Network Security Strengthening Strategy Using Mikrotik Firewall on Small to Medium-Scale IT Infrastructure

Ardy Januantoro
Universitas 17 Agustus 1945 Surabaya, ardyjanuantoro@untag-sby.ac.id
Supangat
Universitas 17 Agustus 1945 Surabaya, supangat@untag-sby.ac.id

Abstract

The growing concern over cyber attacks, particularly on small to medium-scale information technology infrastructures, has made network security a critical priority. This study focuses on mitigating threats such as unauthorized access and Denial of Service (DoS) attacks through the implementation of a Mikrotik-based firewall. The research methodology includes an analysis of network security needs, comprehensive firewall configuration, and the application of layered security strategies. The implementation utilizes Mikrotik features, including firewall rules, Network Address Translation (NAT), and Layer 7 filters, to enhance resilience against various types of attacks without compromising network performance. The results of this study show that this approach significantly reduces security incidents following the recommended configuration. This research provides practical guidance for network administrators to optimize the use of Mikrotik as an effective firewall solution in protecting small to medium-scale IT infrastructures.

Keywords: Firewall, Network Security

Introduction

In recent years, cyberattacks have emerged as one of the most serious threats to digital security, particularly in the business, government, and public service sectors. The rapid adoption of information technology and increasing reliance on internet networks have opened vulnerabilities for cybercriminals to exploit system weaknesses. These attacks can range from data theft, sabotage, to the disruption of critical services, leading to significant financial and reputational damage. Organizations worldwide are increasingly concerned about the potential damage that cyberattacks could inflict, especially as the scale and complexity of these attacks continue to rise in line with technological advancements.

Threats to network security vary widely, from Denial of Service (DoS) attacks, unauthorized access, to malware and ransomware-based attacks. DoS can cripple network operations by

overwhelming data traffic, while unauthorized access allows hackers to take control of networks and access sensitive data. Additionally, threats like man-in-the-middle attacks, which steal or alter information sent between parties, as well as SQL injection, which exploits database system vulnerabilities, further complicate the network threat landscape. Protection against these threats is critical for organizations that rely on technology for business continuity.

Several studies have been conducted to address security issues in information technology, such as research on the application of firewalls for attack detection in big data[1], the implementation of secure networks using firewalls[2], handling flooding attacks[3], analysis of common cyberattack trends[4][5], challenges in cyberattack trends[6], the implementation of network security techniques[7], security protection for sensitive data[8], firewall analysis on routers[9], as well as network security and machine learning analysis[10]

Mikrotik is one of the router devices that can function as a firewall. The Mikrotik firewall is commonly used to enhance network security, particularly for small to medium-sized environments. By utilizing various features such as Network Address Translation (NAT), Layer 7 filtering, and firewall rules, Mikrotik allows network administrators to create layers of protection capable of resisting a wide range of threats. Firewall rules can be configured to block suspicious access, while NAT can hide internal networks from direct access, reducing the risk of external attacks. Additionally, Layer 7 filtering enables the identification of more sophisticated attack patterns, such as those carried out at the application level.

The implementation of a Mikrotik firewall begins with an analysis of network security needs to understand the potential threats present. After that, firewall configuration can begin by establishing basic rules (firewall rules) to restrict unwanted access and applying NAT to protect internal networks. Then, Layer 7 filtering can be applied to monitor suspicious traffic based on certain attack patterns. All configurations must be thoroughly tested to ensure the system operates optimally without compromising network performance. Additionally, regular monitoring and periodic updates of security rules are highly recommended to keep the firewall effective in responding to evolving threats.

Methodology

This chapter aims to evaluate the effectiveness of the Mikrotik-based firewall in enhancing network security for small to medium-scale information technology infrastructures. The methodology used in this research consists of several stages, including needs analysis, design, implementation, testing, and evaluation.

1. Network Security Needs Analysis

In the initial stage, an analysis was conducted on the network security needs of small to medium-sized organizations. Data regarding the most common threats, such as Denial of Service (DoS), unauthorized access, and application-based attacks, were collected through interviews with network administrators and a literature review. In addition, a review of the existing network architecture was carried out to identify critical points vulnerable to attacks.

2. Designing the Mikrotik-Based Firewall Configuration

After the needs analysis, the next step was to design a Mikrotik-based firewall configuration. This design includes creating firewall rules, implementing Network Address Translation (NAT), and configuring Layer 7 filters. These features were chosen for their ability to handle common network threats and for their efficiency in protecting the network without compromising performance. The firewall design was also tailored to the specific needs of the network under study, taking into account the scale and type of traffic being handled.

3. Implementation of the Firewall Configuration

In this stage, the designed Mikrotik firewall was implemented in a real network environment of a medium-sized organization. Implementation was carried out by configuring the Mikrotik device according to the rules that had been previously designed. This process involved applying firewall rules to restrict harmful traffic, NAT to protect the internal network, and Layer 7 filters to detect application-based attacks[11]. All configurations were implemented step by step and tested to ensure there were no conflicts with the ongoing network operations.

4. Testing and Attack Simulation

Once the implementation was complete, tests were conducted to evaluate the firewall's effectiveness in handling identified threats. This testing involved simulating cyberattacks, including DoS, unauthorized access, and application-based attacks, to assess how the Mikrotik firewall responded to these threats. The testing process included monitoring network traffic and recording the firewall's response to the simulated attacks. Network testing tools such as Wireshark and penetration testing software were used to verify the firewall's performance in blocking or mitigating the impact of the attacks.

5. Performance and Effectiveness Evaluation

The final stage of this research was to evaluate the performance and effectiveness of the implemented firewall configuration. This evaluation included analyzing test data to determine whether there was a reduction in the number of security incidents after the Mikrotik firewall was applied. Additionally, performance analysis was conducted to ensure that the firewall did not significantly hinder network performance. The results of this evaluation were used to assess how effective the Mikrotik-based firewall solution was in improving network security in small to medium-sized organizations.

6. Recommendation Development

Based on the evaluation results, practical recommendations were developed for network administrators on how to optimize the use of Mikrotik as a firewall solution. These recommendations include best practices in firewall configuration, network monitoring, and handling evolving threats.

Results and Discussion

1. Network Security Needs Analysis

The result of the needs analysis process is the creation of a network topology diagram to determine the optimal placement of the Mikrotik router within the network. The diagram is presented in the section below.

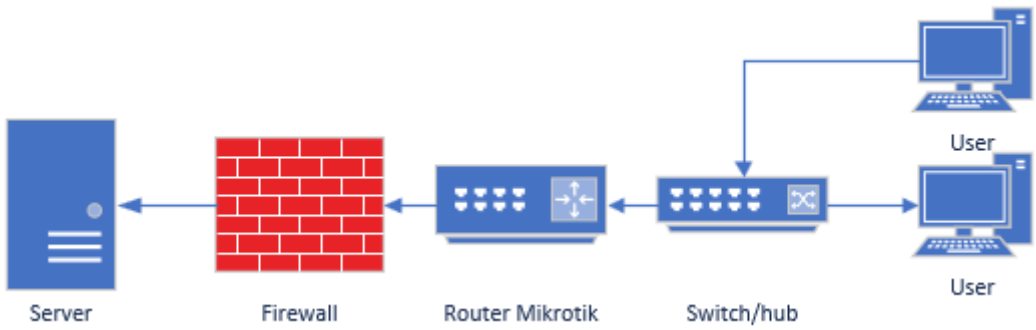

Figure 1. Topologi jaringan

In the diagram above, the position of the router is shown in front of the server, indicating that the Mikrotik router works in conjunction with the firewall to protect the server from various threats. The firewall functions as the first layer, filtering incoming and outgoing traffic.

2. Designing the Mikrotik-Based Firewall Configuration

The configuration focuses on setting up rules, firewall policies, and Network Address Translation (NAT).

3. Implementation of the Firewall Configuration

The firewall implementation is tailored to meet the needs identified in the previous process.

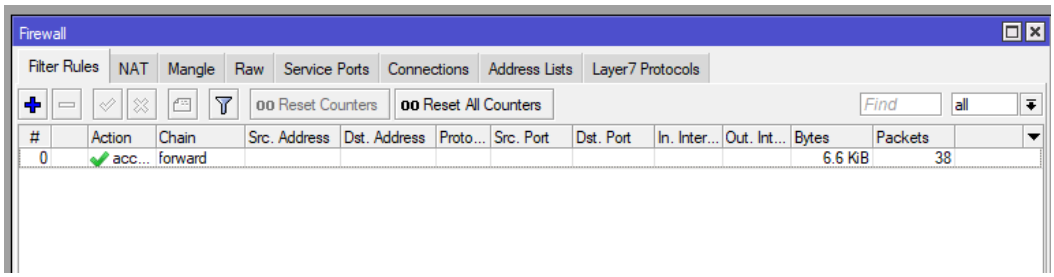

Figure 2. Mikrotik Firewall Configuration

4. Testing and Attack Simulation

The attack testing results can be seen in the following table:

Table 1. Testing and tools

No	Serangan	Tools/Tecnique
1	DDoS	Hping3
2	Port Scanning	Nmap
3	Brute Force Attack	Hydra

4	Unauthorization Attack	Insider Attack
5	SQL Injection	SQLMap
6	XSS	BrupSuite
7	SYN Flood Attack	Hping3

In the table above, several types of attacks are listed as network security standards. The subsequent column details the tools and techniques used.

5. Performance and Effectiveness Evaluation

This section explains the results of the performance and effectiveness evaluation. The data is presented in the following table:

Table 2. Effectiveness results

No	Serangan	Tools/Tecnique	Effectiveness results
1	DDoS	Hping3	100%
2	Port Scanning	Nmap	100%
3	Brute Force Attack	Hydra	100%
4	Unauthorization Attack	Insider Attack	90%
5	SQL Injection	SQLMap, Paramater Input, Union Operator	80%
6	XSS	BrupSuite	0%
7	SYN Flood Attack	Hping3	100%

In the evaluation above, it can be seen that the average effectiveness is 81%. For DDos, Port Scanning, Brute Force Attack, and Syn Flood Attack, the effectiveness reached 100%, indicating that the firewall worked optimally. However, for certain attacks, the Mikrotik firewall performed slightly below perfect, with effectiveness rates of 90% for Unauthorized Access Attack and 80% for SQL Injection. As for XSS attacks, the firewall was unable to detect them.

Conclusion

Based on the results, the Mikrotik firewall is highly effective in protecting against network-based attacks. However, for script-based attacks, the firewall is less optimal in mitigating such threats. This is due to the default configuration of the Mikrotik firewall, which is unable to read the values of packets sent by users. While it is possible to use Mikrotik scripts, they are less efficient and have limited capabilities. For future research, it is recommended to use specialized packet inspection firewalls, such as Snort, or to implement secure coding practices in the applications to be published.

Acknowledgments

Special thanks to Universitas 17 Agustus 1945 Surabaya for providing the necessary resources and support throughout the study. The author also extends appreciation to my team who

provided valuable insights during the data collection phase. Lastly, heartfelt thanks to colleagues and family for their continuous encouragement and motivation, which greatly contributed to the successful completion of this research.

References

[1] Q. Zhang, Z. Luo, and J. Zhang, "Analysis of the Application of Firewall and Intrusion Detection Technology in Network Security in the Era of Big Data," in Proceedings - 2023 2nd International Joint Conference on Information and Communication Engineering, JCICE 2023, 2023. doi: 10.1109/JCICE59059.2023.00042.

[2] A. D. Tudosi, D. G. Balan, and A. D. Potorac, "Secure network architecture based on distributed firewalls," in 2022 16th International Conference on Development and Application Systems, DAS 2022 - Proceedings, 2022. doi: 10.1109/DAS54948.2022.9786092.

[3] S. V. Morzhov and M. A. Nikitinskiy, "Development and research of the PreFirewall network application for floodlight SDN controller," in Moscow Workshop on Electronic and Networking Technologies, MWENT 2018 - Proceedings, 2018. doi: 10.1109/MWENT.2018.8337255.

[4] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, vol. 7, 2021, doi: 10.1016/j.egyr.2021.08.126.

[5] A. OULED-DIAF, F.-Z. HARIDI, and S. KHELIL, "A Comprehensive Discussion on Network Security," International Journal of Research Studies in Computer Science and Engineering, vol. 9, no. 1, pp. 16–23, 2023, doi: 10.20431/2349-4859.0901003.

[6] B. Yamini, P. Radhakrishnan, M. Nalini, B. Maheswari, M. Shanmuganathan, and S. S. R., "Exploring Current Trends and Challenges in Cybersecurity: A Comprehensive Survey," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 10s, 2023, doi: 10.17762/ijritcc.v11i10s.7590.

[7] J. H. Abawajy and R. Islam, "Applications and techniques in information and network security," 2017. doi: 10.1002/cpe.4351.

[8] N. O. Miracle, "The Importance of Network Security in Protecting Sensitive Data and Information", doi: 10.51584/IJRIAS.

[9] J. Liu, "Enhancing Network Security Through Router-Based Firewalls: An Investigation into Design, Effectiveness, and Human Factors," 2024.

[10] Q. Li, B. Liu, and P. Chen, "An overview of cybersecurity based on Network Security Situational Awareness and Machine learning," in 2023 8th International Conference on Intelligent Computing and Signal Processing, ICSP 2023, 2023. doi: 10.1109/ICSP58490.2023.10248496.

[11] D. Wicaksono and I. R. Widiasari, "Sistem Keamanan Jaringan Menggunakan Firewall Dengan Metode Port Blocking Dan Firewall Filtering," vol. 9, no. 2, pp. 1380–1392, 2022, [Online]. Available: http://jurnal.mdp.ac.id