JURNAL INFOTEL
Informatics - Telecommunication - Electronics
Website Jurnal : http://ejournal.st3telkom.ac.id/index.php/infotel
ISSN : 2085-3688; e-ISSN : 2460-0997

Performance Analysis Of Firewall As Virtualized Network Function On VMware ESXi Hypervisor

Ahmad Thoriq Azzam[1*], Rendy Munadi[2], Ratna Mayasari[3]
[123] Telecommunication Engineering, School of Electrical Engineering, Telkom University
[123] Jl. Telekomunikasi Terusan Buah Batu Bandung 40257 Indonesia
*Email corresponding : azzamthoriq@gmail.com

Received 16 February 2019, Revised 03 March 2019, Accepted 25 March 2019

Abstract — Virtualization technology is slowly being used to build network infrastructure called Network Function Virtualization (NFV). It takes network functions such as firewall, load balancer, IPS out of its hardware then uses its software to be run on high specification server. It helps to reduce vendor lock-in and creates a multiplatform network function environment for telecommunication or Internet Service Provider (ISP) company. It has a lot of benefits compared to a traditional network. One of them is reducing the number of hardware that is used in the telecom industry. This technology runs on the hypervisor that is used for the hardware management. One of the important components from NFV is Virtualized Network Function (VNF). In NFV, network devices are run on a server so that a firewall is needed. If an attack occurs on the network, it will interfere the existing network components. This paper focuses on analyzing the performance of two firewall systems: pfSense, and FortiGate. Both firewalls run on the VMware ESXi hypervisor. It compares the firewall performance in normal conditions without attacks and under SYN DoS attacks. Besides, firewall failover capabilities are evaluated. Based on the overall testing results, FortiGate has better performance than pfSense. It has better ability in handling DoS SYN attack because of lower throughput performance degradation and better FTP performance. It is concluded that FortiGate has best performance if it is compared to pfSense.

Keywords – firewall, network function virtualization, hypervisor, pfSense, FortiGate

I. INTRODUCTION

NFV is a network concept that offers new ways to design, deploy, and manage network services by taking the function of network devices in the form of hardware into software. The cause of the emergence of the NFV is initiated by operators or telecom industry that is looking for ways to accelerate the implementation of new network services to support their business strategies and increase revenue growth.

Various types of network devices such as firewalls, load balancers, and routers can be implemented as virtualized software that runs on high-specification servers. This virtualized software is called Virtualized Network Function (VNF). VNF is a version of a network device in the form of software. The separation of software from hardware makes it easier to develop each network function. This development allows a model where resources from hardware infrastructure can be shared through various software network functions. This software can be run on one CPU using virtualization technology [1].

NFV makes it possible for telecom operator to scale up and down network function such as IDS, IPS, and firewall based on the demand and in case of network attack [2]. That is why NFV has an elastic structure which can adapt to any condition under certain times by scale up and down the VNF on the NFV infrastructure.

Virtualization runs on top of a hypervisor, a software that is used to create and manage virtual machines called NFVI based on Fig 1. NFVI is NFV component that provides infrastructure such as hardware and software to run VNF [3]. In this paper, VMware ESXi is used as a hypervisor. VMware ESXi is a bare-metal hypervisor made of full virtualization concept [4]. This concept allows VMware ESXi to partition physical servers into several virtual machines running side by side on the same physical server. So by using VMware ESXi technology we will be able to

https://doi.org/10.20895/infotel.v11i1.425

run multiple machines in one physical server. This technology can reduce operational cost for company because it reduces number of operational devices.

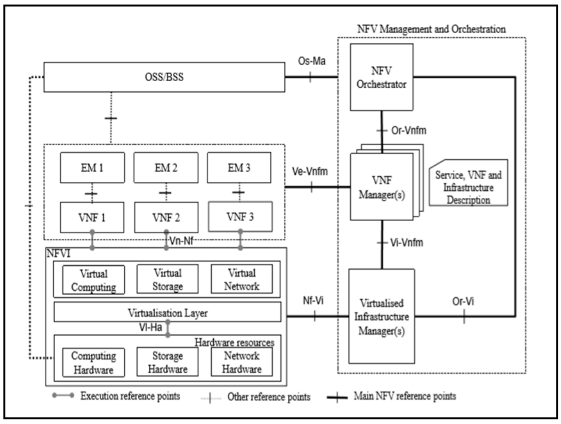

Fig.1. NFV Architectural Framework Based on ETSI

Virtualization runs on top of a hypervisor, a software that is used to create and manage virtual machines called NFVI based on Fig 1. NFVI is NFV component that provides infrastructure such as hardware and software to run VNF [3]. In this paper, VMware ESXi is used as a hypervisor. VMware ESXi is a bare-metal hypervisor made of full virtualization concept [4]. This concept allows VMware ESXi to partition physical servers into several virtual machines running side by side on the same physical server. So by using VMware ESXi technology we will be able to run multiple machines in one physical server. This technology can reduce operational cost for company because it reduces number of operational devices.

NFV provides more advantages than traditional networks. One of them is reducing the number of OPEX and CAPEX's hardware equipment. However, it has security weakness. Specifically, this problem can be found on VNF which is an important part of NFV architecture [1]. VNF is very susceptible to attack from within or outside the NFV environment [5]. Meanwhile, the presence of NFV technology makes it possible to facilitate threats to enter the telco network and to allow Distributed Denial of Service (DDoS) to attack network resources [6].

The suitable network function that has the ability to detect the attack and protect a trusted network from an untrusted network is called firewall [7]. It has the capability to limit access to a certain network by configuring certain security policy. Firewalls in the form of Virtualized Network Function (VNF) or virtual firewall (vFW) in the form of virtualized firewalls can carry out packet filtering and monitoring all traffic that enters the network. The virtual firewall can also be used as a network connectivity validator between virtualized network functions [8]. It is important to make sure that all connectivity between the consumer and the core network in a virtual environment are safe. It can be done by applying policy enforcer function such as a firewall. Virtual firewalls can be run on hypervisor or cloud. It is a solution that can be used to protect virtual networks. This type of firewall has the ability and features that are similar to a firewall in the form of hardware in general. This paper focuses on testing performance between two firewall systems namely pfSense and FortiGate. These firewalls were chosen based on the review result that was conducted by IT central station in 2018. It stated that Fortigate and Pfsense are the top 10 rated firewall technology in 2018 [9]. PfSense, a firewall based on the FreeBSD operating system is equipped with a custom kernel and third-party software as an additional function [10]. It is the best open source firewall system. FortiGate is a firewall built by Fortinet. It offers flexible deployment for the virtual environment [11]. Both firewalls are the top 10 rated firewalls in 2018 [9]. In order to make sure a firewall function service always available to protect the virtual network. We need to deploy firewall in high availability topology so that if one firewall fail to operate there will be another firewall that can operate as back up. Firewall can be deployed in high availability setup using 1:1 protection topology by deploying two identical firewalls [12].

Based on the previous research related to virtual firewall, it was concluded that FW-VNF virtual firewall produces good performance in managing access policies for virtual networks [13]. It is in accordance with the basic concept of a firewall that serves to filter data access to computer networks. Related research [14] was conducted for a simulation of the CARP protocol for failover. It tested the ability of CARP protocol in maintaining the availability of a firewall in case the firewall fails to operate. The last related research [15] was conducted to test pfSense and Endian firewalls performance by using various DoS attacks and port scanning methods.

Based on the related research, this research is conducted to test the firewall's performance in a normal condition without SYN DoS attack and under SYN DoS attacks. It aims to compare pfSense and FortiGate firewalls performance in NFV. This paper compares each testing result by analyzing them according to the specified test parameters. In addition, it was investigated regarding the comparison of the pfSense and FortiGate firewalls' failover capabilities. The purpose of this research is to compare the performance of Fortigate and pfSense firewalls. It intends to find out whether the best open source firewall namely pfSense has the capability to compete with best paid firewall, Fortigate in NFV environment.

II. RESEARCH METHOD

In this section, the design of the testing system is explained. It focuses on explaining topology testing with three scenarios, namely testing the firewall's throughput, and the firewall's performance by running FTP service in normal and under SYN DoS attack. The next scenario is testing high availability of firewall by designing topology test. It involves two firewalls that are formed into the cluster.

The hardware that was used consists of 1 physical server and 2 laptops. The physical server was used to run the firewall as VNF and ubuntu server 18.04 virtual machine on VMware ESXi. The physical server was PC with motherboard MSI H310, 8 GB RAM DDR4, processor Intel Core i5-8400 with 3 Gigabit ethernets. Meanwhile, one laptop was used as a client that requests FTP. Another laptop was used as an attacker that launched DoS SYN attacks using hping3. The first topology as shown in Fig.2, consisted of only 1 client for throughput testing. In this research, throughput testing was conducted by using iperf. This tool has ability to measure throughput by flowing TCP traffic from pc client to VM ubuntu server 18.04 LTS. It was used to get firewall's throughput performance to understand the ability of firewall in distinguishing legal TCP traffic with illegal DoS SYN traffic. If the firewall has a good result in throughput testing, it has a good ability to distinguish traffic flow which is important for the firewall.

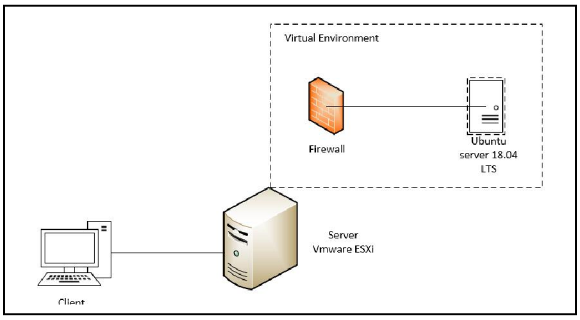

Fig.2. Throughput Testing Topology

The second topology as it is shown in Fig.3, the topology was used for testing firewall's performance as VNF that run on hypervisor. The purpose of this topology testing design was to measure firewall's performance. It was conducted by running file transfer file using FTP in a normal condition without SYN DoS attack and under SYN DoS attack. By using the test result, two firewalls' performance was compared to see which one performed best in normal and under attack condition. The tests that were conducted in this paper used FTP (File Transfer Protocol) service.

This research ran on a server that has VMware ESXi hypervisor installed. Two different firewalls in the form of VNF were installed above the virtualization layer or the hypervisor. An FTP server was installed on VM ubuntu server LTS 18.04. There are three topology testing in this paper namely throughput testing topology, performance testing topology and high availability testing topology.

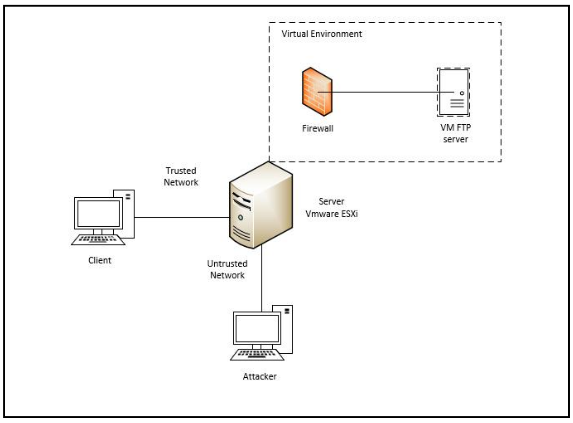

Fig.3. Performance Testing Topology

The third topology testing consists of two firewalls as seen in Fig.4. The firewall cluster consists of the main firewall and backup firewall. It will be active when the main firewall has a system failure or suddenly shut down. The first firewall acts as the main firewall, while the second firewall acts as a backup. The backup firewall only serves as a replacement for the main firewall if there is disruption to the main firewall. This test aims to determine the performance of both pfSense and FortiGate firewalls if system failure on the main firewall occurred. The system failure will then trigger the transfer of packet flow to the backup firewall so that the network can remain protected by a backup firewall.

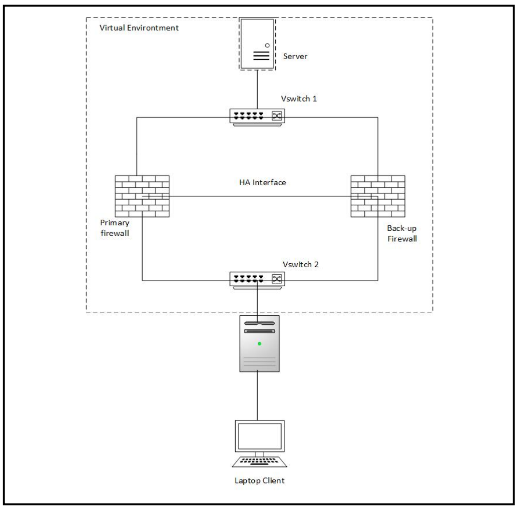

Fig.4. High Availability Testing Topology

The test scenarios are as follows:

A. Throughput Testing

Throughput testing was done by flowing TCP traffic from client to VM server. This test used Fig.2 as topology. The firewall performance was evaluated by comparing throughput measurement with three categories. The first category, client directly flowed traffic to VM Ubuntu server without VNF firewall between client and server. The second category, client flowed traffic to VM ubuntu server through pfSense firewall. The last category, client flowed traffic through the FortiGate firewall. These testing scenarios were done by using iperf as TCP traffic packets generator. The purpose of measuring throughput in the first category was as a reference to determine the smallest performance degradation between pfSense and FortiGate. The smaller degradation value shown a better performance.

B. Performance Testing

This test was done by measuring the performance degradation of FTP (File Transfer Protocol) service. This test used Fig.3 as topology testing. The firewall performance was evaluated by measuring the speed and time for downloading and uploading. It was done by simulating download and upload process by using 848 MB file to the VM ubuntu server. There were two conditions for testing. First, under the normal condition without SYN DoS attack. Second, under DoS SYN attack. It was done by using JSCAPE MFT Monitoring.

C. High Availability Testing

High availability is a failure response mechanism for infrastructure. This test used Fig.4 as topology testing. It required a special configuration. This test was done to determine the ability of both firewalls to do failover. It tested a backup operational mode where the functions of the main system components were taken over by secondary system components and the main component became unavailable due to the system failure. This test was done by sending PING ICMP packet to the destination server. High availability performance was evaluated by using the failover delay parameter. The delay was measured after the main device died or had a system failure until there was a backup device that took over the tasks and functions of the main device. The unit used was second (s).

III. RESULT

This section shows the research result which consists of three testing namely throughput testing, performance testing, and high availability testing.

A. Throughput Testing

In this test, the results of testing between two firewalls and no firewall will be displayed. The purpose of testing with no firewall topology in this study is to see the value of throughput obtained when there is not any firewall installed between VM ubuntu server with the client so that we can compare the result of not installing a firewall between the server and client with installing a firewall between server and client. The throughput testing result can be seen in Table.1.

Table.1. Throughput Testing

Throughput Measurement			
SUT	**No *firewall***	**pfSense**	**FortiGate**
Normal (MB/s)	117.71	117.60	117.52
Attack (MB/s)	56.63	62.17	66.49
Performance degradation (%)	51.89	47.13	43.42

The result of system on normal and under attack data were formed into a graph which can be seen in the following Fig.5.

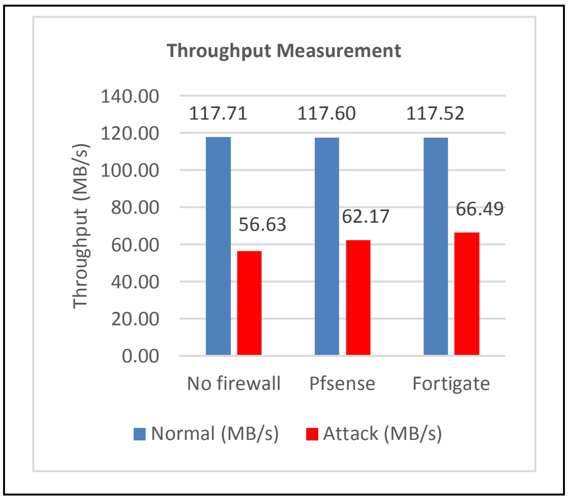

Fig.5. Throughput Measurement Result

In order to measure the amount of variation of a set of data values in this test, the standard deviation values were shown on Table.2.

Table.2. Throughput Testing Standard Deviation

Standard Deviation			
SUT	**No Firewall**	**PfSense**	**FortiGate**
Normal (MB/s)	1.63	1.20	6.24
Under Attack (MB/s)	22.27	99.89	23.40

B. Performance Testing

In this testing, there were four test parameters discussed: download speed, download time, upload speed and upload time. It can be seen on the Fig.6, Fig.7, Fig.8 and Fig.9.

https://doi.org/10.20895/infotel.v11i1.425

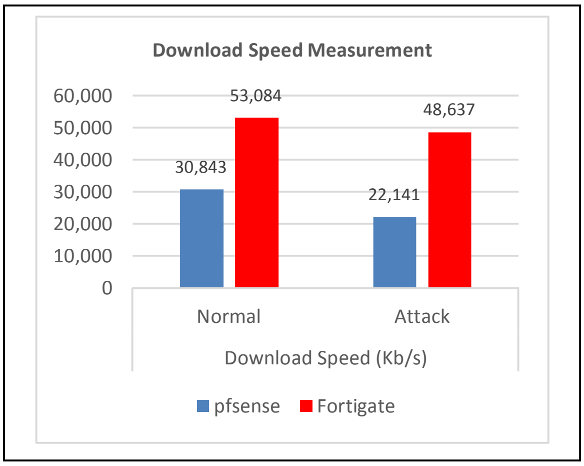

Fig.6. Download Speed Measurement

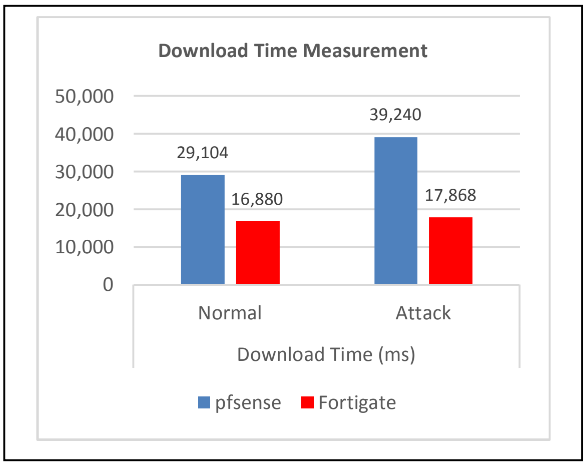

Fig.7. Download Time Measurement

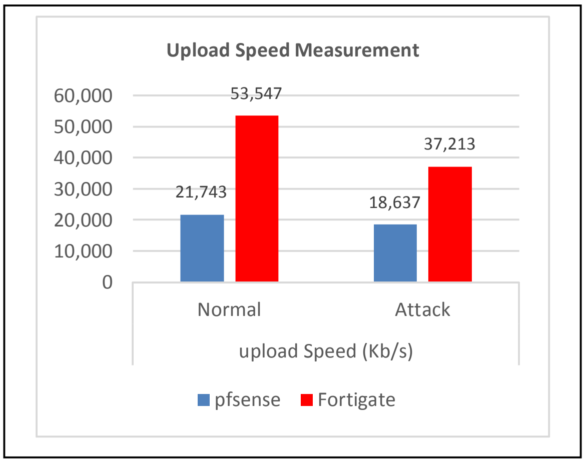

Fig.8. Upload Speed Measurement

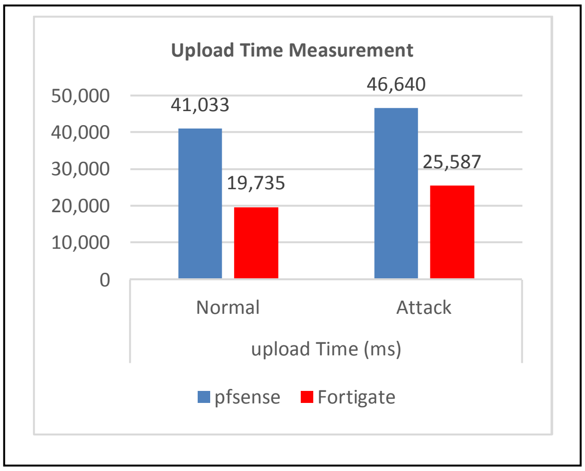

Fig.9. Upload Time Measurement

Table.3. Download Speed Result

Download Speed		
Firewall	**Pfsense**	**Fortigate**
Normal (Kb/s)	30.843	53.084
Attack (Kb/s)	22.141	48.637
Performance Degradation	28%	8%

C. *High Availability Testing*

The test of this metric aims to determine the availability of the firewall when one out of two firewalls tested dies or cannot operate. The result of this test can be seen on Fig.10. This testing used the failover delay parameter. ICMP PING with the command: # ping [ip address] -i 0,01 -D -O was used to get failover delay.

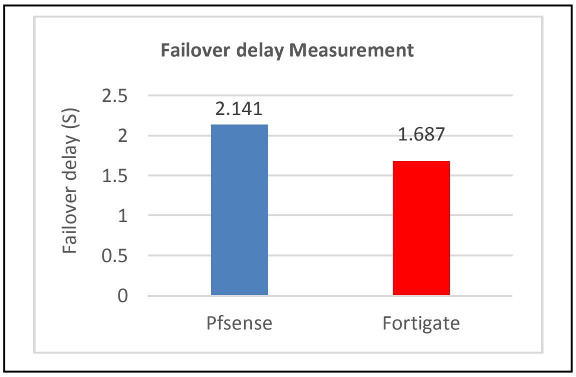

Fig.30. Failover Delay Measurement Result

IV. DISCUSSION

This research was conducted on VMware ESXi by using FortiGate and pfSense. Based on Fig.5 and table.1, the performance of firewalls in a normal condition without a firewall shown expected result. It has a throughput value of 117.71 MB/s with performance degradation 51.89%. However, throughput value decreased to 56.63 MB/s after having a DoS attack on the server. This was caused by the Ubuntu server VM that had been directly exposed to the SYS DoS attack without a firewall as a server protector from attacks. It led to an increase in server resource system usage which resulted throughput's reduction.

By comparing all performance degradation value, FortiGate shows the best performance with a value of 43,42% compared with pfSense, and no firewall. However, pfSense has better performance than FortiGate under normal condition. Meanwhile, it has similar value to the result of without firewall.

Based on the overall FTP testing parameters, FortiGate has the best performance with greater value obtained. It depicts better performance in download and upload speed both normal and under attack condition. As the result, the faster speed causes a shorter time. It means that the lower the value obtained, the better the performance. When both firewalls are faced with DoS SYN attack. It causes performance degradation as seen on the table.3. DoS SYN attack thus affects FTP download and upload performance. In addition, PfSense firewall has a higher performance reduction of 28% compared to FortiGate firewall which only has a performance decrease of 8% for downloading speed.

High availability testing was done by forming a cluster consisted of two firewalls. A firewall functions as main firewall for the main controller of the cluster. Meanwhile, the slave firewall functions as a backup firewall when a system failure occurs in the main firewall. Based on the Fig.10, FortiGate has better performance because it has a smaller value of failover than pfSense. FortiGate firewall uses the FGCP (FortiGate Clustering Protocol) and pfSense uses CARP (Common Address Redundancy Protocol) in its failover mechanism.

V. CONCLUSION

The testing and analysis from both firewalls, pfSense and FortiGate, which were run above VMware ESXi as a hypervisor found different results in each parameter. Overall, FortiGate has the best performance in FTP testing and high availability testing. On the contrary, pfSense has better performance in throughput testing under normal condition. It has similar value to without firewall. Under DoS SYN attack, FortiGate has better performance with a value of 43.42% because it has the smallest performance degradation value compared to others. It happens because Fortigate has DoS sensor which detects and blocks DoS traffic. However, it takes time to pass traffic under normal condition. Fortigate needs time to check the flow of traffic whether it is normal or not before letting it pass through firewall. On one hand, pfSense does not have ability to detect DoS traffic. It makes pfSense more vulnerable in facing DoS attack because it has potential to disable firewall system protection. Based on this research, it is concluded that overall FortiGate has the best performance especially under DoS attack. It means that FortiGate has a better ability in defending DoS SYN attack. It is better for future study to test these firewalls by using different network services such as VoIP. Besides, it should examine further the performance testing by using firewall and without firewall in network topology.

REFERENCES

[1] ETSI, "Network Functions Virtualisation (NFV); Architectural Framework," *ETSI GS NFV 002 v1.2.1*, vol. 1, pp. 1–21, 2014.

[2] T. Alharbi, A. Aljuhani, and H. Liu, "Holistic DDoS mitigation using NFV," *2017 IEEE 7th Annu. Comput. Commun. Work. Conf. CCWC 2017*, 2017.

[3] S. Lal, T. Taleb, and A. Dutta, "NFV: Security Threats and Best Practices," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 211–217, 2017.

[4] S. Pawar and S. Singh, "Performance Comparison of VMware and Xen Hypervisor on Guest OS," *Int. J. Innov. Comput. Sci. Eng. Issue*, vol. 2, no. 3, pp. 56–60, 2015.

[5] A. Aljuhani and T. Alharbi, "Virtualized Network Functions security attacks and vulnerabilities," *2017 IEEE 7th Annu. Comput. Commun. Work. Conf. CCWC 2017*, pp. 1–4, 2017.

[6] M. Daghmehchi Firoozjaei, J. (Paul) Jeong, H. Ko, and H. Kim, "Security challenges with network functions virtualization," *Futur. Gener. Comput. Syst.*, vol. 67, pp. 315–324, 2017.

[7] C. Sheth and R. Thakker, "Performance evaluation and comparative analysis of network firewalls," *2011 Int. Conf. Devices Commun. ICDeCom 2011 - Proc.*, 2011.

[8] Open Networking Foundation, "Network Functions Virtualisation : NFV Security Problem Statement," vol. 1, no. 1, pp. 1–15, 2014.

[9] IT Central Station, "Business Intelligence Tools Buyer ' s Guide and Reviews February 2018," no. February, 2018.

[10] C. M. Buechler and J. Pingle, "pfSense : The Definitive Guide (Version 1.2.3) - The Definitive Guide to the pfSense Open Source Firewall and Router Distribution," p. 479, 2009.

[11] Fortinet, *FortiOS ™ Handbook - Firewall*. 2017.

[12] N. Gray, C. Lorenz, A. Müssig, S. Gebert, T. Zinner, and P. Tran-Gia, "A priori state synchronization for fast failover of stateful firewall VNFs," *2017 Int. Conf. Networked Syst. NetSys 2017*, 2017.

[13] L. A. F. Mauricio, M. G. Rubinstein, and O. C. M. B. Duarte, “Proposing and evaluating the performance of a firewall implemented as a virtualized network function,” *2016 7th Int. Conf. Netw. Futur. NOF 2016*, 2017.

[14] G. Attebury and B. Ramamurthy, “Router and firewall redundancy with OpenBSD and CARP,” *IEEE Int. Conf. Commun.*, vol. 1, no. c, pp. 146–151, 2006.

[15] M. Arunwan, T. Laong, and K. Atthayuwat, “Defensive performance comparison of firewall systems,” *2016 Manag. Innov. Technol. Int. Conf. MITiCON 2016*, pp. MIT221-MIT224, 2017.