Journal of Advancement in Computing (JAC)

Comparison Of Different Firewalls Performance In A Virtual For Cloud Data Center

Umm e Khadija* Iqra Saqib
[1,]College of Computing Riphah International University, Faisalabad
[2]# Faculty of Computing University of Agriculture,Faisalabad
Email: Umm e Khadija 67 @gmail.com
Email: Iqrasaqib125 @gmail.com

A B S T R A C T

Every data centre, whether virtual or physical, relies on its network, and the firewall is an essential part of that network for safe communication. Data centre connection can be protected by a variety of firewall types, including software firewalls, physical firewalls, virtual appliance firewalls, and kernel-integrated firewalls. There are several factors to consider when selecting a firewall, especially in a virtualized data centre, where each firewall works differently in different situations. Virtualized data centres are intended to yield lower budgets, efficient management extensibility, better utilization of available resources, scalability, and energy resilience, among several other advantages. Virtualized data centres are the topic of this study, which examines the application of firewalls. The performance of various types of firewalls, such as software firewalls, physical firewalls, virtual appliance firewalls, and kernel-integrated firewalls, is being analysed. Virtual data centre firewall implementation and performance comparisons explain how to design and which firewall type provides the best performance. In all conditions, it was shown that kernel-integrated firewalls worked properly. Virtual machine IP addresses and networks can vary, and the kernel-based firewall can dynamically update its rules to keep pace with such changes. With its distributed firewall functionality, virtual machines can travel across hypervisors with no disruption to their security settings, if their policies remain the same. A kernel-based, distributed firewall is the best way to protect against viruses.

A R T I C L E I N F O

Article History:
Received 4/8/2022
Revised 5/11/2022
Accepted 5/3/2022
Available,online 15/03/2023

Keywords:
Firewal
machine, appliance
virtualized data
firewall
Data centre
Performance

1.INTRODUCTION

When an organization's application software, software infrastructure and computer hardware are all in one place, it is called a "data center. It is possible to think of a data center as a complex collection of interconnected buildings that house everything from servers to storage devices to networking equipment (such as switches, routers, and cabling. You may get everything you

JAC 2023, DOI: https://doi.org/10.36755/jac.v1i1.49

need at one place, including online services, business software, and e-commerce. SAN, local, fiber channel, SCSI storage, as well as security (firewall, intrusion detection system, IP) are all included in a data center To house, administer, and maintain important computing resources for one or more businesses is the purpose of the data center [1]. There is a physical data center that houses all of the resources that are physically present. Software for all applications is installed on physical servers in a data center, and these servers may communicate using physical media.An earlier study found that in a virtualized data center, both physical and virtual resources are available for use. With the help of a hypervisor, which is installed on a physical server and used as an application programmer, it is possible to virtualize physical servers. It is possible to use physical servers to host virtual machines (VMs) that incorporate virtual hardware.Virtual machines share hardware resources, and these virtual machines can be used to execute an operating system or application software [2].

Network virtualization refers to the process of placing a series of logically separated network partitions on top of an existing physical infrastructure that is already in place. In order to guarantee privacy, security, and a unique set of policies, service levels, and routing decisions, each partition must be logically isolated from the others. Transferring data centers from physical to virtual via a cloud software platform allows for remote access to information and applications[3].

In a virtualized datacenter, data and network traffic are protected by a firewall. In traditional data centers there are just a few types of firewalls and installation options; but, in a virtualized data center a wide variety of firewalls are available [4].It becomes more critical to protect your data as the number of devices and end systems grows. These days, most businesses, offices, and other organizations must use firewalls as an integral part of their computer network [5].Increasing the number of end systems and devices on a network necessitates the use of firewalls in order to protect the network from outside threats. Choosing the right firewall security solution is critical since it affects all traffic between the local and external networks. Firewalls are essential components of network security. In order to prevent network packet delays from increasing, they must ensure the appropriate level of security while still providing satisfactory performance [6].In a virtual network, virtual machines (VMs) can communicate with each other and with real machines on the same network. Connecting virtual machines to the virtual network consists of routers, virtual switches, and firewalls. To supply coax, an uplink is established between the virtual switch and the server's NIC (Network Interface Cards). As there are both virtual and physical links. VNICs (Virtual Network Interface Cards) of two virtual computers are connected to a virtual switch. To communicate with one another, virtual machines employ virtual connection. It does not matter if VM01 wishes to interact with VM02 or not it will send a frame with the source and destination MAC addresses switched. By way of the virtual switch, all incoming traffic from VM01 will be diverted to VM02. Virtual components like VNICs, virtual connections, and others will be used to facilitate this communication. Without the need of any hardware, these switches are referred to as virtual [7-8].

2. RECENT WORK

Every end user in a data center is at risk of cyberattacks. Even if the data is well-processed, there are a number of risks because most VMs are located on the same virtual server. For centuries, people have relied on traditional materials and methods to construct their homes' fire walls and other essentials. It is impossible to identify an attack on audio and video equipment that comes into contact with traditional fire barriers and other products like those. However, a hardware firewall cannot be replaced by many fireplaces, and you must just be visible between two machines in order to use their traffic monitoring features [9].Physical items that interfere with virtual

JAC 2023, DOI: https://doi.org/10.36755/jac.v1i1.49

machine migration are another problem. In all data centers, a firewall is a must for users, according to many examples. Consider the implications of this statement. As an IT security manager, he failed to see any internal threats to the data center, which provides all of the important services [10].

The configuration of a firewall is more important than the configuration of other computer systems. " However, many people are afraid of putting up a firewall or data center for two reasons. Unit testing is one example of a performance [11]. Currently, most firewalls are still in development and are designed for older systems, but they nevertheless provide the necessary protection and security features. Most firefighting realtors still design bank operational settings that have an unknown variable of what the firewall should be in the data center if this sort of firewall is positioned in a location that cannot support such a load [12]. Data centers require a firewall for numerous reasons, as stated in this article. Media management is critical in data centers, where the firewall must be implemented in a variety of physical, embedded, and virtual modes of implementation [13].

Access management and security are critical in the data center. Monitoring the traffic between devices is made possible by a well-built firewall and anti-intrusion system. If you are looking for a way to monitor packet filtering, you can use an embedded hypervisor (a piece of software) that serves as a virtual data center. It is possible to configure a virtual firewall differently in the hypervisor (built-in) mode and the bridge mode (Virtual Appliance). Using the same hooks from which all firewall functions are performed, a virtual firewall can be installed in a network [14]. In the event of a visible network failure, the built-in hypervisor functions as a firewall, which is faster than the firewall mode. At the kernel level, it acts as a firewall, filtering incoming packets[15].Each visible and machine gun traffic can pass through the built-in firewall since it functions as a diversion firewall, as demonstrated in the research on NSX .It has a centralized management console with a variety of rules, controls and processing methods. Helps the distribution chain by integrating into existing systems of security [16]. A network-based security platform is used to mix antivirus products and services from different vendors. Suggested that NSX cloud, other security solutions like antivirus, IPS, and IDS, and NSX should be able to interact with one another and integrate. Agencies involved in firefighting, firefighting equipment and supplies, and law enforcement In-depth discussions were held on topics like firewalls, benchmarks, and performance evaluations. As part of the test, the firewall was computed and analyzed to see how much the policy affected it. Various firewall, security, and network scanning programs can be used to check firewall security[17].As they learned during a test of performance, adding more security checks to the firewall actually degraded the system's performance. Workers' reduced output had little impact on overall cost, other from the gradual rise caused by more rules and regulations [18].

3. PROPOSED METHOD

What constitutes a study's "research design" are the goals, objectives, and methods by which those goals and objectives will be attained. Specifically, research design is a portion of the blueprint for collecting, measuring, and analyzing data for research, addressing at least four issues: which questions to investigate, which data to gather, which data to collect it in, and which outcomes to draw [19]. Furthermore elucidated that the primary goal of the study design is to assist prevent the circumstance where the evidence does not address the initial research question. When conducting research, the problem at hand is one of logic, not logistics. By using this technique, the research problem in this study can be effectively tackled, hence research design can be seen as the overarching strategy utilized to combine the many parts of the study in a smooth and systematic way. In accordance

JAC 2023, DOI: https://doi.org/10.36755/jac.v1i1.49

to, there are two types of research strategies: (i) qualitative and (ii) quantitative. Surveys and experiments in the social sciences are often used as illustrative instances of quantitative research and are evaluated in light of the merits and limitations of statistical, quantitative research methodologies and analysis. Further, case studies are sometimes held up as shining instances of qualitative research, which takes an interpretative approach to data, investigates "things" in the context in which they are found, and takes into account the personal interpretations that individuals ascribe to those circumstances. The comparative study design was used to investigate the relative merits of several firewalls in the context of the virtual data center [20].

As a result, this study adopted a quantitative comparative research strategy. Because it is possible to acquire useful comparison data from datacenters while using a comparative research design that employs many firewall types, this strategy was used for this study. Benefits of research using a comparative design include more control over technique, easier access to previously unavailable data, and the potential to more broadly apply results. Researchers can learn more about the prevalence, distribution, and relationships between different factors through comparison studies [21].Therefore, quantitatively oriented field investigations constitute the comparative research design. According to a study's time, money, and other resources are proportional to its complexity and rigor. In order to be sure that the increased accuracy, confidence, generalizability, etc., that comes with a more complex design is worth the additional time and money, it is important to constantly evaluate the results.

What's more, a descriptive study is the best method for this investigation. Therefore, it depicts a situation that may be explained by the measurement of an event or action, and this can be achieved through the use of instructional or informative insights. The frequency, mean, and standard deviation are all examples of measurements of central tendency, and recurrence estimations are examples of measures of dispersion (diversity). The findings of a descriptive study of firewalls in a virtual data center may be displayed in tables based on percentages, the mean, and the standard deviation, while those of a comparative study can be shown in charts depicting the strength of the relationships between the variables [22].

4. RESULTS AND DISCUSSION

Ping, ICMP delay, FTP, VM, RM, and latency are all examples of performance parameters, with throughput serving as a benchmark for determining a network's upper limit. packets received by one node at a given time is referred to as "unit time". The Ping is a network management software diagnostic utility that is used to determine whether a host is accessible on a network. Ping is a component of the Internet Control Message Protocol (ICMP) family. A timestamp is included in each packet sent by Ping, and this can be used to calculate the time it takes for a packet to travel to the remote host. ICMP is a network-layer Internet protocol that sends error messages and other information about packet processing back to the source, and this is referred to as the latency of a packet. The ICMP delay is the time it takes for a packet to get from the sender to the receiver. There are a number of significant messages generated by ICMPs, such as "Destination Unreachable," "Echo Request and Reply," "Time Exceeded," and "Timestamp Request and Reply." PfSense is a firewall/router computer software distribution based on FreeBSD that may be installed on a physical or virtual machine to create a dedicated firewall/router for a network. Web-based management means no knowledge of the underlying FreeBSD system is required to configure and upgrade it.

In order to avoid being mapped by malicious networks, network managers frequently disable ICMP on network equipment. (e.g., Nmap and Nessus scans). A wide range of malicious activities, including but not limited to: ping sweeps, ping

JAC 2023, DOI: https://doi.org/10.36755/jac.v1i1.49

flooding, ICMP tunneling, and ICMP redirects, can all be carried out using the enabled ICMP protocol. As a "quick fix" security precaution, network managers occasionally disable ICMP traffic on their firewalls due to all of the possible ICMP assaults and the fact that TCP/IP still "mostly" works when ICMP traffic is disabled. Network security and performance may be negatively impacted by the removal of the ICMP protocol from the operating system When the ICMP protocol is restricted, it disables critical mechanisms. Tests for ICMP communication latency can uncover network connectivity and security issues.

In order to get accurate findings, pfSense software uses ICMP communication delays to perform the lab setup. The machines under test are Inspur 3060 servers, each of them contains a 8-core Dell Power Edge, R320 32 GB DDR3 RAM, 2.6 GHz Processor (8 Cores), 500 GB HDD, 4.1Gbps NIC and 7th Generation HP 380, 2.6GHz Processor, 32 GB DDR3 RAM (8 Cores), 4 1Gbps NICs 1 TB HDD, one serving a real machine and the other as a virtual machine. All of them are connected to a test intranet, with Firewall specification as: Physical CISCO ASA 5505, Virtual Appliance CISCO ASA 1000v, Integrated & Distributed VMWare NSX, and with Application PFSense. Our experiment is controlled computer, with Operating Systems & Hypervisors as: VMWare Hypervisor ESXi Version 6.0 Windows OS Server 2012, Windows 7,10.

In order to make it simpler to receive information over the actual Internet, a fully virtualized networking configuration was created in the lab. In this setup, a ping from a virtual computer to a real system can be generated. 10 ICMP packets generated, ten times each, and then sent them as a 1.23 GB file to the Physical Machine through FTP. Delay has been measured on pfSense software which is an open source firewall evaluation software and firewall in itself as well.

5. RESULTS AND DISCUSSIONS

The findings are based on a 10x ICMP communication delay with a packet size of 10,000 bytes between the physical machine (Source) and the virtual machine. (Destination). Each time the 10 ICMP packets are transmitted, the delays are investigated. The graphs are created using MS Excel; the x axis represents the time of the message according to the order in which it was sent, and the y axis represents the delay in receiving time, which is measured in milliseconds.The delays between a physical machine and a virtual machine using ICMP (Internet Controlled Messaging Protocol) without a firewall are as follows.

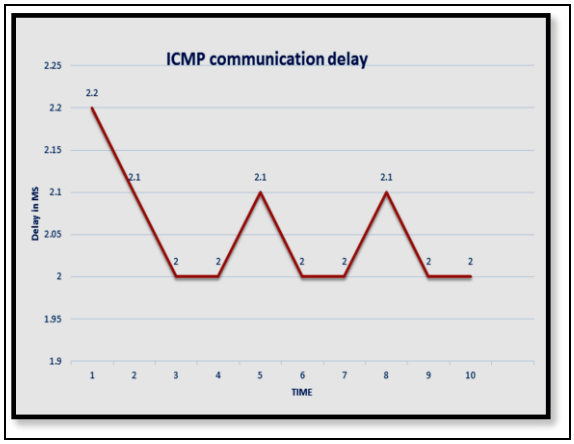

Fig.1 ICMP Delays Between a RM and a VM Without Firewall

Figure 1 illustrates the result output of ICMP (Internet Controlled Messaging Protocol) communication delays between a physical machine and a virtual machine without firewall measured in milliseconds and packet size in 10000 bytes. The numbers on y axis from 1-10 show the10 packets of ICMP communication delays (where the packet size was10000 bytes for each packet) in the intervals of milliseconds shown on the x axis ranging from 1.9-2.25ms with the increment of 0.05ms each time. And the latency looks very similar at delay on 2ms and the number of time intervals at 3, 4, 6, 7, 9, and 10. And again at 2.1ms on the number of time intervals at 2, 5, and 8. Latency steadily increases only on

JAC 2023, DOI: https://doi.org/10.36755/jac.v1i1.49

interval 1 at 2.2ms. ICMP (Internet Controlled Messaging Protocol) Physical Firewall delays between physical machines and virtual.

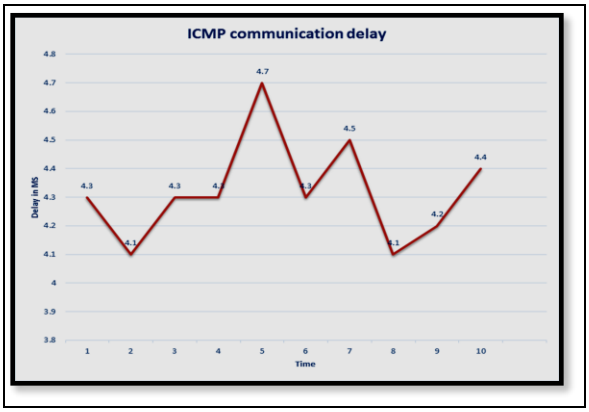

Fig.2 ICMP delays between a RM and VM with Physical Firewall through Light Load

Figure 2 illustrates the result output of ICMP (Internet Controlled Messaging Protocol) communication delays between a physical machine and a virtual machine with physical firewall and light load measured in milliseconds and packet size in 10000 bytes. The numbers on y axis from 1-10 show the10 packets of ICMP communication delays (where the packet size was10000 bytes for each packet) in the intervals of milliseconds shown on the x axis ranging from 13.8- 4.8ms with the increment of 0.02ms each time. And the latency looks very similar at delay on 4.3 ms and the number of time intervals at 1,3, 4, and 6. And again at 4.1ms on the number of time intervals at 2, and 8. It changes at delay 4.5 ms and the number of intervals is 7, and 4.4 ms at the interval of 10 Latency steadily increases only on interval 5 at 4.7ms.

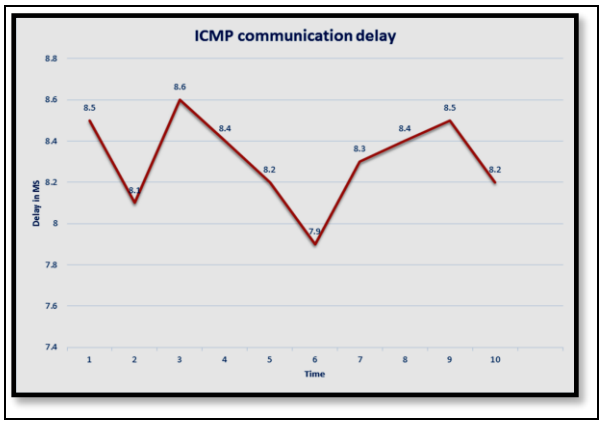

Fig.3 ICMP delays between a RM and VM with Physical Firewall and Full Load Delays

Figure 3 illustrates the result output of ICMP (Internet Controlled Messaging Protocol) communication delays between a physical machine and a virtual machine with physical firewall and full load measured in milliseconds and packet size in 10000 bytes. The numbers on y axis from 1-10 show the10 packets of ICMP communication delays (where the packet size was10000 bytes for each packet) in the intervals of milliseconds shown on the x axis ranging from 7.4- 8.8ms with the increment of 0.02ms each time. And the latency looks very similar at delay on 8.2ms and the number of time intervals at 5 and 10. And again at 8.4ms on the number of time intervals at 4, and 8 and 8.5ms on the number of time intervals at 1, and 9. It changes at delay 8.1ms and the number of interval is 2, and 7.9ms at the interval of 6, 8.3ms at the interval of 7 Latency steadily increases only on interval 3 at 8.6ms.

6. CONCLUSION

As part of my research, I investigated how well various types of firewalls worked in a virtualized data center. To monitor traffic as it moves through a virtual machine, it must be installed at the kernel level. In all conditions, it was shown that kernels with firewalls grafted into them worked properly. Even if multiple virtual machines are connected to the same virtual switch, the switch can nevertheless monitor and filter traffic on each of them separately. The traffic is filtered out in this circumstance other firewalls, such as physical firewalls, virtual appliance firewalls, and application firewalls, use IP-based policies and are unable to detect and update their policies if a virtual machine's IP or network changes. To ensure continual virtual machine connectivity, network managers must alter their current policy. Virtual machine IP addresses and networks can vary, and the kernel-based firewall can dynamically update its rules to keep pace with such changes. With its distributed firewall functionality, virtual machines can travel across hypervisors

JAC 2023, DOI: https://doi.org/10.36755/jac.v1i1.49

with no disruption to their security settings, if their policies remain the same on all of them. A kernel-based, distributed firewall is the best way to protect against viruses.

REFERENCES

[1] Afamugat, N. (2022). Building an ethical hacking environment.Metropolia 2(24),1-53.

[2] Agbenyegah, F. K., & Asante, M. (2017). Impact of firewall on network performance. International Journal of Scientific & Technology Research, 6(3), 32-38.

[3] Ahmadin, M. (2022). Social Research Methods: Qualitative and Quantitative Approaches. Jurnal Kajian Sosial dan Budaya: Tebar Science, 6(1), 104-113.

[4] Akhtar, D. M. I. (2016). Research design. Research Design 18(1),1-17.

[5] Alam, T., Ullah, A., & Benaida, M. (2022). Deep reinforcement learning approach for computation offloading in blockchain-enabled communications systems. Journal of Ambient Intelligence and Humanized Computing, 1-14.

[6] Aldribi, A., Traoré, I., Moa, B., & Nwamuo, O. (2020). Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking. Computers & Security, 88(3), 101646.

[7] Alfayyadh, B., Ponting, J., Alzomai, M., & Jøsang, A. (2010). Vulnerabilities in personal firewalls caused by poor security usability. In 2010 IEEE International Conference on Information Theory and Information Security, 17th to 19th December,Beijing, China,(pp:1-50).

[8] Alhasan, A. J., & Surantha, N. (2021). Evaluation of Data Center Network Security based on Next-Generation Firewall. International Journal of Advanced Computer Science and Applications, 12(9),518-525.

[9] Amin, H. J. (2021). Effect of Entrepreneurial Marketing Dimensions on Small and Medium Enterprises Performance in Nasarawa State. Economics and Business Quarterly Reviews, 4(2),1-14.

[10] Anwar, R. W., Abdullah, T., & Pastore, F. (2021). Firewall Best Practices for Securing Smart Healthcare Environment: A Review. Applied Sciences, 11(19), 9183.

[11] Balaji, K., Sai Kiran, P., & Sunil Kumar, M. (2022). Power aware virtual machine placement in IaaS cloud using discrete firefly algorithm. Applied Nanoscience,73(3) 1-9.

[12] Bari, M. F., Boutaba, R., Esteves, R., Granville, L. Z., Podlesny, M., Rabbani, M. G., ... & Zhani, M. F. (2012). Data center network virtualization: A survey. IEEE communications surveys & tutorials, 15(2), 909-928.

[13] Beck, K. F., & Hämäläinen, J. (2022). Mapping the field of international comparative research in school social work. International Social Work, 65(2), 203-223.

[14] Beerbaum, D. O. (2021). Applying Agile Methodology to regulatory compliance projects in the financial industry: A case study research. Available at SSRN (4)26, 3834205.

[15] Bell, E., & Bryman, A. (2007). The ethics of management research: an exploratory content analysis. British journal of management, 18(1), 63-77.

[16] Bodei, C., Degano, P., Galletta, L., Focardi, R., Tempesta, M., & Veronese, L. (2018). Language-independent synthesis of firewall policies. In 2018 Ieee European Symposium On Security And Privacy (Euros&P), 24th to 26th April,London,UK, (pp:1791-5587).

[17] Caiazzi, T., Scazzariello, M., Alberro, L., Ariemma, L., Castro, A., Grampin, E., & Di Battista, G. (2022). Sibyl: a Framework for Evaluating the Implementation of Routing Protocols in Fat-Trees. In NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium Conference, 25th to 29th April, Budapest, Hungry,(pp:217811).

[18] Ouhame, S., Hadi, Y., & Ullah, A. (2021). An efficient forecasting approach for resource utilization in cloud data center using CNN-LSTM model. Neural Computing and Applications, 33(16), 10043-10055.

[19] Ouhame, S., Hadi, Y., & Ullah, A. (2021). An efficient forecasting approach for resource utilization in cloud data center using CNN-LSTM model. Neural Computing and Applications, 33(16), 10043-10055.

[20] Ouhame, S., Hadi, Y., & Ullah, A. (2021). An efficient forecasting approach for resource utilization in cloud data center using CNN-LSTM model. Neural Computing and Applications, 33(16), 10043-10055.

JAC 2023, DOI: https://doi.org/10.36755/jac.v1i1.49

[21] Sebai, D., & Shah, A. U. (2022). Semantic-oriented learning-based image compression by Only-Train-Once quantized autoencoders. Signal, Image and Video Processing, 1-9.
[22] Ullah, A., & Nawi, N. M. (2021). An improved in tasks allocation system for virtual machines in cloud computing using HBAC algorithm. Journal of Ambient Intelligence and Humanized Computing, 1-14.

JAC 2023, DOI: https://doi.org/10.36755/jac.v1i1.49