Revista de Informática Teórica e Aplicada - RITA - ISSN 2175-2745
Vol. 32, Num. 3 (2025) 66-76

RESEARCH ARTICLE

Optimizing Mikrotik-Based Network Security using Address List, Firewall Filter Rules, and Raw Firewall

Otimização da segurança de rede baseada em Mikrotik usando lista de endereços, regras de filtro de firewall e firewall bruto

Febrian Wahyu Christanto[1]*, Putri Cholillah[1], Alauddin Maulana Hirzan[1]

Abstract: The rise of hacking access rights in computer networks has made it easy for cybercriminals to steal personal data. Based on Surfshark data during January 2020 - January 2024 explain that Indonesia became the country with the 8th most breached accounts in the world with an estimated 94.22 million breached digital accounts. Until now cyber sequrity in Indonesia is still weak in average. To minimize the occurrence of router hacking and cyber sequirty this research will implement network security optimization using the address list method, firewall filter rules, and firewall raw on Mikrotik Routers with conduct several tests. Security tests using Denial of Service (DoS) and Brute Force attack techniques carried out results evident that the use of firewall filter rules is effective to preventing Brute Force attacks that try to get the router device password with the CPU Load value dropping from 95% to 5%. However it is less effective to prevent DoS attacks with 800,000 attack packets because the CPU Load value only drops from 95% to 72%. This is still far from normal conditions. Security optimization using the raw firewall method proved more effective in preventing DoS attacks with the CPU Load value successfully dropping to 43%. So to secure the network from DoS attacks it is not enough just to use the built-in features of the Mikrotik router but also requires the support of other additional devices to increase its effectiveness in reducing the CPU load to a normal number below 10%.
Keywords: brute force — denial of service — firewall filter rules — mikrotik — network security

Resumo: O aumento dos direitos de acesso de hackers em redes de computadores facilitou o roubo de dados pessoais pelos criminosos cibernéticos. Com base nos dados do Surfshark entre janeiro de 2020 e janeiro de 2024, explica-se que a Indonésia se tornou o país com a oitava maior quantidade de contas violadas do mundo, com uma estimativa de 94,22 milhões de contas digitais violadas. Até o momento, a segurança cibernética na Indonésia ainda é fraca em média. Para minimizar a ocorrência de invasão de roteadores e sequestro cibernético, esta pesquisa implementará a otimização da segurança da rede usando o método de lista de endereços, regras de filtro de firewall e firewall bruto nos roteadores Mikrotik, com a realização de vários testes. Testes de segurança usando técnicas de ataque de negação de serviço (DoS) e de força bruta foram realizados, e os resultados evidenciaram que o uso de regras de filtro de firewall é eficaz para evitar ataques de força bruta que tentam obter a senha do dispositivo do roteador, com o valor de carga da CPU caindo de 95% para 5%. No entanto, é menos eficaz para evitar ataques de DoS com 800.000 pacotes de ataque porque o valor da carga da CPU só cai de 95% para 72%. Isso ainda está longe das condições normais. A otimização da segurança usando o método de firewall bruto mostrou-se mais eficaz na prevenção de ataques de DoS, com o valor da carga da CPU caindo para 43%. Portanto, para proteger a rede contra ataques de DoS, não basta apenas usar os recursos integrados do roteador Mikrotik, mas também é necessário o suporte de outros dispositivos adicionais para aumentar sua eficácia na redução da carga da CPU para um número normal abaixo de 10%.
Palavras-Chave: força bruta — mikrotik — negação de serviço — regras de filtro de firewall — segurança de rede

[1] *Department of Information Technology, Universitas Semarang (USM), Indonesia*
***Corresponding author**: febrian.wahyu.christanto@usm.ac.id
DOI: http://dx.doi.org/10.22456/2175-2745.142954 • **Received:** 02/10/2024 • **Accepted:** 24/05/2025

1. Introduction

With the rapid development of the Internet, the use of computer networks is becoming more and more common[1, 2]. In January 2024 there will be 5.35 billion internet users worldwide or 62.3% of the global population. However, the more internet and computer networks are used, the more threats to network security are lurking[3]. For instance someone with malicious intentions can infiltrate devices over the network and hijack the data[4] or steal user credentials such as credit card details or user ID passwords[5]. Such attacks may cause financial damage to individuals, institutions, big companies, and even state governments. Therefore, network security is a very important element and must be considered in maintaining the confidentiality, integrity, and availability of data[6, 7].

With more than 185 million internet users, Indonesia is one of the countries with the highest number of internet users in the world. As of January 2024, the country ranked fifth after China, India, the United States, and Brazil[8]. Based on Surfshark data during January 2020-January 2024 there were around 3.96 billion digital accounts that were breached in 250 countries. During this period, Indonesia became the country with the 8th most breached accounts in the world with an estimated 94.22 million leaked accounts[9]. Data of 10 countries with the biggest data breach in 2020-2024 is in Figure 1. President of ISACA Indonesia Chapter Syahraki Syahrir said that weak network security in Indonesia is not only caused by the technology because every technology has vulnerabilities. But it is caused by network management, administrator problems, and also the configuration process whether it is correct. Literacy related to cyber security is still weak in Indonesia, so it is very important to continue to provide education to every IT professional to carry out good governance related to cyber security[10, 11].

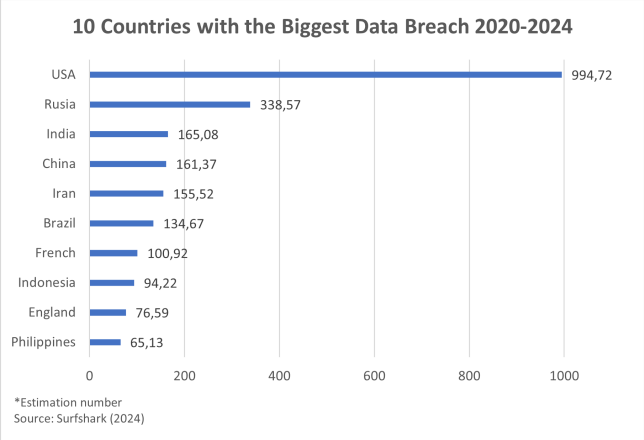

Figure 1. 10 Countries with the Biggest Data Breach 2020-2024[9]

The main target of attackers before entering the main network system or data center in general is to reduce or turn off router performance[12, 13]. The threat of cyber attacks such as DoS and Brute Force attacks can now easily attack servers or routers using tools that are easily available on the internet[14]. Denial of Service (DoS) attacks pose a serious threat to network security aiming to disrupt the availability of services or network resources through excessive data traffic[15]. For instance, disruptions caused by DoS attacks affect bandwidth, network traffic, and applications[16]. DoS attacks targeting bandwidth send an overwhelming number of data packets, aiming to overload and deplete bandwidth resources[17]. Conversely, DoS attacks targeting network traffic flood the network with large volumes of TCP, UDP, or ICMP packets. Brute force attacks can be carried out manually but often use tools such as THC Hydra, Medusa, Ncrack, etc to automate testing passwords at high speed[18, 19]. Hackers often use brute force attacks to break system security, access private accounts, or damage the system by trying all possible usernames and passwords that the attacker has prepared in a wordlist[20, 21]. The results of the attack carried out with Brute Force on the existing network make the network slow, and all network users will be disconnected[22, 23].

Based on the problems described, this research will improving the network security system by implementing the address list configuration, firewall filter rules, and firewall raw on Mikrotik to detect and block DoS and Brute Force attacks automatically. Where when there are unnatural packets entering, grouping will be done using the address list. After the attacker's IP address and destination IP address have been captured using the address list, the IP address will be dropped by firewall filter rules or firewall raw. That way the potential for attacks can be minimized and suspicious activities can be immediately identified and dealt with before causing greater losses. Then it is hoped that in the future it can be used as a reading reference related to network security using firewall filter rules and raw firewall on Mikrotik to prevent DoS and Brute Force attacks.

2. Related Work

Mikrotik is an operating system that can be used as a reliable network router including various complete features for networks and wireless[24]. Mikrotik on standard Personal Computer (PC) based hardware is known for its stable quality control and flexibility for various types of data packets and handling of the routing process[25, 26]. Mikrotik which is made as a computer-based router is very useful for an Internet Service Provider (ISP) who wants to run several applications ranging from the lightest to the most sophisticated[27]. Apart from routing it can be used for access capacity (bandwidth) management, firewalls, wireless access points, hotspot systems, virtual private network servers, and many more[28]. The address list method is one of Mikrotik's features which is a technique for grouping several IP addresses into one which can increase efficiency in using resources on the Mikrotik router thereby saving scripts (settings)[29]. The address list method makes it easier to handle an address configuration. So with the address list you can create a list of addresses you want to mark without having to disturb important configurations

Table 1. Previous Research

Research Title	Attack Type	Research Result
Enhancement Detection Distributed Denial of Service Attacks using Hybrid N-Gram Techniques[30]	DDoS Attacks	Advantages of a hybrid approach to detecting DoS attacks
Cyber-Secure SDN: A CNN-Based Approach for Efficient Detection and Mitigation of DDoS attacks[31]	DDoS Attacks	Mitigation system with BRS and CNN for DDoS attack detection in SDN environments
SDN based Intrusion Detection and Prevention System using Manufacturing Usage Description: A Survey[32]	DoS Attacks and Port Scanning	Port Scanning and DoS Attacks can be detected and stopped in real time
Mikrotik Login Security with Port-Knocking and Brute Force Firewall at PT. Time Excelindo[33]	Brute Force Attacks	Port-Knocking and Firewall systems effectively prevent Brute Force attacks
Brute Force Attack on Real World Passwords[34]	Brute Force Attacks	Implementing a firewall on a router can prevent Brute Force attacks

in other features[35, 36]. The implementation of the firewall and address list features on the Mikrotik router is good to use because it can provide network security and limit the IP addresses that can be accessed and cannot be accessed[37].

A firewall is a system or network security device that monitors incoming and outgoing network traffic and decides whether to allow or block certain traffic based on specified security rules[38]. Filter Rules are one of the features found in the firewall. This feature is usually used to filter access (filter rules) and create policies regarding whether or not traffic is permitted on a network, identical to accept, reject, or drop[39, 40]. Firewall raw will examine the data received and track the connections made to determine whether the connection is allowed or denied. Rejected data is data sent by ports that have been blocked from accessing by the firewall raw. Then the firewall will block the unauthorized IP address if it tries to make a request. Data that is allowed to enter the network is data sent by ports that are not blocked by the firewall raw[41]. Conceptually, firewall raw can perform filtering like firewall filter rules. And usually used to protect the network from DoS attacks. Firewall raw can also be used to bypass or drop certain connections so as not to burden the router[42]. Applying the firewall raw method produces several benefits, including saving resource usage, this is because the firewall raw makes it possible to skip or drop a connection before entering the connection-tracking process[43].

Before this research was carried out, several discussions and research results needed to be studied in more depth to add the necessary information. Some of the literature includes research related to improving network security, Mikrotik, address lists, firewall filter rules, and firewall raw. Several previous researches that have been carried out related to improving network security against DoS and Brute Force attacks using firewalls are listed in Table 1.

Based on Table 1, shows several results from previous research related to increasing network security using the firewall feature on Mikrotik. The difference between this research and previous research is that the previous research carried out the development of an existing computer network system, whereas the author built a simple network system that was used to simulate performance analysis of address lists, firewall filter rules, and firewall raw to optimize network security using a Mikrotik router so that it does not require many devices. The next difference is that in previous research, no one has used two attack methods at once, Brute Force and DoS, in network security testing. This research will compare the test results of each security condition to determine the security level of the Mikrotik router when using the firewall filter rules and firewall raw methods. This is what is offered in this research.

3. Proposed Method

PPDIOO (Prepare, Plan, Design, Implement, Operate, and Optimize) is a process of optimizing network performance which is considered a method that is by the research objective, namely to optimize computer network security[44]. The stages start from the ”Prepare” stage which analyzes system requirements starting from hardware, software, or literature studies needed to implement the address list method, firewall filter rules, and firewall raw on the Mikrotik router. The hardware requirements used include a Mikrotik RB941 router which has a maximum bandwidth of around 20 Mbps, 3 laptops and several UTP cables. While the software used includes the Windows Operating System, Ubuntu Operating System, Mikrotik RouterOS, Hping3 DoS Tools, Ncrack Brute Force Tools, Nmap, and Winbox. The ”Plan” stage is the stage of planning the process of improving network security using firewall filter rules and address lists on the Mikrotik router. As well as planning test scenarios and conditions using DoS and Brute Force attack techniques. The flow of the research plan from the process of determining the network topology, installing the required software, connecting the device to the internet, configuring proxy, testing using attacks, recording and analyzing test results can be seen in Figure 2.

The next stage is ”Design” where the researcher designs and describes the topology that will be used in the research as well as designing security schemes and network security testing schemes. The topology used can be seen in Figure 3.

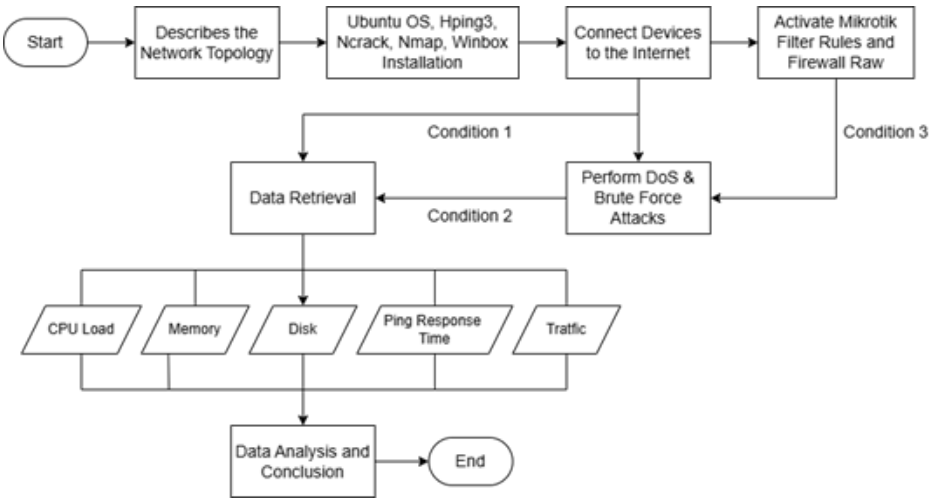

Figure 2. The Flow of Research Plan

The topology used connects the Mikrotik router with the nearest WiFi, and then spreads the internet to clients. Meanwhile, the laptop for the Mikrotik configuration is connected to the router via a UTP cable in Ether2. The IP address to be used when configuring the device can be seen in Table 2. At this stage, researchers also designed a scheme for testing DoS and Brute Force attacks against Mikrotik routers. Where the attacking laptop attacks the AP-Bridge interface, while the monitoring laptop is connected to the router via UTP cable and carries out monitoring during the attack and repairs the router configuration if problems occur. Meanwhile, the client laptop checks the internet connection speed shared by the router when an attack occurs. The test scheme can be seen in Figure 4.

To improve network security, firewall filter rules, and address lists are implemented where the firewall filter rules will check the data received and track the connections made to determine whether the connection is permitted or rejected. Rejected data is data sent by a port that has had access blocked. Then the firewall filter rules will include the attacker's IP address in the address list if they try to make a request. Data that is allowed to enter the network is data sent by ports and IP addresses that are not blocked by firewall filter rules. The security scheme using firewall filter rules can be seen in Figure 5.

After the design stage has been completed, the research process continues to the "Implementation" stage by installing software and configuring things related to the research. The configuration starts with the Mikrotik router running the standard internet connection function by being configured as a Repeater, where the router captures the surrounding WiFi signal in Station mode and shares it back to the user in AP Bridge mode, but only uses one WLAN interface. With wireless configuration, IP addressing, DNS, and routing and NAT Masquerade configuration for local network security. After the client successfully gets an internet connection from the router, the router is configured to detect and block DoS and Brute Force attacks using firewall filter rules, address lists, and firewall raw.

The next stage is "Operate" by testing DoS and Brute Force attacks against the Mikrotik router under several security conditions. During this stage, researchers detect errors, correct configurations, and monitor performance activities by measuring several indicators. Several indicators that are measured when testing DoS attacks include CPU, memory, disk, ping response time, and traffic[45]. Meanwhile, Brute Force attacks use the CPU indicator and the success of the attack is an attack that tries to log into the router by trying the password and username which are successfully detected. Testing was carried out using the Ubuntu Operating System, for DoS attacks using the Hping3 tool using the Syn Flood technique on port 80 and ICMP Flood[46]. Based on the DoS attack report in the first quarter of 2021 released by Securelist from Kaspersky, DoS attacks are carried out with an average duration of under 4 hours[47]. Therefore this research takes the duration of testing and monitoring of DoS attacks for approximately 30 minutes for each security condition, assuming that the resulting value of the DoS attack can be seen in the monitoring tools, so as to produce a value with the right level of accuracy in each indicator. For Brute Force attacks, use the Ncrack tool by carrying out attacks on ports 22 (SSH) and 23 (Telnet).

Meanwhile, the security conditions tested against DoS and Brute Force attacks include normal conditions before attack testing (Condition 1) where the Mikrotik router runs the standard function of an internet connection with a configuration as a repeater. This condition aims to see the router's

Table 2. IP Address Topology

Device	***Port***	**IP Address**
ISP	WLAN	192.168.1.6/24
Mikrotik RB941	Ether2	192.168.10.1/24
Virtual WLAN	AP-Bridge	192.168.20.1/24

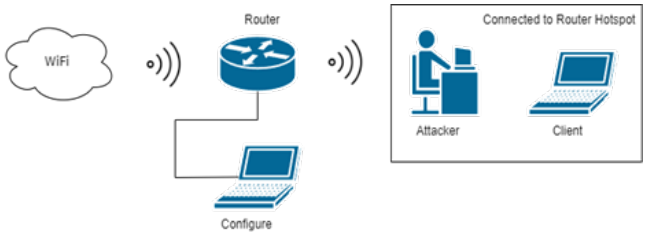

Figure 3. Network Topology

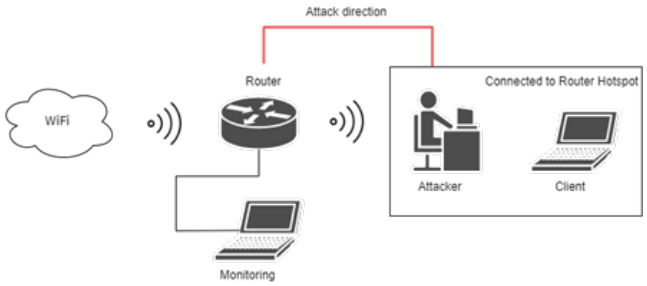

Figure 4. Test Scheme

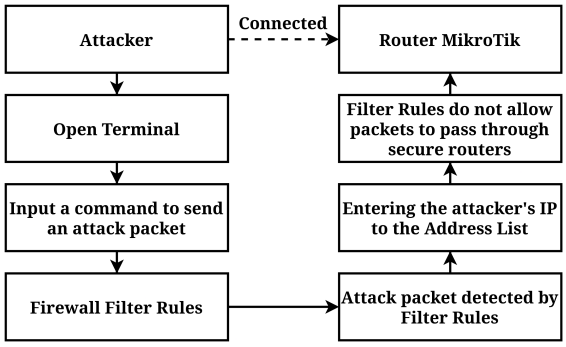

Figure 5. Security Scheme

resource consumption in normal conditions without a firewall and without any DoS or Brute Force attacks. Conditions without security from DoS and Brute Force attacks (Condition 2) Where in this condition DoS and Brute Force attacks are tested against Mikrotik routers which are in normal condition and without any firewall filter rules configuration. Finally, security conditions using firewall filter rules (Condition 3) in this condition the router is configured to detect and block DoS and Brute Force attacks using firewall filter rules and address lists. In the "Optimize" stage, researchers analyzed and compared the test results for each security condition and optimized the prevention of DoS attacks using a firewall raw.

4. Results and Discussion

There are several ways you can protect your Mikrotik router from Brute Force attacks, including using a username and password combination that is unique and hard to guess, closing unused services or you can also mark the attacker's IP address and then drop it. This research uses the technique of marking the attacker's IP address and then dropping it using the firewall filter rules and address list features so that the attack detection and blocking process is automated. The configuration script is in Table 3.

In this research, to prevent routers from DoS attacks, the researchers used the technique of marking the attacker's IP address and then dropping it using the firewall filter rules and address list features, so that the attack detection and blocking process is automated. The configuration script is in Table 4.

DoS testing using Syn Flood and ICMP Flood techniques is carried out alternately in each condition with a duration of 30 minutes, as well as Brute Force testing on ports 22 (SSH) and 23 (Telnet) is carried out alternately in each condition. At the same time, monitoring and recording of the average value of each indicator being measured is also carried out. The recapitulation of the results of data collection and processing from Brute Force testing is in Figure 6 and Table 5.

As shown in Figure 6, the log detected that there were many attempts to enter the router device by attackers using Brute Force causing the CPU workload to increase significantly by 95% as in Figure 7.

However, when security was carried out using firewall filter rules and address lists, as shown in Figure 8, the attacker's IP address was successfully captured using the address list, and 140 suspicious data packets originating from the attacker's IP address were dropped, which means the data packets were rejected from entering the network routers. This causes a

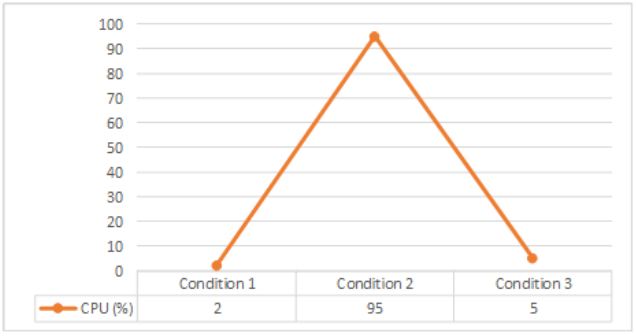

Figure 6. Graph of Brute Force Test Data Processing Results

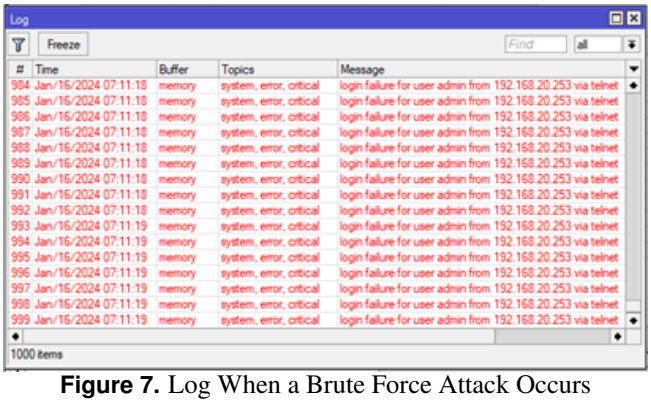

Figure 7. Log When a Brute Force Attack Occurs

Table 3. Brute Force Attack Prevention Rules with Firewall Filter Rules

Rules	Information
chain=input action=drop protocol=tcp dst-port=23,22 src-address-list=detect-bruteforce	Block Telnet and SSH from IPs in the detect-bruteforce list using action = drop
chain=output action=accept protocol=tcp src-port=23 content="Login failed, incorrect username or password" dst-limit=1/1m, 2,src-and-dst-addresses/1m	To prevent Telnet attacks on the router, use the chain = output to catch brute force attempts via the router's replies. The content parameter captures the reply sent by the router to the user attempting Telnet. Set dst.limit to allow only 3 login attempts within 1 minute. If more than 3 failed attempts occur, the router will identify the user as engaging in a brute force attack.
chain=output action=add-dst-to- address-list protocol=tcp src- port=23 content="Login failed, incorrect username or password" address-list=detect-bruteforce address-list-timeout=10d	To block brute force attackers, use action=add-dst-to-address-list to add the IP address of the perpetrator to the detect-bruteforce address list. The IP will then be blocked for 10 days, preventing further login attempts.
chain=input action=accept protocol=tcp chain=input action=accept protocol=tcp dst-port=22 connection-state=new dst-limit=1/1m,2,src-and-dst-addresses/1m	Since SSH encrypts packets, the reply message from the router cannot be read directly. Instead, when a user enters an incorrect username or password, the SSH service uses the Connection State parameter to flag users who failed to log in. This allows the system to track and handle failed login attempts securely.
chain=input action=add-src-to-address-list protocol=tcp dst-port=22 connection-state=new address-list=detect-bruteforce address-list-timeout=10d	Rules for adding Brute Force perpetrators to the detect-bruteforce address list

Table 4. DoS Attack Prevention Rules with Firewall Filter Rules

Rules	Information
chain=detect-dos action=drop in-interface= AP-Bridge src-address-list=detect-dos-attacker dst-address-list=detect-dos-target	A rule blocks traffic from the detect-dos-attacker source address list and the detect-dos-target destination address list.
chain=input in-interface=AP-Bridge action= jump jump-target=detect-dos	Another rule marks incoming traffic from the AP-Bridge interface, directing it to the next rule.
chain=detect-dos action=return protocol=tcp tcp-flags=syn dst- limit=32,32,src-and-dst-addresses/1s	For detecting DoS attacks, TCP traffic is monitored with a destination limit of 32 packets per second. If the packet rate is equal to or exceeds this threshold, it proceeds to the next rule; otherwise, it is ignored.
chain=detect-dos action=return protocol=icmp dst-limit=32,32,src- and-dst-addresses/1s	Similarly, ICMP traffic is monitored with a destination limit of 32 packets per second. If the rate is equal to or exceeds this value, it continues to the next rule; otherwise, it is ignored.
chain=detect-dos action=add-src-to-address-list address-list=detect-dos-attacker address-list-timeout=10m	The attacker's IP address from detected traffic is added to the detect-dos-attacker address list and blocked for 10 minutes.
chain=detect-dos action=add-dst-to-address-list address-list=detect-dos-target address-list-timeout=10m	The destination IP, identified as the DoS attack target, is added to the detect-dos-target address list and blocked for 10 minutes.

Table 5. Brute Force Test Data Processing Results

Data	Conditions During Testing		
	Initial Stage Without Firewall and No Attacks Yet	Without Firewall and an Attack Happens	Firewall Enabled and Attack Happens
CPU Load	2.00%	95.00%	5.00%

significant decrease in CPU performance load until it returns to 5% normal conditions.

Furthermore, to recapitulate the results of taking and processing the average data from the DoS Syn Flood and ICMP Flood tests in each condition, you can see Figure 9 and Table 6.

It was observed that there was a significant increase in CPU workload during DoS attacks in Condition 2 (C2) of 95%. This occurs because a large number of requests are generated by DoS attacks, causing CPU consumption to increase rapidly to serve these requests. On the other hand, if you compare Condition 2 (C2) and Condition 3 (C3), security has been carried out using firewall filter rules and address lists, as can be seen in Figure 8, the attack packet originating from the attacker's IP address was successfully dropped after two attempts, which means the packet the data is denied entry to the router's network. CPU consumption value decreased to 48.5%. In the ping response time indicator from Condition 1 (C1) to Condition 2 (C2) there was a significant increase of 45ms. This is caused by a DoS attack which causes latency or the length of time required to send data packets from the sender to the recipient to increase. This impact can also be seen from the connection to the target becoming unstable, making the router difficult to access. However, when security is carried out with firewall filter rules and address lists as in Condition 3 (C3), there is a significant decrease compared to Condition 2 (C2). Even the ping response time value can return to normal. As for other indicators, namely traffic, memory, and disk, from Condition 1 (C1) to Condition 3 (C3) did not show any significant changes. In other words, testing attacks using Syn Flood and ICMP Flood techniques do not have a significant impact on router consumption in terms of memory, disk, and router network traffic as shown in Figure 10.

Brute Force and DoS attacks also have an impact on the client's laptop internet speed. This is proven by the recapitulation of speed test results for download speed on client laptops in Table 7. The Syn Flood attack greatly affected the client's download speed, from the normal speed shown in Condition 1 (C1) which was 9.91 Mbps to a drastic drop to 2.24 Mbps when the attacker sent the attack packet to the router. However, after the router implemented firewall filter rules and address lists to block Syn Flood attacks, the download speed rose to 7.28 Mbps. This proved that the firewall filter rules have succeeded stabilize the bandwidth during attacks.

Next is a recapitulation of speedtest results for upload speed on client Laptops shown in Table 8, showing that each type of attack causes the upload speed to drop significantly from the normal 4.23 Mbps as in Condition 1 (C1), to an average speed of 0.43 Mbps. And after the router implemented firewall filter rules and address lists, upload speeds only increased to an average of 1.21 Mbps. This proves that security using firewall filter rules and address lists is not effective enough in restoring upload speed when an attack occurs.

The results of the comparison of Mikrotik router security from Condition 1 (C1) to Condition 3 (C3) in DoS attack testing, can be concluded that security with firewall filter rules did not succeed in reducing the CPU Load value to a normal state below 10% as in Condition 1 (C1). So the researchers made changes and additions to the configuration, including deactivating the drop rule on the firewall filter rules and replacing it with a firewall raw configuration which is used to drop the attacker's IP address and the target IP address that has been captured by the address list. The firewall raw script in the Table 9.

It can be seen in Figure 11 that the DoS attack packet sent by the attacker was successfully dropped, which indicates that the firewall raw configuration rejected data suspected of being sent by the attacker to the router network.

There is a change in the CPU Load value when testing an attack on a router with a firewall raw configuration. When compared with blocking IP addresses in the address list using firewall filter rules, the CPU Load value managed to drop by 48.5%, but when using a firewall raw, the CPU value managed to drop significantly to 24% as can be seen in Figure 12.

Firewall Raw configuration testing was carried out as before, using DoS attacks with Syn Flood and ICMP Flood techniques with three different numbers of attack packets. The comparison of CPU Load recapitulation from DoS attack test results for firewall filter rules and firewall raw configurations can be seen in Table 10.

From the comparison in Table 10, it can be concluded that with several packets of 70K to 200K, firewall raw can reduce CPU Load by up to 50% of the CPU Load value from testing results using firewall filter rules. This proves that blocking DoS attacks using a firewall raw is more effective in reducing CPU load than using firewall filter rules.

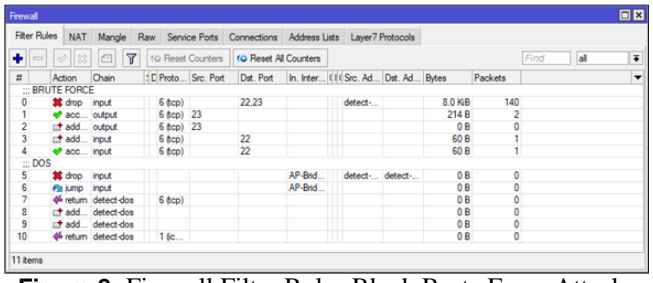

Figure 8. Firewall Filter Rules Block Brute Force Attacks

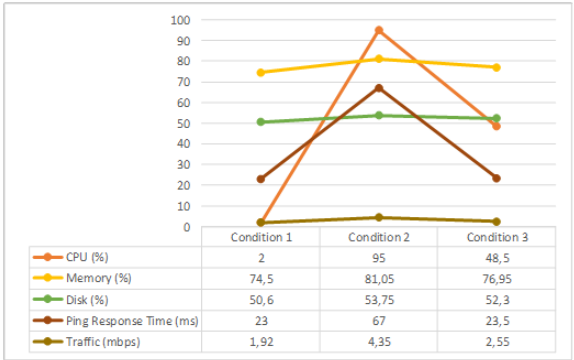

Figure 9. Graph of DoS Test Data Processing Results

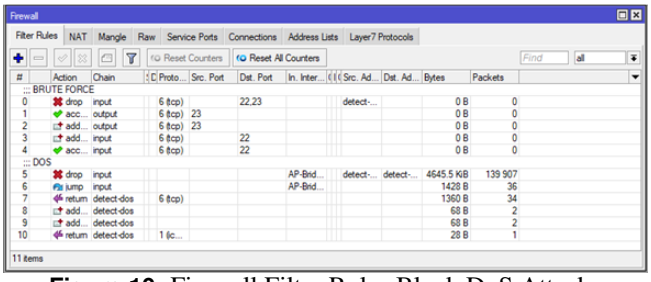

Figure 10. Firewall Filter Rules Block DoS Attacks

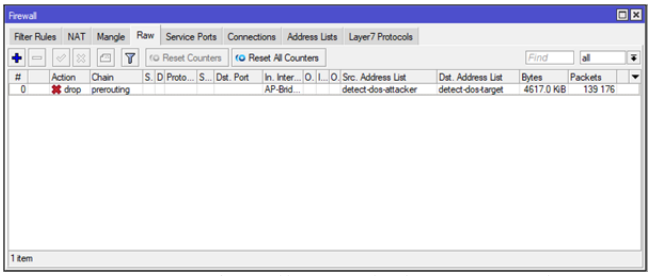

Figure 11. Firewall Raw Blocks DoS Attacks

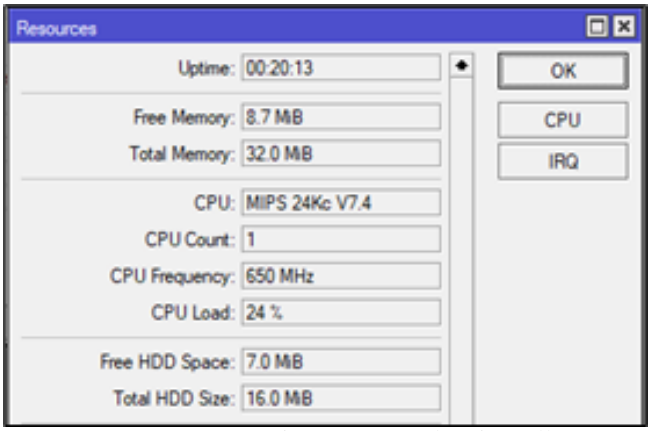

Figure 12. Resources During DoS Attacks Firewall Raw Security Conditions

Table 6. DoS Test Data Processing Results

Data	Conditions During Testing		
	Normal State	Attacked State	Defending State
CPU Load (%)	2	95	48.5
Memory (%)	74.5	81.05	76.95
Disk (%)	50.6	53.75	52.3
Ping Response Time (ms)	23	67	23,5
Traffic (mbps)	1.92	4.35	2.55

Table 7. Recapitulation of Speedtest Results for Download Speed on Client Laptop

Attacks	Download Speed (Mbps)		
	C1	C2	C3
Brute Force	9.91	9.51	8.66
DoS (Syn Flood)	9.91	2.24	7.28
DoS (ICMP Flood)	9.91	5.94	4.67

Table 8. Recapitulation of Speedtest Results for Upload Speed on Client Laptop

Attacks	Upload Speed (Mbps)		
	C1	C2	C3
Brute Force	4.23	0.48	1.56
DoS (Syn Flood)	4.23	0.28	1.05
DoS (ICMP Flood)	4.23	0.54	1.02

Table 9. Firewall Raw Script

Firewall Script
action=drop chain=prerouting
in-interface=AP-Bridge
src-address-list=detect-dos-attacker
dst-address-list=detect-dos-target

Table 10. Results of Comparative Analysis of CPU Load in DoS Testing When Using Firewall Filter Rules and Firewall Raw

Attacks	Config	Total Packages		
		700K	200K	800K
Syn Flood	Filter Rule	46.00%	59.00%	72.00%
	Raw	20.00%	28.00%	43.00%
ICMP Flood	Rilter Rule	51.00%	59.00%	68.00%
	Raw	24.00%	33.00%	43.00%

5. Conclusion

Based on the test results of using the Mikrotik router feature as a medium to increase network security from DoS and Brute Force attacks by using firewall filter rules and address lists, it can be concluded that using firewall filter rules can secure the network system from Brute Force attacks that try to obtain the router device password. and succeeded in reducing the CPU performance load from 95% until it returned to normal conditions with a CPU Load value of 5%. However, router network security which is carried out using firewall filter rules and address lists cannot face DoS attacks with 800,000 attack packets sent. This is proven by the test results in security conditions, the CPU Load value is still high at 72% and is still far from normal conditions. Therefore, the author added a configuration with a firewall raw to optimize security which was proven by successfully reducing CPU consumption by up to 43%.

From the comparative analysis of test results, the effectiveness test results were obtained with the percentage value obtained for Brute Force testing being 94.7% and DoS testing 40.7%. So it can be concluded that firewall filter rules and address lists are very effective in preventing Brute Force attacks but less effective in preventing DoS attacks. So overall to secure the network from DoS attacks it is not enough just to use the built-in features of the Mikrotik router but also requires other additional security support.

Acknowledgements

We want to express our sincere gratitude to Universitas Semarang (Semarang University) for providing the facilities that were essential for the successful completion of this work. The infrastructure and resources available have greatly contributed to the progress and quality of our studies. We are also deeply thankful to the Fakultas Teknologi Informasi dan Komunikasi (Faculty of Information Technology and Communication) for their unwavering moral support throughout this journey. Their encouragement and guidance have been invaluable in overcoming challenges and staying motivated. This work would not have been possible without the combined assistance of these institutions. Thank you for your continued support and dedication to advancing academic and studies excellence.

Author contributions

Febrian Wahyu Christanto was responsible for conceptualizing the study and validating the findings. Putri Cholillah contributed to the design and implementation of the project, as well as data collection. Alauddin Maulana Hirzan handled the writing of the original draft and took charge of the LaTeX formatting. All authors have reviewed and approved the final manuscript.

References

[1] ZHANG, T.; Zhixuan Lv. Development and Integration Between Computer Network Technology and New Media. In: *Proceedings of the 2022 2nd International Conference on Computer Technology and Media Convergence Design (CTMCD 2022)*. Atlantis Press, 2022. p. 135–141. ISBN 2352-538X. Disponível em: ⟨https://doi.org/10.2991/978-94-6463-046-6_17⟩.

[2] SIRAIT, H. History of Computer Networks. *Journal of Tecnologia Quantica*, v. 1, n. 3, p. 117–134, nov. 2024. Section: Articles. Disponível em: ⟨https://journal.ypidathu.or.id/index.php/quantica/article/view/1447⟩.

[3] KILINCER, I. F.; ERTAM, F.; SENGUR, A. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks*, v. 188, p. 107840, 2021. ISSN 1389-1286. Disponível em: ⟨https://www.sciencedirect.com/science/article/pii/S1389128621000141⟩.

[4] SASI, T. et al. A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. *Journal of Information and Intelligence*, v. 2, n. 6, p. 455–513, nov. 2024. ISSN 2949-7159. Disponível em: ⟨https://www.sciencedirect.com/science/article/pii/S2949715923000793⟩.

[5] ABUFARDEH, S.; FALAH, B. The State of Phishing Attacks and Countermeasures. *International Journal of Computer Science and Security (IJCSS)*, v. 17, n. 4, p. 54–71, 2023. ISSN 1985-1553. Disponível em: ⟨https://www.cscjournals.org/library/manuscriptinfo.php?mc=IJCSS-1702⟩.

[6] GUNDUZ, M. Z.; DAS, R. Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, v. 169, p. 107094, mar. 2020. ISSN 1389-1286. Disponível em: ⟨https://www.sciencedirect.com/science/article/pii/S1389128619311235⟩.

[7] YANG, W. Research on the Relationship between Computer Network and Economic Development in Information Environment. *Journal of Physics: Conference Series*, v. 1744, n. 4, p. 042011, fev. 2021. ISSN 1742-6596. Publisher: IOP Publishing. Disponível em: ⟨https://dx.doi.org/10.1088/1742-6596/1744/4/042011⟩.

[8] NURHAYATI, H. Statistic, *Internet Usage in Indonesia - Statistics & Facts*. 2024. Disponível em: ⟨https://www.statista.com/topics/2431/internet-usage-in-indonesia/#topicOverview⟩.

[9] Adi Ahdiat. Infographic, *Indonesia Masuk 10 Negara dengan Kebocoran Data Terbesar*. 2024. Disponível em: ⟨https://databoks.katadata.co.id/infografik/2024/07/02/indonesia-masuk-10-negara-dengan-kebocoran-data-terbesar⟩.

[10] TRILOKA, J.; HARTONO, H.; SUTEDI, S. Detection of SQL Injection Attack Using Machine Learning Based On Natural Language Processing. *International Journal of Artificial Intelligence Research; Vol 6, No 2 (2022): Desember 2022*, 2022. Disponível em: ⟨https://ijair.id/index.php/ijair/article/view/355⟩.

[11] Ficky Ramadhan. News, *Penyebab Kebocoran Data Pribadi di Indonesia Akibat Tata Kelola yang Buruk*. 2024. Disponível em: ⟨https://mediaindonesia.com/teknologi/719594/penyebab-kebocoran-data-pribadi-di-indonesia-akibat-tata-kelola-yang-buruk⟩.

[12] BISWAS, A. K. et al. Attacks Toward Wireless Network-on-Chip and Countermeasures. *IEEE Transactions on Emerging Topics in Computing*, v. 9, n. 2, p. 692–706, jun. 2021. ISSN 2168-6750.

[13] MUKERI, A. F.; GAIKWAD, D. P. Adversarial machine learning attacks and defenses in network intrusion detection systems. *International Journal of Wireless and Microwave Technologies (IJWMT)*, v. 12, n. 1, p. 12–21, 2022. ISSN 2076-9539.

[14] ASLAN, O. et al. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, v. 12, n. 6, 2023. ISSN 2079-9292. Disponível em: ⟨https://www.mdpi.com/2079-9292/12/6/1333⟩.

[15] M. A. Elsadig. Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach. *IEEE Access*, v. 11, p. 83537–83552, 2023. ISSN 2169-3536.

[16] JOO, S. et al. Machine Learning-Based Detection and Selective Mitigation of Denial-of-Service Attacks in Wireless

Sensor Networks. *Computers, Materials \& Continua*, v. 82, n. 2, 2025. ISSN 1546-2226.

[17] XU, K. et al. Research on Multi-Layer Defense against DDoS Attacks in Intelligent Distribution Networks. *Electronics*, v. 13, n. 18, 2024. ISSN 2079-9292.

[18] ALHAMED, M.; RAHMAN, M. M. H. A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. *Applied Sciences*, v. 13, n. 12, 2023. ISSN 2076-3417.

[19] HAMZA, A. A.; AL-JANABI, R. Jumma surayh. Detecting Brute Force Attacks Using Machine Learning. *BIO Web Conf.*, v. 97, 2024. Disponível em: ⟨https://doi.org/10.1051/bioconf/20249700045⟩.

[20] GAUTAM, T.; SINGH, U. An approach for detecting password pattern in dictionary attack. *Mililink Journal of Advanced Materials Science*, v. 215, p. 2765–2780, 2022.

[21] WIDIANTO, S. R. et al. Python gmail dictionary attack using wordlist. *AIP Conference Proceedings*, v. 2714, n. 1, p. 030033, maio 2023. ISSN 0094-243X. Disponível em: ⟨https://doi.org/10.1063/5.0128464⟩.

[22] PARK, J. et al. Network log-based SSH brute-force attack detection model. *Computers, Materials & Continua*, v. 68, n. 1, 2021.

[23] PAMUNGKAS, C. et al. Analysis of brute force attacks using National Institute of Standards and Technology (NIST) methods on routers. *Journal of Informatics Information System Software Engineering and Applications (INISTA)*, v. 5, n. 2, p. 115–125, maio 2023.

[24] A. Daniel; I. A. Suleiman. Design and Implementation of MikroTik Router-Operating System Introduction. *Direct Research Journal of Engineering and Information Technology*, v. 11, n. 8, p. 138–144, 2022. ISSN 2354-4155.

[25] SUKARSA, I. M.; PIARSA, I. N.; PUTRA, I. G. B. P. Simple solution for low cost bandwidth management. *Telkomnika (Telecommunication Computing Electronics and Control)*, v. 19, n. 4, p. 1419–1427, 2021. ISSN 2302-9293.

[26] BASAR, A. R. et al. Computer Network Design Using the Simple Queue Method in Maximising Network Performance in Companies. *Journal of Computer-based Instructional Media*, 2023. Disponível em: ⟨https://api.semanticscholar.org/CorpusID:266245608⟩.

[27] WIHARTI, W. et al. Load Balancing and Fail Over MikroTik Implementation Using Per Connection Classifier (PCC) on Two Internet Providers Interconnection. *International Journal of Advanced Science Computing and Engineering*, v. 5, n. 2, p. 129–135, ago. 2023. Section: Articles. Disponível em: ⟨https://www.ijasce.org/index.php/IJASCE/article/view/135⟩.

[28] SARI, A. et al. Bandwidth Management Design Using the Simple Queue Method in Mikrotik RouterOS and The Winbox Application. *INTERACTION: Jurnal Pendidikan Bahasa*, v. 10, n. 1, p. 396–402, jul. 2023. Disponível em: ⟨https://unimuda.e-journal.id/jurnalinteraction/article/view/4441⟩.

[29] PURNOMO, V. I.; ANINDITO, B.; JUNAEDI, L. Design of Load Balancing Using Static Route Address List Method In The Case Study of Tambakrejo Village Tulungagung. *IJEEIT: International Journal of Electrical Engineering and Information Technology*, v. 5, n. 1, p. 22–27, 2022. ISSN 2615-2096.

[30] MASLAN, A.; MOHAMAD, K. M.; FOOZY, C. F. M. Enhancement detection distributed denial of service attacks using hybrid n-gram techniques. *KOMNIKA (Telecommunication Computing Electronics and Control)*, v. 20, n. 1, p. 61–69, 2022. ISSN 2302-9293.

[31] NAJAR, A. A.; NAIK, S. M. Cyber-Secure SDN: A CNN-Based Approach for Efficient Detection and Mitigation of DDoS attacks. *Computers & Security*, v. 139, p. 103716, abr. 2024. ISSN 0167-4048. Disponível em: ⟨https://www.sciencedirect.com/science/article/pii/S0167404824000178⟩.

[32] MAZHAR, N. et al. SDN based Intrusion Detection and Prevention Systems using Manufacturer Usage Description: A Survey. *International Journal of Advanced Computer Science and Applications*, v. 11, dez. 2020.

[33] Iwan Giri Waluyo; KURNIAWAN, D. Mikrotik Login Security with Port-Knocking and Brute Force Firewall at PT. Time Excelindo. *International Journal of Integrative Sciences*, v. 2, n. 7, p. 971–978, jul. 2023. Section: Articles. Disponível em: ⟨https://journal.formosapublisher.org/index.php/ijis/article/view/4782⟩.

[34] SWATHI, K. Brute Force Attack on Real World Passwords. *Int. J. Res. Public Rev*, v. 3, p. 552–558, 2022.

[35] SARI, L. O. et al. Implementation of Bandwidth Management and Access Restrictions Using PCQ and Firewall Methods in SMP Tunas Bangsa Network. *International Journal of Electrical, Energy and Power System Engineering*, v. 5, n. 3, p. 73–79, nov. 2022. Section: Articles. Disponível em: ⟨https://ijeepse.id/journal/index.php/ijeepse/article/view/117⟩.

[36] Md. Zihadul Islam et al. Communication and bandwidth optimization technique using MikroTik. *International Journal of Advanced Research in Computer and Communication Engineering*, v. 13, n. 5, 2024.

[37] Lutfi, Salkin et al. Optimal Filter Assignment Policy Against Distributed Denial of Service Attack on Router Mikrotik. *MATEC Web Conf.*, v. 372, p. 04008, 2022. Disponível em: ⟨https://doi.org/10.1051/matecconf/202237204008⟩.

[38] TIWARI, A.; PAPINI, S.; HEMAMALINI, V. An enhanced optimization of parallel firewalls filtering rules for scalable high-speed networks. *Materials Today: Proceedings*, v. 62, p. 4800–4805, 2022. ISSN 2214-7853. Disponível em: ⟨https://www.sciencedirect.com/science/article/pii/S2214785322016881⟩.

[39] YIN, X.-X. et al. A Review on the Rule-Based Filtering Structure with Applications on Computational Biomedical Images. *Journal of Healthcare Engineering*, v. 2022, n. 1, p. 2599256, jan. 2022. ISSN 2040-2295. Publisher: John Wiley & Sons, Ltd. Disponível em: ⟨https://doi.org/10.1155/2022/2599256⟩.

[40] Yunif Lukman Hakim; Hendro Wijayanto. Combination of Filtering and Switching Methods for Network Security from Pornographic Content. *International Journal of Computer and Information System (IJCIS)*, v. 5, n. 3, p. 132–191, 2024. ISSN 2745-9659.

[41] Wirda Fitriani; Fachrid Wadly; Zuhri Ramadhan. NETWORK SECURITY IMPLEMENTATION FROM DDOS ATTACKS WITH MIKROTIK ROUTERS. *International Journal Of Computer Sciences and Mathematics Engineering*, v. 3, n. 2, p. 18–29, out. 2024. Section: Articles. Disponível em: ⟨https://ijecom.org/index.php/IJECOM/article/view/93⟩.

[42] MAULANA, A.; SUHARTO, N.; HARIYADI, A. Application of MikroTik Firewall for Website Access Restriction and Prevention of DoS (Denial of Service) Attacks on Internet Networks Al-Mahrusiyah Vocational School Lirboyo. *Journal of Telecommunication Network (Jurnal Jaringan Telekomunikasi)*, v. 13, n. 1, p. 81–86, mar. 2023. Disponível em: ⟨https://jartel.polinema.ac.id/index.php/jartel/article/view/547⟩.

[43] MASUM, A.; SACHCHA, M. R. *Security Analysis of Government & Financial Websites of Bangladesh*. [S.l.]: International Journal of Education and Management Engineering, 2022. v. 12.

[44] GOLDARA, R.; PATACSIL, J. An Optimized Wireless Network Architecture for Department of Agriculture, Region 1. *Data Science: Journal of Computing and Applied Informatics*, v. 6, n. 1, p. 12–34, jan. 2021. Disponível em: ⟨https://talenta.usu.ac.id/JoCAI/article/view/7873⟩.

[45] PRRIYADARSHINI, M. A.; DEVI, S. R. Detection of DDoS Attacks Using Supervised Learning Technique. *Journal of Physics: Conference Series*, v. 1716, n. 1, p. 012057, dez. 2020. ISSN 1742-6596. Publisher: IOP Publishing. Disponível em: ⟨https://dx.doi.org/10.1088/1742-6596/1716/1/012057⟩.

[46] ARMOOGUM, S.; MOHAMUDALLY, N. A. A Comprehensive Review of Intrusion Detection and Prevention Systems against Single Flood Attacks in SIP-Based Systems. *International Journal of Computer Network and Information Security*, 2021. Disponível em: ⟨https://api.semanticscholar.org/CorpusID:245469155⟩.

[47] Alexander Gutnikov; Oleg Kupreev; Ekaterina Badovskaya. Report, *DDoS attacks in Q1 2021*. 2021. Disponível em: ⟨https://securelist.com/ddos-attacks-in-q1-2021/102166/⟩.