ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Cloud Computing Security with VPN

M. Judith Bellar

Dept. of Computer Science and IT, Kodaikanal Christian College, Kodaikanal, India

Abstract: Cloud Storage is a service where data is remotely maintained, managed, and backed up. The service is available to users over a network, which is usually the internet. It allows the user to store files online so that the user can access them from any location via the internet. The provider company makes them available to the user online by keeping the uploaded files on an external server. As the cloud provides many features it has some drawbacks too. However, while the features are useful for providing basic computation and storage resources, they fail to provide the security and that many customers would like. Security is a top concern among organizations evaluating cloud service providers. While most service providers allow customers to implement their own security measures, few of them have comprehensive security tools to offer their customers. Among these tools, one of the most important to customers and service providers alike is the ability to securely interconnect physical and virtual datacenters with virtual private networks (VPNs). This paper describes how secure connectivity to public cloud networks with VPN.

Keywords: Cloud Computing, VPN, Security, Firewall, Tunneling.

I. INTRODUCTION

Cloud computing has generated a lot of interest and competition. This is due to service delivery model which provides that involves computing and storage for users in all market including financial, health care and government. These advances in computing put cloud computing as one of the latest developments of computing models. Its development can be considered much advanced than that of distributed computing, parallel processing and grid computing and so on. With cloud computing, multi-level virtualization and abstraction can be achieved. This can validated using an effective integration of variety of computing, storage, data, applications and other resources. This integration will allow users to easily use powerful computing and the storage capacity of cloud computing. It will also allow the use of networking as that achieved in distributed processing or grid computing. However, wireless networks have the same risks and vulnerabilities that exist in a conventional wired network and there are also numerous other types of threats specific to them. Therefore, cloud security that use wireless network is becoming a key differentiator and competitive edge between cloud providers. This paper introduces security issues for the cloud and presents firewall implementation with VPN (Virtual Private Network) technology to provide security to the network.

II. SECURITY ISSUES FOR CLOUD COMPUTING

Google and other well known computing resources have entered the cloud computing field. This adoption will increase heavily because of the high demand on computing resources in search engine or data warehouses and data mining. This demand comes from the large increase in computing and multimedia in everyday activities. However, cloud computing users should be aware of security threats that can occur because cloud computing uses networks to grant access to the resources required.

Thus any security threats that might occur with network might occur with cloud computing. Furthermore, the security of cloud computing should consider security issues and technologies related the entire field. This encompasses the entire cloud computing infrastructure. These include but are not limited to networks, databases, operating systems, virtualization, resource scheduling, transaction management and load balancing and concurrency control and memory management. One of the major problems facing cloud computing security is the resource allocation and scheduling control by the data owner. Thus a form of security authority needs to be deployed by cloud computing security to provide the owner the control required. The seeker should be aware of the allocation and scheduling required. This is called an authority coordinator and its presence is essential to secure the data in the yet to be proven secure environment such as cloud computing. Within these security aspects, the security concerns can be categorized as:

Traditional security: These concerns involve computer and network intrusions or attacks on clouds.

Availability: These forms of security concerns will centre on critical applications and data being available. Availability concerns can extend to migrate to another provider, uptime periods of current provider or long-term viability of the cloud provider.

Third-party data control: Within cloud computing, there is a third party that holds data and applications. This part is very complex, transparent and need to be understood very well by cloud computing users.

Data Security: This security concern will provide the physical and logical control of data. It is concerned with virtualization, vulnerabilities attack, phishing scams and other potential data breaches such as data leakage and interception, economic and distributed denial of service and loss of encryption keys.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Privacy and Legal Issues: This issue is essential especially when dealing with globally distributed network.

III. VPN

VPN (Virtual Private Network) technology provides a way of protecting information being transmitted over the Internet, by allowing users to establish a virtual private "tunnel" to securely enter an internal network, accessing resources, data and communications via an insecure network such as the Internet.

VPN (Virtual Private Network) is a generic term used to describe a communication network that uses any combination of technologies to secure a connection tunneled through an otherwise unsecured or distrusted network. Instead of using a dedicated connection, such as a leased line, a "virtual" connection is made between geographically dispersed users and networks over a shared or public network, like the Internet. Data is transmitted as if it were passing through private connections. VPN transmits data by means of tunneling. Before a packet is transmitted, it is encapsulated (wrapped) in a new packet, with a new header. This header provides routing information so that it can traverse a shared or public network, before it reaches its tunnel endpoint. This logical path that the encapsulated packets travel through is called a tunnel. When each packet reaches the tunnel endpoint, it is "decapsulated" and forwarded to its final destination. Both tunnel endpoints need to support the same tunneling protocol. Tunneling protocols are operated at either the OSI (Open System Interconnection) layer two (data-link layer), or layer three (network layer). The most commonly used tunneling protocols are IPSec, L2TP, PPTP and SSL. A packet with a private non-routable IP address can be sent inside a packet with globally unique IP address, thereby extending a private network over the Internet.

A. VPN Security

VPN uses encryption to provide data confidentiality. Once connected, the VPN makes use of the tunneling mechanism described above to encapsulate encrypted data into a secure tunnel, with openly read headers that can cross a public network. Packets passed over a public network in this way are unreadable without proper decryption keys, thus ensuring that data is not disclosed or changed in any way during transmission. VPN can also provide a data integrity check. This is typically performed using a message digest to ensure that the data has not been tampered with during transmission. By default, VPN does not provide or enforce strong user authentication. Users can enter a simple username and password to gain access to an internal private network from home or via other insecure networks. Nevertheless, VPN does support add-on authentication mechanisms, such as smart cards, tokens and RADIUS.

IV. PROPOSED CLOUD COMPUTING SECURITY USING VPN

The proposed system will attempt to provide secure delivery of data to and from the cloud. One of the adopted technologies is the Virtual Private Network (VPN). With VPN private and secured sub networks can be constructed. This principle has been widely applied in wired local-area network (LAN), remote access networks and can be also applied to wireless local-area network (WLAN). This will replace Wired Equivalent Privacy (WEP) solutions. It adopts standard encryption algorithms to ensure the security of data transmission. Furthermore, VPN usually implemented with the aid of IP security (IPSec). This can be considered as the standard way for VPN implementation. The IPSec and VPN have revised and well established in this way to provide the robust security standard with acceptable data confidentiality, authentication, and access control regardless of the transmission medium. "By integrating wireless LANs into an IPSec infrastructure, allows WLAN infrastructure to focus on simply transmitting wireless traffic, while the VPN would secure it."

A. Network simulation scenarios

The simulation procedure using of OPNET simulator adopted in this research consists of number scenarios which study the performance of the system in different cases. The cloud computing has been modeled with and without VPN to study the performance of VPN and to study the effect of firewall with VPN in the system to secure cloud in different scenarios. Each scenario has been subjected to three applications types (File Transfer (FTP), web browsing (HTTP) and Email applications). In the simulation, two servers represented two departments have been assumed. The impact of firewall and VPN on cloud computing has been investigated in terms of throughput, load, delay, and traffic received. Further parameters used in these scenarios are:

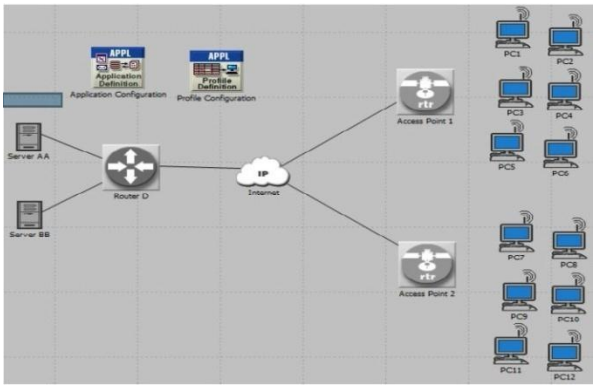
I- Two access points: named (wireless_ethernet_slip4_router), which had two Ethernet interface and 4 serial line.
II- No. of workstations: named (wlan_wkstn) which represent clients that communicate with internet.
III- Two IP router: named (ethernet4_slip8_gtwy), which represent router with 4 Ethernet interface and 8 serial line interface. ip cloud: named (ip 32 clouds) which represents the Internet
IV- Two servers: named (PPP Server) which represents point to point server to represent two departments.
v- Firewall: ethernet2_slip8_firewall, which prevents any access for the required application to the server.
VI- VPN configuration: VPN tunnel would be used to allow specific clients from the source to access specified application from the server.
Links: named (PPP-DS1) to connect the parameters used for the modeled system. Profile and application configuration defines the application of the system.

B. Cloud computing without VPN

In this scenario, the number of workstations connected to two access points (Access Point 1, Access Point 2) which are configured two BSS.

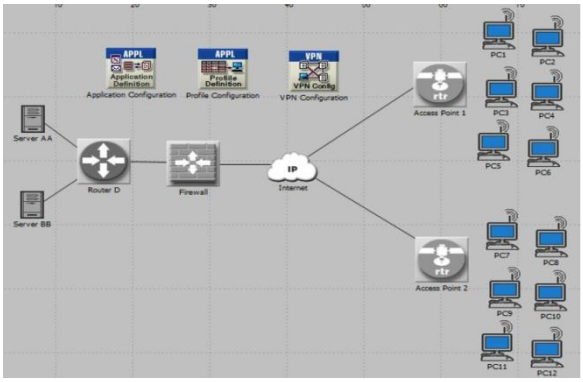
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015



These access points are connected by PPP-DS1 to Router S connected by PPP-DS1 to IP cloud (Internet) connected by PPP-DS1 to Router D connected by PPP-DS1 to two Servers (Server AA, Server BB) which represents two departments.

C. Cloud computing with firewall and VPN



In this scenario, number of workstations connected to two access points (Access Point 1, Access Point 2) which configured two BSS. These access points connected by PPP-DS1 to Router S connected by PPP-DS1 to IP cloud (Internet) connected by PPP-DS1 to Firewall to Router D connected by PPP-DS1 to the Server. In the previous scenario, firewall was used to prevent any external access to email of server regardless the source of the traffic. In this scenario, the VPN tunnel would be used to allow one of the clients (PCs) from Access Point1 to access Email from the server AA. The firewall will not filter the traffic created by Access Point1 because the IP packets in the tunnel will be encapsulated inside an IP datagram.

V. EXAMPLE: JUNIPER NETWORKS

This model demonstrates how secure connectivity to public cloud networks provided by the service provider can address the security, performance, and reliability needs of enterprise customers as they deploy large-scale cloud services. Juniper Networks, as an industry networking leader, offers enhanced and open standards-based SDN and Network Function Virtualization (NFV) solutions to meet the networking service needs of the service provider, the public cloud provider, and the enterprise business.

Over the last few years, the hybrid/public cloud computing model has gained increased acceptance in the enterprise business community as a means to provide quick, low-cost, and scalable services. The availability of SaaS, PaaS, IaaS, and many other variant services from the cloud offers flexible choices that meet varying business needs. The key driver for cloud adoption is the ability to provide "always-on access to applications" with increased application availability at a large scale, in a quick and secure fashion, and at an overall reduced cost.

Enterprise IT owners worldwide use VPNs to meet the connectivity needs of their businesses with security, performance and availability. As these enterprise owners look to deploy cloud-based solutions more extensively, they expect a similar experience; in essence, they are looking for enterprise-grade network services when connecting to the public cloud. However, many businesses connect to public cloud providers over the Internet. Recent industry research indicates that security, reliability, low latency, and predictable performance are priorities for enterprise business owners as they build private clouds or deploy a hybrid cloud model.

Service providers have an opportunity to address some of the service gaps that exist in the public cloud services chain today. Services that extend the performance metrics of their VPN, offering to provide connectivity to the hybrid/public cloud infrastructure, are desperately needed by performance-conscious enterprise organizations. Consequently, service providers are looking at ways to define and deliver managed services in this new agile and open, multivendor services driven-market. On the technology side there are several innovative solutions surfacing on the market to meet the virtualized, on-demand availability and growth needs of the enterprise. As the demand grows for open and agile solutions on a large scale, virtualizing the network, storage and computing resources in an integrated fashion have become a critical need. Today's network architecture experts are stepping up to integrate increased virtualization in an effort to improve the time to market for service delivery in a dynamic and automated environment.

This model reviews how service providers can leverage their deployed physical architecture with Juniper and seamlessly integrate virtual solutions with SDN and service chaining with NFV as they apply to offering a secure cloud interconnect service over a VPN and support the enterprise's IT needs with a hybrid cloud model.

Today, service providers have the opportunity to insert themselves into the cloud services chain and evolve their network architecture to support the agility and distributed scalability of cost-conscious enterprise business customers. Juniper Networks is at the forefront of providing leading-edge, simple, agile, and open standards-based scalable solutions to meet the critical needs of today's enterprise. Juniper's solution is designed to help its customers create revenue by offering scalable systems and enabling network processes automation using open, standards-based network protocols. With Juniper's SDN framework and proven routing and security portfolio,

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

service providers can seamlessly support the needs of physical and virtual solutions for years to come.

VI. CONCLUSIONS

This study introduces VPN technology for securing cloud in wireless network. OPNET Modeler simulator was used as a simulation tools to investigate the impact of VPN and firewall security systems on throughput, delay and traffic received on the system and individual nodes of the network. The applications considered for the mentioned investigation are e-mail application and web browsing application. The followings can be made:

I- The integration of VPN with Firewall in cloud computing will reduce the throughput. This is because the number of bits transmitted per second is less than the cloud computing without VPN. This is because the VPN with firewall would not allow every access to the server. Furthermore, the delay in system without VPN is slightly larger than the cloud computing with VPN.
II- No traffic received and sent from server AA for e-mail application in cloud computing with firewall and no VPN. This is because the firewall would prevent any email access to the server AA and the existence of VPN in the system would allow specified stations (PC's) to access server AA. However, there would be no traffic received and sent for server BB in (VPN firewall) and (firewall no VPN) systems. This is now because VPN acts as a tunnel to allow email access to server AA only.
III- In web browsing applications, there would be traffic sent and received in the case of cloud computing with VPN and without VPN. This is because the VPN firewall would prevent only access to the server for email application but not web applications. VPN technology is a suitable way to secure cloud computing and decreasing the traffic in the system to achieve the desired level of security. The security was provided in VPN technology should be provided with firewall that allows only specific access to the server.

REFERENCES

[1] Maneesha Sharma, Himani Bansal, Amit Kumar Sharma, "Cloud Computing: Different Approach & Security Challenge", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231- 2307, Volume-2, Issue-1, pp. 421-424, March 2012.
[2] Young B. Choi, Jeffrey Muller, Christopher V. Kopek and Jennifer M. Makarsky "Corporate wireless LAN security: threats and an effective security assessment framework for wireless information assurance", Int. J. Mobile Communications, Vol. 4, No. 3, pp 266 – 290, 2006.
[3] Songjie, Junfeng Yao, Chengpeng Wu, "Cloud computing and its key techniques", International Conference on Electronic & Mechanical Engineering and Information Technology, pp. 320-324, 12- 14 August, 2011.
[4] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan and Bhavani Thuraisingham, "Security Issues for Cloud Computing", International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010.
[5] Richard Chow, Philippe Golle, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", CCSW'09, November 13, 2009, Chicago, Illinois, USA. , ACM 978-1-60558-784-4/09/11, pp. 85-90, 2009.
[6] Aderemi A. Atayero, Oluwaseyi Feyisetan, "Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption", Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 10, pp. 546-552, October 2011.
[7] Weili Huang, Fanzheng Kong , "The research of VPN on WLAN" , International Conference on Computational and Information Sciences, 2010 IEEE, PP 250 – 253.
[8] H. Bourdoucen, A. Al Naamany and A. Al Kalbani, "Impact of Implementing VPN to Secure Wireless LAN", World Academy of Science, Engineering and Technology 51, pp 625 – 630, 2009.
[9] Charlie Scott, Paul Wolfe, Mike Erwin, "Virtual Private Networks, Second Edition", O'Reilly, Second Edition January pp 12, 1999.
[10] www.opencontrail.org IDG survey report (70% of respondents say the number one barrier to deploying cloud solutions is security concern.)
[11] http://www.idgenterprise.com/report/idg- enterprises-cloud-computing Infonetics research: Operators reveal where in their networks they plan to deploy SDN first.
[12] http://www.infonetics.com/pr/2013/SDN-and-NFV-Survey-Highlights.asp.

BIOGRAPHY

Judith Bellar is an Assistant Professor in department of Computer Science and Information Technology of Kodaikanal Christian College, Kodaikanal, Tamilnadu, India and is in teaching profession for about 2 years. She completed his masters in Computer Applications in year 2012 from Bharathidasan University, Tamilnadu, India and received his bachelors of Information Technology from SCSVMV University, Tamilnadu, India in 2010. Her areas of specialization are Programming Languages, Cloud Computing and Mobile Computing.