IOP Conf. Series: Materials Science and Engineering **732** (2020) 012081 doi:10.1088/1757-899X/732/1/012081

Performance analysis of Proxmox VE firewall for network security in cloud computing server implementation

Y Ariyanto*, B Harijanto, V A H Firdaus and S N Arief

Information Technology Department, State Polytechnic of Malang, Malang, Indonesia

*yuri@polinema.ac.id

Abstract. Virtualization server uses the hypervisor technology in its implementation. Hypervisor is one of the virtualization techniques. Where this technique runs several operating systems together in one host. Cloud computing is a combination of the use of internet-based computer technology. The Open source Proxmox VE (Virtual Environment) is a virtual machine operating system. Where virtual machines are built from the Debian Linux operating system, with the modified RHEL kernel. A firewall is a system designed to prevent attacks on the network. Firewalls can be software or hardware that filters network traffic. Proxmox VE Firewall provides a way to protect network infrastructure. In Proxmox VE firewall allows setting rules for all hosts in a cluster or for virtual machines. In this study, the performance of the firewall from the server virtualization using ProxmoxVE will be examined. This study is intended to determine the performance of the firewall default from Proxmox VE. Firewall testing is done by creating filtering rules in the Proxmox VE cloud server. The results of this study will provide an analysis of the performance of the Proxmox VE firewall that runs on cloud servers. The analysis presents that iptables firewall rules can be applied to cloud servers.

1. Introduction

Cloud computing has given a new standard in the process of computing where resources are easily virtualized and provides services that can be accessed in real time easily anywhere via a computer network [1]. So that makes cloud computing can have a big impact on progress and innovation in the IT industry [2]. In addition, the resources needed can be in accordance with user requests. Cloud computing is also a new computing paradigm where the Internet is used to connect to network service providers [3]. Cloud computing provides three main services: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Furthermore, cloud providers implement various types of cloud models, such as public cloud, private cloud and hybrid cloud. Figure 1 based on the NIST standard illustrates various services and models in cloud computing.

In cloud computing technology the end user does not need to know the physical location of services and data. Cloud computing deals with computing, storage, software, and data access. Cloud computing removes computing and data from end users and organizations [4]. The main benefits offered by cloud computing to tenants are cost reduction and increased scalability.

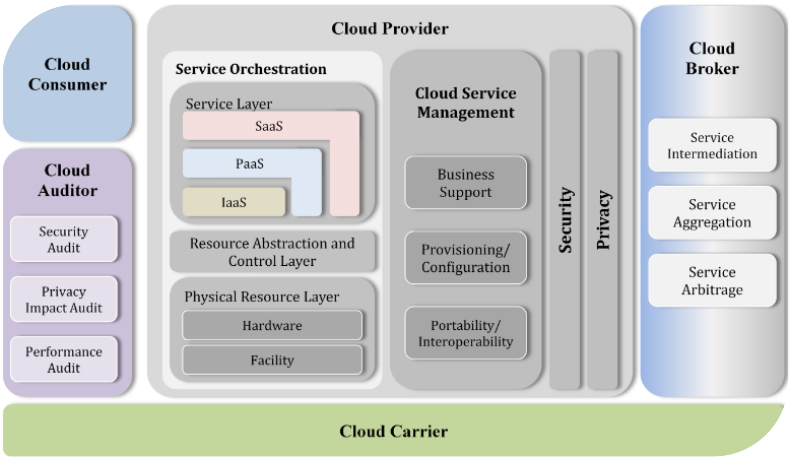

Figure 1. NIST based cloud computing model.

Virtualization applications are widely used in cloud computing. Through Xen and KVM, Lucas Nussbaum [5] built a High Performance Computing (HPC) cluster. At in the data center of BMW Group, virtualization helps reduce electricity consumption by up to 70%. One of the virtualization technologies used in this study is hypervisor technology to provide efficiency in the use of resources by cloud computing.

While cloud computing provides many potential benefits for its users, it also introduces new security threats. With the popularity of Cloud Computing, Cloud security is becoming a vital problem in the Cloud computing domain. The main reason behind this potential security problem is that data and information are now taken from the company. Implementing special security controls for cloud storage is now very important. Typically, any threat that has been faced in a physical data center will be present in a cloud-based data center, but with the added complexity of the long-distance link between the two, plus the lack of ownership and direct control.

The need for cloud security can be overcome by deploying a new layer of protection through virtual security devices, which can facilitate the user's environment to utilize application visibility through user awareness to manage traffic and bandwidth intelligently. And Firewalls play an important role in network security, especially for secure cloud computing servers. Cloud-based virtual firewalls can meet a number of security requirements in the Cloud, including: Secure Data Center, Secure Remote Access, Identity, Management.

The overall cloud-based firewall implementation environment is different from the classic in-house version. Compared to conventional firewalls, cloud-based firewalls can offer several additional features such as scalability, availability, and extensibility [6-8]. However, firewall policies are confidential and can be used to find security holes by attackers, so companies don't want to disclose their firewall policies to the cloud because they don't fully trust the cloud. In short, the challenge here is to apply a firewall to the cloud without affecting the performance of the cloud server.

In this study we implemented a cloud-based virtual firewall using proxmoxVE. In particular, the result of new threats that develop against cloud storage so that it requires a firewall system placed on the cloud. However, the addition of these makes the performance of the cloud tends to be slow. So it is necessary to conduct a performance analysis of cloud computing servers that consider the need to implement a virtual firewall using proxmoxVE.

2. Methods

In this paper we use Top Down Approach using Network Development Life Cycle (NDLC), figure 2, for analysis and design methods. The design of Cloud Server based firewall aims to improve the security side of the network and data security on the cloud server. The Network Development Life Cycle (NDLC)

stage consists of five stages, which include: a) Analysis, analyzing the need to conduct research, existing problems and network topology needs; b) Design, design of cloud server based firewall network topology using proxmoxVE as in figure 3; c) Prototype simulation, we simulated to ensure the concept is working well before deployment stage; d) Implementation; deploy the design to the real server device and also we do next step e) Monitoring, for testing and analysis of the performance of cloud-based firewalls. The last step e) Management, do maintenance systems that have been built to run according to the design concept and can be maintained related to the element of reliability and reliability of the system.

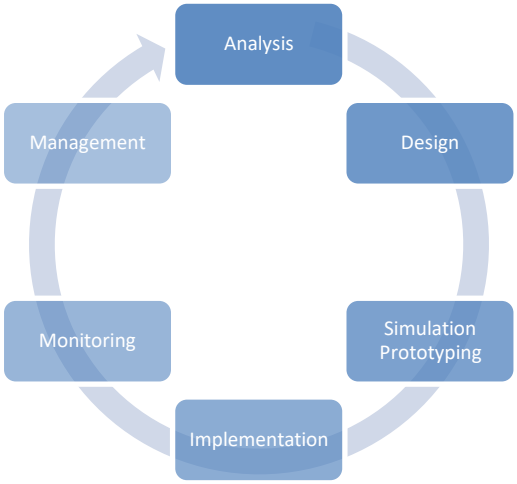

Figure 2. Network Development Life Cycle (NDLC).

Cloud computing using a virtual firewall on ProxmoxVE can provide increased security against potential threats to data and networks on cloud servers. At this stage we will explain the processes and methods to protect the cloud with a virtual firewall on proxmoxVE. In this paper, we design includes conceptual design and architectural design. Conceptual design includes some basic ideas about how to overcome the challenges / threats of attacks on the side of a computer network and the existence of system failures and communication failures. While the architecture design includes architectural aspects in integrating the network into the existing Cloud Server service architecture. With this design, it is expected to ward off the threat of attack and can provide solutions and solutions to the problems of network security. Common network security challenges are: Eavesdropping and Denial of Service Attacks.

Eavesdropping is an attack by intercepting and reading messages by unwanted recipients [9]. Here, we present a more complex solution to counteract and support the sending of data against the threat of wiretapping with protocols that use encryption algorithms for valid and solid security. Denial of Service Attacks, Because the system by default can only accept new messages as a whole, except for a single start. To use up system resources, attackers who carry out DOS attacks, can take advantage of the first message feature. He continued to send the first message that was intercepted to the server. The message is attached with the essence of the combination of the original IP address, the key, and the message itself. It is not possible for an attacker to change the message to look like a new request message, without violating integrity [10].

The next stage is the design of the cloud architecture system that will be made, the design of the architectur design is shown in Figure 3.

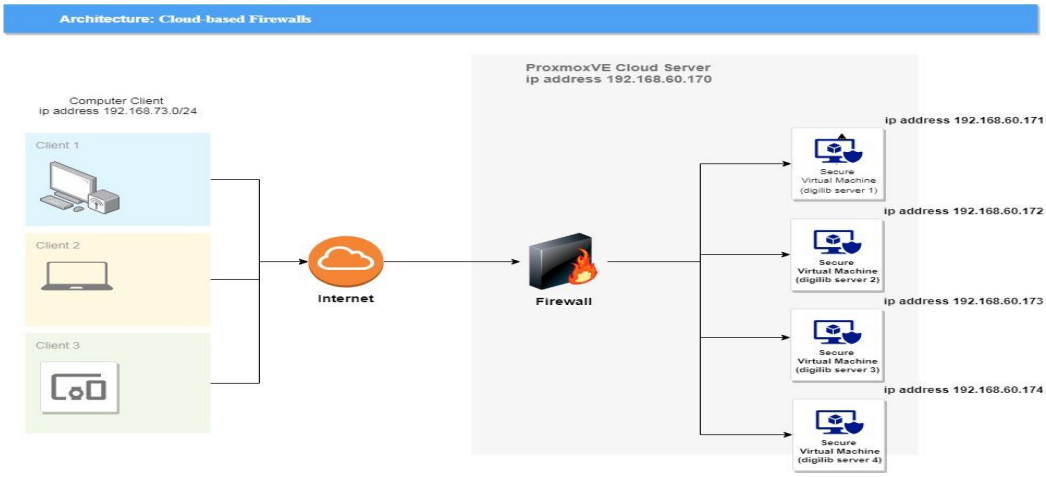

Figure 3. The architecture design.

The architecture design will be created using proxmoxVE, the firewall feature in Proxmox is a stateful firewall. A stateful firewall is not just a data packet filter, but it also keeps a constant track of the state of active network connections, such as TCP or UDP protocols. It is also known as dynamic packet filtering, which matches firewall rules with the nature of active connections, providing better protection than simply filtering packets. We set up a firewall for an entire cluster level, specific node levels, and also for each VM. For the firewall configuration rules, we setting the firewall rules to secure the cloud server. Through rules, we can define the flow of traffic and the type of traffic that will be allowed or dropped. The firewall configuration rules are shown in table 1 as well.

Table 1. Rule firewall data center.

No	Rule Firewall
1	iptables –t filter –A INPUT –p tcp –m multiport --dport 21,22 –s 192.168.60.171,192.168.60.172,192.168.60.173,192.168.60.174 –j DROP
2	iptables –A INPUT –p tcp –m multiport --dport 21,22 –s 192.168.73.0/24 –j DROP
3	iptables –A INPUT –p ICMP –s 192.168.73.0/24 –j DROP

3. Results and discussion

Testing on a cloud server system, carried out to get the results of research. Testing the cloud server system by applying firewall rules that have been made. The implementation of Proxmox cloud server architecture design is shown in figure 4.

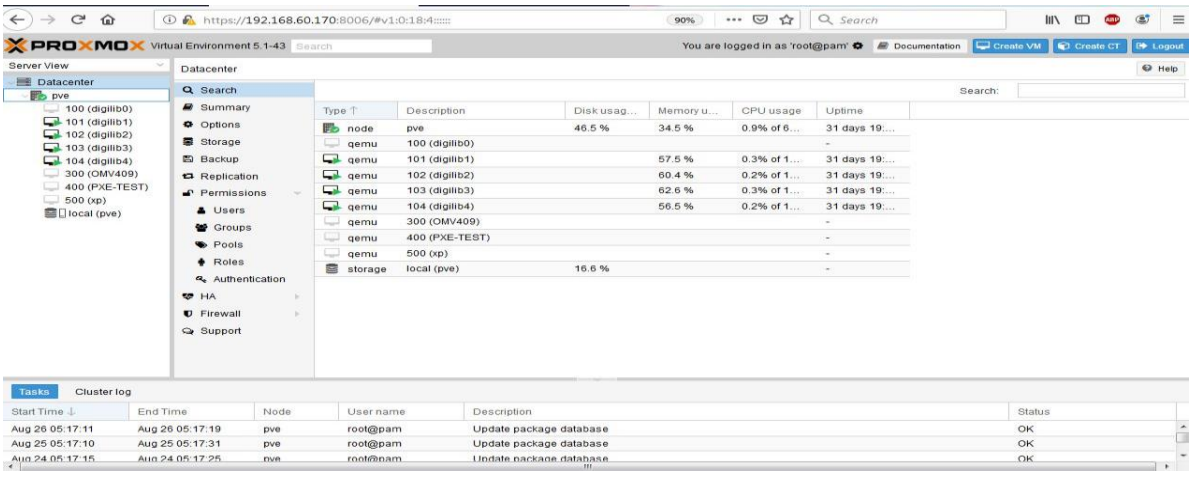

Figure 4. Implementation ProxmoxVE.

The implementation of the DataCenter firewall rules on the Proxmox cloud server is shown in the figure 5.

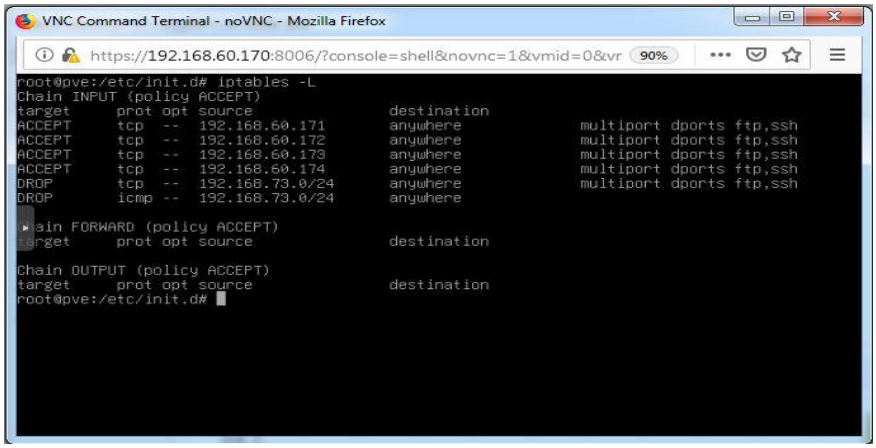

Figure 5. Implementation rule firewall datacenter.

In figure 5, the firewall rules shown in the datacenter are shown. Firewall rules line 1 to 4, allow server 1 to server 4 to enter and access the datacenter using the SSH and FTP protocols. Then the firewall rules lines 5 through 6, do not allow computers with IP addresses outside the cloud server network to access the SSH, FTP and ICMP protocols.

The results and performance analysis of the ProxmoxVE firewall are based on testing the firewall rules in table 1. The results and analysis are shown in table 2.

Table 2. Performance analysis ProxmoxVE firewall.

No	Computer	Ip Address	Protocol	Status
1	Digilib server 1	192.168.60.171	SSH, FTP	Running
2	Digilib server 2	192.168.60.172	SSH, FTP	Running
3	Digilib server 3	192.168.60.173	SSH, FTP	Running
4	Digilib server 4	192.168.60.173	SSH, FTP	Running
5	Client	192.168.73.0/24	SSH,FTP	Closed
6	Client	192.168.73.0/24	ICMP	Closed

Application of firewall rules on the ProxmoxVE cloud server has no effect on the performance of memory and CPU usage on virtual computers. The performance of memory and CPU usage on the ProxmoxVE cloud server is shown in the figure 6.

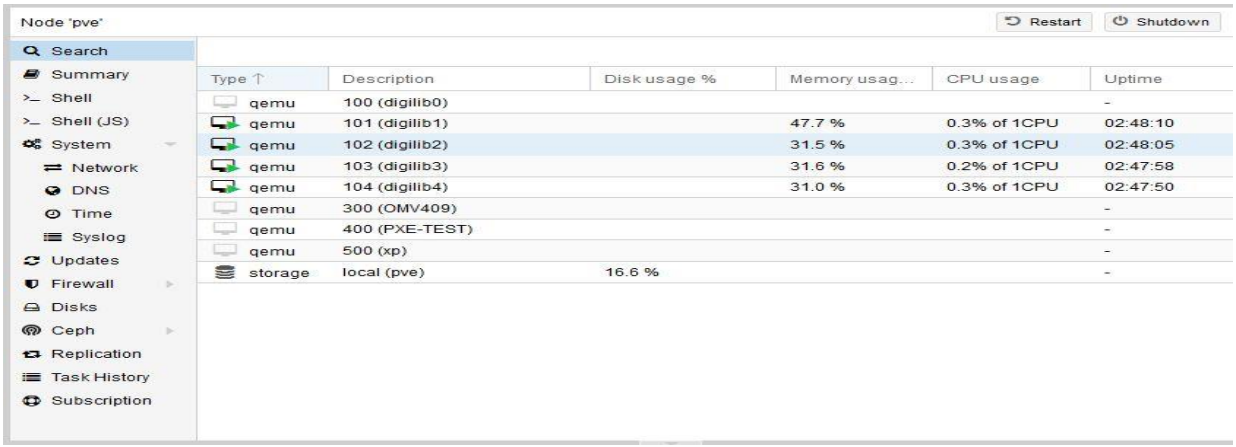

Figure 6. Performance ProxmoxVE cloud server.

4. Conclusion

From the test results, it can be concluded that all ProxmoxVE firewall rules can run properly, based on the scenario that has been created. The use of a firewall is expected to filter incoming and outgoing data traffic through the datacenter. The benefits of data fitering are expected to increase data security on cloud computing servers. Application of firewall rules on the ProxmoxVE cloud server has no effect on the performance of virtual computers. Virtual computer performance has no effect on firewall rules, it is shown that on average virtual computers use 0.3% cpu and 31% memory.

Acknowledgment

The authors would like to thank to the Indonesian Directorate General of the Higher Education (DIKTI) and State Polytechnic of Malang who have supported this research project.

References

[1] Singh A 2013 *Cloud search* Dell Cloud service application
[2] Furht B and Escalante A 2010 *Handbook of CloudComputing* (Cambridge: Springer)
[3] Behl A 2011 Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation *World Congress on Information and Communication Technologies (WICT)* pp 217-222
[4] Jadeja Y and Modi K 2012 Cloud computing-concepts, architecture and challenges. International Conference on Computing *Electronics and Electrical Technologies (ICCEET)* pp 877-880
[5] Nussbaum L, Anhalt F, Mornard O and Gelas J P 2009 Linux-based virtualization for HPC clusters
[6] Curran K and Carlin S 2011 Cloud computing security *Int. J. Ambient Comput. Intell.* **3**(1) pp 14–19
[7] Alaluna M, Vial E, Neves N and Ramos F M 2019 Secure Multi-Cloud Network Virtualization *Computer Networks*
[8] Bays L R, Oliveira R R, Buriol L S, Barcellos M P and Gaspary L P.2013 Security-aware Optimal Resource Allocation for Virtual Network Embedding *in: Proceedings of the 8th International Conference on Network and Service Management, CNSM '12, International Federation for Information Processing, Laxenburg, Austria* pp 378–384
[9] Maggi F, Volpatto A, Gasparini S, Boracchi G and Zanero S 2011 A fast eavesdropping attack against touchscreens *7th International Conference on Information Assurance and Security (IAS)* pp 320-325
[10] Joshi B, Vijayan A and Joshi B 2012 Securing Cloud ComputingEnvironment Against DDoS Attacks *Proc. IEEE Int'l Conf. Computer Comm. and Informatics (ICCCI '12)*