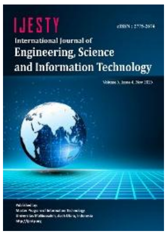
International Journal of Engineering, Science and Information Technology
Volume 5, No. 4 (2025) pp. 637-643
eISSN: 2775-2674
Website: http://ijesty.org/index.php/ijesty
DOI: https://doi.org/10.52088/ijesty.v5i4.1791
Research Paper, Short Communication, Review, Technical Paper



Firewall Analytics in DNS and SYN Flood Protection on Mikrotik CCR in the North Aceh District Government

Nanda Imanda[1]*, Dahlan Abdullah[1], Fajriana[2], Nurdin[1], Munirul Ula[2]

[1]*Department of Information Technology, Faculty of Engineering, Universitas Malikussaleh, Aceh, Indonesia*
[2]*Department of Informatics, Faculty of Engineering, Universitas Malikussaleh, Aceh, Indonesia*

**Corresponding author Email: nanda.237110201016@mhs.unimal.ac.id*

The manuscript was received on 25 April 2025, revised on 27 June 2025, and accepted on 22 October 2025, date of publication 28 December 2025

Abstract

This study investigates the implementation of an analytical firewall on the Mikrotik Cloud Core Router (CCR) device for network protection against Domain Name System (DNS) and Synchronise Flood (SYN Flood attacks in the information technology infrastructure of the North Aceh Regency Government. DNS-based attacks and SYN Flood have demonstrated a significant disruptive capacity for the continuity of electronic public services, illustrating the urgency of robust security protocols on government infrastructure. The study implemented a quantitative-experimental approach, with methodological triangulation in empirical data acquisition through controlled attack simulations, firewall log analysis, and semi-structured interviews with technical personnel. Experiments are designed with variations in attack intensity to evaluate system resilience thresholds, while firewall log analysis facilitates the identification of anomalous patterns through detection algorithms. The analytics process applies parametric evaluation to temporal mitigation metrics, packet processing capacity, and operational implications on network performance, complemented by descriptive statistical analysis that explores data distribution and temporal trends. The results indicate the differential effectiveness of the specific firewall configuration against a specific attack typology, with an empirical determination of optimisation parameters for real-time mitigation. This research contributes to the corpus of knowledge regarding the security of government networks through the derivation of protective models that are adaptive to the operational characteristics of public infrastructure. The findings have substantive implications for cybersecurity policy formulation in the administrative context of local governments, with extensive significance for the implementation of network architectures that are resilient to volumetric attacks and protocol exploitation.

Keywords: *Analytical Firewall, Mikrotik CCR, DNS, SYN Flood, Cyber Attack Mitigation.*

1. Introduction

The rapid development of information technology today makes computer networks an important infrastructure in supporting various sectors, including the government sector. However, along with these advances, there have been major challenges related to network security, one of which is Denial of Service (DoS) attacks, especially SYN Flood and DNS Flood. These attacks can cause a failure of the network system by flooding the server or router with excess traffic that exceeds its manageable capacity, resulting in the network becoming unresponsive or even shutting down completely. Mikrotik CCR, as a router device used by many agencies, including the North Aceh Regency Government, must be protected from such potential attacks to ensure the sustainability and operational security of the government network [1] [2].

Threats to Indonesia's government networks, especially at the regional level, are becoming increasingly significant as the reliance on digital technology to support public services increases. SYN Flood and DNS Flood attacks are types of attacks that can exploit vulnerabilities on routers, including Mikrotik CCR. This research is relevant because it can contribute to identifying the right protection methods, which can be used to protect government network infrastructure from attacks that have the potential to damage operational systems [3][4]. Mikrotik, as the router of choice for many agencies, including local governments, requires more in-depth analysis and evaluation regarding its resistance to flooding attacks that are growing [5][6].

Several previous studies have explored the use of firewalls in DoS attack mitigation, including SYN Flood and DNS Flood, using Mikrotik devices. For example, research conducted by Fakhmi and Gultom shows that a raw firewall on Mikrotik can reduce the impact of SYN Flood attacks by blocking suspicious connections before connecting to the server [7][8]. In addition, another study by Aprilianto et al.

found that DNS filters applied to Mikrotik firewalls can significantly reduce UDP DNS Flood attack traffic, up to 60% compared to conditions without firewalls [9]. However, few studies focus on a comprehensive analysis of firewall applications in handling both types of attacks on Mikrotik CCR, especially in local government settings [10].

Although there have been many studies that have assessed the effectiveness of firewalls on Mikrotik in handling SYN Flood and DNS Flood attacks, existing studies show a lack of studies that specifically analyse the use of Mikrotik CCR in the context of local governments, especially the North Aceh Regency Government. Existing research has also focused more on testing firewall performance separately without providing a comparison between the use of Filter Rules and Raw Firewall in a single integrated system. Therefore, this study aims to fill this gap by comparing the two firewall methods in protecting government networks from the increasing DoS threats [1][3].

This research will focus on the analysis and evaluation of the use of firewalls in Mikrotik CCR in protection against SYN Flood and DNS Flood attacks in the North Aceh Regency Government. The two firewall methods that will be tested are Filter Rules and Raw Firewall available on Mikrotik CCR. This analysis will involve testing network performance parameters such as CPU usage, ping response time, and connection stability in the event of an attack. Thus, this study will provide insight into the effectiveness of the two firewall methods in maintaining the stability and security of local government networks from potential DoS attacks [11].

This research is expected to provide significant benefits for the North Aceh Regency Government, especially in strengthening its information and communication technology (ICT) infrastructure. The results of this study can be used as a reference in strengthening government network security policies by choosing the right firewall solution. In addition, this research can also be a reference for other agencies in Indonesia that use Mikrotik as the main router in maintaining resilience to DoS threats, thereby supporting the sustainability of safe and stable government network operations.

2. Literature Review

2.1. Network Security

According to Khairunnisa et al. (2024 network security is a crucial aspect in the government's information system because cyber threats continue to develop and can have a serious impact on public services. Therefore, a systematic and integrated approach is needed in the implementation of network security policies and technologies [12].

The Government of Indonesia has implemented an Electronic-Based Government System (SPBE), which requires a secure and stable network as the basis for its operations. Putra et al. stated that the success of the implementation of SPBE is highly dependent on the security, integration, and availability of information networks owned by government institutions. If network security is ignored, it will open a gap for cyber attacks that can cause service interruptions, data manipulation, and public privacy violations. Thus, investment in technology and network security policies is a major need that cannot be delayed anymore [13].

2.2. Types of Cyber Attacks

A cyberattack is an organised or random attempt that aims to damage, steal, or disrupt a computer network system. In the world of digital governance, some common types of attacks include malware, Phishing, ransomware, and DDoS attacks that often attack critical infrastructure. Aritonang explained that network systems that are not fully protected are vulnerable to these attacks, especially when they are connected to the internet extensively. These attacks can go undetected, causing long-term damage to the credibility and sustainability of government services. Therefore, it is important for every government agency to understand the types of cyber threats and take preventive measures. In this discussion, the focus is on two types of attacks that are relevant to network security, namely DNS Flood and SYN Flood [14].

2.3. Firewall

A firewall is a network security system that functions to monitor and control data traffic entering and exiting a network based on predetermined security rules. The basic concept of a firewall is to be a barrier between a trusted internal network and an untrusted external network, such as the Internet. Firewall: It can be hardware, software, or a combination of both, and serves as a gatekeeper for information to prevent illegal access. In research conducted by Ricky in 2023, it was stated that firewalls in modern networks are a vital part of the defence system, as they can detect and block suspicious activity before it reaches the core system. With this strategic role, Firewalls become a mandatory component in network infrastructure, both in government and private agencies [15].

2.4. CCR Mikrotik

Mikrotik Cloud Core Router (CCR) is one of the high-performance networking device lines developed by Mikrotik company and is designed to meet the needs of large-scale network routing and management. CCR is equipped with the RouterOS operating system that enables a wide range of network management features, ranging from dynamic routing, bandwidth management, to Virtual Private Network (VPN). These devices are commonly used in institutional and enterprise environments that require a high level of stability and throughput [16], [17]. According to Hafifah and Nur Hayati (2020, Mikrotik CCR is very suitable for use in laboratory infrastructure or institutional networks because it is supported by a multicore processor and large RAM capacity that supports high traffic. The device's ability to perform data processing in parallel makes it superior to other mid-range routers [18].

2.5. Theoretical Framework and Analytical Model

The theoretical framework is the conceptual foundation that underlies this study by explaining the relationship between relevant variables in the context of DNS system protection and SYN Flood attack mitigation on the network infrastructure of the North Aceh Regency Government. This research relies on several interrelated concepts and theories to build a comprehensive analysis model. The firewall performance analysis model used in this study is based on three main parameters: throughput, latency, and attack mitigation effectiveness. This model was developed by integrating various approaches to network security analysis that have been proven valid in previous studies.

2.6. Firewall-Based DDoS Mitigation Framework

The firewall-based DDoS mitigation framework developed in this study consists of four main components that are integrated in a comprehensive security system. The framework is designed to provide multi-layered protection against DDoS attacks, with a particular focus on DNS and SYN Flood attack mitigation [19], [20].

1. Traffic Anomaly Detection: The traffic anomaly detection component acts as an early warning system that identifies suspicious traffic patterns that may indicate a DDoS attack [21].
2. Filtering and Rate Limiting: The filtering and rate limiting components serve to limit the volume of traffic that reaches the target system and filter malicious traffic based on certain characteristics [22].
3. Blacklisting and Dynamic Whitelisting: The dynamic blacklisting and whitelisting components implement adaptive mechanisms to allow or block traffic based on the behaviour and reputation of the source [23].

3. Method

3.1. Research Approach

This study adopts a quantitative and experimental approach to analyse the effectiveness of firewalls on Mikrotik Cloud Core Router (CCR) devices in protecting the network infrastructure of the North Aceh Regency Government from DNS and SYN flood attacks.

3.2. Research Location and Time

This research was carried out on the computer network infrastructure owned by the North Aceh Regency Government, located in a government office complex in Lhokseumawe, Aceh Province. The infrastructure includes a data centre, a local area network (LAN), and an interconnection system between agencies managed by the North Aceh Regency Communication and Information Office. The selection of this location is based on strategic considerations in the form of the complexity of government networks that represent the characteristics of public sector information technology infrastructure with significant security needs. The research lasted for six months, from January to June 2023

3.3. Data Collection Techniques

The methodological triangulation approach is systematically structured, starting from the initiation of the process and identification of data needs, then branching into three complementary data collection modalities: (1) attack simulation experiments with a five-stage protocol including environmental configuration, instrumentation calibration, simulation execution, parameter measurement, and documentation; (2) firewall log analysis with the stages of extraction, normalization, anomaly identification, categorization, and temporal analysis; and (3) interviews with the IT team through purposive respondent selection, instrument preparation, implementation, transcription, and thematic analysis.

1. Controlled Experiments
   Simulated DNS and SYN flood attacks are carried out in a controlled environment using calibrated penetration testing tools. The experimental protocol was systematically designed, taking into account parameters (variation in attack intensity, diversification of attack vectors, measurement of systemic impact, evaluation of mitigation mechanisms).
2. Comprehensive Log Analysis
   Empirical investigation of the log records of the Mikrotik CCR firewall system was carried out with a retrospective analytical approach, covering (historical data extraction, implementation of analytical framework, multiple correlation analysis, and digital forensic characterisation).
3. Semi-Structured Interviews
   The qualitative investigation was carried out through a series of semi-structured interviews with technical stakeholders within the North Aceh Regency Government, with protocols (purposive samples, validated instruments, thematic exploration, systematic documentation).

3.4. Data Analysis Techniques

The sequential methodological framework is initiated from the starting point and culminates in the derivation of results. This methodological structure is characterised by analytical bifurcation that facilitates the processing of data through two complementary parallel channels. The first channel focuses on simulated DNS and SYN attack experiments, which are then subjected to a criterionological evaluation for conformity determination with performance analysis. Data that meets the inclusion criteria is processed through parameter extraction, followed by performance analysis that focuses on three operational dimensions: mitigation speed, packet processing capacity, and implications for network infrastructure.

The second channel involves the collection of firewall log data, which, after passing a feasibility evaluation for statistical analysis, undergoes a normalisation procedure for standardisation of formats. Descriptive statistical analysis was then applied with a focus on central tendency metrics, dispersion parameters, and temporal patterns in the data. Both analytic channels incorporate a validation mechanism in the form of feedback loops in cases that do not meet the analytical criteria, ensuring the methodological integrity of the research process. The convergence of results from the two channels occurs at the point of analytical integration, which facilitates the comprehensive synthesis of multidimensional findings. The process culminates in the interpretation and reporting of results, resulting in conclusions based on methodologically validated empirical evidence.

4. Result and Discussion

4.1. Network Security System Baseline Performance Analysis

The baseline performance analysis of the network security system is a fundamental stage in this study, which aims to establish comprehensive baseline metrics before the implementation of security measures.

4.1.1. Network Architecture Documentation

The network infrastructure of the North Aceh Regency Government is characterised by a hierarchical topology that integrates various administrative entities in one cohesive digital ecosystem. MikroTik Cloud Core Router (CCR) is positioned as a core router that manages the distribution of traffic between network segments and provides internet access for the entire government infrastructure.

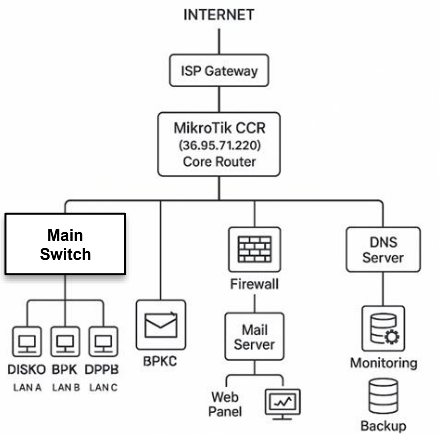


Fig 1. North Aceh Regency Government Network

The main device used is the Mikrotik Cloud Core Router (CCR) model CCR1036-12G-4S with a 36-core Tilera TILEGx36 processor with a speed of 1.2 GHz, 4 GB of RAM, and 16 GB of NAND storage. The device has 12 Gigabit Ethernet ports and 4 SFP ports, runs the RouterOS operating system version 7.15, and uses a public IP address of 36.95.71.220. The network infrastructure is divided into three segments, namely Segment A for DISKOMINFO (Communication and Information Service) with a network of 192.168.10.0/24, gateway 192.168.10.1, DHCP range of 192.168.10.100-200, around 50 workstations, and dedicated bandwidth of 100 Mbps; Segment B for BPKD (Regional Financial Management Agency) with a network of 192.168.20.0/24, gateway 192.168.20.1, DHCP range of 192.168.20.100-200, about 30 workstations, and dedicated bandwidth of 50 Mbps; and Segment C for DPPKB (Population Control and Family Planning Office) with a network of 192.168.30.0/24, gateway 192.168.30.1, DHCP range of 192.168.30.100-150, about 25 workstations, and dedicated bandwidth of 30 Mbps.

4.1.2. System Capacity Analysis

The capacity analysis was carried out to measure the utilisation of CCR MicroTik resources under normal operational conditions and provide an overview of the reserve space for the implementation of security mechanisms and potential attack loads. The results show an average CPU utilisation of 12.5% with a peak of 25.0% in the peak activity period, indicating sufficient processing capacity for additional firewall rules. The average memory utilisation of 35.2% with a peak of 45.0% also indicates the availability of space for extensive logging and expansion of connection tables.

1. System Resource Utilisation
   Resource utilisation measurements are carried out comprehensively on the critical components of MikroTik CCR, which include CPU, memory, network interface, and connection tables.
2. Headroom Capacity Analysis
   Headroom analysis is performed to determine the available capacity for the implementation of additional safety mechanisms without disrupting normal operational performance. This headroom calculation uses a safety margin of 80% of the system's maximum capacity, following capacity management best practices.
3. Estimated Impact of Firewall Implementation
   Firewall implementation experience on similar devices, overhead estimates are calculated to project the performance impact generated after the implementation of the analytical firewall.
4. Packet Processing Capacity
   Packet processing capacity analysis was conducted to understand the extent to which the system is capable of handling high traffic volumes, especially in Distributed Denial of Service (DDoS) attack scenarios.
5. Network Interface Performance Analysis
   Network interfaces are a crucial component in handling high traffic, so utilisation analysis is needed to ensure that capacity can support operational needs and potential expansion.
6. System Readiness Assessment
   Based on the results of a comprehensive capacity analysis, a thorough evaluation was carried out on the readiness of the system to support the implementation of a more sophisticated analytical firewall
7. Future Capacity Projections
   Future capacity projections show medium-term sustainability even with organisational growth and a more comprehensive implementation of security systems.

4.1.3. Normal Traffic Profile

Normal traffic profiles are a characterisation of network usage patterns under standard operating conditions, which is essential for establishing detection thresholds in the implementation of security systems. Analysis was conducted on protocol distribution, DNS query patterns, and TCP connection behaviour in various network segments.

4.1.4. Baseline Comprehensive Interpretation

The baseline analysis shows that the North Aceh Regency Government's network infrastructure is in stable operational condition and optimal for the implementation of advanced security systems. Key characteristics identified include:

1. High Operational Stability
2. Adequate Headroom Capacity
3. Predicted Temporal Patterns
4. Normal Protocol Distribution
5. Consistent Connection Behavior

4.2. Network Security System Baseline Performance Analysis

The implementation of firewall analytics in MikroTik CCR is a critical stage in this study, which aims to provide comprehensive protection against DNS and SYN Flood attacks.

1. Configuration Implementation Methodology
   The implementation of firewall analytics configuration is carried out using a layered defence approach that integrates various protection mechanisms at different levels. The configuration is based on two main files, namely gateway_router.backup and kpde_gateway.rsc, which contain comprehensive settings for the protection of the North Aceh Regency Government's network.
2. Basic Firewall Rules Configuration
   Basic firewall rule configuration is a key foundation in a network security architecture that selectively controls incoming and outgoing traffic according to pre-designed criteria. This approach ensures that only traffic that meets the security policy is allowed, while all unidentified connections are automatically blocked.
3. Implementation of DNS Flood Protection
   Protection against DNS Flood attacks is implemented through a combination of rate limiting, connection tracking, and dynamic address lists to detect abnormal query patterns. The configuration is designed to mitigate attacks without disrupting the normal operation of the system based on a pre-performed baseline analysis.
4. SYN Flood Protection Implementation
   Protection against SYN Flood attacks is implemented using a combination of connection tracking, SYN cookies, and rate limiting at the TCP connection level. This mechanism is designed to detect and mitigate attacks that effectively exploit the weaknesses of the TCP protocol's three-way handshake system.
5. Dynamic Address List Configuration
   The implementation of dynamic address lists allows the system to automatically identify and block the source of the attack based on the detected behaviour pattern. This mechanism serves as an adaptive defence system that can respond to attacks in real-time without the need for manual intervention from administrators.
6. Logging and Monitoring Configuration
   The implementation of a comprehensive logging and monitoring system allows administrators to perform forensic analysis and continuous optimisation of security configurations.
7. Firewall Performance Optimisation
   Performance optimisation is done to ensure that the implementation of firewall analytics does not cause significant degradation to network throughput and latency. Optimisation configuration includes adjusting system parameters related to packet processing and connection management to achieve maximum efficiency.
8. Configuration Validation and Testing
   After the implementation of the complete configuration, a series of tests was carried out to validate the effectiveness and stability of the system under various operational conditions. Testing includes configuration syntax verification, performance impact evaluation, and false positive level measurement to ensure the system does not disrupt normal operations.
9. Configuration Implementation Conclusion
   The implementation of firewall analytics on the North Aceh Regency Government's MikroTik CCR has been successfully carried out by integrating a layered protection mechanism against DNS and SYN Flood attacks. The configuration implements 47 active firewall rules, 6 dynamic address lists, and a comprehensive monitoring system with a performance impact of at least less than 5% overhead.

4.3. DDoS Attack Impact Analysis

The analysis of the impact of DDoS attacks is a critical stage in this study, which aims to measure how much impact the attack has on the network performance of the North Aceh Regency Government.

1. Attack Impact Measurement Methodology
   The DDoS attack impact measurement is carried out using a comparative methodology by comparing network performance before and during the attack. Simulated attacks were carried out against six different targets: Cloudflare DNS (1.1.1.1), Google DNS (8.8.8.8), local mail server (36.95.71.219), panel web server (36.95.71.220), YouTube, and Detik.com sites to represent different types of services.
2. Network Latency Analysis During Attacks
   Network latency analysis showed a significant increase in response time on all targets during DDoS attacks. The measurements were made using ping data, from which the system's response was recorded during the attack period.
3. Evaluate Packet Loss During an Attack
   The packet loss evaluation shows the impact of DDoS attacks on service availability and overall network connection reliability. The measurement is done by calculating the percentage of packets that are lost or unresponsive during the attack period compared to normal conditions.

4.4. Effectiveness of Firewall Mitigation

The effectiveness of firewall mitigation is a critical evaluation of the capabilities of the security system that has been implemented in reducing the impact of DDoS attacks on the network infrastructure of the North Aceh Regency Government.

4.5. Analysis of Overall System Performance

The overall system performance analysis is a comprehensive evaluation of the impact of the implementation of firewall analytics on MikroTik CCR on the network performance of the North Aceh Regency Government.

1. Performance Overhead of Firewall Implementation
   The implementation of firewall analytics on MikroTik CCR causes measurable performance overhead but is still within the tolerance limit for government system operations. Measurements are made against critical metrics such as CPU utilisation, memory consumption, network throughput, and latency to identify the impact of security implementation on overall performance.
2. The Trade-off Between Security and Performance
   An analysis of the trade-offs between security and performance shows that the implementation of firewall analytics provides a significant improvement to the security posture at minimal and acceptable performance sacrifices. The evaluation was carried out using a security-performance matrix framework that compares the level of protection obtained with the performance degradation caused by each security component.

4.6. Discussion and Implications for Government Networks

The discussion of the results of this research has significant strategic relevance for the implementation of network security in the government environment, especially the North Aceh Regency Government and other local government agencies in Indonesia. Contextualization of the research findings shows that the implementation of firewall analytics on MikroTik CCR can provide an effective and efficient security solution to protect government information technology infrastructure from the threat of DDoS attacks.

1. Relevance of Results for the North Aceh Regency Government
   The discussion of the results of this research has significant strategic relevance for the implementation of network security in the government environment, especially the North Aceh Regency Government and other local government agencies in Indonesia. Contextualization of the research findings shows that the implementation of firewall analytics on MikroTik CCR can provide an effective and efficient security solution to protect government information technology infrastructure from the threat of DDoS attacks.
2. Conformity with Public Service Needs
   The implementation of firewall analytics shows high conformity with the characteristics and needs of public services that have high expectations of availability, reliability, and security from the public. The analysis shows that the implemented configuration is able to maintain the performance of public services under attack conditions without significantly reducing the quality of user experience.

5. Conclusion

Based on the results of research that has been carried out on the implementation of firewall analytics in DNS and SYN Flood protection in Mikrotik CCR in the North Aceh Regency Government, it can be concluded that the following can be concluded:

1. The CCR Mikrotik Firewall has proven to be effective in detecting and preventing DNS Flood and SYN Flood attacks on the North Aceh Regency Government network. Data analysis showed that under normal conditions, the system was able to maintain a packet loss of 0% and an average latency of 18 ms for external connections and 16 ms for local servers.
2. The identification of weaknesses in the Mikrotik CCR firewall configuration shows several aspects that need to be improved, including: a lack of optimal rate limiting implementation, the absence of a real-time traffic anomaly detection mechanism, and threshold configurations that have not been adjusted to the characteristics of government traffic.
3. The impact of the attack on network performance was significant, with an increase in packet loss of up to 48.33% and a latency degradation of up to 8 times that of normal conditions. This shows the importance of implementing a robust protection system to maintain the continuity of government services.
4. The implementation of the SYN-Protect firewall rules with a limit of 400 connections per 5 seconds has been proven to reduce the impact of attacks, although it does not eliminate disruption to the system.
5. Firewall log analysis showed an attack pattern consistent with the characteristics of DNS Flood and SYN Flood, where there was a significant spike in the number of unresolved TCP requests and connections.
6. Monitoring the router's CPU load showed a drastic increase during the attack, even causing the router to undergo an automatic reboot, indicating the importance of resource management optimisation in firewall configuration.

References

[1] W. Yunus and M. E. Lasulika, "Security system analysis against flood attacks using tcp, udp, and icmp protocols on mikrotik routers," *Int. J. Adv. Data Inf. Syst.*, vol. 3, no. 1, pp. 11–19, 2022.

[2] M. Faisal, N. Nurdin, F. Fajriana, and Z. Fitri, "Information and Communication Technology Competencies Clustering For Students For Vocational High School Students Using K-Means Clustering Algorithm," *Int. J. Eng. Sci. Inf. Technol.*, vol. 2, no. 3, pp. 111–120, 2022, doi: 10.52088/ijesty.v2i3.318.

[3] Y. Gautam, K. Sato, and B. P. Gautam, "Layer Based Firewall Application for Detection and Mitigation of Flooding Attack on SDN Network," Muroran Institute of Technology, 2022.

[4] D. Mustofa, A. Wirasto, A. Muttakin, D. N. Astrida, and D. I. S. Saputra, "Implementation of Load Balancing Per Connection Classifier on Mikrotik for Internet Services at Private Vocational Schools," *SAGA J. Technol. Inf. Syst.*, vol. 1, no. 3, pp. 104–113, 2023.

[5] A. I. Haris, B. Riyanto, F. Surachman, and A. A. Ramadhan, "Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari

Serangan DoS dan Pengaruhnya Terhadap Performansi," *Komputika J. Sist. Komput.*, vol. 11, no. 1, pp. 67–76, 2022.

[6] S. Sapriadi, Y. Yunus, and R. W. Dari, "Prediction of the Number of Arrivals of Training Students with the Monte Carlo Method," *J. Inf. dan Teknol.*, vol. 4, pp. 1–6, 2022, doi: 10.37034/jidt.v4i1.168.

[7] M. Fakhmi and L. M. Gultom, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall Raw (Studi kasus: Sekolah Menengah Kejuruan Negeri 3 Bengkalis)," in *Seminar Nasional Industri dan Teknologi*, 2021, pp. 260–277.

[8] C. S. Silvia, M. Ikhsan, M. Safriani, and T. P. Gusmilia, "Efficiency Rainwater Harvesting at the Roof Campus Buildings," *Int. J. Eng. Sci. Inf. Technol.*, vol. 1, no. 3, 2021, doi: 10.52088/ijesty.v1i3.80.

[9] D. Aprilianto, T. Fadila, and M. A. Muslim, "Sistem pencegahan UDP DNS Flood dengan filter Firewall pada router Mikrotik," *Techno. com*, vol. 16, no. 2, pp. 114–119, 2017.

[10] D. B. Sufardy, "Penggunaan PFSense dan Suricata Sebagai Alat Pendeteksi danPencegahan Serangan Keamanan Jaringan pada Web server," 2024.

[11] A. J. Alhasan and N. Surantha, "Evaluation of Data Center Network Security based on Next-Generation Firewall," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 9, 2021.

[12] P. A. Khairunnisa, N. Annisa, J. Parhusip, and others, "Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI: Studi Kasus di Indonesia," *Tek. J. Ilmu Tek. Dan Inform.*, vol. 4, no. 2, pp. 9–16, 2024.

[13] M. G. S. Putra, F. Falahah, and A. F. Santoso, "Analisis Dan Perancangan Arsitektur Enterprise Sistem Pemerintahan Berbasis Elektronik (Spbe) Pada Domain Data Di Lingkungan Badan Pengelolaan Keuangan Daerah (Bpkd)," *eProceedings Eng.*, vol. 11, no. 4, 2024.

[14] Y. S. Aritonang, P. Siagian, and S. Aryza, "Inovasi dan Tantangan dalam Pengembangan Sistem Transmisi Tenaga Listrik Berbasis Teknologi Tinggi Ultra High Voltage untuk Meningkatkan Keandalan dan Efisiensi Energi (Sebuah Tinjauan Literatur)," *J. Inform. dan Tek. Elektro Terap.*, vol. 12, no. 3S1, 2024.

[15] A. R. Rozzaqi and others, "Analisa Jaringan Kampus pada Lingkungan Kampus Multi-Lokasi Universitas PGRI Semarang," *JIPETIK J. Ilm. Penelit. Teknol. Inf. \& Komput.*, vol. 4, no. 2, pp. 112–120, 2023.

[16] F. Fitri, "Analisa Kinerja VPN dengan Layer 2 Tunneling Protocol dan IPSec Menggunakan Router Mikrotik (Studi Kasus RSU Bunda Margonda)," Sekolah Tinggi Teknologi Terpadu Nurul Fikri, 2023.

[17] A. R. Rozzaqi, W. Wijayanto, and F. Amin, "IMPLEMENTASI USER MANAGER DENGAN DATA RESMI UNTUK MONITORING PENGGUNAAN JARINGAN DI LINGKUNGAN KAMPUS," *J. Ilm. Teknosains*, vol. 10, no. 2/Nov, pp. 65–71, 2024.

[18] N. Hafifah and A. Nurhayati, "Analisis Keamanan Jaringan LAN berdasarkan Log Data CCR (Cloud Core Router) pada Laboratorium SMK Telkom Jakarta," *eJournal Mahasiswwa Akad. Telkom Jakarta*, 2020.

[19] V. T. Aditya, "Manajemen Ancaman dan Keamanan Jaringan melalui Penggunaan Firewall dengan Mikrotik pada PT Dinamika Mediakom," Universitas Islam Indonesia, 2024.

[20] A. Martani, S. Sukirman, and J. Junaedy, "Jaringan komputer dengan mikrotik." PT MAFY MEDIA LITERASI INDONESIA, 2024.

[21] H. Ulfa, A. I. Basuki, G. M. Suranegara, and A. Fauzi, "DDoS Protection System for SDN Network Based on Multi Controller and Load Balancer," *SISTEMASI*, vol. 13, no. 2, pp. 555–571, 2024.

[22] M. K. Zein, M. Is' ad, A. S. Wardhana, and M. Pradana, "Implementasi Smart Home Berbasis ESP32 dan Integrasi Protokol MQTT, Node-RED serta Google Assistant melalui NORA," *J. Instrum. Hardw.*, vol. 2, no. 2, pp. 29–37, 2024.

[23] H. P. Fitrian, F. Anisa, M. Agustina, N. Masitoh, and A. Gunawan, "OPTIMALISASI KONEKTIVITAS JARINGAN KAMPUS MELALUI SIMULASI ARP DAN DHCP MENGGUNAKAN CISCO PACKET TRACER," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 2, pp. 1978–1986, 2025.