Bulletin of Network Engineer and Informatics
E-ISSN 2986-8017 | P-ISSN 2987-4858
https://bufnets.tech

Vol. 4 No 1 – April 2026
DOI: 10.59688/fq83hq56

AUTOMATION OF CYBER ATTACK MITIGATION ON ROUTEROS USING N8N ORCHESTRATION PLATFORM

Arief Budi Pratomo

Informatics System, Universitas Nusa Megarkencana
Jl. A.M. Sangaji No.49, Cokrodiningratan Kecamatan, Yogyakarta, Indonesia
e-mail: budiprato@gmail.com

Received : 07 February 2026	Accepted : 07 March 2026	Published : 18 April 2026

Abstract

The security of network infrastructure using MikroTik RouterOS is frequently compromised by automated cyber attacks, such as brute force and port scanning, which require rapid mitigation to prevent unauthorized access. This research aims to develop an automated mitigation system by utilizing n8n as a low-code workflow orchestrator to enhance response efficiency. The research method involves integrating RouterOS syslogs with n8n via a webhook or database trigger, which then automatically executes blocking commands through the MikroTik API when a threat is detected. The results demonstrate that the system can identify and isolate malicious IP addresses within seconds, significantly reducing the window of vulnerability compared to manual administrative intervention. In conclusion, the implementation of n8n provides an effective and scalable solution for real-time cyber attack mitigation, ensuring better network stability and security.

Keywords: *Automation, Mitigation, RouterOS, n8n, Cyber Security*

1. INTRODUCTION

The rapid advancement of information technology has made network infrastructure a primary target for various cyber threats [1]. Among the many operating systems used for routing, MikroTik's RouterOS is widely utilized across small to large-scale enterprises due to its versatility and feature-rich environment [2],[3]. However, this popularity also attracts malicious activities, particularly automated attacks such as brute force on SSH, Winbox, and Telnet services, as well as intensive port scanning [4]. These attacks, if not mitigated promptly, can lead to unauthorized access, resource exhaustion, and potential network downtime.

Traditionally, network administrators rely on manual log monitoring and static firewall rules to defend their systems [5]. This manual approach is often insufficient in facing modern, high-frequency automated attacks, as the time gap between detection and manual intervention provides a window of opportunity for attackers to succeed [6]. Therefore, there is an urgent need for an automated orchestration system that can respond to threats in real-time without requiring constant human oversight.

This research proposes an automated mitigation system by integrating RouterOS with n8n, a powerful low-code workflow automation tool [7],[8]. By leveraging the RouterOS API and syslog capabilities, n8n acts as a central brain that parses incoming security logs, identifies malicious patterns, and automatically pushes defensive configuration changes back to the router to block the source of the attack [9]. This approach not only increases the speed of response but also reduces the operational burden on network security teams.

2. RESEARCH METHODOLOGY

This section provides an explanation of the research stages, describing the logical sequence followed to achieve the expected research outcomes. The methodology is designed to create a closed-loop

automation system between MikroTik RouterOS and the n8n orchestration platform. The research is conducted through several structured phases as follows:

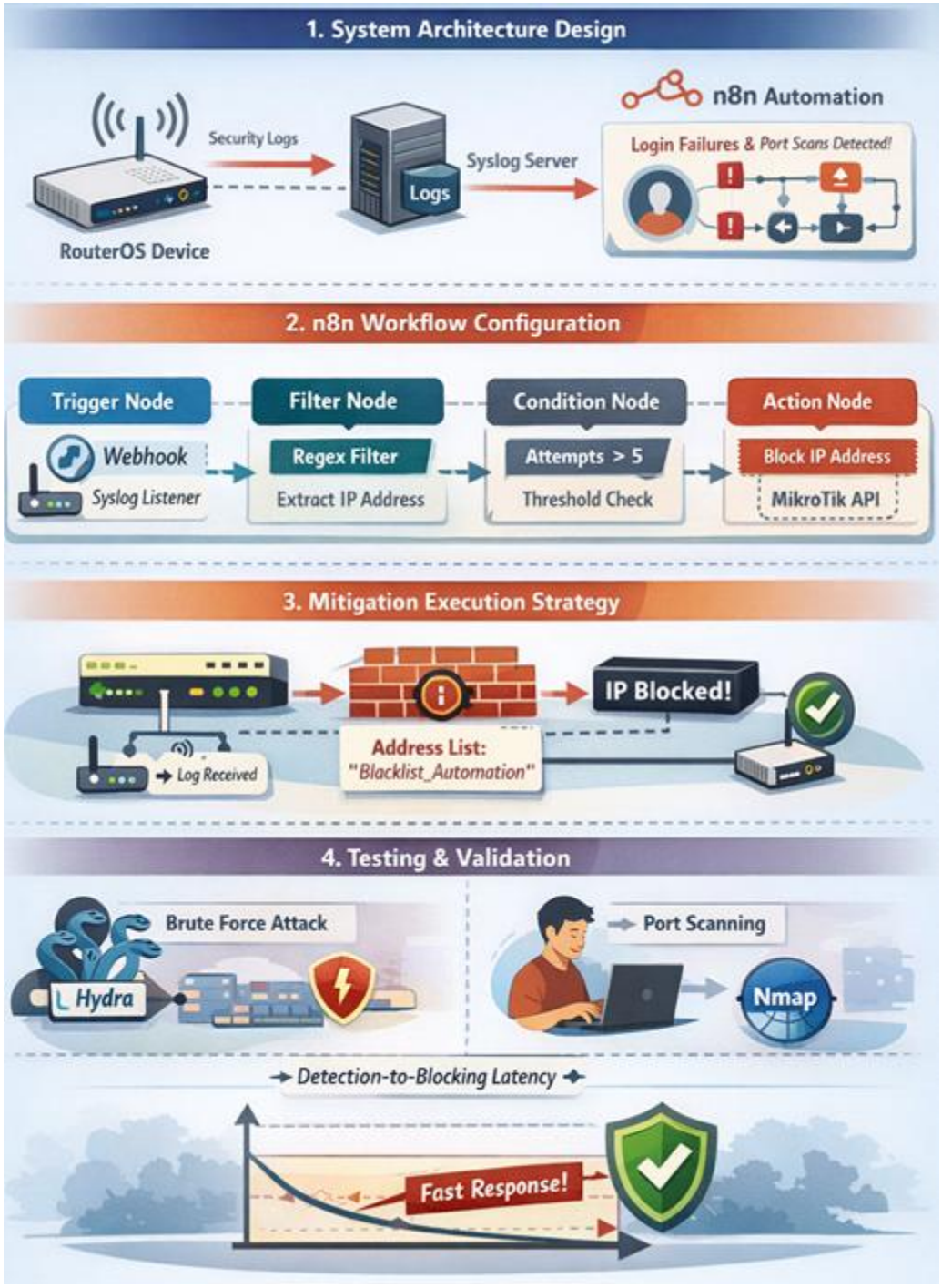

Figure 1. Ilustration of System Architecture
[Source:Author, 2026]

The system begins with an architectural design that integrates the network layer with the automation layer, where the RouterOS device is configured to send security logs through the Syslog protocol to a centralized server that functions as a data listener and triggers the n8n workflow whenever patterns such as login failures or port scanning are detected. Within n8n, the workflow is built using a low-code approach, starting with a trigger node that captures incoming log data in real time, followed by a

filter node that applies regular expressions to extract the attacker's IP address, a condition node that checks whether the number of attempts exceeds a defined threshold, and an action node that executes mitigation commands through the MikroTik HTTP API or SSH [10]. The mitigation strategy relies on dynamic firewall updates, where confirmed malicious IP addresses are automatically added to a designated address list called "Blacklist_Automation," and a preconfigured firewall rule drops all traffic originating from any IP in that list [11]. Finally, the system is tested and validated using simulated attacks, such as brute force attempts with Hydra and port scanning with Nmap, with performance evaluated based on detection-to-blocking latency to ensure the automated response is significantly faster than manual intervention.

3. RESULT AND DISCUSSION

3.1 Data Description

To ensure accurate detection and automated handling of network threats, several key variables are defined and processed within the n8n workflow. These variables are extracted from incoming log data and used as parameters for filtering, decision-making, and mitigation actions [12-15]. The following table presents the main data variables involved in the attack identification process.

Table 1: Data Variables for Attack Identification
[Source: Author, 2026]

No	Variable	Data Type
1	src_address	String
2	dst_port	Integer
3	log_message	String
4	attempt_count	Integer
5	action_status	String

The variables listed above serve as the primary parameters for identifying suspicious activities and triggering automated responses. By structuring the log data into these defined variables, the system can perform real-time analysis, apply threshold-based conditions, and execute appropriate mitigation actions efficiently within the n8n workflow.

3.2 Discussion

The implementation of n8n as an orchestrator enables the system to process incoming syslogs from RouterOS in near real time. Based on the experimental results, the time required to execute a blocking command can be calculated using a simple latency equation:

$$T^{total} = T^{detection} + T^{processing} + T^{execution} \quad (1)$$

Where T^{total} is the total mitigation time. In manual scenarios, T^{total} often exceeds several minutes. However, with n8n automation, the processing time (Tprocessing) is reduced to less than 1 second. The system successfully adds the attacker's IP to the RouterOS address list and triggers the firewall rule to drop subsequent packets. This prevents resource exhaustion on the router during a brute force attack.

To evaluate the effectiveness of the proposed automation mechanism, a series of controlled simulations were conducted to compare manual mitigation with the automated approach using the n8n workflow. The tests focused on two common attack scenarios, namely SSH brute force and port scanning, and measured the time required for detection, command execution, and overall response.

The manual scenario represents the typical response of a network administrator without automated alerts, while the automated scenario reflects the end-to-end process handled by the n8n system within the same network environment.
The results of the simulation are summarized in the table below:

Table 2: Data Variables for Attack Identification
[Source: Author, 2026]

Attack Type	Mitigation Method	Detection Time (s)	Execution Time (s)	Total Response Time (s)
SSH Brute Force	Manual	90 – 180	30 – 45	120 – 225
SSH Brute Force	n8n Automation	2 – 4	1 – 3	4 – 7
Port Scanning	Manual	180 – 360	30 – 60	210 – 420
Port Scanning	n8n Automation	3 – 6	1 – 3	5 – 9

As shown in Table 2, the n8n automation system significantly outperforms manual intervention. In the manual scenario, the delay is caused by the administrator's need to check logs and manually input firewall rules. In contrast, the n8n workflow processes the syslog trigger instantly and executes the blocking command via the RouterOS API in under 7 seconds for all attack types. This rapid response effectively prevents the attacker from exhausting router resources or finding vulnerabilities.

4. CONCLUSION

This research has successfully demonstrated that an automated mitigation system using the n8n orchestration platform can effectively secure MikroTik RouterOS environments. Our findings, summarized in Table 2, highlight a dramatic performance gap between automation and manual intervention. While a manual response typically takes between 120 and 420 seconds—largely due to the time-consuming process of human log review—the n8n workflow slashes this response time to under 10 seconds. By processing syslog triggers almost instantly and pushing blocking commands via the RouterOS API, the system neutralizes threats before they can exhaust CPU resources or identify network vulnerabilities.
However, this efficiency comes with certain trade-offs. The most notable requirement is the need for an additional dedicated server or cloud instance to host the n8n orchestrator and syslog listener. This setup naturally adds a layer of infrastructure complexity and increases operational costs. Furthermore, the system introduces a single point of dependency; if the external n8n server goes offline, the automated defense mechanism is temporarily disabled. Despite these infrastructure demands, we conclude that n8n remains a highly effective, low-code solution for administrators seeking to implement real-time, automated network security.

ACKNOWLEDGMENTS

The authors would like to express their sincere appreciation to the Informatics System Department at Universitas Nusa Megarkencana for providing the laboratory facilities and technical support required to carry out this research. The authors also extend their gratitude to the academic community of the university for their valuable insights and assistance throughout the writing and simulation process of this study.

REFERENCES

[1] Y. Xu, “Research on Computer Information Network Security Technology and Development Direction,” Journal of Computing and Electronic Information Management, vol. 16, no. 2, pp. 21–24, Mar. 2025, doi: https://doi.org/10.54097/zjqkkb50

[2] A. Indira, “Implementation of a Network Security System Using the Port Knocking Method at Taruna Satria Vocational School Pekanbaru,” INOVTEK Polbeng - Seri Informatika, vol. 9, no. 2, pp. 904–915, Oct. 2024, doi: https://doi.org/10.35314/f5pjjj80

[3] F. Soro et al., “Enlightening the Darknets: Augmenting Darknet Visibility With Active Probes,” IEEE Transactions on Network and Service Management, vol. 20, no. 4, pp. 5012–5025, Dec. 2023, doi: https://doi.org/10.1109/tnsm.2023.3267671
[4] H. Happy, R. Chhikara, and N. Kashyap, “Inside IoT Botnet Ecosystem: A Review of its Evolution, Architecture, & Security Lifecycle,” pp. 1–6, Jul. 2025, doi: https://doi.org/10.1109/ciacon65473.2025.11189518
[5] G. Ramesh, J. Logeshwaran, and A. P. Kumar, “The Smart Network Management Automation Algorithm for Administration of Reliable 5G Communication Networks,” Wireless Communications and Mobile Computing, vol. 2023, p. e7626803, Apr. 2023, doi: https://doi.org/10.1155/2023/7626803
[6] U. Bartwal, S. Mukhopadhyay, R. Negi, and S. Shukla, “Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots,” IEEE Xplore, Jun. 01, 2022. https://ieeexplore.ieee.org/abstract/document/9888808/authors#authors
[7] Yansen Sianhar and Marhalim Marhalim, “PENERAPAN FIREWALL BERBASIS MIKROTIK DALAM OPTIMALISASI JARINGAN DI SEKOLAH MENENGAH KEJURUAN,” Jurnal Informatika Teknologi dan Sains (Jinteks), vol. 7, no. 2, pp. 868–877, Jun. 2025, doi: https://doi.org/10.51401/jinteks.v7i2.5774.
[8] S. A. Imawan and S. Dwiasnati, “IMPLEMENTASI PEMBLOKAN SITUS DENGAN FIREWALL LAYER 7 PROTOCOL MENGGUNAKAN METODE NDLC PADA ROUTER MIKROTIK,” MULTINETICS, vol. 11, no. 1, pp. 22–34, May 2025, doi: https://doi.org/10.32722/multinetics.v11i1.6844
[9] Arief Budi Pratomo, “PENGEMBANGAN SISTEM FIREWALL PADA JARINGAN KOMPUTER BERBASIS MIKROTIK ROUTEROS,” Bulletin of Network Engineer and Informatics/Bulletin of Network Engineer and Informatics, vol. 1, no. 2, pp. 51–51, Oct. 2023, doi: https://doi.org/10.59688/bufnets.v1i2.10
[10] Aristide Tanyi-Jong Akem, Guillaume Fraysse, and M. Fiore, “Real-Time Encrypted Traffic Classification in Programmable Networks with P4 and Machine Learning,” International Journal of Network Management, vol. 35, no. 1, Jan. 2025, doi: https://doi.org/10.1002/nem.2320
[11] A. M. Nugraha, R. M. R. Erlangga, F. C. Cindy, N. Karna, and A. I. Irawan, “Analysis of Network-Wide Ad Blocker Using Mikrotik RouterBoard and Raspberry Pi for Enhancing Network QoS,” 2025 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), pp. 150–157, Jul. 2025, doi: https://doi.org/10.1109/iaict65714.2025.11100661.
[12] Yudi Mulyanto and Akbar Algi Fari, “ANALISIS KEAMANAN LOGIN ROUTER MIKROTIK DARI SERANGAN BRUTEFORCE MENGGUNAKAN METODE PENETRATION TESTING (Studi Kasus: SMK NEGERI 2 SUMBAWA),” Jurnal Informatika Teknologi dan Sains (Jinteks), vol. 4, no. 3, pp. 145–155, Aug. 2022, doi: https://doi.org/10.51401/jinteks.v4i3.1897
[13] F. I. Wijaya, Muhammad Innuddin, and K. A. Latif, “Analisa Penerapan Fitur Firewall pada Mikrotik untuk Mengamankan dari Serangan Denial of Service (DoS),” Panthera Jurnal Ilmiah Pendidikan Sains dan Terapan, vol. 5, no. 3, pp. 570–592, Jul. 2025, doi: https://doi.org/10.36312/panthera.v5i3.546
[14] Febrian Wahyu Christanto, Putri Cholillah, and Alauddin Maulana Hirzan, “Optimizing Mikrotik-Based Network Security using Address List, Firewall Filter Rules, and Raw Firewall,” Revista de Informática Teórica e Aplicada, vol. 32, no. 3, pp. 66–76, 2025, doi: https://doi.org/10.22456/2175-2745.142954
[15] Ardy Januantoro and Supangat, “Network Security Strengthening Strategy Using Mikrotik Firewall on Small to Medium-Scale IT Infrastructure”, International Conference of Innovation and Community Engagement, vol. 1, no. 01, pp. 227-232, Nov. 2024.