Jurnal Teknologi Informasi dan Pendidikan
Volume 17, No. 2, September 2024
https://doi.org/10.24036/jtip.v17i2.845

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

Cost-Effective DDoS Mitigation: Leveraging Nginx Reverse Proxy for Enhanced Server Protection

Victor Benny Alexsius Pardosi[1*]✉
Faculty of Computer Science, Universitas Dharma AUB Surakarta, Surakarta, Indonesia
**Corresponding Author: victor@mct.co.id*

Article Information

Article history:

No. 001
Rec. March 03, 2024
Rev. July 14, 2024
Acc. November 28, 2024
Pub. December 02, 2024
Page. 371 – 382

Keywords:

- *DDoS mitigation*
- *Server protection*
- *DDoS attacks*
- *Cybersecurity*
- *Nginx reverse proxy*

ABSTRACT

The problem addressed in this research is the vulnerability of servers to Distributed Denial of Service (DDoS) attacks, which lead to disruptions, financial losses, and the loss of user trust due to frequent downtime. To mitigate this issue, a cost-effective solution utilizing Nginx reverse proxy servers was proposed. This research aimed to enhance server resilience against DDoS threats while minimizing operational costs. The primary contribution of this study is the introduction of an innovative approach to DDoS mitigation, emphasizing practical implementation steps. The methodology involved configuring a public server with Nginx and DDoS protection capabilities alongside setting up a private server in an office environment. A reverse proxy using Nginx was deployed to filter incoming traffic and counter DDoS attacks. The main outcomes of the research demonstrate successful mitigation of DDoS attacks, significantly reducing their impact on the private server. Testing on both Layers 3 and Layer 4 confirmed the effectiveness of the approach. The methodology's emphasis on practical implementation steps ensures seamless integration into existing infrastructure. In conclusion, this research offers a practical and budget-friendly solution for organizations seeking to enhance their resilience against DDoS threats. By leveraging Nginx reverse proxy servers, servers lacking dedicated protection can effectively safeguard against DDoS attacks, highlighting the importance of proactive measures in cybersecurity.

How to Cite:

Pardosi, V. B. A. (2024). Cost-Effective DDoS Mitigation: Leveraging Nginx Reverse Proxy for Enhanced Server Protection. Jurnal Teknologi Informasi Dan Pendidikan, 17(2), 371-382.
https://doi.org/10.24036/jtip.v17i2.845

1. INTRODUCTION

Distributed Denial of Service (DDoS) attacks aims to inundate targets with an excessive volume of traffic, impairing the functionality of their network resources for legitimate users [1]. DDoS attacks continue to pose significant challenges to organizations worldwide, causing disruptions, financial losses, and erosion of user trust due to frequent downtime [2]. These attacks target servers lacking dedicated protection, exploiting vulnerabilities and overwhelming resources, leading to service outages and compromised operations [3]. Traditional mitigation strategies often involve costly dedicated DDoS protection services or hardware, rendering them impractical for organizations with limited resources or operating in resource-constrained environments. As such, there is a pressing need for innovative and cost-effective approaches to mitigate DDoS attacks while ensuring the availability and reliability of critical services.

In response to this need, this research introduces innovative method utilizing Nginx reverse proxy [4] servers for DDoS mitigation on vulnerable servers. By leveraging the capabilities of Nginx reverse proxy servers, organizations can enhance their resilience against DDoS threats without incurring significant expenses associated with traditional dedicated DDoS protection services. This approach offers a practical and budget-friendly solution for organizations seeking to fortify their defenses against DDoS attacks, particularly in environments where dedicated protection services may not be feasible or cost-effective [9]-[11].

This paper presents an in-depth exploration of the proposed method, emphasizing its practical implementation steps and highlighting its effectiveness in mitigating DDoS attacks. The methodology involves configuring a public server with Nginx and DDoS protection capabilities, alongside setting up a private server in the office or university environment. A reverse proxy using Nginx is deployed to filter incoming traffic and counter DDoS attacks, ensuring the availability and reliability of critical services while minimizing operational costs [12]-[15]. The main outcomes of the research demonstrate successful mitigation of DDoS attacks, underscoring the robustness and efficacy of the proposed approach.

Through this research, we aim to contribute valuable insights into cybersecurity by offering a practical and cost-effective solution for mitigating DDoS attacks on servers lacking dedicated protection. By highlighting the importance of proactive measures in safeguarding against cyber threats, this research seeks to empower organizations to enhance their resilience and protect their critical assets from DDoS attacks.

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

2. RESEARCH METHOD

The research methodology involved a combination of practical implementation and testing to assess the effectiveness of the proposed approach. The following steps were undertaken:

2.1. Public Server Configuration

A public server with Nginx and DDoS protection capabilities was configured to act as a reverse proxy [16]. This server served as the front-end for handling incoming requests and filtering malicious traffic.

2.2. Private Server Configuration

A private server, representing the target server lacking dedicated DDoS protection, was set up in an office environment [17]. This server simulated the vulnerable infrastructure typically found in organizations.

2.3. Reverse Proxy Deployment

Nginx was deployed on the public server as a reverse proxy to forward legitimate requests to the private server while filtering out malicious traffic [18]. The configuration of Nginx was optimized to effectively mitigate DDoS attacks.

2.4. Testing and Evaluation

The effectiveness of the proposed approach was evaluated through testing, including simulated DDoS attacks on Layers 3 and 4 [19]. The impact of these attacks on the private server was assessed, focusing on the ability of the reverse proxy to mitigate the attacks and maintain service availability.

2.5. Analysis

Data collected from the testing phase were analyzed to assess the performance and efficacy of the proposed approach in mitigating DDoS attacks [20]. The results were used to draw conclusions regarding the effectiveness of using Nginx reverse proxy servers for DDoS mitigation in servers lacking dedicated protection.

By employing this research methodology, the study provides practical insights into mitigating DDoS attacks on vulnerable servers using Nginx reverse proxy servers, offering a cost-effective solution for organizations facing DDoS threats.

Jurnal Teknologi Informasi dan Pendidikan
Volume 17, No. 2, September 2024
https://doi.org/10.24036/jtip.v17i2.845

2.6. Implementation

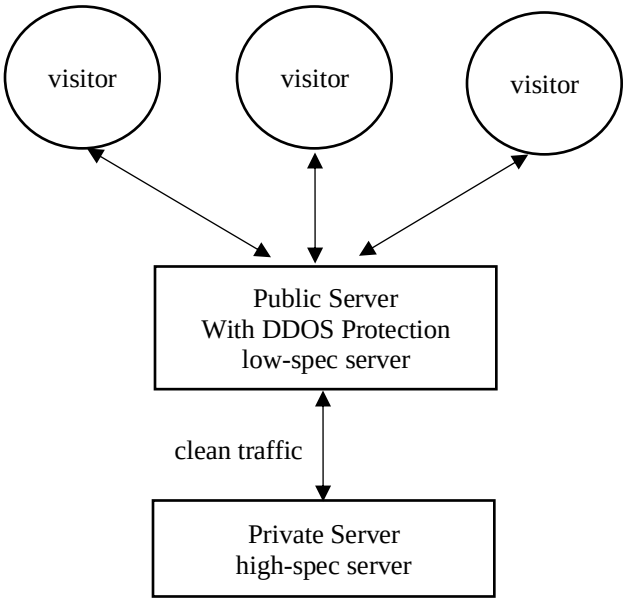


Figure 1. Visitor Traffic Flow

Figure 1 illustrates the flow of visitor traffic in the proposed DDoS mitigation setup. The process begins with the visitor accessing the public server, which is equipped with DDoS protection capabilities. This public server acts as an intermediary, handling and filtering incoming traffic to protect against DDoS attacks. Once the traffic is deemed legitimate, it is forwarded to the private server where the application is hosted. This setup ensures that the private server's IP address remains hidden, reducing its exposure to direct attacks and maintaining continuous service availability.

2.7. Protocols

The Nginx reverse proxy serves as a versatile solution capable of handling requests for both HTTP and non-HTTP servers [21]. For the purpose of this implementation, our focus was primarily on testing using HTTP requests.

2.8. Setting up the Public Server

The initial step involves installing Nginx on the Public Server equipped with DDOS Protection. It's noteworthy that even a small VPS suffices for this task [22]. The Nginx configuration on the public server is as follows:

```
server {
   listen 80; #listen on port 80 for ipv4
```


P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

Volume 17, No. 2, September 2024
https://doi.org/10.24036/jtip.v17i2.845

```
    listen [::]:80; #listen on port 80 for ipv6
    server_name testing.server.name; #domain name

    location / {
        proxy_redirect off;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
        proxy_pass http://xxx.xxx.xxx.xxx:1234;  #private server ip addresss
    }
}

server {
    listen 443 ssl http2; #listen port with ssl
    listen [::]:443 ssl http2; #listen port with ssl (ipv6)
    server_name testing.server.name; #domain name
    ssl_certificate /path/to/ssl/certificate.crt; #cert location
    ssl_certificate_key /path/to/ssl/privatekey.key; #key location

    location / {
        proxy_redirect off;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
        proxy_pass http://xxx.xxx.xxx.xxx:1234; #ip address of private server
    }
}
```

2.9. Setting up the Private Server

Proceeding forward, Nginx is installed on the private server and configured to listen on port 1234 [23]. Additionally, the firewall settings are adjusted to whitelist both the IP address of the author and the IP address of the public server. Upon completion of these steps, users should be able to access the website hosted on the private server seamlessly via the IP address of the public server.

Nginx configuration:

```
server {
    listen 1234; #listen port for private server
    server_name localhost;
    root /var/www/;
```

Volume 17, No. 2, September 2024
https://doi.org/10.24036/jtip.v17i2.845

```
    index index.php index.html index.htm;
        # Set up location for handling requests
        location / {
            # Try to serve requested files, and fallback to index.php if not found
            try_files $uri $uri/ /index.php?$query_string;
        }
        location ~ \.php$ {
            # Include FastCGI configuration for PHP
            include snippets/fastcgi-php.conf;

            # Pass PHP requests to the PHP-FPM socket
            fastcgi_pass unix:/run/php/php7.4-fpm.sock;
        }
}
```

2.10. Firewall Configurations

A firewall is essential for network security as it acts as a barrier between a trusted internal network and untrusted external networks, filtering incoming and outgoing traffic based on a set of predefined rules [5]. In the context of this research, implementing a firewall is crucial to enhance the security posture of the private server vulnerable to DDoS attacks.

For the firewall setup, two options are commonly used: iptables and ufw/firewalld [24]. In this testing scenario, ufw (Uncomplicated Firewall) is chosen for its simplicity and ease of use.

The firewall configuration involves whitelisting specific IP addresses to restrict access to the private server [25]. In this case, only the IP address of the author and the IP address of the public server are whitelisted. Additionally, specific ports are opened to allow incoming traffic for the web server (listening on port 1234) and SSH (listening on a random port for enhanced security).

To configure the firewall using ufw, the following commands are used:

```
# Allow SSH connections
sudo ufw allow <port_number>/tcp
# Allow incoming traffic from the author's IP address
ufw allow from <author_ip_address>
# Allow incoming traffic from the public server's IP address
ufw allow from <public_server_ip_address>
ufw allow 1234/tcp
ufw reload
```


P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

By implementing ufw with a whitelist approach, unauthorized access to the private server is prevented, minimizing the risk of unauthorized intrusions and potential DDoS attacks. This proactive security measure enhances the overall resilience of the private server against external threats while ensuring secure access for authorized users and services.

Overall, the firewall configuration plays a crucial role in bolstering the security of the private server vulnerable to DDoS attacks, mitigating potential risks, and ensuring the integrity and availability of hosted services.

2.11. Testing DDoS Attacks on Layer 3 and 4

In this section, we undertake thorough testing of Distributed Denial of Service (DDoS) attacks directed at Layers 3 and 4 of the networks [6]. Through meticulous evaluation, we gauge the efficacy of our proposed mitigation strategies in thwarting DDoS attacks across different network layers. By simulating real-world scenarios, we subject public servers to 1Gbps DDoS attacks and TCP SYN attack, allowing for a comprehensive assessment of our mitigation measures.

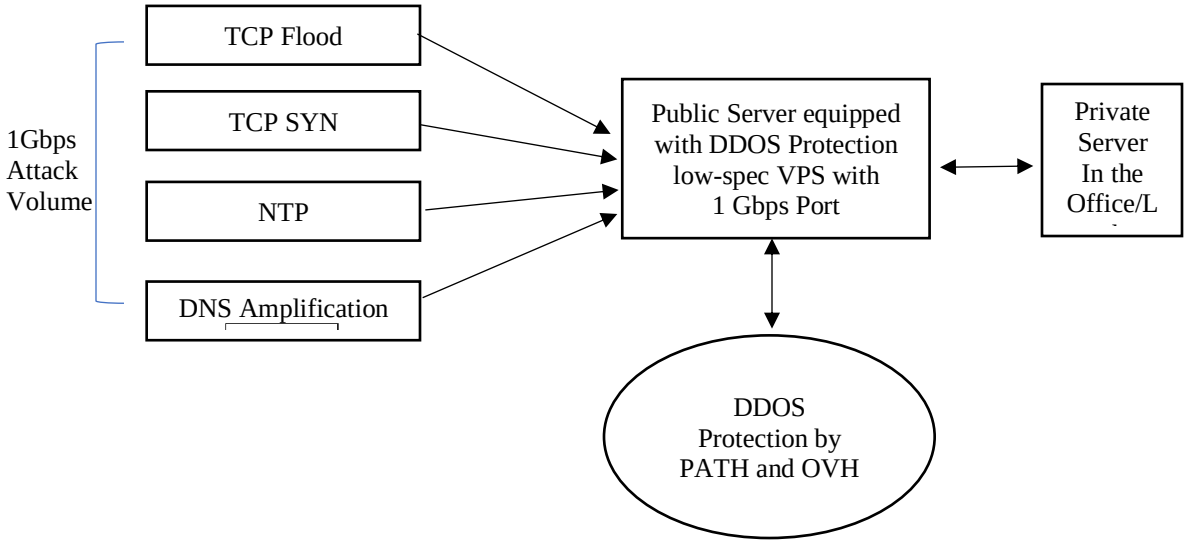


Figure 2. Testing DDoS Attacks

Figure 2 illustrates the testing setup and the flow of DDoS attack traffic. The diagram shows a 1Gbps attack volume being sent using various methods, including TCP Flood, TCP SYN, NTP, and DNS Amplification, directed at the public server equipped with DDoS protection. The public server, a low-spec VPS with a 1Gbps port, is tasked with filtering out the DDoS attack traffic. The DDoS protection provided by services such as PATH and OVH effectively filters the malicious traffic. Once filtered, all legitimate data is forwarded to the private server located in the office or lab. This setup demonstrates the robustness of the

mitigation strategy, ensuring that the private server remains protected from DDoS attacks while maintaining accessibility for legitimate users.

3. RESULTS AND DISCUSSION

Filter

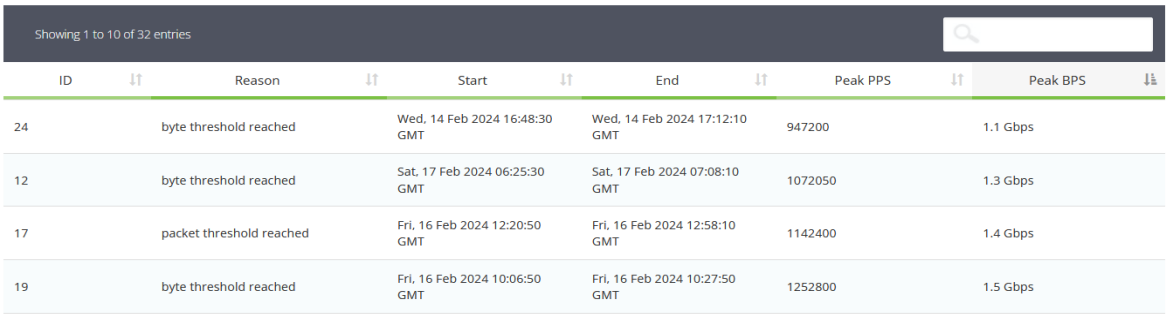
Detection time	End time	Destination IP	Attack vectors
2024-02-09 17:38:57	2024-02-09 17:53:57	[redacted]	TCP_SYN
2024-02-04 14:36:17	2024-02-04 14:51:17	[redacted]	TCP_SYN
2024-02-01 16:09:05	2024-02-01 16:24:05	[redacted]	TCP_SYN
2024-02-01 14:36:52	2024-02-01 14:51:52	[redacted]	TCP_SYN
2024-02-01 02:50:33	2024-02-01 03:05:33	[redacted]	TCP_SYN
2024-01-30 13:35:31	2024-01-30 13:50:31	[redacted]	TCP_SYN

Figure 3. TCP SYN attacks identified and mitigated by OVH Provider

Figure 3 presents a table detailing the TCP SYN attacks that were identified and mitigated by the OVH Provider. The table contains several columns that provide key information about each detected attack:

- Detection Time: The exact timestamp when the TCP SYN attack was first identified by the OVH DDoS protection system.
- End Time: The timestamp indicating when the attack was successfully mitigated and normal traffic flow resumed.
- Destination IP: The IP address of the target server that was being attacked.
- Attack Vectors: Specifies the type of attack vector used, which in this case is TCP_SYN.

The table highlights the efficiency and responsiveness of the OVH Provider's DDoS protection services in detecting and mitigating TCP SYN attacks. Importantly, it was observed that during these attacks, there was no downtime on our application, demonstrating the effectiveness of the mitigation strategies in ensuring continuous service availability and maintaining user trust.



Showing 1 to 10 of 32 entries

ID	Reason	Start	End	Peak PPS	Peak BPS
24	byte threshold reached	Wed, 14 Feb 2024 16:48:30 GMT	Wed, 14 Feb 2024 17:12:10 GMT	947200	1.1 Gbps
12	byte threshold reached	Sat, 17 Feb 2024 06:25:30 GMT	Sat, 17 Feb 2024 07:08:10 GMT	1072050	1.3 Gbps
17	packet threshold reached	Fri, 16 Feb 2024 12:20:50 GMT	Fri, 16 Feb 2024 12:58:10 GMT	1142400	1.4 Gbps
19	byte threshold reached	Fri, 16 Feb 2024 10:06:50 GMT	Fri, 16 Feb 2024 10:27:50 GMT	1252800	1.5 Gbps

Figure 4. DDoS attacks identified and mitigated by PATH Provider

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

Figure 4 presents a tabular representation of the DDoS attacks that were identified and mitigated by the PATH Provider. The figure highlights the following key metrics:

- Peak PPS (Packets Per Second): The graph shows a peak value of up to 1,252,800 PPS, indicating the maximum rate at which packets were being sent to the target during the attack.
- Peak BPS (Bits Per Second): The graph indicates a peak bandwidth usage of up to 1.5 Gbps, which exceeds the capacity of our VPS port (1 Gbps).

Despite the high intensity of the DDoS attacks, surpassing the VPS port capacity, there was no downtime experienced on our system. This underscores the effectiveness of the PATH Provider's DDoS protection services in handling and mitigating high-volume attacks, ensuring uninterrupted service availability. The ability to maintain continuous operation under such attack conditions is a testament to the robustness of the deployed mitigation strategies.

The comprehensive testing of Distributed Denial of Service (DDoS) attacks targeting Layers 3 and 4 of the network stacks yielded significant insights into the effectiveness of the proposed mitigation strategy. Through rigorous evaluation, it was observed that the VPS Provider with DDOS Protection services effectively mitigated 1Gbps DDoS attacks and TCP SYN attacks [7]. Consequently, the website hosted on the private server remained accessible without any downtime during these attacks. This outcome underscores the robustness of the mitigation measures employed in safeguarding against DDoS attacks and ensuring continuous uptime for the hosted services

Furthermore, the successful mitigation of DDoS attacks highlights the cost-effectiveness of the proposed solution compared to traditional DDoS mitigation services. By leveraging VPS Provider with DDOS Protection services, organizations can achieve robust protection against DDoS attacks without incurring the high costs associated with dedicated mitigation services. This cost-saving aspect makes the solution particularly attractive for organizations seeking to optimize their cybersecurity spending while maintaining effective protection against DDoS threats [8].

The analysis of the results underscores the practicality and efficacy of the proposed mitigation strategy in defending against DDoS attacks. By effectively mitigating DDoS attacks while minimizing operational costs, the solution offers a viable and sustainable approach to protecting against DDoS threats. Additionally, the ability to ensure uninterrupted access to hosted services during DDoS attacks enhances the overall resilience of organizations' IT infrastructure, mitigating potential disruptions and minimizing the impact of DDoS attacks on business operations.

This is particularly relevant in scenarios where organizations prefer to manage their own hardware infrastructure but require protection against potential DDoS threats. By implementing the proposed mitigation strategy, organizations can maintain control over their hardware infrastructure while still benefiting from effective DDoS protection.

Table 1. The result of testing

Attack Methods	Public Server		
	DDoS protection services (default VPS protection)	***VPS Specs***	***Result***
TCP SYN Flood TCP Flood NTP DNS Amplification	PATH NETWORK, INC OVH CLOUD	2 Cores 4 GB Ram >50GB Storage	No downtime Both Public and Private server

Table 1 provides an overview of the results from testing various DDoS attack methods on the public and private servers. The testing involved different types of attacks, including TCP SYN Flood, TCP Flood, NTP, and DNS Amplification. The DDoS protection services from PATH NETWORK, INC and OVH CLOUD were employed, along with the default VPS protection. The VPS used in the tests had specifications of 2 CPU cores, 4 GB of RAM, and over 50 GB of storage. The results indicate that there was no downtime experienced on both the public and private servers. This demonstrates that the strategy of using a Nginx reverse proxy to protect systems or applications on servers without dedicated DDoS protection is highly effective. By leveraging this technique, it is possible to avoid downtime even during high-intensity DDoS attacks, thereby ensuring continuous service availability and reliability.

4. CONCLUSION

In conclusion, the findings of this research underscore the effectiveness and practicality of the proposed mitigation strategy in defending against Distributed Denial of Service (DDoS) attacks. Through comprehensive testing targeting Layers 3 and 4 of the network stacks, it was demonstrated that leveraging VPS Provider with DDOS Protection services effectively mitigated 1Gbps DDoS attacks and TCP SYN attacks, ensuring continuous uptime for hosted services.

Furthermore, the cost-effectiveness of the proposed solution compared to traditional DDoS mitigation services highlights its significance as a valuable alternative for organizations seeking robust protection against DDoS threats while optimizing operational costs. The ability to safeguard privately hosted websites and services from DDoS attacks without relying on external mitigation services offers a sense of control and autonomy to organizations, particularly in scenarios where they prefer to manage their own hardware infrastructure but require protection against potential DDoS threats.

Overall, the findings of this research contribute to the body of knowledge in cybersecurity by providing a practical and cost-effective approach to mitigating DDoS attacks. By implementing the proposed mitigation strategy, organizations can enhance their resilience against DDoS threats while maintaining operational efficiency and minimizing

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

the impact of DDoS attacks on business operations. Moving forward, further research and development in this area are warranted to explore additional strategies and technologies for enhancing DDoS protection and mitigating emerging cyber threats.

REFERENCES

[1] Yuan, X., Li, C., & Li, X. (2017, May). DeepDefense: identifying DDoS attack via deep learning. In 2017 IEEE international conference on smart computing (SMARTCOMP) (pp. 1-8). IEEE.
[2] Joosten, R. and Nieuwenhuis, L.J., 2017, March. Analysing the impact of a DDoS attack announcement on victim stock prices. In 2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP) (pp. 354-362). IEEE.
[3] N. Innab and A. Alamri, "The Impact of DDoS on E-commerce," 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Saudi Arabia, 2018, pp. 1-4, doi: 10.1109/NCG.2018.8593125.
[4] Reese, W., 2008. Nginx: the high-performance web server and reverse proxy. Linux Journal, 2008(173), p.2.
[5] Anwar, R.W., Abdullah, T. and Pastore, F., 2021. Firewall best practices for securing smart healthcare environment: A review. Applied Sciences, 11(19), p.9183.
[6] Obaid, H.S. and Abeed, E.H., 2020. DoS and DDoS attacks at OSI layers. International Journal of Multidisciplinary Research and Publications, 2(8), pp.1-9.
[7] Eddy, W., 2007. TCP SYN flooding attacks and common mitigations (No. rfc4987).
[8] Mansfield-Devine, S., 2011. DDoS: threats and mitigation. Network Security, 2011(12), pp.5-12.
[9] Hitchcock, K., Linux System Administration for the 2020s.
[10] Swami, R., Dave, M. and Ranga, V., 2021. Detection and analysis of TCP-SYN DDoS attack in software-defined networking. Wireless Personal Communications, 118, pp.2295-2317.
[11] Shah, S.Q.A., Khan, F.Z. and Ahmad, M., 2021. The impact and mitigation of ICMP based economic denial of sustainability attack in cloud computing environment using software defined network. Computer Networks, 187, p.107825.
[12] Mughal, A.A., 2020. Cyber Attacks on OSI Layers: Understanding the Threat Landscape. Journal of Humanities and Applied Science Research, 3(1), pp.1-18.
[13] Florackis, C., Louca, C., Michaely, R. and Weber, M., 2023. Cybersecurity risk. The Review of Financial Studies, 36(1), pp.351-407.
[14] Mishra, A., Sharma, S. and Pandey, A., 2020, March. A review on DDOS attack, TCP flood attack in cloud environment. In Proceedings of the International Conference on Innovative Computing & Communications (ICICC).
[15] Abubakar, R., Aldegheishem, A., Majeed, M.F., Mehmood, A., Maryam, H., Alrajeh, N.A., Maple, C. and Jawad, M., 2020. An effective mechanism to mitigate real-time DDoS attack. IEEE Access, 8, pp.126215-126227.
[16] Miano, S., Bertrone, M., Risso, F., Bernal, M.V., Lu, Y. and Pi, J., 2019. Securing Linux with a faster and scalable iptables. ACM SIGCOMM Computer Communication Review, 49(3), pp.2-17.
[17] Fjordvald, M.B. and Nedelcu, C., 2018. Nginx HTTP Server: Harness the power of Nginx to make the most of your infrastructure and serve pages faster than ever before. Packt Publishing Ltd.

[18] Alhijawi, B., Almajali, S., Elgala, H., Salameh, H.B. and Ayyash, M., 2022. A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets. Computers and Electrical Engineering, 99, p.107706.
[19] Rai, A. and Challa, R.K., 2016, February. Survey on recent DDoS mitigation techniques and comparative analysis. In 2016 Second International Conference on Computational Intelligence & Communication Technology (CICT) (pp. 96-101). IEEE.
[20] Adi, N. H., Wahdi, Y. W., Dewi, I. P., Lubis, A. L., & Devega, A. T. (2022). The effectiveness of learning media as a supporter of online learning in computer networking courses. Jurnal Teknologi Informasi dan Pendidikan, 14(3), 278-283.
[21] P. Wurzinger, C. Platzer, C. Ludl, E. Kirda and C. Kruegel, "SWAP: Mitigating XSS attacks using a reverse proxy," 2009 ICSE Workshop on Software Engineering for Secure Systems, Vancouver, BC, Canada, 2009, pp. 33-39, doi: 10.1109/IWSESS.2009.5068456.
[22] Hendra, R., & Hanita, M. (2020). The Implementation of Cyber Incident Management Frameworks in Indonesia. Jurnal Teknologi Informasi dan Pendidikan, 13(2), 9-16.
[23] Muttaqin, I. K., Maesaroh, S. S., & Herdiana, O. (2024). Analysis of Information Security Awareness of E-Commerce Users Among Micro Small Medium Enterprises. Jurnal Teknologi Informasi dan Pendidikan, 17(1), 149-160.
[24] Pardosi, V. B. A., Kom, S., Karim, A., TI, M., Ilham, R., Kom, M., ... & Wijaya, A. (2024). SISTEM KEAMANAN KOMPUTER. CV Rey Media Grafika.
[25] Pardosi, V. B. A., Deta, B., Nugroho, F., & Vandika, A. Y. (2024). Sistem Keamanan Informasi. PT Mafy Media Literasi Indonesia.

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id