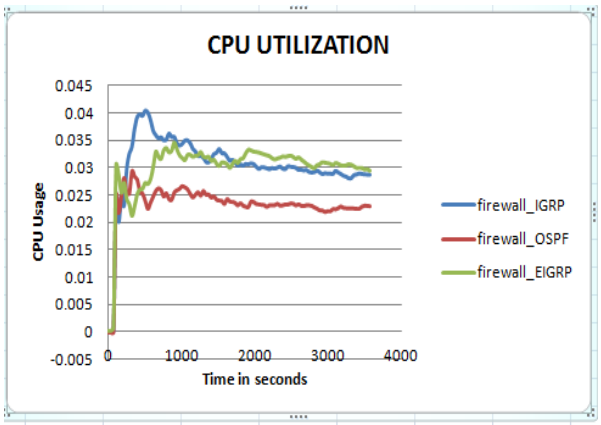

Fig 12:Server cpu utilization for a Firewall scenario.

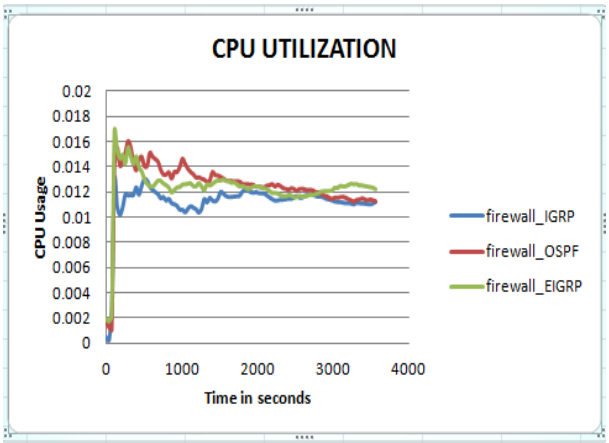

Fig 13. Router CPU utilization for a Firewall scenario.

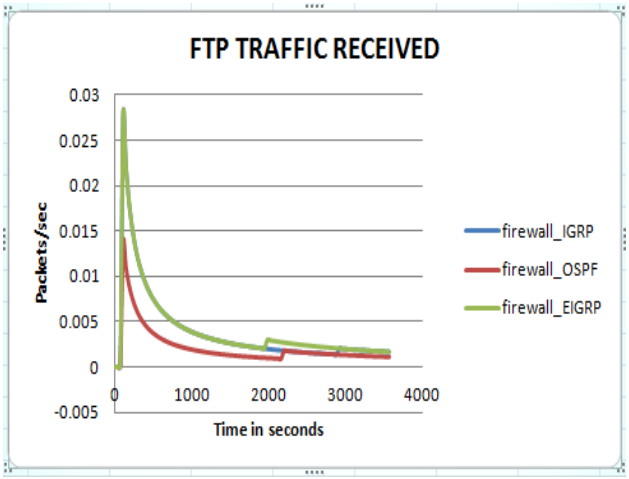

Fig 14: Ftp traffic sent for a VPN_Firewall

6. CONCLUSION

As Cloud Computing is one of the competing technology in current trends and Business are totally depends upon this newly coming technology. So it needs to be secure enough so that the customers, organizations data would not be suffered for data loss and malicious activities. But Cloud Computing is suffering from the security issues as security is the major challenge of Cloud Computing which somewhere hampers the success of this technology. So this paper discussed the proposed method for the improvement of security challenge. The proposed method consists two scenarios the first scenario is with Firewall, Second scenario use VPN Firewall. From the above results, it is proved that the network having VPN_Firewall is more secure as it has less point-to-point link utilization, less delay, less router and server CPU's utilizations and less load on server and the other reason is that VPN_Firewall uses a secure tunnel to pass the confidential data from it through the insecure internet medium and give better results than the only firewall scenario under the EIGRP protocol.

7. REFERENCES

[1] GianlorenzoD'Angelo, et al. - "A loop-free shortest-path routing algorithm for dynamic networks" Elsevier Science

[2] Kiavash Mirzahossein et al.- **"**Analysis of RIP, OSPF, and EIGRP Routing Protocols using OPNET" Springer 2013.

[3] Edward G. Amoroso "from the enterprise perimeter to a mobility-enabled secure cloud**"** Copublished by the IEEE Computer and Reliability Societies 2013Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] Matthew Green,"The Threat in the Cloud**"** Copublished by the IEEE Computer and Reliability Societies 2013

[5] Stanik, Alexander ; Bittner, Patrick ; Byfield, Marvin ; Sander, Fridtjof ; Schoder, Daniel "Local authentication and authorization system for immediate setup of cloud environments" 2013International Conference Advances in Computing, Communications and Informatics (ICACCI)

[6] Li, L.E. ; Liaghat, V. ; Hongze Zhao ; Hajiaghay, M. Dan Li ; Wilfong, G. ; Yang, Y.R. ; Chuanxiong Guo "PACE:

Policy-Aware Application Cloud Embedding" INFOCOM, 2013 Proceedings IEEE.

[7] Khalil, Issa M. ; Khreishah, Abdallah ; Bouktif, Salah ; Ahmad, Azeem "Security Concerns in Cloud Computing" (ITNG) 2013

[8] Masqueen Babu "Performance Analysis of IPSec VPN over VoIP Networks Using OPNET" International Journal of Advanced Research in Computer Science and Software Engineering" 2012

[9] Aruna Malik, Harsh K Verma, Raju Pal "Impact of Firewall and VPN for securing WLAN" International Journal of Advanced Research in Computer Science and Software Engineering 2012.

[10] Nagaraju Kilari, Dr. R. Sridaran, " A Survey on Security Threats for Cloud Computing" International Journal of Engineering Research & Technology sep 2012

[11] R. Kalaichelvi Chandrahasan, S Shanmuga Priya and Dr. L. Arockiam "Research Challenges and Security Issues in Cloud Computing" International Journal of International Journal of Computational Intelligence and Information Security, March 2012.

[12] Mervat Adib Bamiah, Sarfraz Nawaz Brohi "Seven Deadly Threats and Vulnerabilities in Cloud Computing" international journal of advanced engineering sciences and technologies 2011.