UDC 004
DOI: 10.15587/1729-4061.2023.285275

DEVELOPMENT OF HYBRID INTRUSION DETECTION SYSTEM BASED ON SURICATA WITH PFSENSE METHOD FOR HIGH REDUCTION OF DDOS ATTACKS ON IPV6 NETWORKS

Supriyanto Praptodiyono
Doctor of Computer Sciences, Professor,
Vice Dean of Academic Affairs*
Teguh Firmansyah
Corresponding author
Doctor of Electrical Engineering, Lecturer*
E-mail: teguhfirmansyah@untirta.ac.id
Muhamad Haerul Anwar
Bachelor of Electrical Engineering, Student*
Cakra Adipura Wicaksana
Master of Electrical Engineering, Lecturer
Department of Informatics**
Anggoro Suryo Pramudyo
Master of Computer Sciences, Lecturer*
Ali Al-Allawee
Doctor of Computer Sciences, Lecturer
Department of Computer Sciences
University of Haute Alsace
Rue du Grillenbreit str., 34, Colmar, France, 68000
*Department of Electrical Engineering**
**Universitas Sultan Ageng Tirtayasa
Jend. Sudirman str., 3, Cilegon, Indonesia, 42435

Distributed Denial of Service (DDoS) attacks is a problem in computer networks. DDoS attacks pose a significant threat to internet networks as they cause congestion and disrupt the optimal functioning of servers. Detecting the source of these attacks is essential for effective protection. Therefore, in this study, we propose a hybrid strategy that combines Suricata, an intrusion detection system (IDS), with pfSense, a firewall, to address DDoS attacks. Suricata, the IDS, can identify the destination of the attack, which allows pfSense, the Firewall, to block the attack by dropping packets sent by the attacker. As a result, by leveraging this combined approach, we have observed significant improvements in the quality of service (QoS). The results of our study indicate a 1.08 % increase in throughput value, from 1881.97 bytes to 902.44 bytes, demonstrating improved efficiency in data transmission. Additionally, we observed a 57.32 % increase in the average total number of packets sent, from 1382 packets to 3238 packets, indicating better network performance. Furthermore, the proposed strategy significantly reduced delay and jitter values. The delay value decreased by 88.78 %, from 90.76 ms to 10.18 ms, and the jitter value decreased by 88.99 %, from 181.85 ms to 20.03 ms. These improvements signify a notable reduction in latency and packet timing variations, leading to a smoother network experience. Another crucial aspect we evaluated was the CPU utilization. The proposed strategy resulted in a substantial decrease in CPU utilization by 81.23 %, from 78.3 % to 14.7 %. The combination of pfSense and Suricata has proven to be a successful approach, providing robust protection against DDoS attacks, including those utilizing IPv6. This research can be implemented as a solution on a campus ad-hoc network with limited computers

Keywords: CPU utilization, DDoS attacks, Jitter, pfSense, Suricata, DDoS, IDS, IPv6

Received date 18.05.2023
Accepted date 28.07.2023
Published date 30.08.2023

How to Cite: *Praptodiyono, S., Firmansyah, T., Anwar, M. H., Wicaksana, C. A., Pramudyo, A. S., Al-Allawee, A. (2023). Development of hybrid intrusion detection system based on suricata with pfsense method for highly reduction of DDoS attack on IPv6 networks. Eastern-European Journal of Enterprise Technologies, 5 (9 (125)), 75–84. doi: https://doi.org/10.15587/1729-4061.2023.285275*

1. Introduction

Cybercrime has become a pervasive issue, with computers being utilized as tools for criminal activities. It encompasses a wide range of offenses, including theft, fraud, and attacks on computer systems and networks [1–3]. As reported by Check Point Software Ltd, the severity of Cryptomining malware attacks has notably increased in recent years, with approximately 22 % of companies worldwide falling victim to such attacks in 2019 [4–7]. Amidst the rising number of cybercrime cases, it is vital for service providers to possess adequate knowledge and tools to safeguard against and mitigate cyber attacks effectively [8, 9]. In detail, there are several major problems of cyber security such as distributed denial of service (DDoS) attacks, phishing and social engineering, and ransomware.

A DDoS attack occurs when multiple compromised computers, often part of a botnet, are used to flood a target system or network with an overwhelming amount of traffic. This flood of traffic causes the target system to become slow or unavailable, disrupting its normal functioning. DDoS attacks can be financially motivated, politically driven, or simply aimed at causing chaos. Mitigation techniques involve traffic filtering, rate limiting, and employing Content

Delivery Networks (CDNs) to distribute traffic. Phishing is a cybercrime where attackers create deceptive emails, websites, or messages that appear legitimate to trick individuals into revealing sensitive information such as usernames, passwords, or financial details. Social engineering involves manipulating individuals into divulging confidential information or performing actions that compromise security. These attacks often exploit human psychology and trust. Education, email filtering, and multi-factor authentication are essential countermeasures. Ransomware is a type of malware that encrypts a victim's files or locks them out of their system, and then demands a ransom payment in exchange for providing the decryption key or restoring access. Ransomware attacks can spread rapidly across networks and cause significant disruption to businesses and individuals. Prevention includes regular data backups, network segmentation, up-to-date software, and robust cybersecurity measures.

One of the most prevalent forms of cyber attacks is the DDoS attack. According to Nexus Guard, China has recorded the highest number of DDoS attacks, accounting for 317,268 attacks and 19.87 % of the total. In a DDoS attack, the perpetrator floods the victim's server with a massive volume of ACK and SYN packets, mimicking legitimate network activity. This makes it challenging to detect these attacks as abnormal network behavior. Consequently, hackers frequently employ DDoS attacks to disrupt their victims' services, rendering their servers inaccessible and impeding optimal operation [10–12].

To defend against DDoS attacks, service providers must implement robust security measures, including firewalls and intrusion detection systems, to identify and block malicious traffic. Ensuring network security has become crucial to facilitate the secure transfer of data across computer networks. Since data traverses multiple computers before reaching its destination, it creates opportunities for cyber attackers to exploit vulnerabilities and cause harm. Consequently, restricting access to computers and implementing stringent access controls are critical steps in preventing network breaches [13, 14].

Intrusion detection systems employing classical machine learning techniques, as well as the security breaches caused by ransomware, were also investigated in [15, 16]. Nevertheless, when it comes to practical application, challenges arise due to the substantial amount of training data required. An additional algorithm based on the Deep Belief Network, distinguishing between well-formed and malformed packets, was also suggested. However, it encounters the same issue of high computational complexity [17, 18].

The issue of DDoS attacks continues to present a significant and evolving challenge within the realm of computer networks. A DDoS attack entails a malevolent effort to overwhelm a target system or network by flooding it with an overwhelming volume of traffic, rendering it inaccessible or severely hampering its functionality. This persistent problem stems from the inherent vulnerabilities in the design and architecture of networks, making them susceptible to exploitation by malicious actors who leverage botnets and other resources to orchestrate these attacks.

Therefore, studies devoted to countering DDoS attacks with low-complexity computation are of scientific relevance.

2. Literature review and problem statement

The intrusion detection system (IDS) based on Suricata on Linux Debian 9 was also proposed to detect and prevent various attacks, such as brute force, DDoS, and port scanning [19]. The study utilized Cloud Virtual Private Servers (VPS) to create virtual servers, ensuring precise allocation of CPU, RAM, and storage without the need for physical servers. However, the study did not incorporate a Firewall to block, reject, and drop data packets that could harm the network.

In a previous study conducted by [20], the hping3 command was employed to launch a denial of service (DoS) attack using IPv4 addresses. In contrast, the current study utilized the atk6-thcsyn6 command, which floods ACK and SYN packets with IPv6 addresses. One limitation of this study is its focus on specific types and methods of attacks, which could hinder the IDS system's ability to detect new attacks. To detect attacks originating from external sources, it is necessary to utilize software that restricts connections, filters addresses, blocks malicious sites, monitors traffic, and offers other security features [21].

There are several interesting methods to combat DDoS attacks. The paper [22] provides an overview of DDoS attacks, their impact on network infrastructure, and their evolving nature. However, the effectiveness of combating DDoS attacks in maintaining network availability and security is not clear and complex. Moreover, reference [23] explored DDoS attack techniques and variants. There are several different types of DDoS attack techniques, such as volumetric, protocol-based, and application-layer attacks, including amplification attacks (e.g., DNS amplification) and reflection attacks (e.g., NTP reflection) [24]. The discussion of various techniques for detecting DDoS attacks, including anomaly-based, signature-based, and hybrid approaches, was introduced by [25]. Additionally, the exploration of mitigation strategies, such as traffic filtering, rate limiting, and the use of intrusion prevention systems (IPS), was conducted by [26].

The paper [27] proposed a cloud-based DDoS protection approach. It explores the role of cloud-based services and content delivery networks (CDNs) in mitigating DDoS attacks. The paper also discusses the advantages and challenges of outsourcing DDoS protection to third-party providers. However, third-party providers do not provide real-time data.

Furthermore, reference [28] proposed machine learning and AI for DDoS mitigation. It highlights the use of anomaly detection, pattern recognition, and predictive modeling [29]. The papers [29, 30] proposed and explored enhancing DDoS defense and mitigation. The authors also discuss the benefits of dynamic resource allocation, traffic redirection, and programmable network management. However, it has problems in complexity algorithm, performance overhead, and scalability challenges.

Another interesting method, such as policy Collaborative and Global Approaches, is investigated in references [31, 32]. The paper focuses on and discusses the significance of international collaboration, information sharing, and coordinated responses in combatting large-scale DDoS attacks. It also highlights efforts by governmental agencies, industry consortia, and research communities to address DDoS threats. However, this method requires significant computational resources and is not efficient.

Based on this review, several DDoS-related problems persist. These include the absence of real-time data, algorithm complexity, performance overhead, and scalability challenges. These issues demand substantial computational resources, directly impacting Quality of Service (QoS) indicators like high average packet loss, latency, timing, and inefficient CPU utilization.

3. The aim and objectives of the study

The aim of this study is the development of a hybrid intrusion detection system that combines Suricata, an intrusion detection system (IDS) with pfSense, a firewall. This will make it possible to enhance the overall performance and reliability of communication services, commonly referred to as Quality of Service (QoS).

To achieve this aim, the following objectives are accomplished:

– to develop a network topology for mitigation;

– to evaluate the average total number of packets, reduce latency/timing and decrease CPU utilization.

4. Materials and methods

The object of this research is DDoS attack combat strategies using IDS with pfSense. The hypothesis of the study involves blocking the packets sent by attackers through the pfSense firewall, thereby enabling the server computer to operate optimally. The assumptions made in this work are that the router, acting as a central node, manages the flow of data between the devices in this topology. This arrangement simplifies the management and monitoring of network security. The simplifications adopted in this work include researching, simulating, and implementing a solution on a campus ad-hoc network with a limited number of computers.

The software specifications to be utilized in the design of IPv6 networks on the IDS system are as follows:

– Linux Debian 9.5 Operating System: For network design, the server device will employ the Linux Debian 9.5 operating system, specifically installed for conducting DDoS attack tests on the Web Server;

– PfSense Firewalls: pfSense, a free BSD Linux distribution serving as a firewall and router, will be utilized. PfSense will be employed to block the attacker's IP address, preventing attacks on the server;

– Suricata: Suricata, an IDS software, will detect incoming attacks from both internal and external sources. Configuration and installation of Suricata will occur on pfSense;

– Kali Linux Operating System 2021.2: Kali Linux, designed for penetration testing and computer security, will be installed on the attacker PC for experimental attacks on the server.

Additionally, the hardware specifications for this test involve three computers, each employing distinct operating systems: Linux Debian 9.5, Kali Linux, pfSense, and Windows 10.

5. Results of the attack scenario, data collection and system analysis

5. 1. Development of network topology

The Suricata IDS detects the destination of an attack in real-time, providing intrusion prevention and network security monitoring. Suricata was developed by the Open Information Security Foundation (OISF), a non-profit organization funded by the US Department of Homeland Security. The proposed strategy effectively mitigates the impact of attacks by blocking the packets sent by attackers through the pfSense firewall, thereby enabling the server computer to operate optimally.

The hybrid IDS with pfSense firewall approach significantly improves overall network security, serving as a vital tool for safeguarding computer networks against cyber attacks. The findings of this study demonstrate the effectiveness of the proposed approach in real-time attack detection and mitigation, leading to enhanced network performance and reduced risk of cyber threats. Fig. 1 depicts the proposed network topology for mitigation, illustrating the configuration and interaction of the Suricata IDS and pfSense firewall. By effectively detecting and blocking malicious packets, this approach improves overall network performance and reduces the vulnerabilities associated with cyber threats.

Fig. 1 illustrates the network design employed for mitigation. The design consists of several components, including one router (5506-X) functioning as a firewall, two personal computers (PC-PT) serving as the server and the client, one switch, and ten attacker PCs. The server PC operates on Linux Debian 9.5, the client PC utilizes Windows 10, and the attacker PCs are equipped with Kali Linux 2021.1.

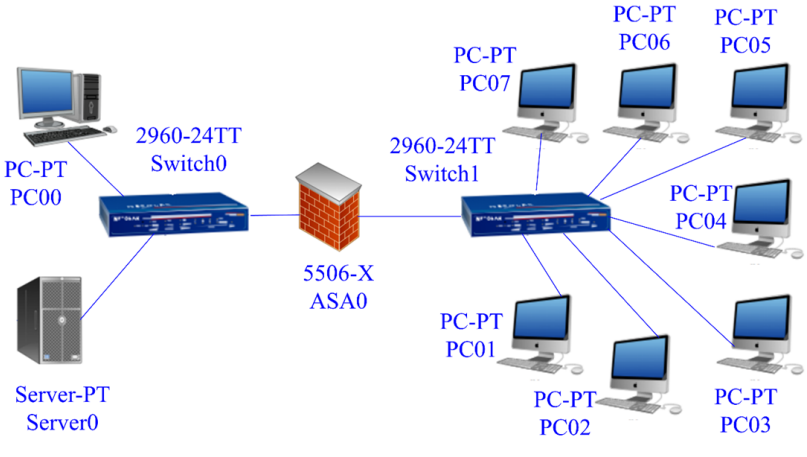

Fig. 1. Network topology for mitigation

The network design depicted in Fig. 1 employs a combination of the Star and Bus topologies to establish a robust network infrastructure capable of withstanding cyber threats. In contrast, the Bus topology is utilized for the firewall and attacker PCs. In this topology, all devices are connected to a common communication channel, creating a linear structure. The router, acting as a central node, plays a crucial role in managing the flow of data between the devices in this topology. The Bus topology simplifies network management and monitoring, enabling effective security measures to be implemented. After designing the network topology as shown in Fig. 1, the next step involves configuring the IP addresses for each device. This configuration allows the devices to communicate with one another seamlessly. To facilitate this communication, Table 1 presents a list of IPv6 addresses assigned to each device depicted in Fig. 1.

Fig. 2 provides a comprehensive view of the commands used to execute the DDoS attack on the server. The atk6-thcsyn6 command is a powerful tool specifically designed for conducting DDoS attacks on IPv6 networks. It empowers the attacker to flood the target server with an extensive volume of packets, leading to a situation of denial of ser-

vice. However, the network incorporates robust security measures, including an Intrusion Detection System (IDS) and the pfSense firewall, which work together to thwart the attack and prevent any damage to the network. When the IDS detects the incoming DDoS attack, it promptly sends an alert to the pfSense firewall. The firewall, in response, blocks the IP address of the attacker, as illustrated in Fig. 3. This action effectively prevents the attacker's device from sending further malicious packets, thereby mitigating the impact of the DDoS attack on the victim's server.

Table 1

IPv6 Addresses on Network Devices

Devices	Mac Address	Ip Address
PfSense	00:0c:29:E5:8c:Ca	2016:Abcd:12ee::1
Server	00:0c:29:68:4d:A9	2016:Abcd:12ee::10
Client	00:50:56:C0:00:08	2016:Abcd:12ee::22
Attacker 1	00:0c:29:74:Bb:5f	2016:Abcd:12ee::12
Attacker 2	00:0c:29:74:Bb:5f	2016:Abcd:12ee::13
Attacker 3	00:0c:29:74:Bb:5f	2016:Abcd:12ee::14
Attacker 4	00:0c:29:74:Bb:5f	2016:Abcd:12ee::15
Attacker 5	00:0c:29:74:Bb:5f	2016:Abcd:12ee::16
Attacker 6	00:0c:29:74:Bb:5f	2016:Abcd:12ee::17
Attacker 7	00:0c:29:74:Bb:5f	2016:Abcd:12ee::18

1. atk6-thcsyn6: is the command used for DDoS attacks on IPv6
2. -S: command used to attack TCP, SYN, and ACK packets.
3. -p: is the command used to list the source port used to attack the victim.
4. -s: is the source IPv6 address.
5. eth0: the interface used by the attacker.
6. 2016:ABCD:12EE::10 The victim's IPv6 address.
7. 5201: victim's destination port.

Fig. 2. The commands used to attack the victim's server

To facilitate the detection of atk6-thcsyn6 attacks, specific rules are implemented in Suricata, the IDS. These rules are designed to identify the characteristic patterns and behaviors associated with such attacks, enabling the IDS to promptly recognize and raise an alert for further action. The rules used in Suricata to detect atk6-tchsyn6 attacks are as follows: alert tcp any any→any any (msg:"Possible DDoS Attack with SYN/ACK Flags"; flags:SA; classtype:misc-activity; priority:1; flow:stateless; threshold: type both, track by_dst, count 50, seconds 1; sid:1000003; rev:1).

In Fig. 4, the attacker initiates a DDoS attack using the atk6-thcsyn6 command. This command generates a significant volume of SYN and ACK packets, which are directed towards the server, resulting in a flood of network traffic. The objective of this attack is to overwhelm the server's resources by inundating it with an excessive number of requests. Consequently, legitimate clients may find it challenging to access the server's services. To mitigate the impact of this DDoS attack, the network employs a comprehensive security system that includes pfSense with preconfigured rules. These rules are designed to identify and prevent DDoS attacks. When the attack traffic passes through pfSense, these rules are applied to analyze the network packets and detect patterns indicative of a DDoS attack. Specifically, the rules are programmed to recognize the atk6-thcsyn6 command, which is characteristic of such attacks.

Upon detecting a DDoS attack, the security system logs the event and immediately alerts the network administrator through the pfSense web interface. This alert enables the administrator to promptly respond and mitigate the attack. By analyzing the information provided, the administrator can identify the IP address of the attacker's device and initiate appropriate actions.

In this case, pfSense automatically takes action by blocking the attacker's IP address. This proactive measure prevents any further traffic from being sent by the attacker's device, effectively neutralizing the ongoing DDoS attack and protecting the server's resources. By leveraging the capabilities of pfSense with its preconfigured rules, the network is equipped to detect and mitigate DDoS attacks. The logging and alerting features of the security system empower the administrator to promptly respond to security incidents, identify the attackers, and take necessary actions to safeguard the network's integrity.

1. Alert: is a signature that is used to provide a warning that an attack is detected.
2. tcp any any: TCP is the protocol you want to use. While any any is the address of the attacker and the port of the attacker. Because it uses any any, all addresses or ports will be detected.
3. -> : is the direction to get to the target.
4. any any: is the target IP address and target port.
5. msg:"Possible DDoS Attack with SYN/ACK Flags": is the message that will be shown in the alert notification.
6. Flags: SA: is a component contained in the packet header. These rules will capture SYN and ACK packets.
7. classtype: attempted-dos: is a keyword that will provide information about the classification and warning rules.
8. Flow: is a rule format used to match the flow direction from/to the client or from/to the server.
9. Priority:1; This format will prioritize rules to match incoming attacks.
10. threshold: type both: is a parameter used to determine the minimum for the rules before giving a warning.
11. track by_dst: this command is used to track according to the destination IP address.
12. count 50, seconds 1: these rules will determine 50 incoming packets in 1 second.
13. sid:1000001; rev:1: is the id of the created rule. While rev is the first revision of the rules.
14. If the DDoS attack is still not detected by IDS Suricata, it will reconfigure the Suricata rules. The following is a schematic image of the attack from the DDoS test:

Fig. 3. The commands used to attack the victim's server by flooding

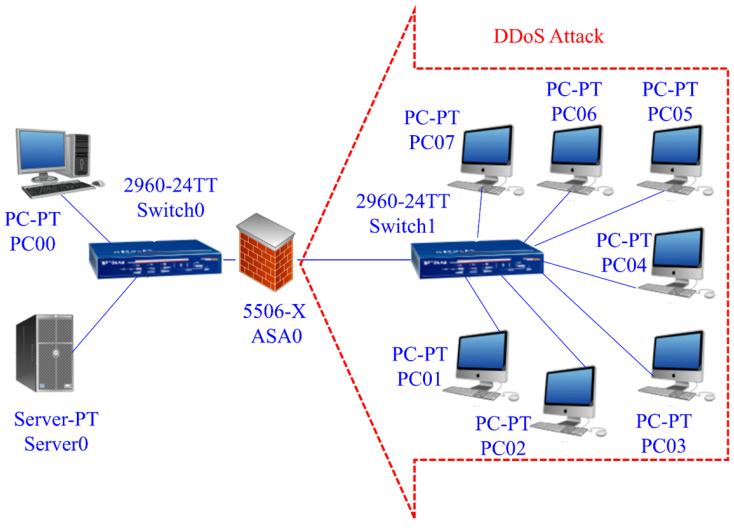

Fig. 4. DDoS attack scenario

The data analyzed in this study pertains to network conditions under both normal circumstances and during attacks. A comparison is made between the data obtained from normal networks and abnormal networks. The measurements were conducted in several scenarios, including when the network was operating normally, when it was under attack without pfSense, and when it was under attack with pfSense installed. The attack was solely performed on the server computer, and the measured parameters included Packet Loss, Jitter, Delay, Throughput, and CPU Utilization.

The first scenario in this study involves the retrieval of data from a network operating under normal conditions. Wireshark software will be utilized to retrieve the data from the client computer. To perform the test, the client computer will transmit TCP packets 30 times within a duration of 30 seconds, utilizing a bandwidth of 10MB via the iperf3 software. Upon completion of the test, the data packets will be captured using Wireshark, and measurements will be taken for Jitter, Delay, Packet Loss, Throughput, and CPU Utilization.

Fig. 5 illustrates the network's condition under normal circumstances. In this particular scenario, Wireshark captures the data on the server computer, which is subsequently analyzed to determine the obtained Quality of Service (QoS) value. In this scenario, the server computer is not protected by the pfSense firewall and is directly targeted by an attacker using a DDoS attack. The test conducted in this scenario is similar to the one carried out in the first scenario, with the distinction that in the second scenario, the attacker launches a DDoS attack on the server computer directly, employing various techniques. In detail, Fig. 5 provides a visual representation of the attack scenario, which occurs in the absence of pfSense firewall and Suricata IDS.

Fig. 5 depicts the scenario in which the server computer is under attack by an assailant without the protection of the pfSense firewall. In this situation, the attacks are directed straight at the server since there are no filter rules in place to detect and prevent such attacks. As a result of the high density of network traffic caused by the attack, the client may encounter difficulties in sending TCP packets to the server computer. Nonetheless, the attack can be detected by the Suricata IDS, which has been configured with appropriate rules.

In this scenario, the server computer is attacked by an attacker using a DDoS attack, which floods the server computer with SYN and ACK packets on port 5201. Fig. 6 shows the scenario in which the server computer is being attacked by an attacker, but is protected by the pfSense firewall and Suricata IDS. The Suricata IDS has been configured with rules to detect incoming attacks, allowing it to identify the attacker's actions as shown in Fig. 6. Once the attack is detected, the pfSense firewall will block the IP address of the attacker, preventing further attacks. Additionally, in this scenario, data is collected to determine the QoS value on the server computer using Wireshark software.

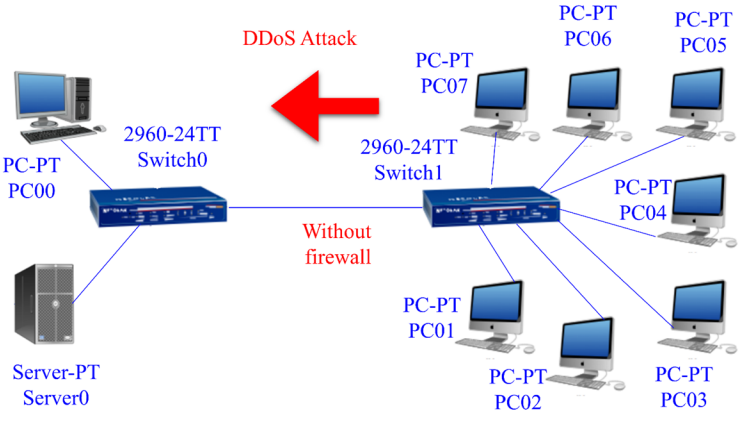

Fig. 5. DDoS attack scenario

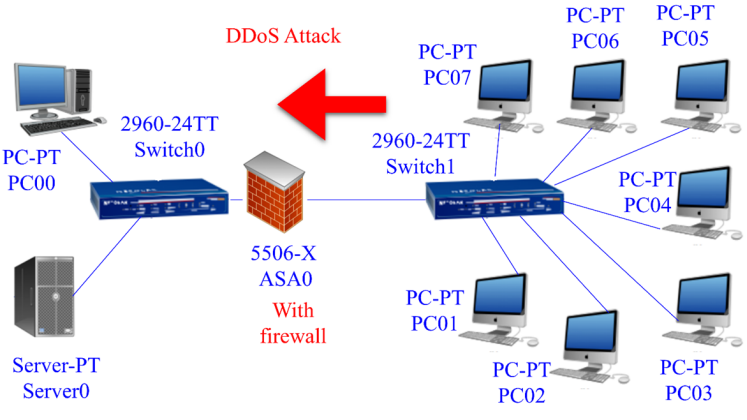

Fig. 6. Conditions attacked with pfSense firewall

In detail, the DDoS attacks originating from PC01 to PC07 through the 2960-24TT switch will be effectively blocked using the robust capabilities of the 5506-X firewall. In the process of identifying and analyzing these attacks, various crucial parameters can be assessed. These parameters include the quantity, source, and nature of the DDoS attack traffic. Subsequently, a pivotal step involves closely monitoring the network's performance to ensure its uninterrupted efficiency. Then, it becomes imperative to pinpoint the precise location of the attacks. This entails discerning

whether the attack originates from PC01 or any other sources, or if it affects all locations simultaneously. The next phase encompasses conducting an experimental approach to validate the effectiveness of the mitigation measures. Through meticulous experimental analysis, the outcomes and success of the firewall's defensive mechanisms can be ascertained.

5. 2. Evaluation of the average total number of packets, latency/timing and CPU utilization

The connection evaluation is applied before attacking investigation. Using ping command, it replies successfully as shown in Fig. 7 and Table 2. In order to detect incoming attacks, an intrusion detection system (IDS) is required.

```
C:\Users\ALL MIGHT>ping 2016:abcd:12ee::10

Pinging 2016:abcd:12ee::10 with 32 bytes of data:
Reply from 2016:abcd:12ee::10: time=1ms
Reply from 2016:abcd:12ee::10: time<1ms
Reply from 2016:abcd:12ee::10: time<1ms
Reply from 2016:abcd:12ee::10: time<1ms

Ping statistics for 2016:abcd:12ee::10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\ALL MIGHT>
```

Fig. 7. Ping connection evaluation

After detecting incoming attacks using the Suricata IDS, the next step is to prevent the attacks from continuing.

Table 2

Ping connection evaluation results

Devices	IP Source	Ip Address Destination	Status
PfSense	00:0c:29:E5:8c:Ca	2016:Abcd:12ee::1	Connected
Server	00:0c:29:68:4d:A9	2016:Abcd:12ee::10	Connected
Client	00:50:56:C0:00:08	2016:Abcd:12ee::22	Connected
Attacker 1	2016:Abcd:12ee::12	2016:Abcd:12ee::10	Connected
Attacker 2	2016:Abcd:12ee::13	2016:Abcd:12ee::10	Connected
Attacker 3	2016:Abcd:12ee::14	2016:Abcd:12ee::10	Connected
Attacker 4	2016:Abcd:12ee::15	2016:Abcd:12ee::10	Connected
Attacker 5	2016:Abcd:12ee::16	2016:Abcd:12ee::10	Connected
Attacker 6	2016:Abcd:12ee::17	2016:Abcd:12ee::10	Connected
Attacker 7	2016:Abcd:12ee::18	2016:Abcd:12ee::10	Connected

The addresses and protocols chosen are IPv6 and TCP since the attacks had TCP protocols and IPv6 addresses. For the source IP, the researchers created a list to make it easier to enter the attacker's IP address, and for the destination, the "LAN net" option was selected to protect all devices on the same local network. Fig. 8 shows the list of attacker's IP addresses. In Fig. 8, there are 7 known attacker IP addresses that have been detected by the Suricata IDS. To simplify the process of entering an IP address without having to repeatedly create firewall rules, the researchers used IP Aliases. Once the rules are created on the pfSense firewall, any attack by the attacker will be successfully blocked. The log image of the pfSense firewall is shown in Fig. 9.

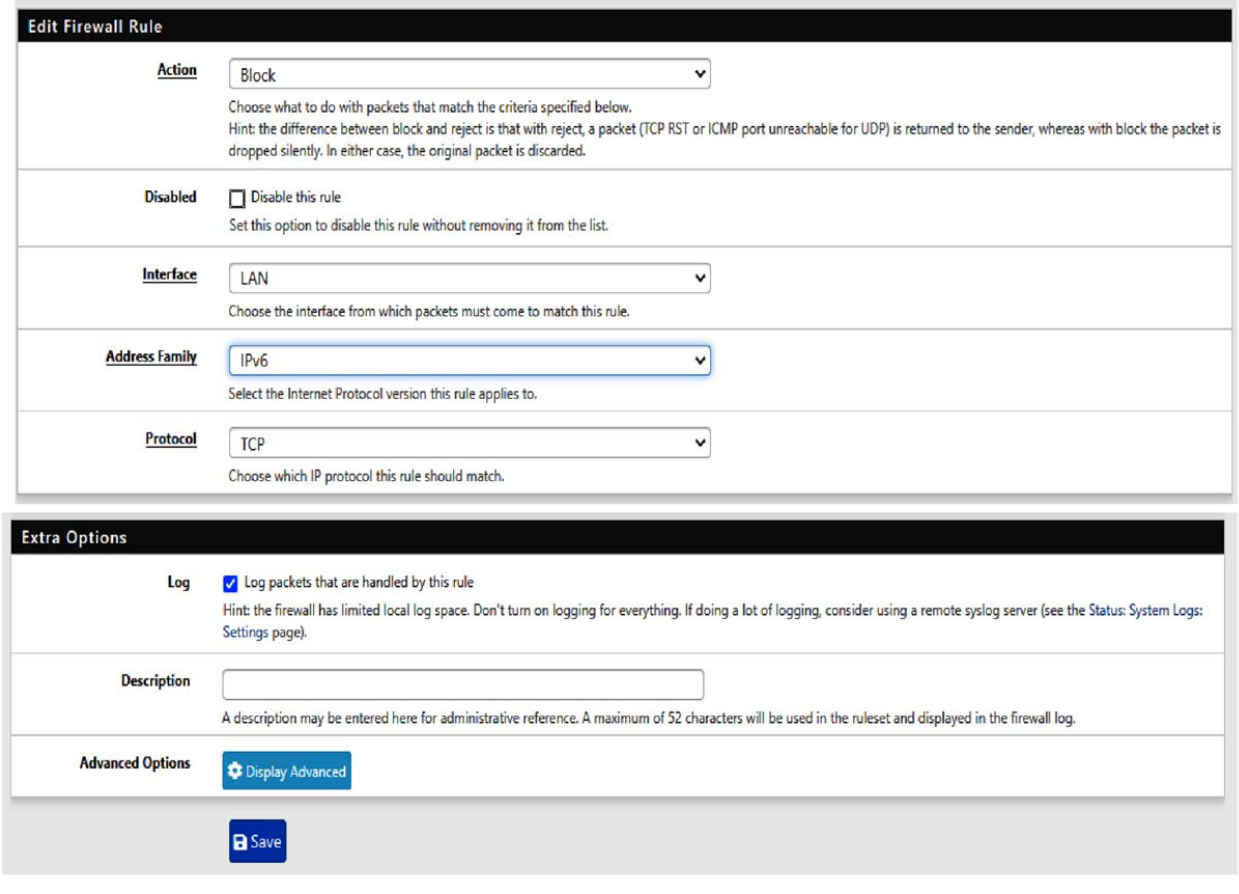

Fig. 8. IP Aliases

Action	Time	Interface	Rule	Source	Destination	Protocol
✕	Dec 10 17:30:23	LAN	USER_RULE (1639111942)	[2016:abcd:12ee::12]:5201	[2016:abcd:12ee::10]:5201	TCP:SA
✕	Dec 10 17:30:23	LAN	USER_RULE (1639111942)	[2016:abcd:12ee::12]:5201	[2016:abcd:12ee::10]:5201	TCP:SA
✕	Dec 10 17:30:23	LAN	USER_RULE (1639111942)	[2016:abcd:12ee::12]:5201	[2016:abcd:12ee::10]:5201	TCP:SA
✕	Dec 10 17:30:23	LAN	USER_RULE (1639111942)	[2016:abcd:12ee::12]:5201	[2016:abcd:12ee::10]:5201	TCP:SA
✕	Dec 10 17:30:23	LAN	USER_RULE (1639111942)	[2016:abcd:12ee::12]:5201	[2016:abcd:12ee::10]:5201	TCP:SA
✕	Dec 10 17:30:23	LAN	USER_RULE (1639111942)	[2016:abcd:12ee::12]:5201	[2016:abcd:12ee::10]:5201	TCP:SA
✕	Dec 10 17:30:23	LAN	USER_RULE (1639111942)	[2016:abcd:12ee::12]:5201	[2016:abcd:12ee::10]:5201	TCP:SA
✕	Dec 10 17:30:23	LAN	USER_RULE (1639111942)	[2016:abcd:12ee::12]:5201	[2016:abcd:12ee::10]:5201	TCP:SA
✕	Dec 10 17:30:23	LAN	USER_RULE (1639111942)	[2016:abcd:12ee::12]:5201	[2016:abcd:12ee::10]:5201	TCP:SA
✕	Dec 10 17:30:23	LAN	USER_RULE (1639111942)	[2016:abcd:12ee::12]:5201	[2016:abcd:12ee::10]:5201	TCP:SA

Fig. 9. Firewall Detects Attacks from 2016:abcd:12ee::12

Fig. 9 demonstrates the successful blocking of attacks directed at the server computer address via port 5201 by the pfSense firewall, even when the attacks included SYN and ACK flags. Following this successful prevention of the attack, five parameters were measured to evaluate the QoS – delay, jitter, packet loss, throughput, and CPU utilization.

To evaluate the throughput, three different scenarios were tested, and measurements were taken to determine the amount of data actually transmitted from the client to the server at a given time. The measurements were conducted using units of Bytes/s and Bit/s. A measurement graph illustrating the results is provided in Fig. 10, which was obtained from the tests conducted. Fig. 10 presents three graphs with different colors: black for normal networks, red for tests conducted without protection from the pfSense firewall, and blue for tests with the firewall protecting the server computer from attackers.

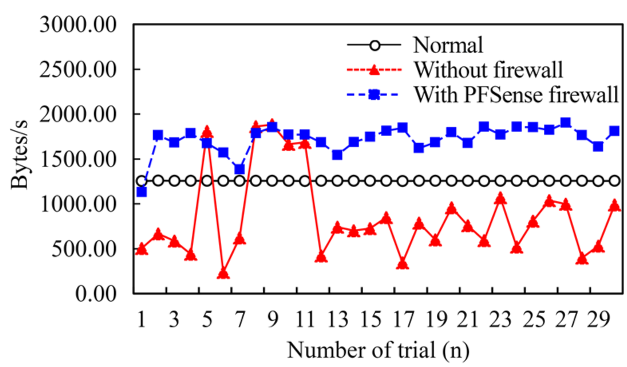

Fig. 10. Throughput Measurement

Fig. 11 presents the results of packet loss analysis conducted in two scenarios. In the first scenario, the packet loss value obtained is 0 %, indicating that the server computer is functioning normally, and communication between the client and server is uninterrupted. This result is considered excellent as achieving a packet loss value of 0 % is optimal for network performance.

The second scenario, represented by the red graph in Fig. 11, shows that the packet loss value varies across tests. In the 3rd, 6th, 9th, and 11th tests, the packet loss value is 0 %. However, due to the DDoS attack carried out by the attacker, the network traffic on the server computer becomes congested, leading to a higher percentage of packet loss. The attack also interrupts the connection between the client and server, resulting in fewer TCP packets reaching the server.

As shown in Fig. 12, the total number of packets sent by the client to the server is the highest in the normal condition with 3479 packets.

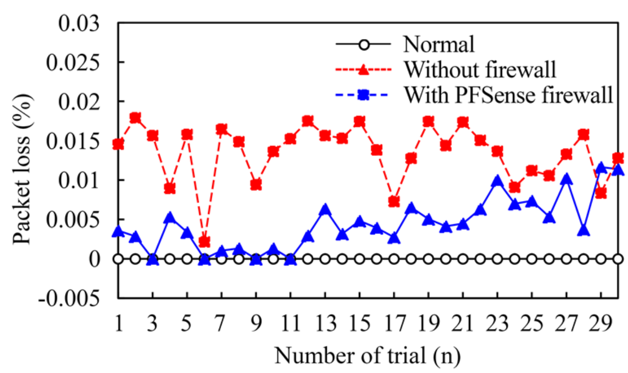

Fig. 11. Packet Loss Measurement

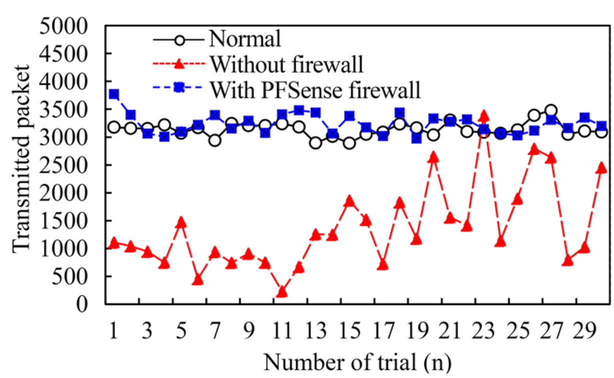

Fig. 12. Total number of packets sent

However, when the server computer is attacked by the attacker, the total number of packets sent decreases significantly. In the 11th test, as seen in the red graph, the total number of packets sent by the client decreased drastically by 93.22 % to 236 packets due to the attack.

6. Discussion of hybrid IDS based on Suricata with pfSense

First, we have successfully developed a network topology as shown in Fig. 1. The network topology utilized in this design combines the star topology for the client and server PCs and the bus topology for the firewall and attacker PCs.

The star topology is employed for the server and client PCs, where each device is directly connected to the switch, forming a star-shaped configuration. This topology offers high scalability and fault tolerance, allowing devices to be easily added or removed without affecting the overall functionality of the network. On the other hand, the bus topology is utilized for the firewall and the attacker PCs. In this topology, all devices are connected to a single communication channel, creating a linear structure.

By combining the Star and Bus topologies and configuring the IP addresses accordingly, this network design aims to establish a resilient and secure environment for data transmission. The proposed network architecture, along with the proper configuration of IP addresses, forms a solid foundation for implementing effective security measures against cyber threats. The proposed attack scenario involves using Distributed Denial of Service (DDoS) techniques with IPv6 addresses. In this attack scenario, the attacker's PC will utilize the atk6-thcsyn6 command to launch a DDoS attack on the server. The objective of the attack is to overwhelm the server by flooding it with a large number of TCP, SYN, and ACK packets, rendering it unavailable to legitimate users. The Suricata IDS successfully detected seven attacks that were directed at the server computer using the TCP protocol and passing through port 5201 with the IP address. The throughput value obtained from the initial test to the final deployment remains constant. This is because the server computer was not attacked, and communication between the client and server proceeded normally.

Second, the evaluation of the average total number of packets/throughput, reduction in latency/timing and decrease in CPU utilization was successfully developed. Fig. 10 shows that when the server computer was attacked and not protected by the pfSense firewall, the lowest throughput value obtained was 237.32 Bytes/s, in the 6^{th} test, representing a decrease of 81.11 %. This reduction was due to DDoS attacks, which congested the network traffic of the server computer and depleted its resources. However, the attack was successfully detected by the Suricata IDS, enabling the source of the attack to be identified. In the final scenario depicted by the green graph, the highest throughput value was obtained in the 27^{th} test, with a value of 1902.45 Bytes/s, representing an increase of 1.08 % compared to the previous scenario. The lowest value in this scenario was obtained in the first test with a throughput value of 1128.42 Bytes/s, representing an increase of 78.97 %. The use of the pfSense firewall resulted in an increase in the throughput value, as attacks by attackers were effectively blocked, enabling the server computer's performance to return to normal and preventing attack interference. Overall, the results indicate that the pfSense firewall was effective in protecting the server computer from attacks and maintaining normal network performance.

The highest percentage of packet loss observed in this scenario is 1.17 %, recorded in the 29^{th} test. The number of packets sent by the client is depicted in the graphic image below the red graph, enabling a better understanding of the impact of the attack on the network's behavior. It is important to note that packet loss can adversely affect network performance, causing latency and impacting the user experience. Therefore, monitoring and analyzing packet loss is crucial to maintaining optimal network performance.

Then, when the server computer is protected by the pfSense firewall, the total number of packets sent by the client increases by 93.74 % to 3772 packets. Although the attacker attempted to attack the server computer, the pfSense firewall successfully blocked the attack, allowing the server to function normally.

This research limitations include its focus on a campus ad hoc network with limited computers. Future studies could improve by expanding to larger computer number, diverse networks not only for campus networks to obtain broader insights.

7. Conclusions

1. This study successfully developed a network topology. The configuration and interaction of the Suricata IDS and pfSense firewall were effectively detecting and blocking malicious packets. This approach improves overall network performance and reduces the vulnerabilities associated with cyber threats.

2. The results of our study indicate a 1.08 % increase in throughput value, from 1881.97 bytes to 902.44 bytes, demonstrating improved efficiency in data transmission. Additionally, we observed a 57.32 % increase in the average total number of packets sent, from 1,382 packets to 3,238 packets, indicating better network performance. Furthermore, the proposed strategy significantly reduced delay and jitter values. The delay value decreased by 88.78 %, from 90.76 ms to 10.18 ms, and the jitter value decreased by 88.99 %, from 181.85 ms to 20.03 ms. These improvements signify a notable reduction in latency and packet timing variations, leading to a smoother network experience. Another crucial aspect we evaluated was the CPU utilization. The proposed strategy resulted in a substantial decrease in CPU utilization by 81.23 %, from 78.3 % to 14.7 %. These findings emphasize the importance of implementing robust network security measures, particularly when defending against DDoS attacks. Future research can further explore advanced techniques and strategies to enhance the effectiveness of IDS and firewall systems in protecting network infrastructures.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

The study was performed with financial support by Direktorat Riset, Teknologi, and Pengabdian Masyarakat under the Ministry of Research, Technology and Higher Education of Indonesia, 2023.

Data availability

The data will be made available on reasonable request.

References

1. Choi, K.-S., Lee, C. S., Louderback, E. R. (2020). Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 27–43. doi: https://doi.org/10.1007/978-3-319-78440-3_2
2. Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., Khan, M. K. (2020). Comprehensive Review of Cybercrime Detection Techniques. IEEE Access, 8, 137293–137311. doi: https://doi.org/10.1109/access.2020.3011259
3. Cascavilla, G., Tamburri, D. A., Van Den Heuvel, W.-J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers & Security, 105, 102258. doi: https://doi.org/10.1016/j.cose.2021.102258
4. Staroletov, S. (2022). Software Architecture for an Intelligent Firewall Based on Linux Netfilter. 2022 25th Conference on Innovation in Clouds, Internet and Networks (ICIN). doi: https://doi.org/10.1109/icin53892.2022.9758121
5. Cinar, A. C., Kara, T. B. (2023). The current state and future of mobile security in the light of the recent mobile security threat reports. Multimedia Tools and Applications, 82 (13), 20269–20281. doi: https://doi.org/10.1007/s11042-023-14400-6
6. Oloyede, O. A., Yekini, A. N., Akinwole, K. A., Ojo, O. (2021). Firewall Approach To Computer Network Security: Functional Viewpoint. International Journal of Advanced Networking and Applications, 13 (03), 4993–5000. doi: https://doi.org/10.35444/ijana.2021.13308
7. Heino, J., Hakkala, A., Virtanen, S. (2022). Study of methods for endpoint aware inspection in a next generation firewall. Cybersecurity, 5 (1). doi: https://doi.org/10.1186/s42400-022-00127-8
8. Ho, H. T. N., Luong, H. T. (2022). Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis. SN Social Sciences, 2 (1). doi: https://doi.org/10.1007/s43545-021-00305-4
9. Moneva, A., Leukfeldt, E. R., Klijnsoon, W. (2022). Alerting consciences to reduce cybercrime: a quasi-experimental design using warning banners. Journal of Experimental Criminology. doi: https://doi.org/10.1007/s11292-022-09504-2
10. La Rosa, G. (2021). The 5G Technology Nexus: Assessing Threats and Risks of Implementation. Univerzita Karlova.
11. Afolaranmi, A. O. (2022). Towards Understanding the Nexus between Pastoral Care, Social Media, and Sustainable Development in the Post-COVID-19 Era. doi: https://doi.org/10.21203/rs.3.rs-1630706/v1
12. Gundur, R. V., Levi, M., Topalli, V., Ouellet, M., Stolyarova, M., Chang, L. Y.-C., Mejía, D. D. (2021). Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context. CrimRxiv. doi: https://doi.org/10.21428/cb6ab371.5f335e6f
13. Chowdhury, N., Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. Computer Science Review, 40, 100361. doi: https://doi.org/10.1016/j.cosrev.2021.100361
14. Gupta, B. B., Perez, G. M., Agrawal, D. P., Gupta, D. (Eds.) (2020). Handbook of Computer Networks and Cyber Security. Springer Cham, 959. doi: https://doi.org/10.1007/978-3-030-22277-2
15. Rawat, S., Srinivasan, A., Ravi, V., Ghosh, U. (2020). Intrusion detection systems using classical machine learning techniques vs integrated unsupervised feature learning and deep neural network. Internet Technology Letters, 5 (1). doi: https://doi.org/10.1002/itl2.232
16. Reshmi, T. R. (2021). Information security breaches due to ransomware attacks - a systematic literature review. International Journal of Information Management Data Insights, 1 (2), 100013. doi: https://doi.org/10.1016/j.jjimei.2021.100013
17. Balakrishnan, N., Rajendran, A., Pelusi, D., Ponnusamy, V. (2021). Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things. Internet of Things, 14, 100112. doi: https://doi.org/10.1016/j.iot.2019.100112
18. Naeem, M. A. A., Abubakar, A., Rahman, M. M. H. (2020). Dealing With Well-Formed and Malformed Packets, Associated With Point of Failure That Cause Network Security Breach. IEEE Access, 8, 197554–197566. doi: https://doi.org/10.1109/access.2020.3034383
19. Ouiazzane, S., Addou, M., Barramou, F. (2022). A Suricata and Machine Learning Based Hybrid Network Intrusion Detection System. Lecture Notes in Networks and Systems, 474–485. doi: https://doi.org/10.1007/978-3-030-91738-8_43
20. Gupta, A., Sharma, L. S. (2019). Performance Evaluation of Snort and Suricata Intrusion Detection Systems on Ubuntu Server. Proceedings of ICRIC 2019, 811–821. doi: https://doi.org/10.1007/978-3-030-29407-6_58
21. Praptodiyono, S., Firmansyah, T., Murugesan, R. K., Alaydrus, M., Aprilia, R., Leau, Y.-B. (2021). Improving the security of mobile IPV6 signalling using KECCAK / SHA-3. Journal of Engineering Science and Technology, 16 (3), 2312–2325. URL: https://jestec.taylors.edu.my/Vol%2016%20issue%203%20June%202021/16_3_33.pdf
22. Scarfone, K. A., Mell, P. M. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST. doi: https://doi.org/10.6028/nist.sp.800-94
23. Shams, M., Sookhak, M., Gani, A., Buyya, R., Talebian, H. (2016). A comprehensive survey of network virtualization. Computer Networks, 108, 147–176.
24. Ramachandran, A., Feamster, N. (2006). Understanding the network-level behavior of spammers. ACM SIGCOMM Computer Communication Review, 36 (4), 291–302. doi: https://doi.org/10.1145/1151659.1159947
25. Mirkovic, J., Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34 (2), 39–53. doi: https://doi.org/10.1145/997150.997156

26. Karasaridis, A., Manousakis, K. (2017). Detection and mitigation of DDoS attacks using SDN: A comprehensive survey. IEEE Communications Surveys & Tutorials, 20 (3), 2233–2271.
27. The Treacherous 12: Top Threats to Cloud Computing (2017). Cloud Security Alliance.
28. Kolias, C., Kambourakis, G., Stavrou, A., Gritzalis, D. (2016). Distributed Denial of Service Attacks in Software-Defined Networking with Cloud Computing. IEEE Transactions on Dependable and Secure Computing, 13 (3), 373–378.
29. Ramli, R., Maarof, M. A., Zainal, A. (2017). A survey of machine learning in DDoS attack detection. Journal of Network and Computer Applications, 88, 60–76.
30. Nunes, B. A. A., Mendonca, M., Nguyen, X.-N., Obraczka, K., Turletti, T. (2014). A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. IEEE Communications Surveys & Tutorials, 16 (3), 1617–1634. doi: https://doi.org/10.1109/surv.2014.012214.00180
31. National Cyber Incident Response Plan (2010). U.S. Department of Homeland Security.
32. Steinberger, J., Sperotto, A., Baier, H., Pras, A. (2020). Distributed DDoS Defense:A collaborative Approach at Internet Scale. NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium. doi: https://doi.org/10.1109/noms47738.2020.9110300