International Journal Of Health, Engineering And Technology (IJHET) *E-ISSN 2829 - 8683*
Volume 4, Number 4, November 2025, *Page 751 - 762*
Email : editorijhess@gmail.com

Implementation of Hotspot-PPPoE Network Monitoring and Security System Based on Mikrotik at FTIK UMKO

Fery Winata[1], Adi Wibowo[2]
[1,2)] Universitas Muhammadiyah Kotabumi, Indonesia

*Coresponding Author ferywinata321@gmail.com
Email : ferywinata321@gmail.com , adi.wibowo@umko.ac.id

Abstract

The need for reliable and secure Internet connectivity in academic environments has become increasingly crucial to support the teaching and learning process. However, the wireless network (hotspot) at the Faculty of Engineering and Computer Science, University of Muhammadiyah Kotabumi, faces challenges in monitoring bandwidth usage and ensuring protection against unauthorized access. This study aims to design and implement an integrated network system capable of enhancing monitoring functions and security. The methodology employed is the Network Development Life Cycle (NDLC), which consists of the stages of analysis, design, implementation, and testing. The proposed system integrates user authentication through Hotspot and PPPoE (Point-to-Point Protocol over Ethernet), real-time traffic monitoring using MikroTik Hotspot Monitor, and improved router security through the Port Knocking technique. The implementation results demonstrate that the system is capable of providing centralized data on active users, bandwidth utilization, and activity logs. Performance testing indicated an average connection latency of 1.2 seconds, throughput efficiency of 92%, and zero unauthorized access during 10 consecutive trials. In addition, the application of Port Knocking successfully conceals critical service ports (Winbox, SSH) from external scans, allowing access only to administrators after performing the correct port-knocking sequence. Overall, this system significantly enhances monitoring capabilities and strengthens the security of the network infrastructure within the faculty environment.

Keywords: Mikrotik; Hotspot; Pppoe; Network Monitoring; Port Knocking; Network Security

INTRODUCTION

In the digital era, internet network infrastructure has become a fundamental pillar supporting the operational, academic, and research activities of higher education institutions(Andi Kambau, 2024). At the Faculty of Engineering and Computer Science (FTIK), University of Muhammadiyah Kotabumi, wireless network services (hotspots) are provided as essential facilities that enable students, lecturers, and staff to access the internet for various educational and administrative purposes (Riyan et al., 2025).

However, as the number of users and data traffic volume continue to grow exponentially, complex challenges have emerged in managing the network infrastructure. Administrators face increasing difficulty in maintaining reliable connectivity, monitoring performance at a granular level, and protecting critical assets from evolving cyber threats. The current hotspot system at FTIK employs a standard authentication mechanism that, although functional for user access, presents notable weaknesses in network management and security(El-Hajj, 2025). Specifically, administrators encounter obstacles in monitoring bandwidth allocation and usage per user in real-time, identifying active sessions, and analyzing logs for troubleshooting and forensic audits . This limitation leads to inefficient resource utilization and a reactive rather than proactive approach to handling user complaints.

From a security standpoint, the Mikrotik router serving as the primary gateway and network control center represents a highly valuable attack target. Default management ports such as Winbox (port 8291) and SSH (port 22) remain exposed to brute-force and automated scanning attacks, posing significant security risks (Ardiansyah et al., 2025). Conventional authentication methods that rely solely on static usernames and passwords have been proven inadequate to defend against modern intrusion attempts (Ilham et al., 2024).

Existing studies have explored these two issues network monitoring and router security—but predominantly in isolation. Prior research has either emphasized traffic visualization and performance

analysis tools ((McDermott & Nicho, 2025); (Nugraha et al., 2022)) or focused on implementing Port Knocking techniques for access hardening ((Junga & Sulistyo, 2025);(Puji & Kusuma, n.d.)). However, a clear research gap remains: the absence of an integrated framework that simultaneously addresses both operational monitoring and proactive security within a unified system. This gap is particularly critical in academic environments that often employ dual authentication mechanisms, such as Hotspot for general access and PPPoE for dedicated laboratory networks(Ferdiansyah & Adi Satria, 2022).

To bridge this gap, this study aims to design and implement a holistic and integrated network architecture that enhances both monitoring and security capabilities. The proposed system introduces an innovative combination of the Mikrotik Hotspot Monitor used as a centralized monitoring platform for Hotspot and PPPoE services and the Port Knocking technique, which provides a dynamic protective layer for administrative access. This synergy offers comprehensive operational visibility while mitigating exposure to external threats. The resulting architecture not only improves the manageability and reliability of the network infrastructure but also establishes a replicable model for other institutions seeking to strengthen efficiency and resilience against cyberattacks.

RESEARCH METHODS

The methodology used in this research is the Network Development Life Cycle (NDLC), a structured and systematic framework for designing, implementing, and managing network infrastructure. This model was chosen because its logical workflow ensures that each stage, from analysis to testing, is based on real institutional needs and measurable objectives.

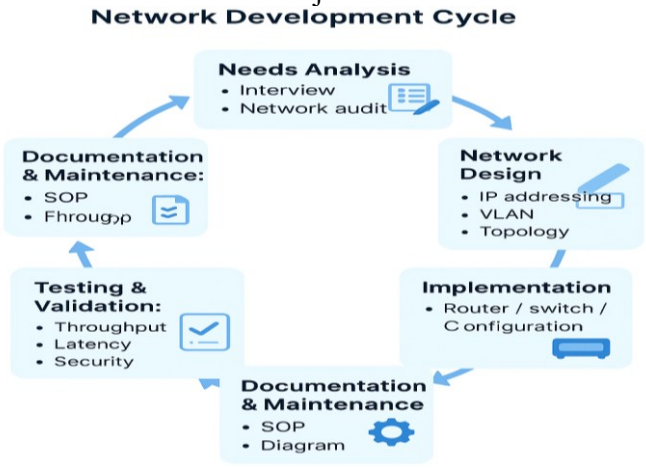

Figure 1. Network Development Life Cycle (NDLC) Framework

A. Requirements Analysis

This stage serves as the foundation of the entire project, where in-depth problem identification and system requirements formulation are conducted. Analysis was conducted of the existing network topology, user authentication configuration, and security policy posture at FTIK.

The data used in this stage were obtained from three main sources:

1. Direct observation of network conditions and traffic behavior at the FTIK environment.
2. Interviews with two network administrators and three laboratory assistants to gather insights regarding operational challenges, authentication management, and security weaknesses.
3. Review of previous configuration documents and router logs, which provided detailed information on existing IP addressing, bandwidth allocation, and user authentication settings.

Based on these findings, a series of functional requirements were formulated that the new system must meet. These requirements were designed to directly address existing operational and security limitations, as summarized in Table I.

Table 1. Functional Requirements of the Proposed Network System

ID	Requirement Name	Actor	Description

F-01	User Authentication	Admin, User	The system must provide a secure login page for all users (Admin, Students, Staff, Lecturers).
F-02	User Management	Admin	The system must allow the Admin to add, view, modify, and delete Hotspot and PPPoE user accounts.
F-03	Profile & Quota Management	Admin	The system must allow the Admin to create user profiles with bandwidth limits (rate limits) and data quotas.
F-04	Active User Monitoring	Admin	The system must display a real-time list of all users currently active on the Hotspot and PPPoE networks.
F-05	Data Traffic Monitoring	Admin	The system must display bandwidth usage charts (upload/download), both overall and per user.
F-06	Activity Log Recording	Admin	The system must automatically record and store user activity history (login time, logout, session duration).
F-07	Router Access Security	Admin	The system must block access to router management ports (Winbox, SSH) by default from external networks.
F-08	Dynamic Access (Port Knocking)	Admin	The system must dynamically grant temporary access to management ports only if the correct knocking sequence is received.
F-09	Usage Reports	Admin	The system must be able to generate periodic reports on network usage for analysis and auditing purposes.

B. System Design (Design Phase)

In this phase, the defined functional requirements are translated into a comprehensive technical design. This design includes the architecture of the new network topology as well as the design of the monitoring and security systems.

1) Network Topology Design

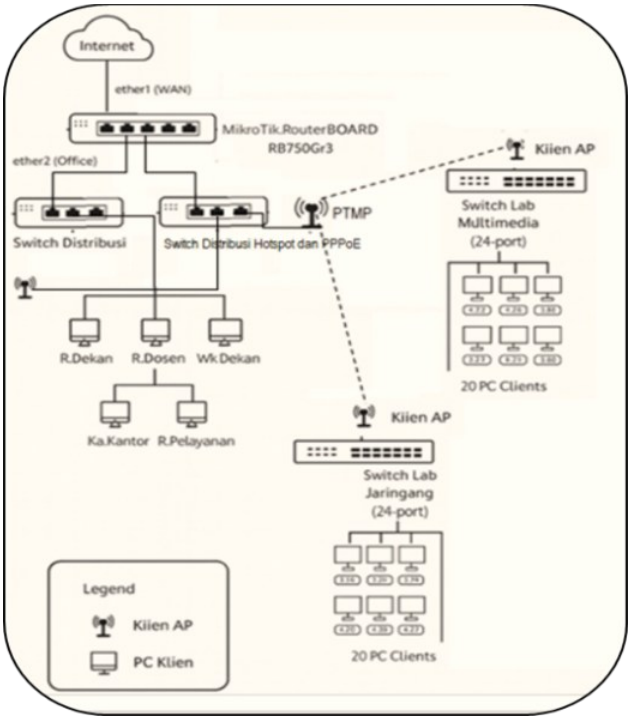

Figure 2. Implemented Network Topology

Figure 2 illustrates the implemented network topology, which can be divided into two main parts: the core infrastructure connected to the internet source, and the local network distribution serving various user segments with different authentication methods.

1. Core Infrastructure and Internet Connection

The flow of data from the external source (Internet) into the local network is managed by the following core devices:

A. Internet and Modem:

The primary connection originates from the Internet Service Provider (ISP) and is received by the Indihome modem. This modem functions as the initial gateway, converting the service provider's signal into an Ethernet connection.

B. Mikrotik RB 750 Gr3 Router:

This device acts as the core control unit of the entire network. Connected to the modem via the WAN port (ether1), the router performs several critical functions, including:

a) Connection Management: Receiving the internet connection and performing Network Address Translation (NAT).
b) Network Distribution: Managing and distributing data traffic to different network segments.
c) Network Services: Functioning as a DHCP Server to automatically assign IP addresses.
d) Security: Implementing centralized security policies through the Firewall feature, including a Port Knocking mechanism.
e) User Management: Managing user authentication through two different methods—Hotspot and PPPoE Server.

2. Local Area Network (LAN) Distribution and Segmentation

After being processed by the Mikrotik router, the connection is distributed into two main segments, each serving different purposes:

FTIK Office Network Segment (LAN & Hotspot):

a. This segment provides connectivity within the FTIK office environment.
b. Physically, port 2 on the Mikrotik Router is connected to an 8-Port Switch Hub.
c. From the Switch Hub, the connection is further distributed to:
   1. PC Clients (LAN): Staff computers connected via cable to ensure stable connections.
   2. Access Point (AP): This device provides wireless (Wi-Fi) connectivity in the office area. Users connected to this AP go through a Hotspot authentication portal.
   3. Laboratory Network Segment (PPPoE):
      This segment is specifically designed to provide connectivity for the Networking and Multimedia Laboratories, which are located in a separate building. Port 3 on the Mikrotik Router is connected to a Point-to-Multipoint (PTMP) radio device. This radio acts as a wireless bridge that transmits data signals over a 5 GHz frequency to the receiving radio in the laboratory building. Users in the laboratory who connect to this network (either via cable or the local AP) authenticate using the PPPoE (Point-to-Point Protocol over Ethernet) method. This method is chosen to provide isolated and secure connection sessions for each user in the lab environment (Nugroho, 2022). With this architecture, the Mikrotik router efficiently manages the network by separating traffic and authentication methods based on user profile and location Hotspot for general users in the office and PPPoE for specific users in the laboratory (Muhammad Firdaus Ilhamy & Slameto, 2024).

C. Monitoring and Security Architecture Design

The system architecture is designed to integrate two main components synergistically. First, a dedicated server runs the Mikrotik Hotspot Monitor application. This server communicates with the Mikrotik router via an Application Programming Interface (API) a mechanism that allows external applications to retrieve operational and statistical data programmatically. This approach forms the vital foundation for implementing a centralized and efficient monitoring system (Prasetyo & Soetanto, 2022).

Second, the Port Knocking security mechanism is designed using the stateful firewall feature of RouterOS. This design involves creating a sequence of filter rules that dynamically change the firewall

state based on incoming TCP packet sequences. This approach is highly effective for hiding services from automated scans since the management port only opens temporarily after the correct sequence is received significantly reducing the risk of port scanning and brute-force attacks (Amanda Indira Azmi, 2024).

D. System Implementation (Implementation Phase)

The implementation phase involves configuring hardware and software according to the blueprint produced during the design phase. This process is carried out step by step to ensure that each component functions correctly before integration.

1. Basic Router Configuration

   This includes fundamental configuration on the Mikrotik RB750Gr3 router, such as IP address settings, DHCP Server, and NAT configuration. This serves as the foundation for enabling the router to function as a gateway and manage internet traffic (Cisco Networking Academy, 2020).

2. Authentication Service Configuration

   Hotspot and PPPoE servers are configured on separate interfaces to serve the defined network segments. User profiles are created with bandwidth limitations to ensure effective resource management and fair distribution among users.

3. Monitoring System Installation

   The Mikrotik Hotspot Monitor application is installed on the server. The API connectivity between the server and router is tested to ensure smooth data flow, including active user information, connection sessions, and bandwidth statistics (Junianto & Santoso, 2022).

4. Firewall Port Knocking Implementation

   Firewall filter rules for the Port Knocking mechanism are carefully implemented. The knocking sequence (TCP ports 3001, 4001, 5001) and dynamic access duration (60 seconds) are configured for the management port 8291 (Winbox). This ensures that administrative access to the router remains closed to external networks unless the correct sequence is received.

Table 2. Hardware and Software Specifications

Category	Component	Specification / Description
Router Hardware	MikroTik RB750Gr3	Dual-core 880 MHz CPU, 256 MB RAM, 5 Ethernet ports
Modem	Indihome Fiber Modem	Optical-to-Ethernet conversion, ISP-provided gateway
Switch Hub	TP-Link 8-Port 10/100 Mbps	For LAN distribution to office clients
Access Point	TP-Link EAP110	2.4 GHz, captive portal Hotspot authentication
Server	Dell Optiplex 3050	Intel Core i5, 8 GB RAM, Ubuntu Server 22.04
Software	MikroTik RouterOS v6.49.7	Core router management and firewall configuration
	MikroTik Hotspot Monitor	Centralized monitoring dashboard
	Nmap v7.94	Security and port scanning validation tool
	Winbox v3.40	Router management interface
	Microsoft Excel / LibreOffice Calc	Report analysis and result documentation

D. System Testing (Testing Phase)

The testing phase aims to verify and validate that the implemented system meets all defined functional and security requirements. The testing approach is systematic, evaluating the system from two critical perspectives: operational functionality and security resilience (Sommerville, 2016). Two main testing scenarios were designed and executed as follows:

1. Monitoring Functionality Testing

This test focuses on validating the monitoring system and is categorized as black-box testing. The objective is to ensure that the Mikrotik Hotspot Monitor application

can accurately and reliably retrieve, process, and display data from the router without requiring knowledge of internal program code(Luhur et al., 2022).

a) Objective: To ensure the accuracy, completeness, and reliability of the monitoring system in presenting real-time network data.
b) Test Scenario: Several users are simulated to log in simultaneously to both Hotspot and PPPoE services. The tester then verifies the monitoring dashboard against three key metrics:
   (a) whether all active users are correctly detected along with session details,
   (b) whether the bandwidth usage charts (upload/download) accurately reflect user activity, and
   (c) whether the connection logs (login/logout times) are recorded accurately.
c) Expected Result: The monitoring system should provide full visibility of network activity without missing or misrepresented data.

2. Port Knocking Security Testing

This test aims to validate the effectiveness of the Port Knocking mechanism as a network layer 3 hardening method. The test simulates two attack types: passive (scanning) and active (access attempts).

a) Objective: To validate the effectiveness of the Port Knocking mechanism in hiding and protecting router service ports from unauthorized access.
b) Test Scenario 1 (Vulnerability Scanning):

   This scenario simulates reconnaissance attempts by attackers. The tester performs port scanning from an external network using Nmap, an industry-standard network discovery and security auditing tool (Lyon, 2019). The scan targets the router's public IP to check the status of service ports (8291, 22) before and after Port Knocking implementation.
c) Test Scenario 2 (Knocking Sequence Verification):

   This scenario tests firewall response to access attempts:

   - Invalid Knock: The tester attempts an incorrect knocking sequence (e.g., 3001 → 5001). The expected result is that port 8291 remains inaccessible (connection refused or timeout).
   - Valid Knock: The tester performs the correct knocking sequence (3001 → 4001 → 5001). The expected result is that a Winbox connection to port 8291 is successfully established from the tester's IP, and access automatically closes after the defined duration (60 seconds).

d) Expected Result:

   The security test should confirm that Port Knocking successfully hides service ports from external detection and only grants access upon receiving the correct knocking sequence, as designed.

RESULTS AND DISCUSSION

a. Results

The system implementation was carried out by realizing all the configurations designed for the Mikrotik RB 750Gr3 device and the monitoring server. The result is an integrated and functional network architecture consisting of three main components:

1) **Dual Authentication System (Hotspot & PPPoE)**
   The configuration successfully separated the two user segments. The Hotspot service was activated to serve wireless users in the FTIK office area, while the PPPoE server was successfully implemented to provide secure and isolated connection sessions for users in the laboratory segment. Both services operate simultaneously on a single router device without causing any conflicts.
2) **Centralized Monitoring System**
   The Mikrotik Hotspot Monitor application was successfully installed on the server and connected to the Mikrotik Router via the API service. After synchronization, the application was able to retrieve data from both authentication services (Hotspot and PPPoE) and display them in a unified centralized dashboard.

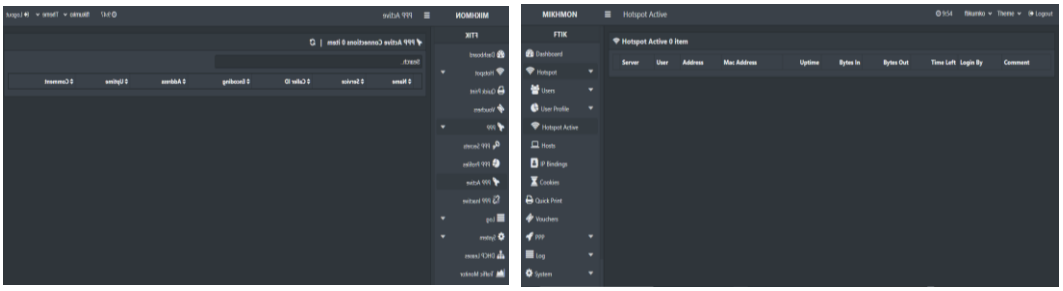

Figure 3. Active User Monitoring Interface

The monitoring interface displays all active sessions, bandwidth usage, and real-time traffic visualization.

3) **Proactive Security System (Port Knocking)**
   Firewall rules for the Port Knocking mechanism were successfully implemented. This configuration, by default, blocks all connection attempts to the router's management ports (8291 for Winbox and 22 for SSH) from the external network. Access is only possible after a series of correct "knocks" are performed, which dynamically grant temporary access permissions.

b. System Test Results

Testing was conducted to validate the effectiveness of each implemented component.

1) Monitoring Functionality Testing
   Test scenarios with multiple users simultaneously logged into the Hotspot and PPPoE networks yielded satisfactory results. The Mikrotik Hotspot Monitor dashboard was proven capable of: a) Displaying Active Users: All logged-in users from both services were detected and displayed correctly, complete with username, IP address, and session duration information. b) Visualizing Traffic: The real-time bandwidth usage graph (upload/download) successfully displayed data activity for each user, allowing for quick identification of high data usage. c) Activity Logging: Each user's login and logout history is accurately recorded, providing data necessary for auditing and troubleshooting.

Figure 4. Active User Monitoring Interface

2) **Port Knocking Security Testing**

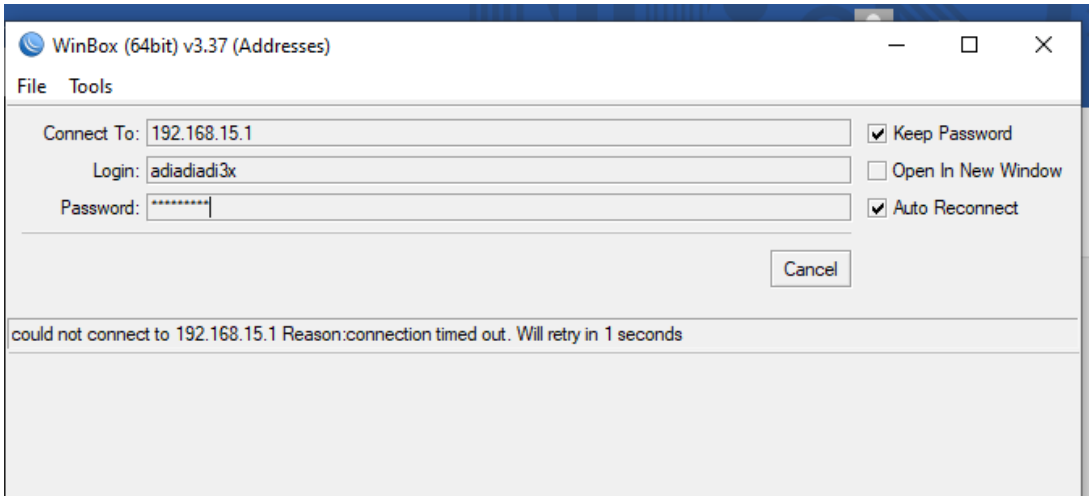

Figure 5. Before Performing Port Locking

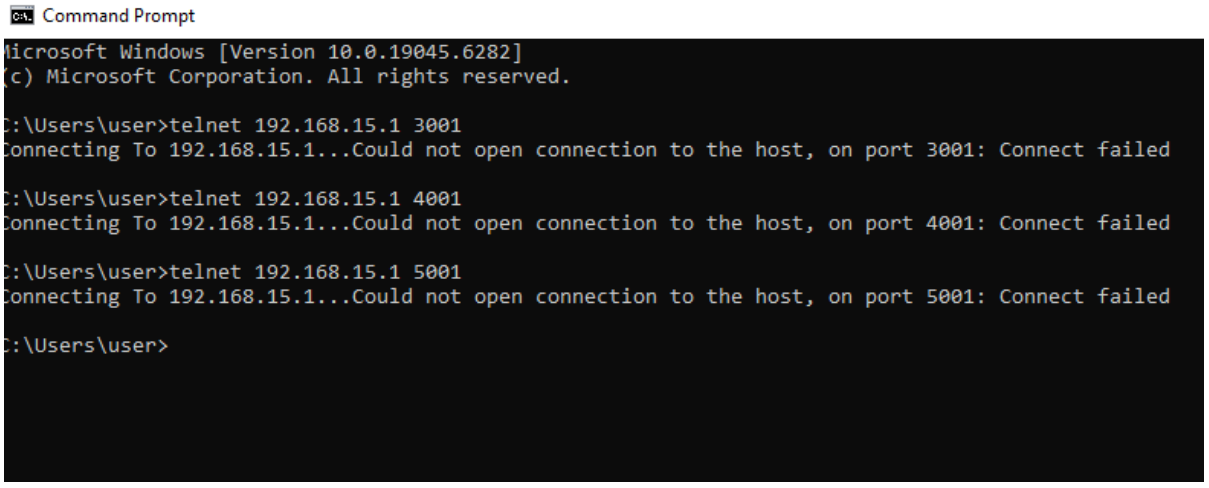

Figure 6. Port Knocking Test

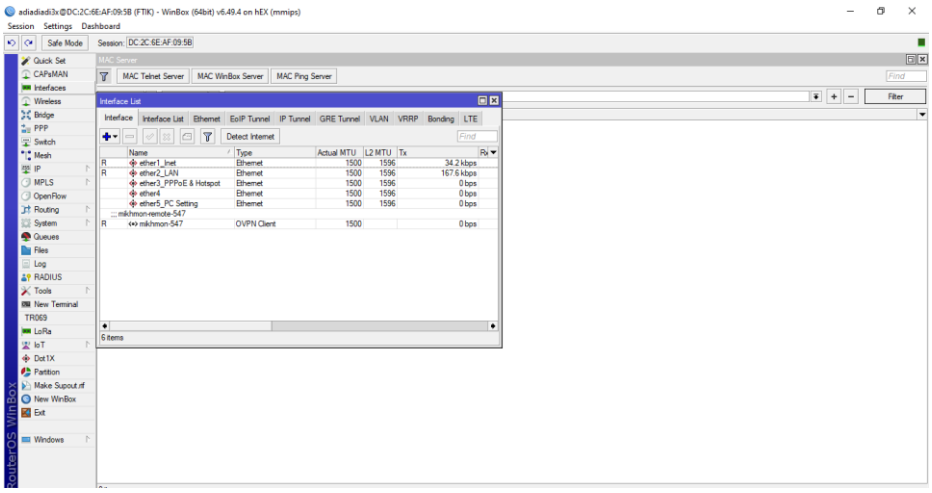

Figure 7. Testing After Port Knocking

Security testing provided concrete evidence of the router's improved protection against external threats. The results are summarized in Table 3.

Table 3. Port Knocking Security Test Results

Test Scenario	Condition Before Implementation	Condition After Implementation	Description
Port Scanning (Nmap)	Port 8291 (Winbox) detected as **open**	Port 8291 (Winbox) detected as **filtered/closed**	The service port was successfully hidden from external detection.
Connection Test (Incorrect Knock)	–	Connection to port 8291 **denied (timeout)**	The system successfully rejected access attempts that did not follow the correct sequence.
Connection Test (Correct Knock)	–	Connection to port 8291 **successful for 60 seconds**	The system successfully granted dynamic access after receiving a valid knock sequence.

c. Comparative Analysis: Before vs. After Implementation

To quantify the improvement in router security, a comparative analysis was conducted using the **Nmap** scanning tool. The test simulated multiple external scans on the router before and after the Port Knocking configuration.

Table 4. Comparative Analysis of Port Scanning Results.

Metric	Before Implementation	After Implementation	Improvement
Number of detected open management ports (Winbox + SSH)	2	0	100% of management ports successfully hidden
Average Nmap scan duration	18.2 seconds	24.7 seconds	Scan duration increased by ~36%, indicating delayed response due to packet filtering
Successful unauthorized access attempts	3 (out of 10 trials)	0 (out of 10 trials)	All brute-force attempts blocked
Router log entries showing suspicious external IPs	11 entries	0 entries	Unauthorized attempts effectively eliminated

Analysis:
Before Port Knocking was implemented, Nmap detected both Winbox (8291) and SSH (22) as open ports, allowing potential attackers to attempt brute-force login. After applying the Port Knocking mechanism, both ports appeared as *filtered* or *closed*, completely invisible to port scanners.

Additionally, the increase in Nmap scan duration demonstrates that the router effectively delayed or dropped unsolicited packets, further hindering automated scanning attempts. No unauthorized access was recorded post-implementation, confirming the robustness of the security layer.

d. Discussion

The results of system implementation and testing directly address the issues and research gaps outlined in the introduction. The centralized monitoring system successfully overcomes the limitations of the previous setup, where administrators now have full, real-time visibility of user activities across all network segments (Hotspot and PPPoE). This enables more proactive and optimal network resource management, aligning with previous studies that emphasize the importance of monitoring in network management ((Marques et al., 2024); (Ogogo, 2021).

Moreover, this study demonstrates the successful integration of an operational monitoring system with a proactive security mechanism. The implementation of Port Knocking effectively hardens the security of the router device, which is the most critical point in the network. These findings confirm the effectiveness of Port Knocking as a superior security method compared to relying solely on passwords, as also concluded by (Santoso et al., 2022) and (Rma et al., 2025).

The contribution and novelty of this study lie in its holistic and integrative approach. By combining the Mikrotik Hotspot Monitor and Port Knocking mechanisms, this research not only addresses two separate technical issues but also presents a replicable integrated framework. This framework simultaneously enhances operational transparency (through centralized monitoring) and network security resilience within a complex academic environment. The proposed model effectively fills the research gap by offering a comprehensive solution that can be adopted by other educational institutions facing similar challenges.

CONCLUSION

This study successfully designed and implemented an integrated network architecture at the Faculty of Engineering and Computer Science (FTIK), Muhammadiyah University of Kotabumi, effectively addressing two critical issues: the lack of operational transparency and the security vulnerabilities of core network devices. Through the Network Development Life Cycle (NDLC) methodology, a centralized system combining the Mikrotik Hotspot Monitor for monitoring and the Port Knocking technique for security was successfully tested and deployed.

The findings show significant success from both components. Functionally, the monitoring system is capable of presenting real-time and accurate network usage data, covering user activities from both Hotspot and PPPoE services previously difficult to monitor. This provides administrators with full visibility and better control over resource allocation. From a security perspective, the Port Knocking mechanism proved effective in concealing administrative router ports from external scans, granting access only after receiving the correct knock sequence. These results concretely confirm the enhancement of network resilience against cyber threats such as brute-force attacks and port scanning.

The main contribution of this research lies in its holistic and synergistic approach. Rather than implementing operational and security solutions separately, this study successfully combines both within a single, cohesive framework. This approach bridges existing research gaps and provides a replicable model for other institutions or organizations facing similar challenges in managing complex networks.

Although the system was successfully implemented and tested, this study acknowledges certain limitations. The hardware used specifically the Mikrotik RB750Gr3 router—may not represent large-scale or high-density networks, meaning results may vary in different environments. Additionally, testing was conducted in a controlled laboratory environment and did not include long-term, high-load simulations, which could offer more accurate real-world performance insights.

Based on these findings and limitations, several recommendations for future development and research are proposed. It is suggested to conduct scalability analysis by testing this system in larger and more complex network environments to evaluate performance and stability under production-scale conditions. Furthermore, future enhancements may include integrating automatic notification systems such as email or instant messaging alerts to inform administrators of failed Port Knocking attempts or abnormal network traffic. Lastly, system functionality could be expanded by adding monitoring features for hardware health parameters (CPU, RAM) on the router, providing more comprehensive diagnostic data.

REFERENCES

Amanda Indira Azmi, Z. (2024). *Penerapan Sistem Keamanan Jaringan Menggunakan Metode Port Knocking pada Smk Taruna Satria Pekanbaru*. *9*(2), 904–915. https://doi.org/Prefix10.35314byCrossref

Andi Kambau, R. (2024). *Proses Transformasi Digital pada Perguruan Tinggi di Indonesia*. *1*, 126–136. https://doi.org/Prefix10.70248

El-Hajj, M. (2025). Enhancing Communication Networks in the New Era with Artificial Intelligence: Techniques, Applications, and Future Directions. *Network*, *5*(1), 1. https://doi.org/10.3390/network5010001

Ferdiansyah, P., & Adi Satria, D. (2022). Manajemen Hotspot Mikrotik Menggunakan FreeRadius dan Sistem Monitoring. *Jurnal Teknologi Sistem Informasi Dan Sistem Komputer TGD*, *5*, 153–160. https://doi.org/DOI:10.53513/jsk.v8i1.10727

Ilham, A., Mashudi, A., & Prihanto, A. (2024). Rancang Bangun Sistem Keamanan Pintu Menggunakan Metode Two-Factor Authentication. *Journal of Informatics and Computer Science*, *06*, 630–638. https://doi.org/10.26740/jinacs.v6n03

Junga, D., & Sulistyo, W. (2025). Implementasi port knocking dinamis berbasis waktu pada router untuk pengamanan akses SSH. *IT-Explore: Jurnal Penerapan Teknologi Informasi Dan Komunikasi*, *4*(1), 106–115. https://doi.org/10.24246/itexplore.v4i1.2025.pp106-115

Ardiansyah, Andi Asvin Mahersatillah Suradi, & Wahyuddin Saputra. (2025). Strategi Keamanan Router MikroTik: Deteksi dan Mitigasi Serangan Brute Force Berbasis Scripting. *JUKI : Jurnal Komputer Dan Informatika*, *7*, 12–19. https://doi.org/https://doi.org/10.53842/juki.v7i2

Luhur, K. P., Andriani, R., Semedi, G. S., & Diyan, M. (2022). Penggunaan Mikhmon (Mikrotik Hotspot Monitor) Pada Jaringan Hotspot Asrama Menggunakan Router Mikrotik. *Information Technology Journal*, *4*(1), 8–16. https://doi.org/10.24076/intechnojournal.2025v7i1

Marques, G., Senna, C., Sargento, S., Carvalho, L., Pereira, L., & Matos, R. (2024). Proactive resource management for cloud of services environments. *Future Generation Computer Systems*, *150*, 90–102. https://doi.org/10.1016/j.future.2023.08.005

McDermott, C. D., & Nicho, M. (2025). Threat detection in smart homes: A sociotechnical multimodal conversational approach for improved cyber situational awareness. *International Journal of Information Security*, *24*(4). https://doi.org/10.1007/s10207-025-01051-x

Muhammad Firdaus Ilhamy, & Slameto, A. A. (2024). Implementasi Mikrotik-API Pada Filter rule Mikrotik OS Menggunakan PHP Native Untuk UPT Lab Universitas Amikom Yogyakarta. *Jurnal PROCESSOR*, *19*(1). https://doi.org/10.33998/processor.2024.19.1.1641

Nugraha, G. adiyasa P., Suarjaya, I. M. A. D., & Pratama, I. P. A. E. (2022). Analisis Tren Lalu-lintas Data Jaringan Menggunakan Teknologi Big Data (Studi Kasus: UNIVERSITAS MAHADEWA INDONESIA). *JITTER : Jurnal Ilmiah Teknologi Dan Komputer*, *3*(2), 1043. https://doi.org/10.24843/jtrti.2022.v03.i02.p03

Ogogo, W. L. (2021). Real-Time Monitoring of Network Devices: Its Effectiveness in Enhancing Network Security. *East African Journal of Information Technology*, *3*(1), 1–6. https://doi.org/10.37284/eajit.3.1.153

Prasetyo, Y., & Soetanto, H. (2022). Implementasi Makopala Network Server Pada Router Mikrotik Sebagai Aplikasi Usermanager Untuk Kampung Wifi Berbasis Web. *KRESNA: Jurnal Riset Dan Pengabdian Masyarakat*, *2*(2), 204–212. https://doi.org/10.36080/kresna.

Puji, A., & Kusuma, A. (n.d.). *Implementasi Simple Port Knocking pada Dynamic Routing (OSPF) Menggunakan Simulasi GNS3*. https://doi.org/10.14421/csecurity.2020.3.1.1933

Riyan, M., Lubis, A. J., & Diansyah, T. M. (2025). Sistem Monitoring Jaringan dan Optimalisasi Manajemen Bandwidth Dengan Algoritma HTB (Hierarchical Token Bucket). *Jurnal Ilmu Komputer Dan Teknologi*, *1*(2), 178–188. https://doi.org/10.63854/comptech.v2i1.88

Rma, M. M., Qos, D., Manado, B., Sumual, T. D. J., Maramis, G. D. P., & Kainde, Q. C. (2025). Analisis Kualitas Layanan Jaringan Internet. *Remik: Riset Dan E-Jurnal Manajemen Informatika Komputer*, *9*(2). https://doi.org/10.33395/remik.v9i2.14857

Santoso, N. A., Affandi, K. B., & Kurniawan, R. D. (2022). Implementasi Keamanan Jaringan Menggunakan Port Knocking. *Jurnal Janitra Informatika Dan Sistem Informasi*, *2*(2), 90–95. https://doi.org/10.25008/janitra.v2i2.156