March-April 2020
ISSN: 0193-4120 Page No. 5854 - 5863

Performance analysis of IIS10.0 and Apache2 Cluster-based Web Servers under SYN DDoS Attack

Subhi R. M. Zeebaree[1], Rizgar R. Zebari[2], Karwan Jacksi[3]
[1]Duhok Polytechnic University Duhok – Kurdistan Region / Iraq.
[2]Duhok Polytechnic University, Duhok – Kurdistan Region / Iraq.
[3]University of Zakho, Duhok – Kurdistan Region / Iraq.

Article Info
Volume 83
Page Number: 5854 - 5863
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 30 March 2020*

Abstract:

Since the last decade, Internet users increased rapidly and most of them are depending on the World Wide Web (WWW) service for achieving daily routine. Having Internet access and especially WWW sometimes users face difficulties because of various security problems. The most dangerous and serious threats that make Internet services impossible is Denial of Service (DoS) and its severe type 'Distributed Denial of Service (DDoS)'. In this paper, the performance of different web servers in Network Load Balancing (NLB), cluster-based and none clustered are analyzed. Furthermore, we evaluate the impact of TCP SYN flood attack with massive concurrent HTTP load traffic on web server's average response time, throughput and average CPU usage. The results show that Internet Information Service 10.0 (IIS10.0) on Windows server 2016 is more vulnerable to attacks compared to Apache2 on Ubuntu 16.04. The results also show that the IIS10.0 NLB clustered web servers is the most suitable mechanism for handling huge HTTP workload.

Keywords: *DDoS attack, SYN DDoS, Apache2 web server, IIS10.0 web server.*

I. Introduction

In the last few years, Internet services especially the World Wide Web (WWW) has been used widely [1]. Nowadays, the Information and Communication Technology made deep effects in the human life. Majority of Internet users, which are more than 3.5 billion users, depend on WWW for several daily life aspects such as communication, e-learning, e-banking, e-marketing, etc. [2]–[5]. On the other hand, the demand now is rapidly, accurately and continuously access to this service under high concurrent load and from almost anywhere and anytime [6], [7]. The most attractive web servers to users who respond to requests in fast for example there is reduction to sales by 1% when every 100 ms is increased to page loading process. Moreover, any online business success greatly rely on response time of end users requests [8], [9]. Also, slowly accessing web servers has negative impression on customers, and 32% of users give up on accessing slow web sites [10], [11].

March-April 2020
ISSN: 0193-4120 Page No. 5854 - 5863

Providing high availability of web services and more responsiveness system to customers can be achieved by using server load balancing. Furthermore, using server load balancing can get acute advantages such as security, scalability and availability of web services. Cluster based web server is the most used and popular type of web server load balancing [12]–[14]. On the other hand, the cluster is a set of interconnected stand-alone computers working together as an integrated and a single computing resource.

Similarly, cluster is considered as a type of parallel or distributed processing system and this style is suitable to small, medium and large internet servers [15], [16]. Additionally, the user's requests or traffic load is distributed among multiple servers in order to reduce latency, increase throughput and to attain maximum performance [17], [18].

Information technology specifically the Internet has several benefits and advantages to the current society such as communication, business, and easy accessing information publicly [18], [19]. Nevertheless, with all assistances of public network or Internet, there are some weaknesses, and network security has been the main challenge to the security community [21], [22]. Due to the fact, there is some vulnerability present in TCP layers in which some attacks can be launched on the Internet [23], [24]. The most serious and harmful is the Denial of Service (DoS) and its extension Distributed Denial of Service (DDoS) [25], [26]. Moreover, initiating these types of attacks is very simple and low-cost, therefore they are occurring very frequently but their effect is severe on users and network resources. An attacker can easily exhaust the victim resources with little or without advanced warning, so that the resource of target will consume and become unavailable to customers [27], [28].

In this paper, the performance of the two broadly used web servers according to the last survey from NETCRAFT [29] on June 2018 will be evaluated. The two web depended servers are: the last versions of IIS (i.e. IIS10.0) on Windows server 2016, and Apache2 on Linux Ubuntu 16.04 Long Term Support (LTS) Server. The main goal of this paper is to analyse the performance of these two web servers in cluster based and none cluster based, also to measure high availability of both web servers under DDoS attacks. Furthermore, the analysing process has done in real installation network on (1 Gbps) Ethernet, while the key metrics of the evaluation are response time, errors, throughput and CPU usage.

II. RELATED WORK

Over the most recent years many researchers have worked on performance of different web servers and some others evaluated the DDoS attacks impact on web servers working routine.

Q. Fan and Q. Wang [30] performed evaluation comparison of different web server architectures under high workload: (1) Asynchronous server such as Node.Js and Nginx. (2) Thread based server include Apache2 and Tomcat BIO. The metrics that comparison based on was response time of the two web servers, and the tests were performed on Linux platform. Moreover, Apache Ben (AB) is used as a benchmark tool in their performance tests. The results didn't observe a big difference of response of those two groups of web server's architectures when the number of concurrent HTTP requests was not more than 400 requests. However, the difference of performance as response time of the two web servers under 800 HTTP concurrency request was 200 ms.

Prakash et al. [31] analyzed the performance of two different open source web servers: Apache which is a process-based web server and Nginx which is an asymmetric multi process event drive architecture. They evaluated both web servers in different tests by using httperf tool for generating HTTP traffic load and measuring web servers' performance. Moreover, they depended on response time, memory usage and error rate as well

as metrics for responsiveness, scalability and efficiency of both web servers. The results showed that when memory usage was significant, the Apache server can't achieve scalability, however the Nginx confirms scalability. Furthermore, the Apache web server response time was twice of that of Nginx web server, that's mean responsiveness of Nginx is better than Apache. In addition, when the HTTP load increased the Nginx error rate increased compared to Apache that's approved that Apache web server outperformed Nginx in efficiency.

Bezboruah and Bora [32] performed evaluation of web service in load balancing cluster and none-cluster Apache web server in Linux platform. They have used Mercury Load Runner tool for virtual users creating and measuring the performance of web server and the evaluation key metrics were average response time and throughput. Their results showed that the response time of cluster web server was greater than that of non-cluster and throughput also was less. However, the load balanced cluster had more stability and handled more web service users.

Bhandari et al. [25] studied the impact of DDoS attacks on web server performance; especially they measured the influence of application layer DDoS attacks on web server. They used NS-2 as simulation and WebTarf as tool to generate legitimated HTTP request as well as for creating HTTP Get attacks. Additionally, they have used average response time, throughput, and dropped transaction as metrics to check the attacks impression on the performance of web server. The results showed that throughput of web server increased by the increased amount of HTTP request received through the server. Also, the results indicated that when the attack targeted the server, the response time of web server increased violently and also the number of dropped transaction increased.

Chen et al. [6] investigated the web server performance with different web page size and number of users. They have used queue model in order to represent physical measurement and web server stress tool to measure the response time and bandwidth of user's clicks as main metrics. The results illustrated that for the requests range (1 to 100) with 10 KB as webpage size, the average response time of the web server was 3.77 ms. Furthermore, with same number of users and page size was 500 KB and the average response time was 1442.07 ms. In the other side, the average bandwidth for each user was 2764.841 KB/S with requests range (1 to 100) and webpage size was 10 KB. However, the average bandwidth for each user was 1513 KB/S when the size of web page was 500 KB and with the same number of users.

Chitra and Satapathy [33] analysed and compared the performance of Node.Js and IIS web servers. Several regular tests were done in different situations to perform the evaluation between the two web servers, they used Apache-Jmeter tool to achieve the comparison tests. Furthermore, they have depended mainly on throughput as a main metric for both web servers performance. The results showed that the Node.Js had a greater throughput compared to IIS web servers and in diverse scenarios.

De la Cruz, J.E.C. and C.A.R. Goyzueta [34] designed a system to provide high availability in cluster based web in Linux platform, they depended on High Availability Proxy (HAProxy) as a load balancer and Domain Name Service (DNS) to handle clients load among cluster nodes. Moreover, they used round robin algorithm to distribute HTTP request for both HAProxy and DNS. The results indicated that the proposed system was simple and easy to use and could accomplish high availability of 99.905%.

Papadie and Apostol [35] evaluated the effect of different DDoS attacks such slowrise and HTTP flood on IIS and Apache web servers' performance.

March-April 2020
ISSN: 0193-4120 Page No. 5854 - 5863

On the other hand, they analysed some techniques which were software defence mechanisms against those attacks on both Linux and Windows servers. They have used High Orbit Ion Cannon (HOIC) tool for creating flood attacks and slowrise for slowrise attacks. However, they used Apache-Jmeter tool to generate simulation users or legitimated traffic. In addition, they depended on response time as a key metric in normal and under attacks condition. Their results indicated that the response time in normal mode was very low in both web servers but in attacks condition, the response time was very high. Moreover, they showed that the mod_qos and IP Tables in Linux system offered best response time and IIS have performed best response time in Windows system.

III. PROPOSED WEB SERVERS SYSTEM

Initially, the study evaluates the performance of different web servers (IIS10.0 on Windows server 2016 and Apache2 on Linux Ubuntu server 16.04 LTS) by hosting on each of them the Duhok Polytechnic university website. Size of website home page is 47 KB and the configuration of both web servers is done in real setup network. Next, preforming the high availability for both platforms (Windows and Linux) through configuring load balancing cluster-based web servers as follows:

In Windows environment, two nodes of computer server are grouped as active/active clustered web servers. Furthermore, NLB feature has installed and configured in both cluster nodes which is provided by Windows Server 2016. The unicast operation mode is selected for allowing periodic communication of cluster hosts from heartbeat messages. Moreover, HTTP traffic is directed to the virtual IP (VIP) address or cluster primary IP which is assigned to all cluster nodes. NLB driver identical copy is run in parallel on each cluster node to concurrently detect incoming traffic and the drivers arrange on a single subnet for cluster nodes. In addition, the driver on each cluster node acts as a filter between TCP/IP stack and the network adapter's driver in order to distribute the incoming network traffic among cluster nodes, this is known as a distributed algorithm [36].

In Linux platform High Availability Proxy (HAProxy) [37] is installed on separate server as a load balancer. For that reason, the efficiency and flexibility of the HAProxy has been used in professional environment with a large number of customers [38]. Moreover, it has ability to provide high availability services for the real servers; therefore, it is configured to work in frontend of real web servers. In addition, it is configured to work at transport layer (layer 4 of OSI model) to speedily distribute requests through web servers (Backend servers) [39]. The end user requests are directed to the HAProxy IP address and then redistributed among the backend part of the cluster which consists of two Apache web servers. The load balancing algorithm used in this installation is round robin which balances the requests between backend web servers equally [40].

Thirdly, for creating high HTTP traffic load or massive number of legitimated requests, the Apache-Jmeter is used because it has shown better result compared to most other load testing tools [41]. Moreover, to evaluate the performance of web servers in cluster based and none cluster-based, client-server Jmeter software (Distributed or remote testing) used. Distributed testing performs more threads or simulates more loads on web servers. By using remote testing a single GUI Jmeter controls N numbers of none-GUI Jmeter and also to collect the results from them [26].

Finally, to measure the impact of DDoS attacks on web servers in clustered and none-clustered, Hping3 [43] used which is command-line and built-in tool inside Linux Backtrack R5. This tool has the ability to generate a huge number of malicious TCP and UDP packets as flood and sending them as fast as possible to the target web servers [44]. Also System Activity Report (SAR) [45] command is used in Ubuntu server, and Get-Counter [30] Windows PowerShell command

March-April 2020
ISSN: 0193-4120 Page No. 5854 - 5863

used in Windows server to measure the CPU usage average in both servers.

IV. EXPERIMENTAL SETUP

For accurate test the performance of web servers in cluster-based and none cluster-based, a real network was constructed and configured. Computers specifications used in the test with the configured network are illustrated in Fig. 1 and Table 1. The Apache-Jmeter master and slaves are installed on HP Pro Desk 400 that has Linux Ubuntu operating system in order to perform efficient HTTP load traffic and to sustain web servers. To setup the network, 1 Gigabit, 24 ports D-link switch and UTP CAT 6 cable are used between computers.

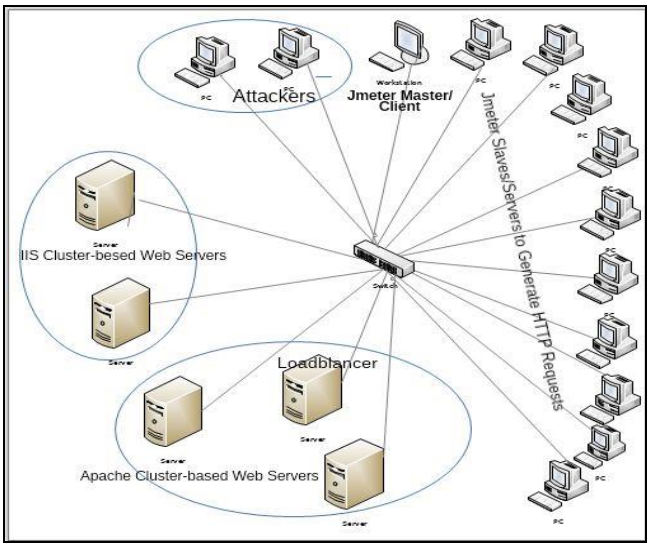

Fig. 1. Test Network of the Study.

Hping3 is used to generate attacks and TCP SYN flood can be executed by the command line (hping3 –c 1000 –d 1024 –S –w 64 –p 80 --flood --rand-source IP address of victims). This means that hping3 will send 1000 TCP SYN packets and each packet size is 1024 bytes in each attacker's computers. As well, it has observed from Backtrack system monitor tool that the above command sends 58 MBps on each attacker's workstation to the victim. Apache-Jmeter is used to generate legitimated HTTP traffic load and evaluate the performance of web servers. Additionally, the period time for each test was 120 seconds and repeated 5 times in order to reach high data accuracy.

Table ***1***. Workstations Specifications

Type	System	CPU	RAM	NIC
Web Servers	Dell OptiPlex	Intel Core I3, 3.3 GHZ	4 GB	1Gbps
Load Balancer	Dell OptiPlex	Intel Core I3, 3.3 GHZ	4 GB	1Gbps
Clients	HP Pro Desk 400	Intel Core I7, 3.4 GHZ	4 GB	1Gbps
Attackers	Dell OptiPlex	Intel Core I3, 3.3 GHZ	4 GB	1Gbps

V. RESULTS AND PERFORMANCE EVALUATION

In this paper, we have evaluated the performance of both of IIS10.0 and Apache2 web servers in several cases. The key metrics of all tests are average response time, error rate, throughput, and average CPU usage of web servers. We have generated 50000, 100000, 150000, 200000, 250000, and 300000 requests by Apache-Jmeter and sent to web servers.

1. Performance Analysis in None Cluster-based Web Servers with/without Attack

Fig.2 illustrates the average response time of both web servers with and without attack. The average response time of IIS was 1ms in first test to third test then it increased to 2ms in the fourth and fifth tests and regularly rose to 3ms in the last test. However, the Apache average response time was similar to that of IIS, but in the last it amplified rapidly to 1139ms. Moreover, the average response time with TCP SYN attacks of Apache increased to 8ms in the first to fifth tests and to highest time which was 2828ms in the last test. Though, for IIS the average increased to 9ms in first three tests and to 10ms respectively in fourth and fifth tests and 17ms in the last test.

Also throughput of web servers is measured in the study as a number of received bits/time [9, 15]. Fig.

March-April 2020
ISSN: 0193-4120 Page No. 5854 - 5863

3 shows that the throughput of both web servers increased linearly from 15 KB/Sec to 90 KB/Sec with and without attacks. However, the throughput of IIS is more affected by SYN TCP attack than Apache throughput because it is fluctuated from 44 KB/Sec to 38 KB/Sec and then raised to 48 KB/Sec and to 57 KB/Sec respectively.

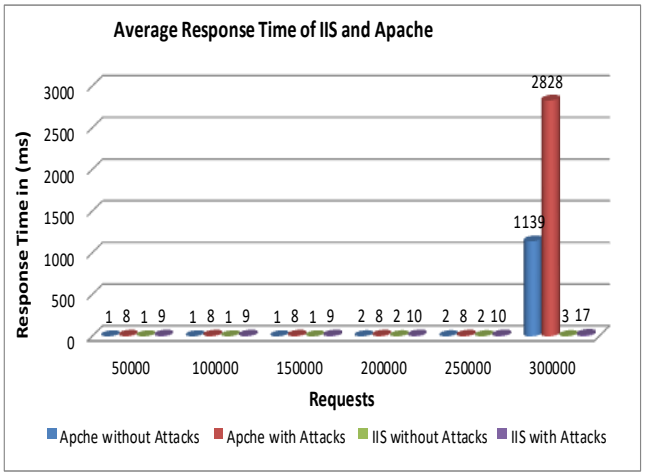

Fig. 2. Average Response Time of IIS and Apache in none clustered-based

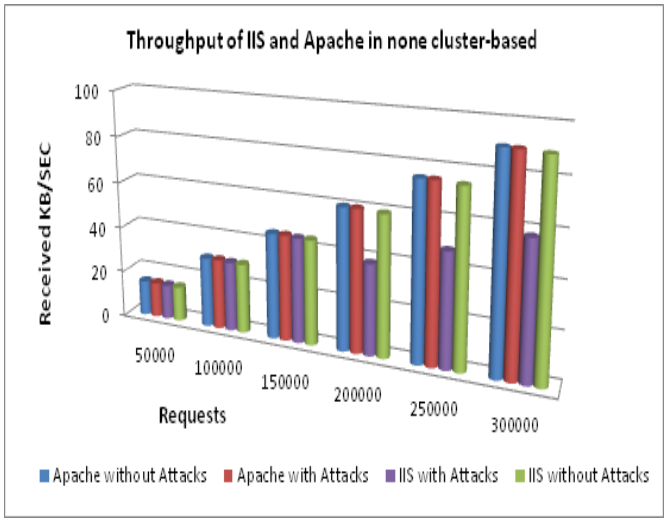

Fig. 3. Throughput of IIS and Apache in none clustered-based

The average of CPU usages is demonstrated in Fig. 4 and it is clearly shown that HTTP traffic load consumed the Apache CPU by 4% more than IIS. Yet, the same rates of load with TCP SYN attacks have more impact on IIS because the average of CPU usage was 17.2% in the first test and increased to reach 38.14% in the last test. While the average CPU usage of Apache with attacks was 12.01% and rose gradually to 26.63% in the last test.

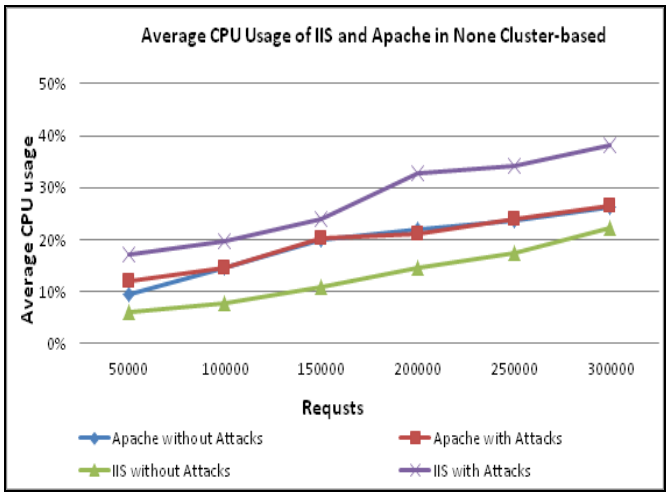

Fig. 4. Average CPU Usage of IIS and Apache in none clustered-based

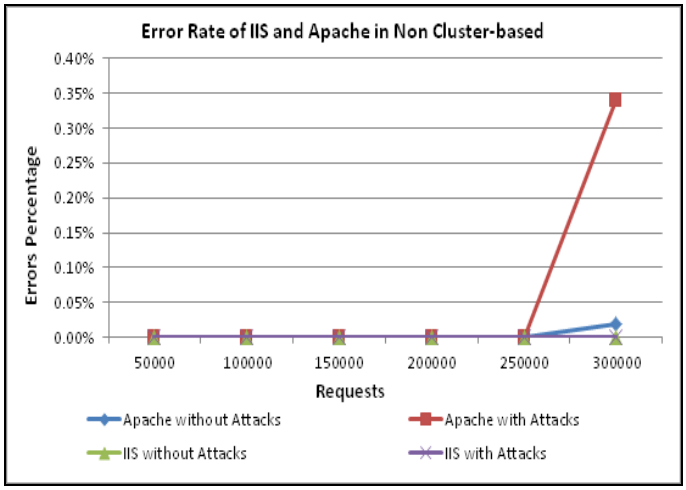

Fig. 5. Error Rates of IIS and Apache in none clustered-based

Moreover, error rate which is referred to the percentage of HTTP requests with errors is shown in Fig. 5 and the error rate was zero for all tests of both web servers. However, the Apache have 0.02% error rate in the last test and 0.34% in the last test with attack.

2. Performance Analysis in NLB Cluster-based Web Servers with/without Attack

Fig. 6 displays the IIS average response time without attacks which was 1ms in first test and remained 1ms to the last test, but with attacks it

March-April 2020
ISSN: 0193-4120 Page No. 5854 - 5863

increased to 6 ms in all tests. However, average response time of Apache was 2 ms in first and second tests, and then increased to 3ms in the third test. Subsequently, it amplified to 7005 ms and 7168 ms in the fourth and fifth tests and finally to 23703 ms in the last test. Furthermore, the Apache average response time increased from 4ms and 5ms in the first and second tests to 2980 in the third test, and rapidly raised to 25300ms, 38402 and 45894ms in the last three tests.

The throughput of web servers is illustrated in Fig. 7; the IIS throughput gradually from 10 KB/Sec to 57.94 KB/Sec in all tests with and without attacks. But the Apache throughput was increased from 7.07 KB/Sec to 27.88 KB/Sec in the first four tests in both cases with and without attacks. However, the throughput of Apache without attacks raised slowly from fourth to the last tests (27.88 KB/Sec to 28.12 KB/Sec and 30.59 KB/Sec). Also with attack it varied from 24.94 KB/Sec to 24.08 and then to 26.63 KB/Sec in the last three tests.

Error rates of both web servers in network load balancing cluster-based is displayed in Fig. 8. The IIS error rates were zero in all tests with or without attacks. The Apache error rates were also zero for first three tests with and without attacks. But for last three tests it is increased from 1.49% to 1.66% and then to 11.82 without attack, and from 12.38% to 21.42 and to reach 29.19 with attacks.

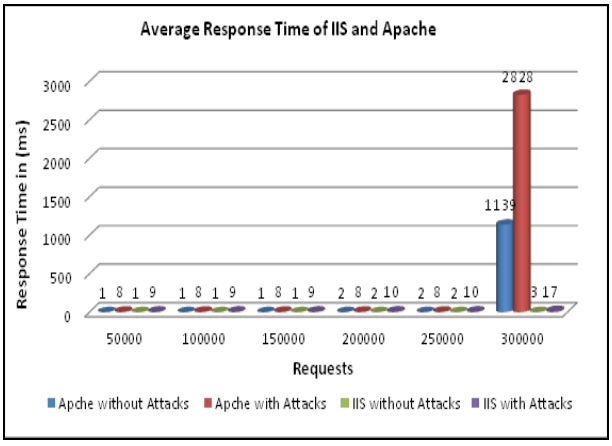

Fig. 6. Average Response Time of IIS and Apache in clustered-based

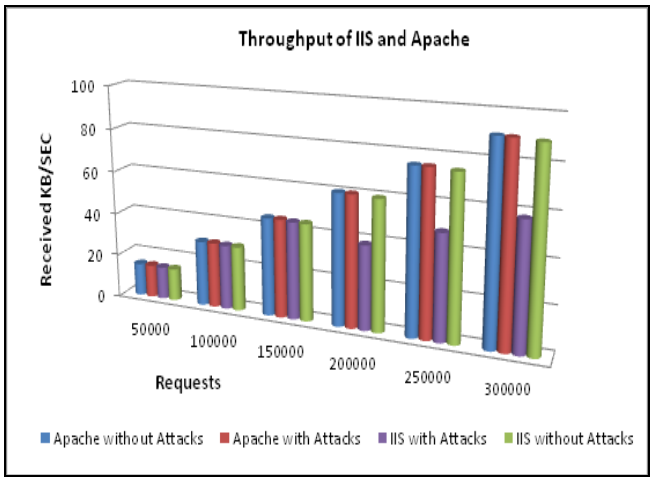

Fig.7. Throughput of IIS and Apache in clustered based

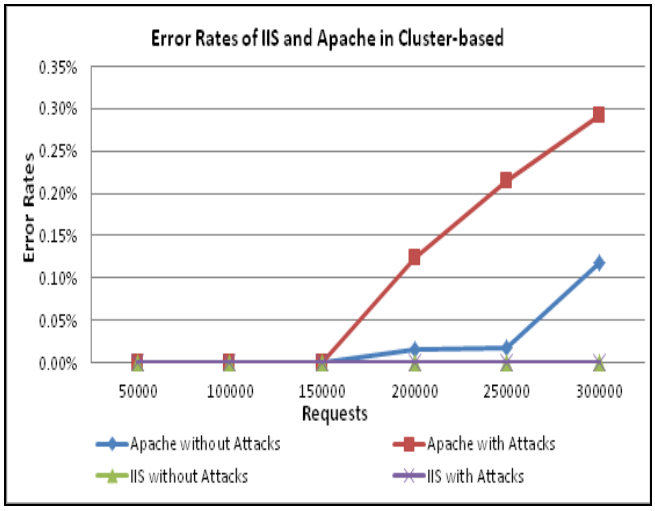

Fig. 8. Error rates of IIS and Apache in clustered based

Table 2. Average CPU usage of IIS10.0 Servers

Requests	Apache without Attack		Apache with Attack	
	1st Sever	2nd Server	1st Sever	2nd Server
50000	4.09	4.1	12.74	12.15
100000	5.64	5.68	14.72	15.38
150000	7.16	7.75	16.65	16.92
200000	8.86	8.64	19.54	17.95
250000	16.48	16.8	20.05	19.22
300000	18.18	18.58	23.01	21.39

The average CPU usage of cluster-based web servers (IIS and Apache) is explained in Table 2 and Table 3. It is clearly seen that the Apache average CPU usage is not affected by TCP SYN attack. For example, in the second test was (9.4%

for first server and 9.78% for second server) without attack and increased to (9.4% for first server and 9.6% for second server) with attack. However, the IIS was most vulnerable to attacks because the average of server's CPU usage increased significantly from (7.16% for first server and 7.75 for second server) to (16.65% for first and 16.92 for second server) with and without attack.

Table3. Average CPU usage of Apache2 Servers

Requests	IIS without Attack		IIS with Attack	
	First Sever	Second Server	First Sever	Second Server
50000	4.09	4.1	12.74	12.15
100000	5.64	5.68	14.72	15.38
150000	7.16	7.75	16.65	16.92
200000	8.86	8.64	19.54	17.95
250000	10.41	10.07	20.05	19.22
300000	12.55	12.35	23.01	21.39

VI. CONCLUSIONS

The study evaluated the performance of different web servers in cluster-based and non-cluster-based and impact of TCP SYN flood attack is analysed. The evaluation process is done under high HTTP traffic workload (50000) requests to (300000) requests in six tests. In non-cluster-based, the experimental results indicated that the IIS10.0 web server performed better performance in normal condition without attack. It also achieved the best response time from all tests and attained throughput increased regularly from (15 KB/Sec) in the first test to (90 KB/Sec) in the last test. Moreover, the average CPU usage of the IIS10.0 was less consumed compared to the other web server. However, the Apache2 web server throughput and average CPU usage was not affected by DDoS attack a lot in comparison to IIS10.0. Whereas, the throughput of Apache was (15.08 KB/Sec) in the first test and reached (90 KB/Sec) and average CPU usage utilized similarly in both cases. But IIS10.0 average CPU usage reached the highest value in the last test with attack range of (38.18%).

On the other hand, in the clustered web servers the average response time of IIS10.0 was (1 ms to 6 ms) in all tests (with and without attacks), while Apache2 accomplished worst average response time in the last test with attacks. The throughput of both web servers in cluster-based was reduced comparing to the throughput of them in non-cluster-based. Furthermore, the attack was the main reason for the increased rates off error of Apache2. However, the attack did not influence on the average CPU usage of Apache2 web servers but the IIS10.0 web servers average CPU usages was twice during attack condition. The results illustrated that using network load balancing cluster-based web servers is more appropriate technique for handling massive HTTP load traffic.

REFERENCES

[1] K. Jacksi and S. M. Abass, "Development History of the World Wide Web."

[2] L. Čegan and P. Filip, "Advanced web analytics tool for mouse tracking and real-time data processing," in *2017 IEEE 14th International Scientific Conference on Informatics*, 2017, pp. 431–435.

[3] R. Abdulkadir, M. A. Ahmed, U. F. Abdulhamid, and A. U. Diso, "Mitigation of TCP and UDP Based Distributed Denial of Service Attacks," *TEST Eng. Manag.*, vol. 82, pp. 12225–12232, Feb. 2020.

[4] K. J. A Zeebaree SRM Zeebaree, "Designing an Ontology of E-learning system for Duhok Polytechnic University Using Protégé OWL Tool," *J Adv Res Dyn Control Syst Vol*, vol. 11, no. 5, pp. 24–37, 2019.

[5] A. AL-Zebari, S. R. M. Zeebaree, K. Jacksi, and A. Selamat, "ELMS–DPU Ontology Visualization with Protégé VOWL and Web VOWL," *J. Adv. Res. Dyn. Control Syst.*, vol. Volume 11, no. 01-Special Issue, pp. 478–485, 2019.

[6] C.-P. Chen, G.-J. Lin, Y.-H. Lin, H.-P. Song, and Y.-W. Bai, "Performance measurement and queueing model of Web servers with a variation of Webpage sizes," in *2015 International Symposium on Next-Generation Electronics (ISNE)*, 2015, pp. 1–4.

[7] Z. N. Rashid, S. R. Zebari, K. H. Sharif, and K. Jacksi, "Distributed Cloud Computing and Distributed Parallel Computing: A Review," presented at the 2018 International Conference on Advanced Science and Engineering (ICOASE), 2018, pp. 167–172.

[8] M. N. Vora and D. Shah, "Estimating effective web server response time," in *2017 Second International*

Conference on Information Systems Engineering (ICISE), 2017, pp. 37–44.

[9] S. R. Zeebaree and K. Jacksi, "Effects of Processes Forcing on CPU and Total Execution-Time Using Multiprocessor Shared Memory System," *Int. J. Comput. Eng. Res. TRENDS*, vol. 2, no. 4, pp. 275–279, Apr. 2015.

[10] Y. Yan, P. Guo, B. Cheng, and Z. Zheng, "An experimental case study on the relationship between workload and resource consumption in a commercial web server," *J. Comput. Sci.*, vol. 25, pp. 183–192, 2018.

[11] K. Jacksi, N. Dimililer, and S. R. Zeebaree, "State of the Art Exploration Systems for Linked Data: A Review," *Int. J. Adv. Comput. Sci. Appl. IJACSA*, vol. 7, no. 11, pp. 155–164, 2016, doi: dx.doi.org/10.14569/IJACSA.2016.071120.

[12] M. A. Saifullah and M. M. Mohammed, "Scalable load balancing using enhanced server health monitoring and adimission control," in *2015 IEEE International Conference on Engineering and Technology (ICETECH)*, 2015, pp. 1–4.

[13] K. Jacksi, "Design And Implementation Of Online Submission And Peer Review System: A Case Study Of E-Journal Of University Of Zakho," *Int. J. Sci. Technol. Res.*, vol. 4, no. 8, pp. 83–85, 2015.

[14] K. Jacksi, S. R. M. Zeebaree, and N. Dimililer, "LOD Explorer: Presenting the Web of Data," *Int. J. Adv. Comput. Sci. Appl. IJACSA*, vol. 9, no. 1, 2018, doi: 10.14569/IJACSA.2018.090107.

[15] P. López and E. Baydal, "Teaching high-performance service in a cluster computing course," *J. Parallel Distrib. Comput.*, vol. 117, pp. 138–147, 2018.

[16] K. Jacksi, N. Dimililer, and S. R. M. Zeebaree, "A Survey of Exploratory Search Systems Based on LOD Resources," in *PROCEEDINGS OF THE 5TH INTERNATIONAL CONFERENCE ON COMPUTING & INFORMATICS*, COLL ARTS & SCI, INFOR TECHNOL BLDG, SINTOK, KEDAH 06010, MALAYSIA, 2015, pp. 501–509.

[17] M. W. P. Maduranga and R. G. Ragel, "Comparison of load balancing methods for Raspberry-Pi Clustered Embedded Web Servers," in *2016 International Computer Science and Engineering Conference (ICSEC)*, 2016, pp. 1–4.

[18] M. A. Sadeeq, S. R. Zeebaree, R. Qashi, S. H. Ahmed, and K. Jacksi, "Internet of Things Security: A Survey," presented at the 2018 International Conference on Advanced Science and Engineering (ICOASE), 2018, pp. 162–166.

[19] S. S. Kolahi, K. Treseangrat, and B. Sarrafpour, "Analysis of UDP DDoS flood cyber attack and defense mechanisms on Web Server with Linux Ubuntu 13," in *2015 International Conference on Communications, Signal Processing, and their Applications (ICCSPA'15)*, 2015, pp. 1–5.

[20] K. Jacksi, "Database Teaching in Different Universities: A Phenomenographic Research," *Int. J. Emerg. Technol. Comput. Appl. Sci.*, vol. 2, no. 12, pp. 96–100, May 2015.

[21] K. Jacksi, "Design and Implementation of E-Campus Ontology with a Hybrid Software Engineering Methodology."

[22] K. Jacksi and S. Badiozamany, "General method for data indexing using clustering methods," *Int. J. Sci. Eng.*, vol. 6, no. 3, pp. 641–644, Mar. 2015.

[23] K. Anuradha, S. N. S. Rajini, T. Bhuvaneswari, and V. Vinod, "TCP /SYN Flood of Denial of Service (DOS) Attack UsingSimulation," *TEST Eng. Manag.*, vol. 82, pp. 14553–14558, Feb. 2020.

[24] R. Ibrahim, S. Zeebaree, and K. Jacksi, "Survey on Semantic Similarity Based on Document Clustering," *Adv. Sci. Technol. Eng. Syst. J.*, vol. 4, no. 5, pp. 115–122, 2019, doi: 10.25046/aj040515.

[25] B. Singh, K. Kumar, and A. Bhandari, "Simulation study of application layer DDoS attack," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015, pp. 893–898.

[26] S. R. M. Zeebaree, R. R. Zebari, K. Jacksi, and D. A. Hasan, "Security Approaches For Integrated Enterprise Systems Performance: A Review," vol. 8, no. 12, p. 6, 2019.

[27] M. Semerci, A. T. Cemgil, and B. Sankur, "An intelligent cyber security system against DDoS attacks in SIP networks," *Comput. Netw.*, vol. 136, pp. 137–154, 2018.

[28] A. Hasso, K. Jacksi, and K. Smith, "Effect of Quantization Error and SQNR on the ADC Using Truncating Method to the Nearest Integer Bit," presented at the 2019 International Conference on Advanced Science and Engineering (ICOASE), 2019, pp. 112–117.

[29] "January 2020 Web Server Survey | Netcraft News." [Online]. Available: https://news.netcraft.com/archives/2020/01/21/january-2020-web-server-survey.html. [Accessed: 06-Mar-2020].

[30] Q. Fan and Q. Wang, "Performance comparison of web servers with different architectures: A case study using high concurrency workload," in *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*, 2015, pp. 37–42.

[31] P. Prakash, R. Biju, and M. Kamath, "Performance analysis of process driven and event driven web servers," in *2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO)*, 2015, pp. 1–7.

[32] T. Bezboruah and A. Bora, "Performance evaluation of hierarchical SOAP based web service in load balancing cluster-based and non-cluster-based web server," *Int. J. Inf. Retr. Res. IJIRR*, vol. 5, no. 4, pp. 19–30, 2015.

[33] L. P. Chitra and R. Satapathy, "Performance comparison and evaluation of Node. js and traditional web server (IIS)," in *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*, 2017, pp. 1–4.

[34] J. E. C. de la Cruz and C. A. R. Goyzueta, "Design of a high availability system with HAProxy and domain name service for web services," in *2017 IEEE XXIV International Conference on Electronics, Electrical*

Engineering and Computing (INTERCON), 2017, pp. 1–4.

[35] R. Papadie and I. Apostol, "Analyzing websites protection mechanisms against DDoS attacks," in *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2017, pp. 1–6.

[36] Y.-L. Liu, C.-T. Shih, Y.-J. Chang, S.-J. Chang, and J. Wu, "Performance enhancement of a Web-based picture archiving and communication system using commercial off-the-shelf server clusters," *BioMed Res. Int.*, vol. 2014, 2014.

[37] E. Konidis, P. Kokkinos, and E. Varvarigos, "Evaluating Traffic Redirection Mechanisms for High Availability Servers," in *2016 IEEE Globecom Workshops (GC Wkshps)*, 2016, pp. 1–5.

[38] S. K. Mishra, B. Sahoo, and P. P. Parida, "Load balancing in cloud computing: a big picture," *J. King Saud Univ.-Comput. Inf. Sci.*, 2018.

[39] "An Introduction to HAProxy and Load Balancing Concepts," *Easy Cloud*. [Online]. Available: http://easycloudsupport.zendesk.com/hc/en-us/articles/360001916092-An-Introduction-to-HAProxy-and-Load-Balancing-Concepts. [Accessed: 06-Mar-2020].

[40] A. B. Prasetijo, E. D. Widianto, and E. T. Hidayatullah, "Performance comparisons of web server load balancing algorithms on HAProxy and Heartbeat," in *2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, 2016, pp. 393–396.

[41] R. Abbas, Z. Sultan, and S. N. Bhatti, "Comparative analysis of automated load testing tools: Apache jmeter, microsoft visual studio (tfs), loadrunner, siege," in *2017 International Conference on Communication Technologies (ComTech)*, 2017, pp. 39–44.

[42] B. Erinle, *Performance Testing with JMeter 3*. Packt Publishing Ltd, 2017.

[43] S. R. Zeebaree, K. F. Jacksi, and R. R. Zebari, "Impact analysis of SYN flood DDOS attack on HAPROXY and NLB cluster-base web servers," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 19, no. 1, Jul. 2020, doi: 10.11591/ijeecs.v19.i1.pp%p.

[44] D. Kshirsagar, S. Sawant, A. Rathod, and S. Wathore, "CPU load analysis & minimization for TCP SYN flood detection," *Procedia Comput. Sci.*, vol. 85, pp. 626–633, 2016.

[45] S. Ali, "Managing Large-Scale Infrastructure," in *Practical Linux Infrastructure*, Springer, 2015, pp. 1–24.