JTERA (Jurnal Teknologi Rekayasa), Vol. 11, No. 1, Juni 2026, Hal. 199-208 p-ISSN 2548-737X
Terakreditasi "**Peringkat 3**" oleh Kemdiktisaintek, Nomor : 10/C/C3/DT.05.00/2025 e-ISSN 2548-8678
DOI: 10.31544/jtera.v11.i1.2026.199-208

From Exposed Risk to Controlled Risk: Evaluating MikroTik Firewall Rules in Network Security

Muzakir [1*], Ulfa Merlinda[2], Teuku Farizal[3], Murhaban[4], Suryadi[5], Mukhlizar[6] , Muzakkir[7]
[1]Department of Management, Universitas Teuku Umar, Aceh Barat 23617, Indonesia
[2,4,5]Department of Information Technology, Universitas Teuku Umar, Aceh Barat 23617, Indonesia
[3]Department of Civil Engineering, Universitas Teuku Umar, Aceh Barat 23617, Indonesia
[6]Sekolah Tinggi Agama Islam Negeri Teungku Dirundeng, Aceh Barat Indonesia
[7]Department of Communication Science, Universitas Teuku Umar, Aceh Barat 23617, Indonesia;
murhaban@utu.ac.id

Abstrak

Ketergantungan instansi pemerintah pada layanan berbasis internet menjadikan keamanan jaringan sebagai fondasi penting dalam menjaga keberlanjutan layanan publik, kerahasiaan data, serta kepercayaan masyarakat. Namun, keberadaan firewall tidak selalu menjamin keamanan apabila efektivitas aturannya tidak dibuktikan melalui pengujian empiris. Penelitian ini mengevaluasi aturan firewall MikroTik sebagai mekanisme kontrol keamanan untuk mengubah kondisi jaringan dari risiko terpapar menjadi risiko yang terkendali. Metode yang digunakan adalah eksperimen sebelum dan sesudah penerapan firewall melalui tiga skenario serangan, yaitu packet sniffing berbasis ARP spoofing menggunakan Ettercap, port scanning menggunakan Zenmap, dan Distributed Denial of Service (DDoS) menggunakan Hping3. Wireshark dan Winbox digunakan untuk memantau lalu lintas jaringan, respons sistem, serta efektivitas mitigasi firewall. Hasil pengujian menunjukkan bahwa sebelum firewall diaktifkan, packet sniffing menangkap paket DHCP dan metadata IP-MAC, port scanning mengidentifikasi 8 port terbuka, serta DDoS menyebabkan penggunaan memori mencapai 84%. Setelah aturan firewall diterapkan, aktivitas sniffing hanya menampilkan DHCP Discover normal, port terbuka tidak lagi terdeteksi, dan paket DDoS dijatuhkan sebelum membentuk koneksi yang efektif. Firewall MikroTik menunjukkan keandalan pemblokiran paket sniffing hingga 82 paket dalam skenario pengujian. Temuan ini menegaskan bahwa firewall berperan sebagai kontrol keamanan berbasis bukti.

Kata kunci: Firewall Mikrotik; keamanan jaringan; packet sniffing; port scanning; mitigasi DDoS

Abstract

The dependence of government institutions on internet-based services has made network security a critical foundation for maintaining continuity of public services, data confidentiality, and public trust. However, the presence of a firewall does not necessarily ensure security unless the effectiveness of its rules is empirically validated. This study evaluates MikroTik firewall rules as a security control mechanism to transform network conditions from exposed to controlled risk. A before-and-after experimental design was employed using three attack scenarios: ARP spoofing-based packet sniffing with Ettercap, port scanning with Zenmap, and Distributed Denial of Service (DDoS) attacks with Hping3. Wireshark and Winbox were used to monitor network traffic, system responses, and the effectiveness of firewall mitigation. The results show that before firewall activation, packet sniffing captured DHCP packets and IP-MAC metadata, port scanning identified eight open ports, and DDoS attacks increased memory utilization to 84%. After the firewall rules were implemented, sniffing activity was limited to normal DHCP Discover traffic, open ports were no longer detected, and DDoS packets were dropped before they could establish effective connections. The MikroTik firewall demonstrated its ability to block up to 82 packet-sniffing-related packets in the tested scenario. These findings confirm that firewall rules can serve as evidence-based security controls.

Keywords: MikroTik firewall; network security; packet sniffing; port scanning; DDoS mitigation

I. INTRODUCTION

Digital transformation in the public sector has positioned the Internet network as a critical

infrastructure for supporting public services, data exchange, institutional communication, and information system integration. In the context of local government institutions, network security can no longer be regarded merely as a technical issue; rather, it has become an essential component of digital service governance. When a network lacks an effective protection mechanism, the resulting risks are not limited to connectivity disruption. Still, they may also include the exposure of network information, service unavailability, and declining public trust in government digital systems. [1][2].

A key problem in network security is that cyber threats can arise from relatively simple techniques yet have serious consequences for traffic confidentiality, service visibility, and system availability. Packet sniffing, ARP spoofing, port scanning, and Distributed Denial of Service (DDoS) attacks are commonly used to examine network weaknesses. Packet sniffing and ARP spoofing allow attackers to observe network traffic and metadata. At the same time, port scanning identifies active services via open ports, which may serve as a basis for further exploitation [3][4]. Meanwhile, DDoS attacks threaten system availability by flooding the target with excessive traffic, potentially degrading device performance and disrupting access for legitimate users [5][6][7][8].

Firewall technology is one of the primary mechanisms for controlling network traffic. In practice, a firewall filters packets, restricts access, hides services that should not be publicly exposed, and prevents suspicious connections. MikroTik is widely used in organizational networks for its configurable security features, including firewall rules, NAT, address lists, bridge filters, connection limits, and rate limits. However, the mere existence of a firewall does not automatically guarantee network security. Firewall effectiveness depends on the accuracy of rule design, the characteristics of the attack, and the configuration's ability to respond to abnormal traffic patterns [9][10].

The central problem addressed in this study is that firewalls are often considered effective simply because they have been configured, whereas their effectiveness must be empirically verified. A network that appears administratively protected is not necessarily capable of preventing traffic interception, hiding service ports from scanning activities, or mitigating packet floods that may compromise system stability. Therefore, firewall evaluation should focus on determining whether the implemented security rules can actually transform the network condition from exposed risk to controlled risk [8][10][11].

In response to this problem, this study evaluates MikroTik firewall rules for network security using a before-and-after experimental design. The evaluation involves three attack scenarios: packet sniffing, port scanning, and DDoS. Packet sniffing is used to examine potential exposure of network traffic and metadata. Port scanning is used to assess the extent to which active services remain visible to attackers. DDoS attacks are used to test a network's ability to maintain system availability under excessive traffic conditions. All scenarios are tested under two conditions: before firewall activation and after implementing MikroTik firewall rules.

This study positions "exposed risk" as the initial condition in which effective firewall rules have not yet been applied to the network. Under this condition, attackers may still observe basic network traffic, map open ports, and overload the target through large volumes of attack packets. Conversely, "controlled risk" refers to the state after firewall rules have been implemented, in which attack activity can be restricted, service visibility reduced, suspicious packets blocked, and system stability better maintained [12][13][14].

Accordingly, the focus of this study is not merely on how MikroTik firewall rules are configured, but on demonstrating their effectiveness empirically through changes in network responses. The evaluation focuses on key indicators, including network traffic exposure, the success or failure of packet sniffing, the number of detected ports, the firewall's ability to block attack packets, and system stability during DDoS attacks. This approach makes the study evidence-based by assessing firewall effectiveness through comparisons of network conditions before and after the implementation of security rules. The main contribution of this study is an empirical evaluation of MikroTik firewalls across multi-attack scenarios that represent three fundamental aspects of network security: traffic confidentiality, service visibility control, and system availability.

II. METHOD

A. System Design

The system design in this study was developed to evaluate the reliability of a MikroTik firewall in securing the internet network of a government institution. The system was constructed using an experimental approach by comparing network conditions before and after the firewall configuration was applied. The architecture consisted of three main components: an attacker device, a target device, and a MikroTik router serving as the network security device. The attacker device was used to conduct attack simulations: Ettercap for ARP spoofing-based packet sniffing, Zenmap for port scanning, and Hping3 for Distributed Denial of Service (DDoS) [15]. The target device served as the test object, receiving network traffic and becoming the attack target. The MikroTik router functioned as a firewall that managed, filtered, and restricted data traffic through firewall rules, bridge filters, address lists, and Network Address Translation (NAT). All network activities were observed using Wireshark to obtain technical evidence, including packet patterns, target responses, open ports, and changes in network traffic.

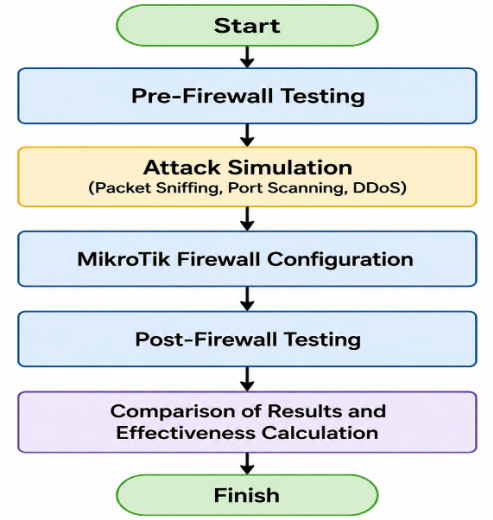

Figure 1. Testing flowchart

System testing was conducted under two conditions: before the firewall was activated and after the firewall was configured. In the initial condition, the network was tested without specific firewall protection to determine its vulnerability to packet sniffing, port scanning, and DDoS attacks. [16].. The MikroTik firewall was then configured using Winbox, with rules tailored to each attack's characteristics. After firewall activation, the same attack scenarios were repeated to measure changes in network response. The system design was evaluated based on the firewall's ability to reduce malicious traffic, conceal port information, prevent the establishment of attack connections, and maintain target-device stability. Firewall effectiveness was calculated using Equation (1):

$$E_f = \frac{A_b}{A_t} \times 100\% \quad (1)$$

Where E_f denotes firewall effectiveness, A_b is the number of attacks successfully blocked, and Nt is the total number of attacks tested. A_t A higher effectiveness value indicates that the firewall is more effective at protecting the network from attacks.

B. Experimental Environment

The experimental environment in this study resembles a local network scenario used in institutional operational activities. The test involved three main elements: the attacker computer, the victim computer, and the MikroTik device, which served as both a security mechanism and a manager of network communication flows. The attacker's computer was used to execute several attack scenarios, whereas the victim computer was positioned as a network access device and observation target. The MikroTik device was placed between network connections to control packet flow, enforce access restrictions, and filter activities flagged as suspicious, as illustrated in Figure 2. Through this design, the experiment demonstrates how a network-security device responds to both normal and malicious traffic during testing.

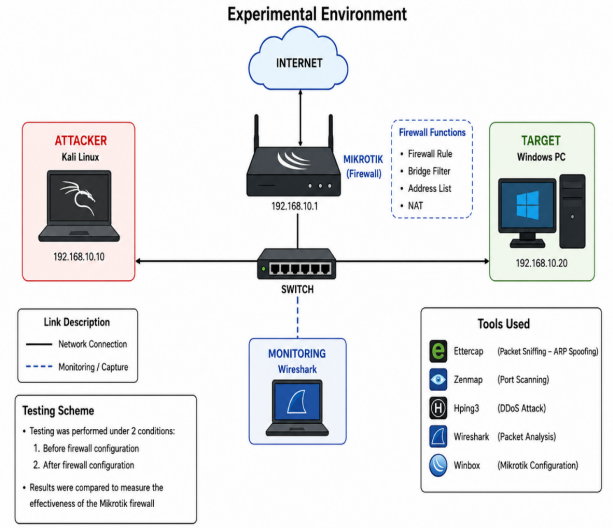

Figure 2. Experimental environment

The software used in the experiment, as shown in Figure 2, included Winbox, Wireshark, Ettercap, Zenmap, Hping3, and Kali Linux. Winbox was used to access and configure the firewall on the MikroTik router. Wireshark was used to monitor and analyze network packets during testing. Ettercap was used to simulate ARP spoofing-based packet sniffing, Zenmap to identify open ports on the target device, and Hping3 to simulate Distributed Denial of Service (DDoS) attacks [11]. Testing was conducted under two conditions: before firewall

configuration and after firewall activation. The results from both conditions were compared based on network responses, packet-capture results, detected port status, and the number of packets successfully blocked by the MikroTik firewall.

C. Experimental Scenarios and Network-Attack Evaluation

Network security testing before the MikroTik firewall implementation was conducted to identify the network's vulnerabilities to various cyberattacks. In the initial stage, the attacker's computer, the target computer, and the MikroTik router were connected to the same local network so that all devices could communicate properly. At this stage, the MikroTik router remained in its default state, with no specific firewall configuration. The first test used Ettercap to simulate ARP spoofing-based packet sniffing. [17]. The attacker scanned hosts, selected the victim target and network gateway, and executed ARP poisoning to redirect the victim's data traffic to the attacker's device. All network activities were monitored using Wireshark to observe captured packets. The next test involved using Zenmap's Intense Scan method to detect open ports on the target computer. In addition, a Distributed Denial of Service (DDoS) attack was simulated using Hping3 by repeatedly sending TCP, UDP, or ICMP packets to the target. This test aimed to assess the impact of increased network traffic on connection stability and target device performance.

The next stage involved implementing the firewall on the MikroTik router using Winbox, configuring security rules based on the characteristics of the tested attacks. The firewall was configured to restrict suspicious ARP activity, detect port-scanning patterns, and control excessive connections that could potentially trigger DDoS attacks. The configuration used packet filtering, address lists, connection limits, and rate limits to block abnormal network traffic automatically. After the firewall configuration was applied, attack testing was repeated using the same tools and scenarios as in the previous stage. All network traffic was again monitored using Wireshark to observe changes in network security conditions after the firewall was activated. [18]. The results before and after firewall implementation were compared based on packet-sniffing success, the number of detected ports, network stability during attacks, and the firewall's ability to block suspicious packets. These analyses were used to evaluate the effectiveness of the MikroTik firewall in enhancing computer network security.

D. Firewall Effectiveness Analysis Against Network Attacks

The data were analyzed using test results from three attack types. Packet sniffing was tested using Ettercap to assess the attacker's ability to capture network traffic. Port scanning was performed with Zenmap to identify open ports on the target device, while DDoS testing was conducted with Hping3 to assess the impact of packet flooding on system stability. The analysis compared attack success rates before and after firewall deployment. The main indicators observed included attack status, the number of packets successfully blocked, the number of open ports, and changes in target-device performance. [16]. To measure the firewall's ability to withstand attacks, the Block Ratio was calculated using Equation (2):

$$PBR = \frac{P_b}{P_s} \times 100\% \quad (2)$$

Where BR is the percentage of the firewall's ability to block attack packets, P_b is the number of attack packets successfully blocked, and P_t is the total number of attack packets sent or detected during the testing process.

For the DDoS attack, the analysis focused on changes in CPU load on the target device before and after the firewall was activated. DDoS was analyzed in more detail because this attack floods the network with a large number of packets, potentially increasing CPU utilization, degrading performance, and disrupting services. The measurement compared Central Processing Unit utilization during the attack before firewall implementation and after the MikroTik firewall was configured. The equation used is shown in Equation (3):

$$CPU_{Reduction} = \frac{CPU_{Before}}{CPU_{After}} \times 100\%. \quad (3)$$

CPUbefore denotes the percentage of CPU utilization during the DDoS attack before firewall activation, whereas CPUafter denotes the CPU utilization percentage after firewall implementation. A higher CPU-reduction value indicates the firewall's greater ability to reduce the impact of DDoS attacks. The results were then described qualitatively to show the effectiveness of the MikroTik firewall in improving network security at Diskominsa Aceh Barat Daya. If, after firewall activation, the number of attack packets decreases, open ports are no longer detected, and CPU utilization remains stable during DDoS attacks, the firewall can be considered effective at blocking attacks and maintaining network stability.

III. RESULTS AND DISCUSSION

A. Vulnerability Analysis and Firewall Mitigation Effectiveness

Figure 4 confirms that before the MikroTik firewall was activated, the local network was significantly exposed. The highest vulnerability score, 9.5, was observed in the DDoS scenario, which falls into the critical category. This finding indicates that service availability was the weakest aspect, as the system lacked a filtering mechanism capable of withstanding repeated TCP SYN flood attacks. Packet sniffing obtained a score of 7.5 and was classified as highly vulnerable, indicating that local traffic could still be observed through ARP spoofing. Although credentials could not be extracted because the target website used HTTPS, the attacker could still obtain basic network information such as IP addresses, MAC addresses, and DHCP communication patterns. Meanwhile, port scanning obtained a score of 6.5 and was classified as vulnerable because services on the target device could still be mapped through open ports. Thus, this baseline graph indicates that before firewall deployment, the network faced not only partial technical risks but also multidimensional vulnerabilities involving confidentiality, service exposure, and availability.

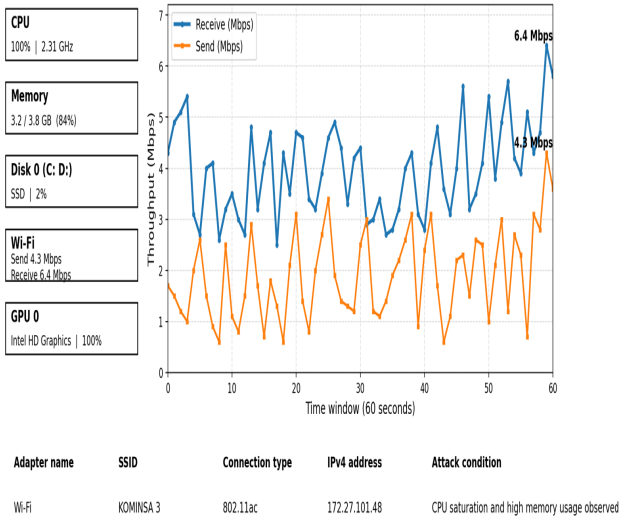

Figure 3. CPU display during the attack

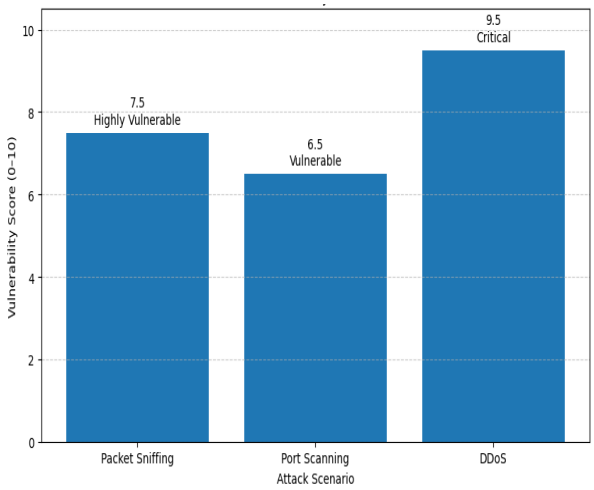

Figure 4. Baseline network vulnerability before MikroTik firewall activation

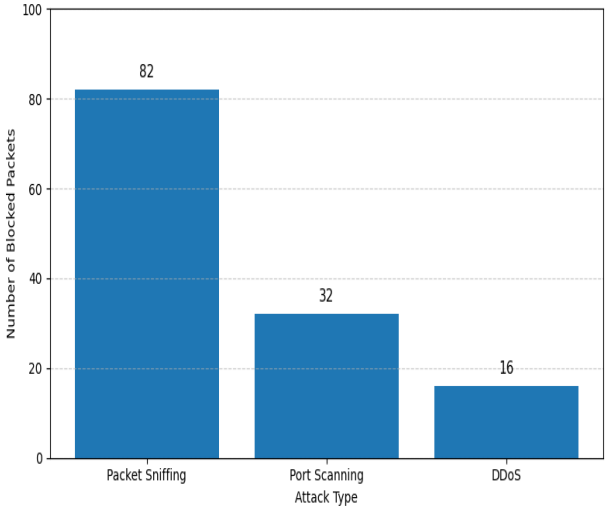

Figure 5. Blocked Packets After MikroTik Firewall Activation

Figure 5 illustrates the change in network conditions after the MikroTik firewall was activated, measured through the number of attack packets successfully blocked. The firewall rule recorded the highest number of blocked packets during packet sniffing (82), followed by port scanning (32) and DDoS (16). This pattern shows that the firewall operated selectively according to the characteristics of each attack traffic pattern. In packet sniffing, packet blocking reflected the firewall's ability to restrict ARP/DHCP traffic that could be used for network reconnaissance. In port scanning, blocking indicated that the firewall reduced the attacker's ability to obtain responses from the target ports, making reconnaissance ineffective. In the DDoS attack, although fewer packets were blocked, the mitigation impact remained significant because the firewall dropped SYN packets before a connection was established. [19]. The relationship between the two graphs demonstrates a shift from exposed risk to controlled risk. In other words, attacks could still be

detected, but they did not develop into successful access, service mapping, or system disruption.

B. *Firewall Reliability Level*

The results presented in Table 1 show the activity outcomes of the three attack scenarios before the MikroTik firewall rules were activated. This stage served as a baseline to observe the original network response when no traffic-filtering mechanism was applied. The first scenario was ARP spoofing using Ettercap. This attack was successfully executed, indicating that the attacker was able to manipulate local communication and observe traffic between the target and the network. Although the attacker did not obtain the username and password because the accessed website used HTTPS, DHCP packets consisting of request, offer, and acknowledgment messages were still captured along with IP and MAC address information. This finding shows that HTTPS protection shielded user credentials, while network metadata at the local layer remained exposed.

Table 1. Results of the three attack activities before the firewall rules were activated.

No.	Activity	Software	Description	Result
1	ARP Spoofing Process	Ettercap	Successful	The attacker did not obtain the target's username and password because the website used HTTPS instead of HTTP. However, the attacker successfully captured DHCP packets, including request, offer, and acknowledgmen packets, along with IP and MAC addresses.
2	Port Scanning Process	Zenmap	Successful	The scan displayed several open ports, namely 80, 135, 139, 443, 445, 3306, 5357, and 8080.
3	DDoS Attack Process	Hping3	Successful	A large number of TCP, UDP, and ICMP packets were sent to the target.
4	Network Activity Monitoring Process	Wireshark	Successful	The tool displayed the network activities the attacker performed against the target.

Table 2. Results of the three attack activities after the firewall rules were activated

No.	Activity	Software	Description	Result
1	ARP Spoofing Process	Ettercap	Unsuccessful	The attacker failed to perform sniffing on the target. The result only displayed DHCP Discover packets, which are broadcast packets used to obtain an IP address from the DHCP server.
2	Port Scanning Process	Zenmap	Unsuccessful	The scan did not display any open ports.
3	DDoS Attack Process	Hping3	Unsuccessful	The attacker was unable to send a large number of TCP, UDP, and ICMP

				packets to the target.
4	Network Activity Monitoring Process	Wireshark	Successful	The tool displayed the network activities the attacker performed against the target.
5	Attack Mitigation Process Using Firewall Rules	Winbox	Successful	The Firewall Rule feature available in Winbox successfully mitigated all three attack scenarios.

The second scenario was port scanning using Zenmap. The test results in Table 2 show that several open ports were successfully identified before firewall activation: 80, 135, 139, 443, 445, 3306, 5357, and 8080. This condition indicates that the target device still responded to the attacker's scanning attempts, allowing active services to be mapped to inform potential follow-up attacks. The third scenario was a DDoS attack using Hping3 by sending large numbers of TCP, UDP, and ICMP packets to the target. This attack demonstrated a risk to service availability because the target received a high traffic load. In addition, Wireshark successfully displayed network activities performed by the attacker against the target [20]. Overall, the results at this initial stage indicate that before the firewall rules were activated, the network remained vulnerable to traffic interception, service mapping, and disruption of system availability.

C. *Security Control Transition*

The security-control transition represents the change in the reliability level of network-security controls before and after the MikroTik firewall rules were activated. Figure 6 shows that before the firewall implementation, the three security dimensions were at 0%, indicating the absence of an effective control mechanism to withstand attacks. In the traffic-confidentiality dimension, packet sniffing still allowed the attacker to observe basic network traffic, including DHCP, IP, and MAC address information. In the service-visibility-control dimension, port scanning still revealed active services via open ports. Meanwhile, in the system-availability dimension, DDoS attacks could still potentially overload the target by transmitting large numbers of packets. [19]. This initial condition shows that before firewall activation, the network was exposed to reconnaissance, service mapping, and disruption of system availability.

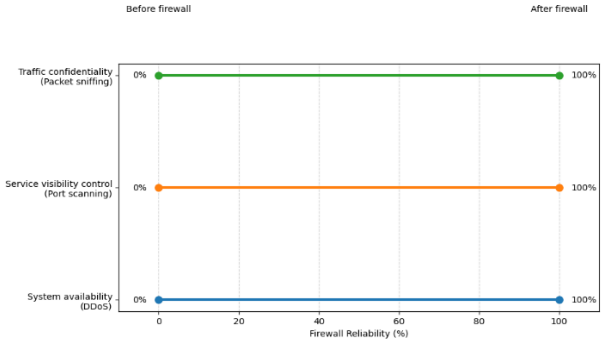

Figure 6. Security control transition before and after MikroTik firewall activation

After the MikroTik firewall rules were enabled, the security control level increased to 100%. This improvement indicates that the firewall consistently performed its protective function across all testing scenarios. In packet sniffing, the firewall limited the information the attacker could observe, so sensitive traffic was no longer significantly exposed. In port scanning, the firewall reduced service visibility by preventing the display of open port lists. In a DDoS attack, the firewall filtered out malicious packets before connections were formed, thereby maintaining system availability. The transition pattern from 0% to 100% demonstrates that the MikroTik firewall functions not merely as a packet blocker but also as a security control mechanism that transforms the network condition from vulnerable to controlled. Therefore, this graph strengthens the evidence that the firewall reliability in this study is comprehensive across the three main aspects of network security: traffic confidentiality, service visibility control, and system availability.

IV. CONCLUSION

This study confirms that MikroTik firewall rules can transform a government institution's network from an attack-exposed condition into a more controlled and measurable security environment. Through a before-and-after firewall implementation experiment, the findings reveal that an unprotected network remained exposed to IP–MAC metadata via ARP spoofing-based packet sniffing, displayed open ports via port scanning, and experienced DDoS pressure that drastically increased CPU utilization. After the firewall rules were activated, the risk pattern changed significantly: sniffing activity was limited to normal DHCP Discover traffic, service

ports were no longer detected, and DDoS packets were dropped before establishing effective connections. These findings demonstrate that the MikroTik firewall functions not only as a packet-filtering mechanism but also as an evidence-based security control that reduces traffic exposure, limits service visibility, and maintains system availability. The main contribution of this study is the development of a multi-attack before-and-after evaluation model that is academically relevant for assessing government network security. This model may also serve as a basis for developing more adaptive, auditable, and empirically grounded network security policies.

REFERENCE

[1] M. Mijwil, "The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment," *Mesopotamian J. CyberSecurity*, vol. 3, no. 1, 2023.

[2] V. Figueroa, L. Enrique, S. Crespo, A. S. David, and E. Fernández-medina, "Building a holistic cybersecurity framework for e-Government based on a systematic analysis of proposals," *Int. J. Inf. Secur.*, vol. 24, no. 3, pp. 1–19, 2025, doi: 10.1007/s10207-025-01024-0.

[3] M. Kumar and C. S. Dash, "Detecting and Preventing ARP Spoofing Attacks Using Real - Time Data Analysis and Machine Learning," *Int. J. Innov. Res. Comput. Sci. Technol.*, no. 5, pp. 47–55, 2024.

[4] Z. Al-khazaali and A. Sabah, "Characteristics of Port Scan Traffic : A Case Study Using Nmap," *J. Eng. Sustain. Dev.*, vol. 29, no. 01, pp. 26–35, 2025.

[5] T. U. Chai, H. G. Goh, S. Liew, and V. Ponnusamy, "Fragmentation Attacks in Smart Factory," *Systems*, 2023.

[6] W. I. Khedr and A. E. Gouda, "P4-HLDMC : A Novel Framework for DDoS and ARP Attack Detection and Mitigation in SD-IoT Networks Using Machine Learning, Stateful P4, and Distributed Multi-Controller Architecture," *Math. Artic.*, 2023.

[7] S. Y. N. A. C. K. Packets *et al.*, "Detection and Mitigation of SYN Flooding Attacks through SYN/ACK Packets and Black/White Lists," *Sensors*, pp. 1–14, 2023.

[8] Y. Su, D. Xiong, K. Qian, and Y. Wang, "A Comprehensive Survey of Distributed Denial of Service Detection and Mitigation Technologies in Software-Defined Network," *Electron. Rev.*, 2024.

[9] M. L. Arsalan and H. T. Sukmana, "Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing Menggunakan Firewall Rule (Studi Kasus : Pt . Akurat . Co) Wi-Fi Network Security Against Packet Sniffing Attacks Using Firewall Rule (Case Study : Pt . Accurate . Co)," *CyberSecurity dan Forensik Digit.*, vol. 6, no. 2, pp. 30–38, 2023.

[10] M. A. Rozan and M. Tahir, "Implementation and Security Testing of Mikrotik Router Against Cyber Attacks Using Firewall and Penetration Testing," *J. Artif. Intell. Eng. Appl.*, vol. 4, no. 3, 2025.

[11] R. A. Bakar and B. Kijsirikul, "Enhancing Network Visibility and Security with Advanced Port Scanning Techniques," *Sensors*, vol. 23, pp. 1–27, 2023.

[12] R. B. Saputra and A. T. Zy, "DDoS Attack Detection and Mitigation with Dynamic Firewall Technique," vol. 7, no. 2, 2025, doi: 10.35842/ijicom.

[13] F. W. Christanto, P. Cholillah, and A. M. Hirzan, "Optimizing Mikrotik-Based Network Security using Address List, Firewall Filter Rules, and Raw Firewall," 2025.

[14] S. Islam, M. A. Uddin, D. Hossain, and S. Ahmed, "Analysis and Evaluation of Network and Application Security Based on Next Generation Firewall," vol. 1, no. 1, 2023.

[15] V. Hnamte and J. Hussain, "Telematics and Informatics Reports Enhancing security in Software-Defined Networks : An approach to efficient ARP spoofing attacks detection and mitigation," *Telemat. Informatics Reports*, vol. 14, no. March, p. 100129, 2024, doi: 10.1016/j.teler.2024.100129.

[16] A. S. Review, "Applied Sciences Machine Learning Techniques to Detect a DDoS Attack in SDN :," *Appl. Sci.*, vol. 13, pp. 1–27, 2023.

[17] A. Ali, M. Husain, and P. Hans, "Intelligent ARP Spoofing Detection using Multi-layered Machine Learning Techniques for IoT Networks," *arXiv*, pp. 1–5, 2025.

[18] J. M. Pittman, "Reproducing Random Forest Efficiency in Detecting arXiv : 2302. 09317v1 [cs. CR] 18 Feb 2023," *arXiv*, 2023.

[19] A. El-sayed, H. Ramadan, E. R. Mohamed, and O. M. Elkomy, "OPEN SFARP : a multi-layered real-time security framework for hybrid ARP and DDoS attack defense in SD-IoT networks," *Sci. Rep.*, vol. 15, pp. 1–32,

2025.
[20] J. M. Pittman, “Machine Learning and Port Scans: A Systematic Review,” arXiv, pp. 0–2, 2023.