International Journal of Safety and Security Engineering
Vol. 12, No. 5, October, 2022, pp. 577-588
Journal homepage: http://iieta.org/journals/ijsse

Network Forensics Against Volumetric-Based Distributed Denial of Service Attacks on Cloud and the Edge Computing

Anton Yudhana[1], Imam Riadi[2], Sri Suharti[3*]

[1] Department of Electrical Engineering, Universitas Ahmad Dahlan, Yogyakarta 55164, Indonesia
[2] Department of Information System, Universitas Ahmad Dahlan, Yogyakarta 55164, Indonesia
[3] Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta 55164, Indonesia

Corresponding Author Email: sri2007048006@webmail.uad.ac.id

https://doi.org/10.18280/ijsse.120505

Received: 8 September 2022
Accepted: 15 October 2022

Keywords:
cloud computing, DDoS, edge computing, firewall, ICMP-flood

ABSTRACT

Cyber attacks are increasingly rampant and even damage the reputation of companies, agencies, and services. DDoS attacks have been overgrowing in the last year, which has resulted in substantial losses. Volumetric-based Distributed Denial of Service (DDoS) is a hazardous attack type because it can consume server resources, causing the server to be unable to serve customer requests. The network design consisting of hardware and software becomes the essential capital that is a determinant of the quality of a network in the long term. A firewall is one way to stop the occurrence of DDoS. Forensics and mitigation in this study apply Packet Filtering Firewall and Circuit Level Gateway Firewall against ICMP-Flood DDoS attacks. The research methodology is a simulated experiment on cloud and edge computing networks. Forensics and mitigation in cloud computing are carried out at layer 3, the Internet Protocol layer TCP/IP model, by applying a Packet-Filtering Firewall with a success rate of 64%-69% traffic reduction. In contrast, the success of reducing server resource usage is 73.75%. At the same time, Edge computing is carried out at layer 4, namely the Transport Protocol layer TCP/IP model, by applying a Circuit-Level Gateway Firewall with a success rate of reducing traffic by 55%-98.88%. In comparison, the success of lowering server resource usage is 96% and restoring traffic and paralyzed servers to normal position.

1. INTRODUCTION

Edge computing refers to processing, analyzing, and storing data closer to where it is generated to enable rapid, near-real-time analysis and response. Some companies have consolidated operations in recent years by centralizing data storage and computing in the cloud. Cloud computing is being pushed to its limits by the needs of the services and applications it supports, from data storage and processing to system responsiveness. Cyber attacks are currently experiencing an exciting development with various targets and patterns [1-5]. DDoS is a malicious attack that blocks the traffic of a server service by flooding the target or the surrounding infrastructure [6-8]. Millennials are targets and attackers to disrupt and undermine reputation. Business competition is straightforward with DDoS attack tricks because all business processes use computer networks and the internet [9-12]. Delivery of DDoS in large quantities or often referred to as botnets will cause servers to freeze and last for days, causing companies, agencies, and business people to lose big [13-15]. Kaspersky Laboratories and International B2B stated the results of their research on DDoS caused enormous losses to the company's online resources by crippling the company's online services with an average loss of $52,000 to $444,000 [16]. Kaspersky DDoS Intelligence also mentioned that in the second quarter of the year compared to the first quarter of 2020, DDoS increased sharply by 30% almost every day. On April 9, 2020, Kaspersky DDoS Intelligence also mentioned that in the second quarter of the year compared to the first quarter of 2020, DDoS increased sharply by 30% almost daily. On April 9, 2020, the second quarter of a DDoS attack occurred with a volume of nearly 300 attacks, and in the first quarter of 2020, there were 242 attacks compared to 2018. Akamai NETSCOUT Arbor also confirmed a DDoS attack in March 2018 of 1.7 Tbps [17], this was also stated by Securelist mentioned that in the first quarter of 2020, there was an 80% increase in DDoS from the previous year. Kaspersky DDoS Intelligence provides information that in the eighth week of 2022, February 21-27 22 the peak of DDoS attacks occurring on February 25, 2022 [18]. DDoS attacks from quarter to the next quarter saw a significant increase with a very extraordinary volume reaching Terabyte, launched continuously. The main motive for DDoS attacks is to drop server performance through network traffic so that it cannot serve customer requests [19-21]. In 2022 according to Kaspersky, DDoS intelligence DDoS has increased by 4.5 times from the previous year, a very drastic increase; this is the highest DDoS attack of all time and lasts a long time. DDoS attacks were detected in 44.34%, with targets in the United States at 45.02% of all targets.

The most significant DDoS attacks were on Sundays lasting less than 4 hours, with some 94.95% of attacks lasting approximately 23 days or 549 hours [18]. China is one of the deviant bots that attack the SSH honeypot as much as 20.41%, and Telnet attacks bots as much as 41.21% [22, 23]. Big companies that have become victims of DDoS are Github,

Amazon Web Service, Cloudflare and Bank of America [24]. Cyber security company Tech Radar Pro stated in 2021 that DDoS attacks continue to increase using 33 protocols to target both webservers and servers, especially with the attack that can be carried out efficiently and virtually; this attack can also be carried out by multiplying attacks to bring down the target network and server [25, 26]. According to Akmay, DDoS can attack with 800 Gbps powerful attacks targeting gambling in Europe with gradual attacks, and the first stage was carried out in August 2022 at 200 Gbps and ended in September 2020 at 500 Gbps. In February 2021, it increased to 800 Gbps. According to anti-DDoS, Radware stated in August and September of 2020 that it would have to pay 10 bitcoins to stop a DDoS attack.

Based on data on the increase in DDoS, the high risk, and a large amount of loss for individuals and organizations, it is necessary to research DDoS detection as the basis for developing a reliable and affordable security system. This security system can detect and prevent DDoS so that the server is reliable in facing the development of attacks in the cyber world, and losses can be minimized. DDoS attacks have been overgrowing in the last year. The trend is shorter attack duration with a much larger attack volume per second, resulting in huge losses. Network quality and server quality in such a way that customer satisfaction and the reputation of a business or non-business organization, community, or individual are very dependent on the resources that have been built by the organization or individual so that the network design consisting of hardware and software becomes the essential capital that as a determinant of the quality of a network in the long term. Conventional detection techniques for DDoS attacks require extensive and expensive computations, both hardware and software, but this research proposes an easy and inexpensive way to detect and stop Volumetric-based DDoS on ICMP-Flood, namely a network security system with firewall filtering tested at layer 3 and layer 4 on the cloud network and the edge network. This study aims to maintain the web server's performance from ICMP-Flood DDoS attacks using a Firewall. Two variables used in this study consist of fixed and independent variables, fixed variables on DDoS, namely ICMP-Flood DDoS, and independent variables on packet filtering Firewalls on Cloud Environment Networks and Edge Environment Networks. Research results state that Circuit Level Gateway Firewall that works at layer 4 TCP/IP model maintains network quality by 87.00%. In comparison, Packet Filtering Firewall works at layer 3 TCP/IP model and maintains network quality by 70.25% in stopping DDoS-based volumetric on ICMP-Flood.

2. MATERIALS AND METHODS OF RESEARCH

2.1 Distributed Denial of Service (DDoS)

A Denial of Service (DDoS) attack is a malicious distributed attack on an online network that becomes disabled for users, and this DDoS attack will burden and paralyze server services [27-30]. The distribution of DDoS in a global attack will infiltrate various devices, which are often referred to as botnets. A very dangerous DDoS attack works by flooding traffic through a network connection, indicating a slow service or service is lost or unavailable. DDoS in some investigations flooding the server indicates a single or range of DDoS, in some investigations flooding the server, indicates a single or range of Internet Protocol (IP) addresses, traffic flooding in device or web browser usage, and high demand as unexplained spikes in a single endpoint. In addition, there are abnormal patterns every 5 minutes or other abnormal clock patterns. The general description of DDoS is as follows in Figure 1.

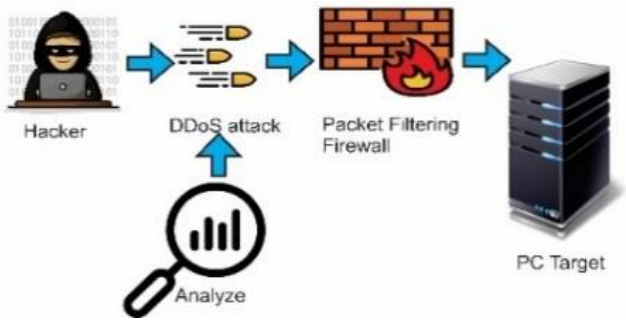


Figure 1. DDoS block diagrams

2.2 System models

This research uses Cloud Network and Edge Network Environment in running DDoS network forensics based on Volumetric ICMP-Flood.

2.2.1 Cloud network environment

Cloud Network Environment is a new technology that works with shared hosts, providing distributed access and virtualization [23]. On Cloud Network Environment, it works with VirtualBox and GNS3 software as a cloud network environment provider. This Cloud Network applies the use of a web server with the Ubuntu operating system, while the DDoS attacks based on Volumetric DDoS ICMP Flood use the KaliLinux operating system, which is at layer 3, which is realistic and valid. Cloud Network Environment implements DDoS ICMP-Flood using the KaliLinux operating system, while forensics and mitigation to prevent DDoS in this study apply the use of Packet Filtering Firewall with Fortigate operating system, which is implemented on layer 3 TC/IP model. The design of the Cloud Network Environment in this study is shown in Figure 2.

Figure 2 describes the Cloud Network Environment Design chart on GNS3, providing information on the use of computer network hardware and software in DDoS attack forensics. The black band indicates the use of network cables. KaliLinux is an attacker who will attack the web server on the Ubuntu operating system. Cloud Network Environment configuration data for each device is shown in Table 1.

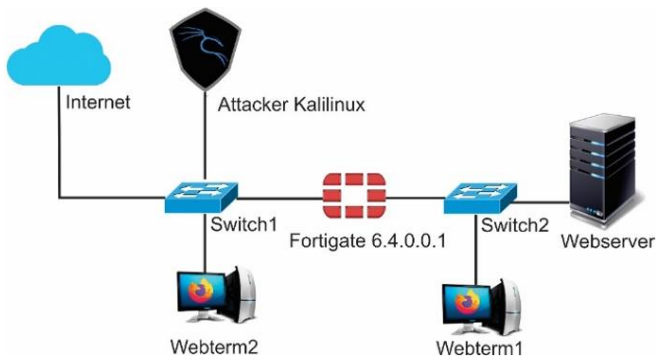


Figure 2. Design cloud network environment

Table 1. Cloud network environment configuration

Device	Software	Port	IP address
Web Server	Win. Server Os	Port 1	192.168.2.55/24
Webterm 1	FireFox	NIC	192.168.2.3/24
Firewall	Fortigate 6.4	Port 1 Port 2	192.168.56.106/24 192.168.2.1/24
Switch 1	-	NIC	-
Switch 2	-	NIC	-
Webterm 2	FireFox	NIC	192.168.56.110/24
Attacker	KaliLinux 2018 ICMP- Flood	NIC	192.168.56.99/24

Table 1 shows that this research consists of 7 main devices consisting of one PC web server with Ubuntu, two PC web terms with Firefox software, two switches as network connectors, a PC Attacker with the Kali Linux operating system as an ICMP-Flood based on Volumetric. The network configuration has two networks, namely 192.168.2.0/24 and 192.168.56.0/24.

2.2.2 Edge network environment

Edge Network Environment is a technology on computer networks that implements hardware and software that resides on the device or the endpoint of the device. All devices can communicate between one device and another device face-to-face. Edge Network Environment is a technology that works on shared hosts to provide distributed access in real time. In the Edge Network Environment using a Web Server with the Windows Server 2019 operating system, the attacker implements the ping of death software as a volumetric-based ICMP-Flood DDoS. Meanwhile, network forensics uses Wireshark and, as DDoS prevention, implements Circuit-Level Gateway Firewall on Mikrotik Router hardware. The design of the Edge Network Environment in this study is shown in Figure 3.

Figure 3 describes Edge Network Environment Design chart providing information on the use of computer network hardware and software in DDoS attack forensics. The black line shows the use of a network UTP cable with a different network, the attacker's PC will attack using Windows 10 with Ping of Death. At the Edge Network, Environment configuration data for each device is shown in Table 2.

Table 2 shows At the Edge Network Environment Configuration in this study consisting of 8 main devices consisting of one web server with the Windows Server 2019 operating system; one Mikrotik RB951Ui-2HnD RouterBoard as a forensic and firewall tool; Three PCs with Windows 10 operating system as a traffic comparison; two switches as network connectors; one Attacker with Windows 10 operating system with Ping of Death application as Volumetric-based ICMP Flood. The network configuration has two networks, namely 192.168.200.0/ 24 and 192.168.100.0/24.

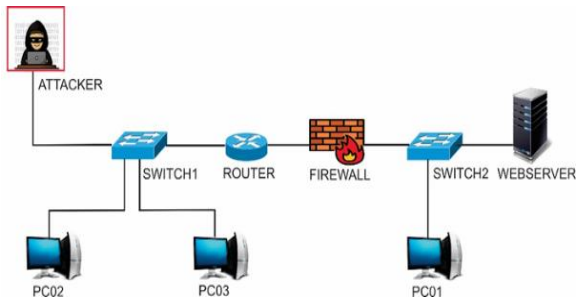


Figure 3. Design edge network environment

Table 2. Edge network environment configuration

Device	Software	Port	IP address
PC01	Windows 10	NIC	192.168.200.30/ 24
Web Server	Windows Server 2019	NIC	192.168.200.10/ 24
RouterBoard Mikrotik RB951Ui-2HnD	Firewall	Eth1	192.168.200.1 / 24
		Eth2	192.168.100.1 / 24
PC01	Windows 10	NIC	192.168.100.31/ 24
PC02	Windows 10	NIC	192.168.100.32/ 24
Attacker	Windows 10 ICMP-Flood	NIC	192.168.100.30/ 24
Switch 1	-	NIC	-
Switch 2	-	NIC	-

2.3 Proposed approach

This study aims to experiment with the Cloud and Edge Network Environment in the case of DDoS attacks on computer networks.

2.3.1 Research subject

The research subjects used were the Cloud network and the Edge Network Environment with KaliLinux as a DDoS Attacker and Ubuntu on the target server. The strength of cloud computing is that it is easy to manage and free to choose the device; if one device is not compatible, it can be replaced with another device. In cloud computing, apply a packet filtering firewall at layer 3 with Fortigate software to stop DDoS attacks that interfere with network traffic by dropping servers.

2.3.2 Stages of experimental research

This experimental type of research consists of three first stages, namely the scanning phase by simulating an attack on the target server by disrupting traffic using ICMP-Flood volumetric-based DDoS. The second stage of the preventive phase includes the forensic process on the network, namely looking for suspected IPs and illegal IPs, analyzing the number of packets and the number of bytes, and analyzing traffic anomalies. The third or final stage is mitigation, as the process of implementing packet filtering firewalls to stop and prevent ICMP-Flood volumetric-based DDoS properly. The experimental flow in this study is shown in Figure 4.

Figure 4 providing information on the stages of experimental research work on forensics and network mitigation DDoS has seven steps that do not interfere with the occurrence of connections or network traffic and devices. The first stage is to search and find traffic that has the potential to disrupt network traffic going to the server. The second stage is a static analysis that detects the characteristics of an illegal attack as a suspected DDoS. The third stage is the dynamic analysis which detects the characteristics of illegal attacks on cloud and edge computing networks. The fourth stage analyzes illegal attacks through behaviour patterns of log activities on network traffic according to the criteria in the Access Control List. The fifth stage decides whether the attack is an ICMP-Flood DDoS or not. The sixth stage prevents ICMP-Flood DDoS attacks by implementing a Firewall. The seventh stage is to obtain the percentage of Firewall test results at layers 3

and 4 as forensics and mitigation in cloud networks and edge computing networks.

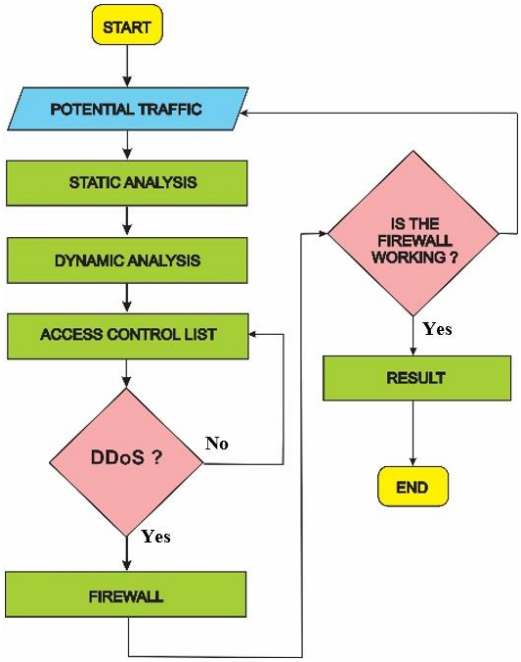


Figure 4. Flow of experimental research stages

3. RESEARCH RESULTS AND ANALYSIS

The following are the results of DDoS forensic research using packet filtering firewalls in the cloud and the edge network environment that allow ICMP-Flood prevention or risks to traffic and target servers on the network.

3.1 Potential traffic

Forensic preparation and mitigation in the test environment are carried out with volumetric-based DDoS attacks on web servers that implement ICMP-Flood Ping of Death on cloud and edge computing networks. The tools used in cloud computing network environment forensics and mitigation are shown in Table 3, while the edge network environment forensics and mitigation tools are shown in Table 4 as follows.

Table 3. Tool cloud computing network

No	Tool	Version	Function
1.	KaliLinux	Kali2018 Linux 2.6/3.x/4.x(64-bit)	DDoS ICMP-Flood
2.	Web Server	Turnkeylinux/Word press:latest	Web Server
3.	WebTerm	Webterm	Network Test Host
4.	Fortigate	6.4.0.0	Forensic and mitigation
5.	Fortigate	6.4.0.0	Packet Filtering Firewall

Table 3 describes forensic tools in the cloud network environment as support for volumetric-based DDoS mitigation on the ICMP protocol, namely KaliLinux as a DDoS tool, Fortigate to capture traffic logs, and Packet Filtering Firewall.

Table 4. Tool edge network environment

No	Tool	Version	Function
1.	Ping of Death	-	DDoS ICMP-Flood
2.	Wireshark	Version 3.4.8 (v3.4.8-0-g3e1ffae201b8)	Traffic Capture
3.	Mikrotik	951ui-2Hnd	Forensic and mitigation
4.	Mikrotik	951ui-2Hnd	Circuit-Level Gateway Firewall

Table 4 describes forensic tools on the Edge Network Environment as support for volumetric-based DDoS mitigation on the ICMP protocol, namely Ping of Death as a DDoS tool, Wireshark for capturing traffic logs, and Mikrotik as Circuit-Level Gateway Firewall.

3.2 Analyze ICMP-Flood DDoS attack virtual interface on cloud network environment

Analysis of the ICMP-Flood DDoS attack interface on the cloud Network Environment includes server development, client development, attack process, and mitigation. Some of these jobs will appear to run smoothly through the testing stages, namely testing connectivity from web term to server during normal conditions, testing during DDoS attacks to target servers, and implementing a Packet Filtering Firewall. The analysis of the test results is as follows:

3.2.1 Analysis of testing readiness results from KaliLinux attacker to server on cloud network environment

The results of the static analysis to determine the ICMP-Flood DDoS characteristics in the Cloud Network Environment and apply the ping of Death tool running on the KaliLinux operating system has a one-time limit value in sending and receiving data packets from the connectivity from the KaliLinux Attacker to the target Ubuntu web server as shown in Table 5.

Table 5. Testing readiness from Kalilinux attacker to server on cloud network environment

No.	Property	Status
1	Link encap	Local Loopback
2	Inet addr	127.0.0.1/24
3	Up loopback running MTU	65536
4	Metric	1
5	Rx packet error	0
6	Rx dropped	0
7	Over runs	0
8	Frame	0
9	Tx packet error	0
10	Tx dropped	0
11	Over runs	0
12	Carrier	0
13	Collision	0

Table 5 describes virtual network communication on its computer on the loopback device given by the IP address 127.0.0.1/24 with mask 255.255.255.0, which is mapped from localhost with a network adapter with the name Lo. This server resource is running on its computer and running automatically, which will be used for troubleshooting and early diagnostics.

Table 6. DDoS attacker network connectivity test results before an attack is carried out on the target server

No	Second to-	IP address source	IP address target	icmp_seq	ttl	Time (ms)
1	1	192.168.56.99	192.168.2.55	1	63	9.16
2	2	192.168.56.99	192.168.2.55	2	63	7.15
3	3	192.168.56.99	192.168.2.55	3	63	14.3
4	4	192.168.56.99	192.168.2.55	4	63	5.34
5	5	192.168.56.99	192.168.2.55	5	63	6.95
6	6	192.168.56.99	192.168.2.55	6	63	3.76
7	7	192.168.56.99	192.168.2.55	7	63	6.12
8	8	192.168.56.99	192.168.2.55	8	63	5.84
9	9	192.168.56.99	192.168.2.55	9	63	5.57
10	10	192.168.56.99	192.168.2.55	10	63	4.72

Table 7. Connectivity test results during an attack from an ICMP-Flood DDoS attacker to a server in the network environment cloud C

No	Second to-	IP address source	IP address target	icmp_seq	ttl	Time (ms)
1	1	192.168.56.99	192.168.43.2	487	255	75.213
2	2	192.168.56.99	192.168.43.2	488	255	147.792
3	3	192.168.56.99	192.168.43.2	489	255	92.125
4	4	192.168.56.99	192.168.43.2	490	255	52.506
5	5	192.168.56.99	192.168.43.2	491	255	106.960
6	6	192.168.56.99	192.168.43.2	492	255	94.054
7	7	192.168.56.99	192.168.43.2	493	255	58.340
8	8	192.168.56.99	192.168.43.2	494	255	82.966
9	9	192.168.56.99	192.168.43.2	495	255	82.236
10	10	192.168.56.99	192.168.43.2	496	255	98.630

3.2.2 Analysis of connectivity test results before the attack from the ICMP-Flood DDoS attacker on the server in the cloud network environment

Analysis of network connectivity testing before an attack from a DDoS Attacker with IP number 192.168.56.99 to the target server with IP 192.168.43.2 in 10 times sending and receiving data on the ICMP protocol has the results as shown in Table 6.

Table 6 describes the IP address of the web server, namely 192.168.2.55, ICMP_seq=1 with an increment of 1, which means that the packet number sent sequentially from 1 to 10 indicates that the packet was sent and responded to appropriately and no packets were lost. This ICMP will provide information and report network errors if the destination can be connected or cannot be connected or reachable, besides the ICMP also reports errors and other information based on the Processing of IP packets back to the source. TTL=63 is a packet that is not lost and goes through the same device and path because every ping has the same TTL. The round-trip information for sending fast packets is indicated by the time less than 1 second from each client before a DDoS attack occurs. Analysis of Connectivity Test Results Before the attack from the ICMP-Flood DDoS Attacker on the server in the Cloud Network Environment.

3.2.3 Analysis of connectivity test results during an attack from an ICMP-Flood DDoS attacker to a server in the cloud network environment

Before the attack, analysis of network connectivity testing from a DDoS Attacker with IP number 192.168.56 99 to the target server with IP 192.168.2.55 in 10 times sending and receiving data on the ICMP protocol has the results as shown in Table 7.

Table 7 describes the IP address of the target web server 192.168.2.55, icmp_seq=1 from numbers 487 to 496, which states the serial number of packets sent sequentially with packets sent and responded to correctly and no packages lost, TTL=255 is a packet not lost and through the same device and the same path because from every ping has the same TTL. Time shows round-trip information for fast packet delivery; this is indicated by a time that is more than 15 minutes on each sequence; this shows the connectivity of each client when a DDoS attack occurs is very long and the path is congested, and the server cannot serve the client slows in responding so Request Time Out (RTO).

3.2.4 Resources performance analysis before the attack from the ICMP-Flood DDoS attacker to the server in the cloud network environment

Resources performance before the attack from the ICMP-Flood DDoS Attacker to the server in the Cloud Network Environment, resources usage anomaly occurred as shown in the picture on July 20, 2022, at 07.39 to 07.50 AM. The figure of resource usage performance before the ICMP-Flood DDoS is established as shown in Figure 5.

Figure 5 shows the occurrence of CPU usage anomalies starting at 07.39 to 07.40 PM by 4%, at 07.45 to 07.46 PM by 24%, from 07.48 to 07.49 PM by 36%, and from 07.49 to 07.50 PM by 4%. This shows that the CPU usage anomaly is not more than 50% and the server is running well and normally, and the server can be reached from the client properly.

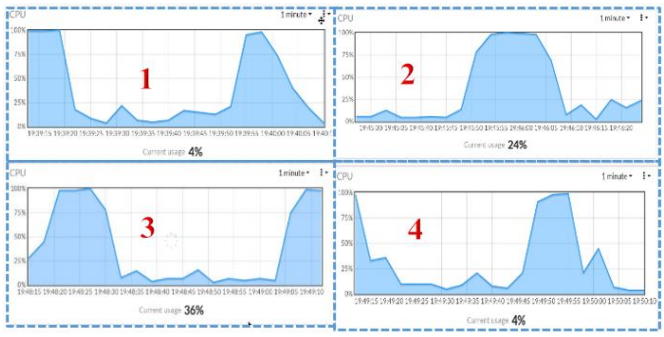


Figure 5. Resources performance analysis before the attack in the cloud network environment

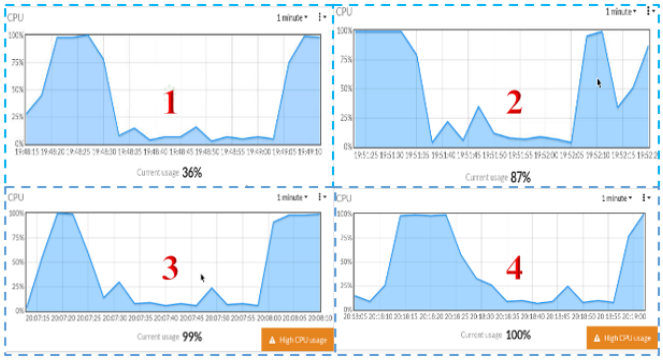


Figure 6. Resources performance analysis during attack in the cloud network environment

3.2.5 Analysis of resource performance during an attack from an ICMP-Flood DDoS attacker to a server in the cloud network environment

Resource performance during an attack from an ICMP-flood DDoS Attacker to a server in the Cloud Network Environment, an anomaly in resource usage occurs, as shown in the figure on July 21, 2022, from 01.37 to 01.54 AM. The formation of the performance of resource usage after the ICMP-flood DDoS is shown in Figure 6.

3.2.6 Analysis of packet filtering firewall in forensics and mitigation of ICMP-Flood DDoS attacker to the server in cloud network environment

Packet Filtering Firewall limits the IP to the server through layer 3 by embedding the Fortigate Firewall Policy with the configuration shown in Table 8.

Table 8. Analysis of packet filtering firewall

No.	Policy	Status
1.	Name	Block PC1 to Web server
2.	Incoming Interface	LAN (Port2)
3.	Outgoing Interface	Port1
4.	Source	PC1
5.	Destination	Web server
6.	Schedule	always
7.	Service	PING
8.	Action	ACCEPT

Based on the configuration in Table 8. shows the name of the Packet Filtering Firewall setting is Block PC1 to Web Server with PC1 as ICMP-Flood DDoS Attacker, Incoming LAN interface on port2, outgoing interface using port1, PC1 source and destination is a web server. Scheduling is always done with the service connected to PING correctly, and Action: ACCEPT to Block PC1 to Web Server. The analysis of connectivity testing when the Firewall is applied with the attack path from IP address 192.168.56.99 to the target server with IP 192.168.2.55 in 10 times sending and receiving data on the ICMP protocol has the results as shown in Table 9.

Table 9 specifies the IP address of the target web server 192.168.2.55, icmp_seq=1 from numbers 1 to 10, which states the serial number of packets sent sequentially with packets being sent and responded to correctly and no packages lost. This ICMP will provide information and report network errors if the destination can be connected or cannot be connected or reachable. The ICMP reports errors and other information based on processing IP packets back to the source. TTL=63 is a packet that is not lost and goes through the same device and path because every ping has the same TTL. Round-trip information for fast package delivery is shown in less than 1 second. This indicates that after the implementation of the Packet Filtering and Firewall connectivity is back to running as before the DDoS attack occurred. The results of testing the success of the Packet Filtering Firewall can be seen in the performance of server resources, shown in Figure 7.

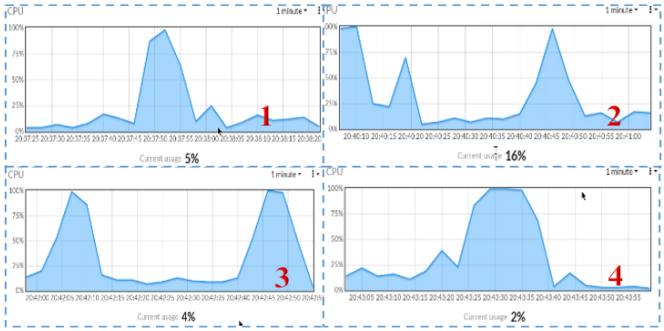


Figure 7. The results of testing the success of packet filtering firewall

Figure 7 shows sampling of occurrences after configuring packet filtering Firewall on Fortigate resource usage anomaly on July 21, 2022, at 8:37 to 8:43 in the first minute of resource usage by 5%, first minute 16%, third minute 4%, and last minute by 2%. This shows that the anomaly of using all resources is very light, and the server performance is smooth. The traffic runs smoothly, so installing a packet filtering Firewall at layer 4 has succeeded in stopping the occurrence of ICMP-Flood DDoS.

3.2.7 Interface readiness analysis before an ICMP-Flood DDoS attack occurs on the edge network environment

Analysis of network connectivity testing before an attack from a DDoS Attacker with an IP address of 192.168.0.1 to a target server with an IP address of 192.168.0.200 in 10 times sending and receiving data on the ICMP protocol has the results as shown in Table 10.

Table 10 describes the IP address of the target web server, which is 192.168.0.200, with the Attacker's IP address 192.168.0.1; Reply shows the answer from the host giving a reply. TTL is the time duration in seconds to record data packets in the network, which is 128 ms. Time is the response time required from the host below 100ms, which is under 1 ms, and the network looks very smooth and sound, while the number of data packets sent through the Windows Operating System is 32 bytes. This indicates that the amount of data transmitted is average.

3.2.8 Interface analysis during ICMP-Flood DDoS attacks on the edge network environment

Before the attack, analysis of network connectivity testing from a DDoS Attacker with an IP address of 192.168.0.1 to a target server with an IP address of 192.168.0.200 in 10 times sending and receiving data on the ICMP protocol has the results as shown in Table 11.

Table 11 explains the IP address of the target web server, which is 192.168.0.200 with the attacker's IP address 192.168.0.1; Reply shows the answer from the host giving a reply, while Request time out (RTO) is that the sending host has not received a response from the server because the traffic is hefty. Destination unreachable indicates that the server is truly unavailable. TTL is the time in seconds to record data packets in the network, 128 ms, until the request time out

cannot be detected. Time is the response time required from the host below 100ms, which is taken from 16 ms to 1054 ms, and it looks like the smooth network is down, while the number of data packets sent through the Windows Operating System is 65500 bytes. This shows that the traffic and data packets sent are very dense and the server is down.

3.2.9 Analysis of server resource performance before an ICMP-Flood DDoS attack occurs in the edge network environment

Server resources performance before the attack from the ICMP-Flood DDoS Attacker to the server on the Edge Network Environment, Resource usage anomaly occurred as shown in Figure 8.

Figure 8 shows resource usage before the DDos Attack with 62% usage performance, maximum speed = 2.00 GHz, L1 cache = 128 KB, L2 cache = 512 KB, and L3 cache = 6 MB. With the number of sockets = 1 with cores = 2 and logical processors = 2. This shows that CPU performance decreased by 100% in serving clients with only 10 attacks, so the server went down, which was seen in network connectivity when an attack occurred.

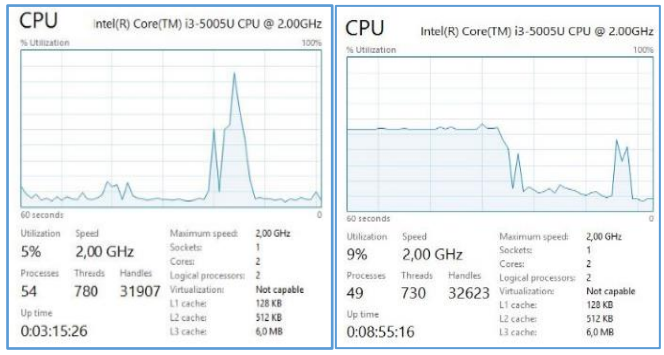


Figure 8. The figure of resource performance before the attack from the ICMP-Flood DDoS attacker to the server on the edge network environment

3.2.10 Analysis of circuit-level gateway firewall in forensics and mitigation of ICMP-Flood DDoS attacker to the server in edge network environment

Circuit-Level Gateway Firewall restricts IP that goes to the server through layer 4 by embedding Filter Rule Firewall Policy on the router with the configuration as shown in Table 12.

Table 9. Circuit-level gateway firewall connectivity test results

No	Second to-	IP address source	IP address target	icmp_seq	ttl	Time (ms)
1	1	192.168.56.99	192.168.2.55	1	63	16.6
2	2	192.168.56.99	192.168.2.55	2	63	5.16
3	3	192.168.56.99	192.168.2.55	3	63	7.88
4	4	192.168.56.99	192.168.2.55	4	63	6.22
5	5	192.168.56.99	192.168.2.55	5	63	5.50
6	6	192.168.56.99	192.168.2.55	6	63	6.28
7	7	192.168.56.99	192.168.2.55	7	63	6.45
8	8	192.168.56.99	192.168.2.55	8	63	8.75
9	9	192.168.56.99	192.168.2.55	9	63	7.24
10	10	192.168.56.99	192.168.2.55	10	63	5.96

Table 10. Test results of DDoS attacker network connectivity before attacking the target server

No	Second to-	IP address source	IP address target	icmp_seq	ttl	Time (ms)
1	1	192.168.0.1	192.168.0.200	Reply	128	32
2	2	192.168.0.1	192.168.0.200	Reply	128	32
3	3	192.168.0.1	192.168.0.200	Reply	128	32
4	4	192.168.0.1	192.168.0.200	Reply	128	32
5	5	192.168.0.1	192.168.0.200	Reply	128	32
6	6	192.168.0.1	192.168.0.200	Reply	128	32
7	7	192.168.0.1	192.168.0.200	Reply	128	32
8	8	192.168.0.1	192.168.0.200	Reply	128	32
9	9	192.168.0.1	192.168.0.200	Reply	128	32
10	10	192.168.0.1	192.168.0.200	Reply	128	32

Table 11. Analysis during ICMP-Flood DDoS attacks on edge network environment

Sec to	IP address source	IP addres target	Status	TTL	Byte	Time (ms)
1	192.168.0.1	192.168.0.200	Reply	128	65500	16
2	192.168.0.1	192.168.0.200	Reply	128	65500	148
3	192.168.0.1	192.168.0.200	Reply	128	65500	1291
4	192.168.0.1	192.168.0.200	Reply	128	65500	1291
5	192.168.0.1	192.168.0.200	Reply	128	65500	1296
6	192.168.0.1	192.168.0.200	Reply	128	65500	1305
7	192.168.0.1	192.168.0.200	Reply	128	65500	1054
8	192.168.0.1	192.168.0.200	RTO	-	-	-
9	192.168.0.1	192.168.0.200	RTO	-	-	-
10	192.168.0.1	192.168.0.200	Desti-nation Un-reacheable	-	-	-

Table 12. Analysis of circuit-level gateway firewall ICMP-Flood DDoS attacks on edge network environment

No.	Policy	Status
1.	Name	Block ping Router
2.	Src. Address	192.168.100.2
3.	Dst. Address	192.168.100.1
4.	Protocol	ICMP
5.	Chain	Input
6.	Action	DROP

Based on the configuration in Table 12 shows the name of the Block ping Router setting is Block 192.168.100.2 as an ICMP-Flood DDoS Attacker that goes to the server with IP 192.168.100.1, INPUT Chain, the protocol used is ICMP, Scheduling is always done when the IP connects then Action: DROP so that it can't communicate or can't attack the target server. The results after forensics and mitigation with the Packet Filtering Firewall are shown in Table 13.

Table 13 describes the IP address of the target web server as 192.168.43.2, while the Attacker's IP Address is 192.168.56.99. Icmp_Seq=1 from numbers 14 to 23, which states the serial number of the packets sent sequentially with the packets being sent and responded to properly and no packets lost. This ICMP will provide information and report network errors if the destination can be connected or cannot be connected or reachable. Besides that, ICMP also reports errors and other information based on processing IP packets back to the source. TTL=63 is a packet that is not lost and goes through the same device and path because every ping has the same TTL. Time is the response time required from the host below 100 ms, which is between 7.21 ms to 48.4 ms, meaning smooth. This shows that after the implementation of the Packet Filtering Firewall, connectivity will resume as before the DDoS attack.

Figure 9 shows resource usage after Circuit-Level Gateway Firewall with 94% usage performance, maximum speed = 2.00 GHz, L1 cache = 128 KB, L2 cache = 512 KB, and L3 cache = 6 MB. With the number of sockets = 1 with cores = 2 and logical processors = 2. This shows resources performance generally by 91% in serving clients, so the server was seen in network connectivity.

Table 13. The results after doing forensics and mitigation with circuit-level gateway firewall

No	Second to-	IP Address Source	IP Address Target	icmp_seq	ttl	Time (ms)
1	1	192.168.56.99	192.168.43.2	14	63	14.6
2	2	192.168.56.99	192.168.43.2	15	63	30.2
3	3	192.168.56.99	192.168.43.2	16	63	11.4
4	4	192.168.56.99	192.168.43.2	17	63	15.9
5	5	192.168.56.99	192.168.43.2	18	63	22.0
6	6	192.168.56.99	192.168.43.2	19	63	33.1
7	7	192.168.56.99	192.168.43.2	20	63	17.21
8	8	192.168.56.99	192.168.43.2	21	63	48.4
9	9	192.168.56.99	192.168.43.2	22	63	13.4
10	10	192.168.56.99	192.168.43.2	23	63	7.21

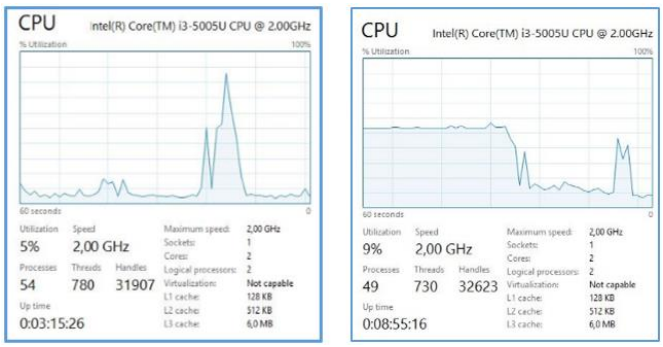


Figure 9. Resource performance after circuit-level gateway firewall on the edge network environment

4. DISCUSSION

Forensics and Distributed Denial of Service mitigation on cloud computing networks and Edge Networks have their differences and advantages. On Cloud Networking, DDoS quickly disrupts server services, while on Edge Networks, DDoS takes time and many attacks to stop server services; this can be seen in Figure 10.

Figure 10 describes the comparison of regular traffic with the occurrence of ICMP-Flood DDoS. The figure shows the time required (ms) for each ICMP sequence when regular traffic is 3.76 ms, and the highest is 14.3 ms, while the lowest ICMP-Flood DDoS is 52.506 ms and the highest is 147, 792 ms. This shows an increase in traffic at the lowest point of 73% while at the highest end of 64%, which causes the server to experience down so that it cannot serve clients.

Figure 11 describes the traffic comparison during DDoS before and after the Firewall was installed. Figure 11 shows the time required (ms) for each ICMP sequence when regular traffic is lowest at 52,506 ms, and the highest is 147,792 ms, while after the Packet Filtering Firewall is configured, the time required for packet delivery and waiting for a reply from the client is the lowest 5.16 ms and highest 16.6 ms. This shows a decrease in traffic at the lowest point of 64% while at the highest end of 69%, which gives the effect of traffic success to return to normal with an average time of each sequence below 1 ms. The comparison of resource usage during regular traffic with ICMP-Flood DDoS is shown in Figure 12.

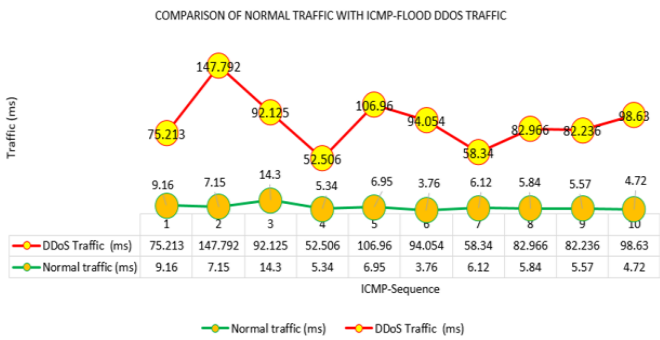
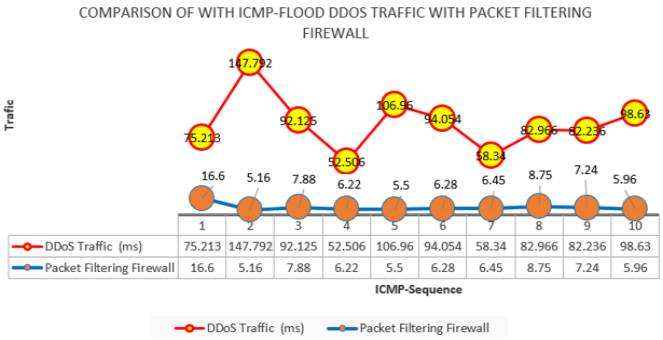


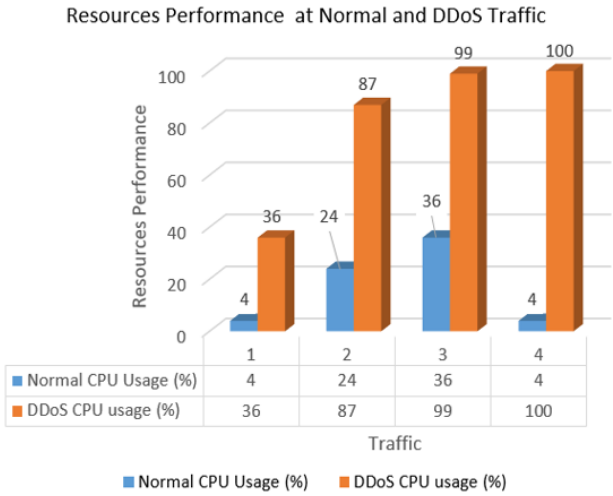
Figure 10. Comparison before and after DDoS attacks on cloud computing network



	1	2	3	4	5	6	7	8	9	10
DDoS Traffic (ms)	75.213	147.792	92.125	52.506	106.96	94.054	58.34	82.966	82.236	98.63
Packet Filtering Firewall	16.6	5.16	7.88	6.22	5.5	6.28	6.45	8.75	7.24	5.96

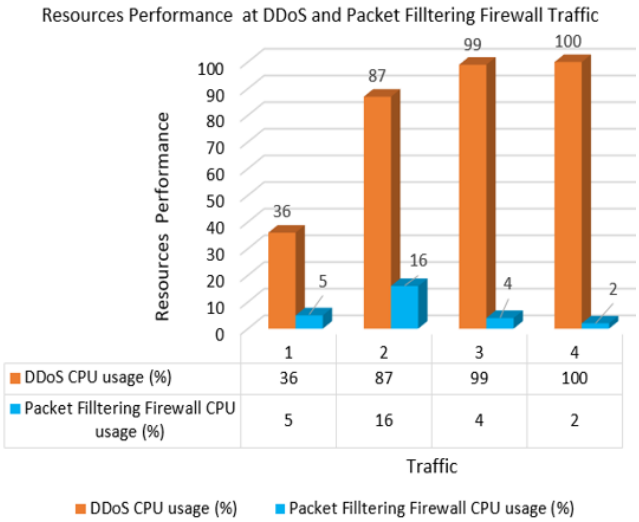
Figure 11. Comparison of traffic during DDoS before and after installing firewall

Figure 12 shows comparison of server resource usage during regular traffic with ICMP-Flood DDoS; normal traffic sampling recorded 4%, 24%, 36%, and 4% with an average of 17.00%. Traffic during DDoS was recorded at 36%, 87%, 99%, and 100%, with an average of 80.50%. This shows an average traffic increase of 63.50%, which causes the server to crash in Cloud Computing. The comparison of resource usage during ICMP-Flood DDoS with Packet Filtering Firewall is shown in Figure 13.



	1	2	3	4
Normal CPU Usage (%)	4	24	36	4
DDoS CPU usage (%)	36	87	99	100

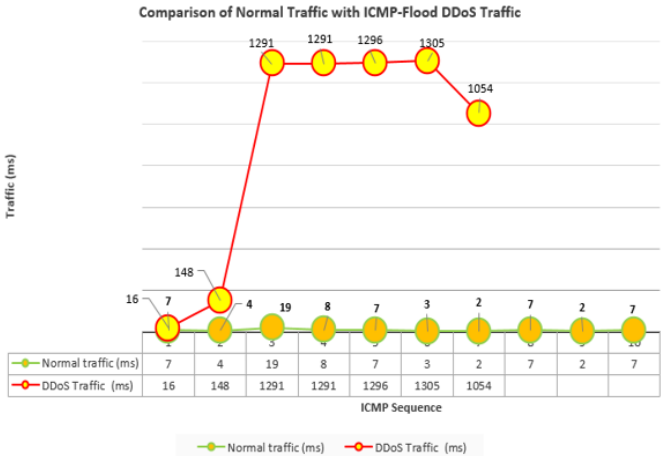
Figure 12. Comparison of resource usage during normal traffic with ICMP-Flood DDoS in cloud computing



	1	2	3	4
DDoS CPU usage (%)	36	87	99	100
Packet Filltering Firewall CPU usage (%)	5	16	4	2

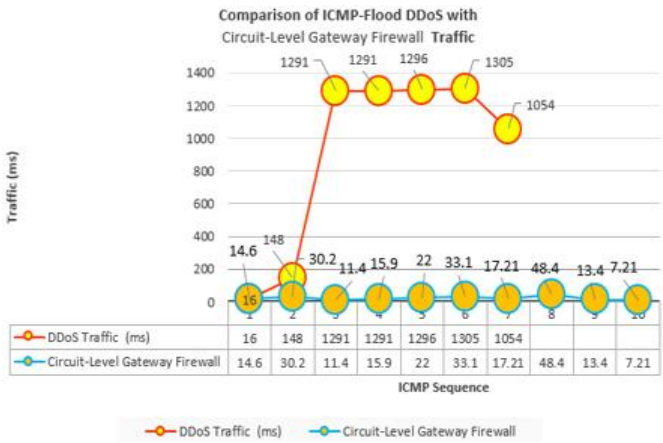
Figure 13. The comparison of resource usage during ICMP-Flood DDoS with packet filtering firewall

Figure 13 shows comparison of server resource usage during regular traffic with ICMP-Flood DDoS; normal traffic sampling recorded 36%, 87%, 99%, and 100% with an average of 80.50%. When Packet Filtering Firewall was installed, traffic was recorded at 5%, 16%, 4%, and 2%, with an average of 6.75%. This indicates a decrease in average traffic of 73.75%, which causes the server to return to normal in Cloud Computing. Furthermore, Forensics and mitigation of Distributed Denial of Service Edge computing networks under normal conditions and conditions during attacks are shown in Figure 14.



Normal traffic (ms)	7	4	19	8	7	3	2	7	2	7
DDoS Traffic (ms)	16	148	1291	1291	1296	1305	1054			

Figure 14. Comparison before and after DDoS attacks on edge computing network



DDoS Traffic (ms)	16	148	1291	1291	1296	1305	1054			
Circuit-Level Gateway Firewall	14.6	30.2	11.4	15.9	22	33.1	17.21	48.4	13.4	7.21

Figure 15. Comparison of ICMP-Flood with circuit-level gateway firewall traffic

Figure 14 describes the comparison of regular traffic with the occurrence of ICMP-Flood DDoS on an Edge Computing Network. The picture shows the time required (ms) for each ICMP sequence during normal traffic; the lowest is 2 ms, and the highest is 19 ms, while the lowest ICMP-Flood DDoS is 16 ms and the highest is 1305 ms until it cannot reach the server. This shows an increase in traffic at the lowest of 87%, while the highest point is 99.80% until saturation so that the server is no longer reachable or the Destination is unreachable; at this layer 4 for forensics and mitigation of Distribution Denial of Service applying Circuit-Level Gateway Firewall with test results as in Figure 15.

Figure 15 describes the comparison of traffic during DDoS before and after installing a Circuit-Level Gateway Firewall. Figure 15 shows the time required (ms) for each ICMP sequence when DDoS traffic occurs, the lowest is 16 ms, and

the highest is 1305 to saturation, while after the Circuit-Level Gateway Firewall is configured, the time required for sending packets and waiting for a reply from the client is the lowest. 7.21 ms and a high of 48.4 ms. This shows a decrease in traffic at the lowest point of 55%. In comparison, at the highest point, the saturation is 1305 towards 48.4 with a percentage of 98.88%, which gives the effect of traffic success returning to normal with the average time of each sequence below 1 ms so that the Circuit-Level Gateway Firewall is implemented at level 4 successfully to stop DDoS. While the comparison of resource usage during regular traffic with ICMP-Flood DDoS is shown in the Edge Computing Network, as shown in Figure 16.

Figure 16 shows the comparison of server resource usage when regular resources are used with ICMP-Flood DDoS, standard traffic sampling recorded 5%, 9%, 5%, and 9% with an average of 7.00%. Traffic during DDoS recorded 83%, 100%, 83%, and 100%, with an average of 84.50%. This shows an average traffic increase of 92.33%, which causes the server to crash on Edge Computing. Forensics and mitigation of Distribution Denial of Service at layer 4 are overcome using Circuit-Level Gateway Firewall with test results as shown in Figure 17.

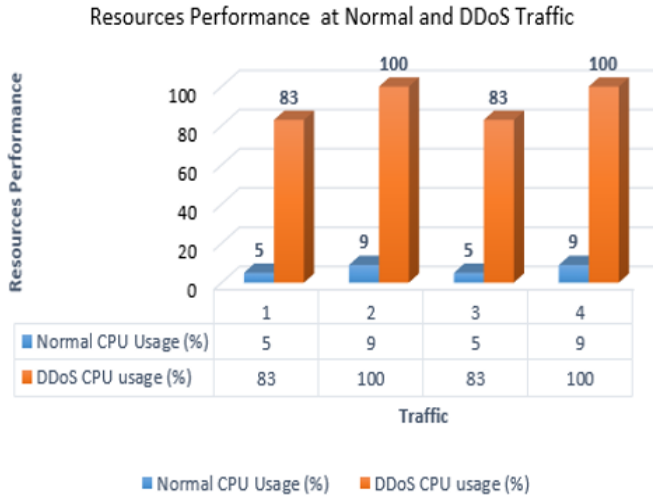


Figure 16. Comparison resources performance at normal DDoS attacks on edge computing network

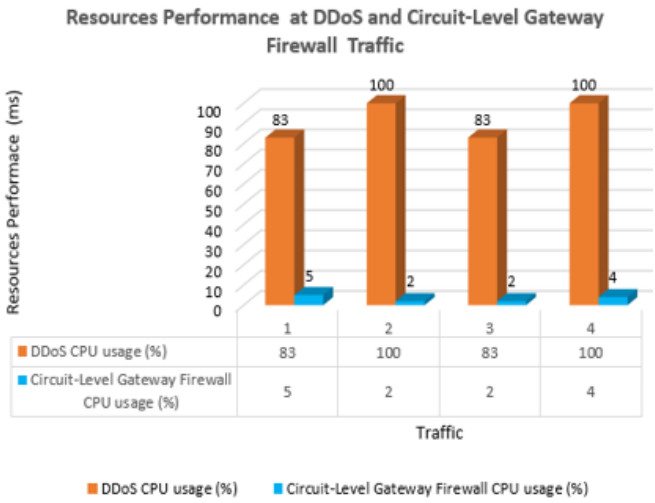


Figure 17. Comparison resources performance at DDoS attacks and circuit-level gateway firewall on edge computing network

Figure 17 shows the comparison of server resource usage during ICMP-Flood DDoS. After implementing Circuit-Level Gateway, ICMP-Flood DDoS traffic sampling was recorded at 83%, 100%, 83%, and 100%, with an average of 91.50%. Meanwhile, the installation of the Circuit-Level Gateway Firewall recorded 5%, 2%, 2%, and 4%, with the average use of server resources being 3.25%. Resource usage This indicates a decrease in resource usage by an average of 96% back to normal resource usage, which states Circuit-Level Gateway Firewall Layer 4 managed to stop the ICMP-Flood DDoS attack. In practice, it has succeeded in stopping ICMP-Flood DDoS attacks on the web server of the SMKN 1 Sewon agency with the same results as the simulation.

5. CONCLUSIONS

Research on ICMP-Flood volumetric-based DDoS in cloud computing and Edge computing networks states that ICMP-Flood DDoS is very dangerous. On cloud computing networks, DDos crowds traffic with an increase of 64% to 73%, while the depletion of server resources also increases by 63,50%. This results in the server crashing and being unable to serve client requests. Forensics and mitigation in cloud computing are carried out at layer 3, the Internet Protocol layer TCP/IP model, by applying a Packet-Filtering Firewall with a success rate of 64%-69% traffic reduction. In contrast, the success of reducing server resource usage is 73.75% and successfully returning traffic and the server that crashes back to normal position. Forensics and mitigation of ICMP-Flood DDoS were also carried out on Edge Computing, with the study showing the occurrence of ICMP-Flood DDoS crowding network traffic with an increase of between 87% to 99.80% to saturation so that it paralyzed the server. Meanwhile, the depletion of server resources also increased by 92.33%. Forensics and mitigation in Edge computing are carried out at layer 4, namely the Transport Protocol layer TCP/IP model, by applying a Circuit-Level Gateway Firewall with a success rate of reducing traffic

REFERENCES

[1] Ridho, F., Yudhana, A., Riadi, I. (2016). Analisis forensik router untuk mendeteksi serangan distributed danial of service (DDoS) secara real time. Annual Research Seminar (ARS), 2(1): 111-116.

[2] Lainjo, B. (2020). Network security and its implications on program management. International Journal of Safety and Security Engineering, 10(6): 739-746. https://doi.org/10.18280/ijsse.100603

[3] Xia, S.M., Guo, S.Z., Bai, W., Qiu, J.Y., Wei, H., Pan, Z.S. (2019). A new smart router-throttling method to mitigate DDoS attacks. IEEE Access, 7: 107952-107963. https://doi.org/10.1109/ACCESS.2019.2930803

[4] Treseangrat, K., Kolahi, S.S., Sarrafpour, B. (2015). Analysis of UDP DDoS cyber flood attack and defense mechanisms on Windows Server 2012 and Linux Ubuntu 13. In 2015 International Conference on Computer, Information and Telecommunication Systems (CITS), Gijon, Spain, pp. 1-5. https://doi.org/10.1109/CITS.2015.7297731

[5] Umar, R., Riadi, I., Kusuma, R.S. (2021). Mitigating sodinokibi ransomware attack on cloud network using

software-defined networking (SDN). International Journal of Safety and Security Engineering, 11(3): 239-246. https://doi.org/10.18280/ijsse.110304

[6] Furutani, N., Ban, T., Nakazato, J., Shimamura, J., Kitazono, J., Ozawa, S. (2014). Detection of DDoS backscatter based on traffic features of darknet TCP packets. In 2014 Ninth Asia Joint Conference on Information Security, Wuhan, China, pp. 39-43. https://doi.org/10.1109/AsiaJCIS.2014.23

[7] Fu, Y., Au, M. H., Du, R., Hu, H., Li, D. (2020). Cloud password shield: A secure cloud-based firewall against DDoS on authentication servers. In 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), Singapore, pp. 1209-1210. https://doi.org/10.1109/ICDCS47774.2020.00154

[8] Sirisha, A., Chaitanya, K., Krishna, K.V.S.S.R., Kanumalli, S.S. (2021). Intrusion detection models using supervised and unsupervised algorithms-a comparative estimation. International Journal of Safety and Security Engineering, 11(1): 51-58. https://doi.org/10.18280/ijsse.110106

[9] Alam, S., Alam, Y., Cui, S., Akujuobi, C., Chouikha, M. (2021). Toward developing a realistic DDoS dataset for anomaly-based intrusion detection. In 2021 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, pp. 1-6. https://doi.org/10.1109/ICCE50685.2021.9427660

[10] Rasheed, M., Badrawi, S., Faieq, M.K., Faieq, A.K. (2017). Detecting and optimizing internet worm traffic signature. Conference: 2017 8th International Conference on Information Technology (ICIT), pp. 870-874. https://doi.org/10.1109/ICITECH.2017.8079961

[11] Beckett, D., Sezer, S., McCanny, J. (2017). New sensing technique for detecting application layer DDoS attacks targeting back-end database resources. In 2017 IEEE International Conference on Communications (ICC), Paris, France, pp. 1-7. https://doi.org/10.1109/ICC.2017.7997376

[12] Zhang, H., Hao, J., Li, X. (2020). A method for deploying distributed denial of service attack defense strategies on edge servers using reinforcement learning. IEEE Access, 8: 78482-78491. https://doi.org/10.1109/ACCESS.2020.2989353

[13] Oo, M.M., Kamolphiwong, S., Kamolphiwong, T. (2017). The design of SDN based detection for distributed denial of service (DDoS) attack. In 2017 21st International Computer Science and Engineering Conference (ICSEC), Bangkok, Thailand, pp. 1-5. https://doi.org/10.1109/ICSEC.2017.8443939

[14] Sanjeetha, R., Prasanna, A., Kumar, D.P., Kanavalli, A. (2018). Mitigation of controller induced DDoS attack on primary server in high traffic scenarios of software defined networks. In 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Indore, India, pp. 1-6. https://doi.org/10.1109/ANTS.2018.8710066

[15] Al'aziz, B.A.A., Sukarno, P., Wardana, A.A. (2020). Blacklisted IP distribution system to handle DDoS attacks on IPS snort based on blockchain. In 2020 6th Information Technology International Seminar (ITIS), Surabaya, Indonesia, pp. 41-45. https://doi.org/10.1109/ITIS50118.2020.9320996

[16] Rashidi, B., Fung, C., Rahman, M. (2018, April). A scalable and flexible DDoS mitigation system using network function virtualization. In NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, pp. 1-6. https://doi.org/10.1109/NOMS.2018.8406314

[17] Morales, C. (2018). NETSCOUT Arbor confirms 1.7 Tbps DDoS attack; the terabit attack era is upon us. NETSCOUT: Westford, MA, Mar, 5.

[18] Wu, Z., Li, W., Liu, L, Yue, M. (2020). Low-rate DoS attacks, detection, defense, and challenges: A survey. IEEE Access, 8: 43920-43943. https://doi.org/10.1109/ACCESS.2020.2976609

[19] Zebari, R.R., Zeebaree, S.R., Jacksi, K. (2018). Impact analysis of HTTP and SYN flood DDoS attacks on Apache 2 and IIS 10.0 Web servers. In 2018 International Conference on Advanced Science and Engineering (ICOASE), Duhok, Iraq, pp. 156-161. https://doi.org/10.1109/ICOASE.2018.8548783

[20] Kent, K., Chevalier, S., Grance, T. (2006). Guide to integrating forensic techniques into incident. National Institute of Standards and Technology.

[21] Yudhana, A., Riadi, I., Ridho, F. (2018). DDoS classification using neural network and naïve bayes methods for network forensics. International Journal of Advanced Computer Science and Applications, 9(11): 177-183. https://doi.org/10.14569/ijacsa.2018.091125

[22] Hussain, F., Abbas, S.G., Husnain, M., Fayyaz, U.U., Shahzad, F., Shah, G.A. (2020). IoT DoS and DDoS attack detection using ResNet. In 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, pp. 1-6. https://doi.org/10.1109/INMIC50486.2020.9318216

[23] Sardana, A., Joshi, R.C. (2008). Honeypot based routing to mitigate DDoS attacks on servers at ISP level. In 2008 International Symposiums on Information Processing, Moscow, Russia, pp. 505-509. https://doi.org/10.1109/ISIP.2008.115

[24] Farion-Melnyk, A., Rozheliuk, V., Slipchenko, T., Banakh, S., Farion, M., Bilan, O. (2021). Ransomware attacks: Risks, protection and prevention measures. 2021 11th International Conference on Advanced Computer Information Technologies (ACIT), pp. 473-478. https://doi.org/10.1109/ACIT52158.2021.9548507

[25] Söderberg, J. (2015). Hacking Capitalism: The Free and Open Source Software Movement. Routledge. https://doi.org/10.4324/9780203937853

[26] Umar, R., Yudhana, A., Faiz, M.N. (2016). Analisis kinerja metode live forensics untuk investigasi random access memory pada sistem proprietary. Prosiding Konferensi Nasional Ke-4 Asosiasi Program Pascasarjana Perguruan Tinggi Muhammadiyah (APPPTM), pp. 207-211.

[27] Apiecionek, Ł., Makowski, W. (2015). Firewall rule with token bucket as a DDoS protection tool. In 2015 IEEE 13th International Scientific Conference on Informatics, Poprad, Slovakia, pp. 32-35. https://doi.org/10.1109/Informatics.2015.7377803

[28] Jiang, M., Wang, C., Luo, X., Miu, M., Chen, T. (2017). Characterizing the impacts of application layer DDoS attacks. In 2017 IEEE International Conference on Web Services (ICWS), Honolulu, HI, USA, pp. 500-507. https://doi.org/10.1109/ICWS.2017.58

[29] Lin, H., Cao, S., Wu, J., Cao, Z., Wang, F. (2019). Identifying application-layer DDoS attacks based on request rhythm matrices. IEEE Access, 7: 164480-

164491. https://doi.org/10.1109/ACCESS.2019.2950820
[30] Praseed, A., Thilagam, P.S. (2018). DDoS attacks at the application layer: Challenges and research perspectives for safeguarding web applications. IEEE Communications Surveys & Tutorials, 21(1): 661-685. https://doi.org/10.1109/COMST.2018.2870658