Implementation of Integrated Wi-Fi Security using RADIUS, LDAP, and Captive Portal at PT XYZ

Ahya Taufiq Akbar[1], Rizky Ardiansyah[2*], Adzikirani Adzikirani[3]

[1,2,3] Digital Telecommunication Network Study Program, Department of Electrical Engineering, State Polytechnic of Malang, 65141, Indonesia.

[1]aufiqakbar@gmail.com, [2]rizkyardiansyah@polinema.ac.id, [3]adzikirani@polinema.ac.id

Abstract— **In the digital era, securing enterprise Wi-Fi networks is critical to safeguard data integrity and control user access. PT XYZ confronts escalating cybersecurity risks—including unauthorized access, brute-force attacks, and credential sharing—necessitating a robust yet efficient authentication framework. This paper proposes and implements an integrated Multi-Factor Authentication (MFA) architecture combining RADIUS, Lightweight Directory Access Protocol (LDAP), and a Captive Portal to enhance Wi-Fi security. The solution enforces layered access control: RADIUS authenticates device MAC addresses, LDAP validates user identities against a centralized directory, and the Captive Portal applies Role-Based Access Control (RBAC) to enforce granular network permissions. A SOPHOS XGS 3100 firewall complements this setup by filtering traffic and blocking malicious login attempts. Performance evaluation shows the system supports up to 289 concurrent users with a peak CPU utilization of 29.09% and stable memory usage at 48%. Quality of Service (QoS) tests yield average download and upload speeds of 141 Mbps and 153 Mbps, respectively, ensuring consistent performance during peak usage. Security robustness is validated via penetration testing, including Deauthentication and Brute Force attacks; password cracking using Hashcat with full ASCII character set requires an estimated 998 years. Results confirm that the integrated MFA approach significantly mitigates unauthorized access risks while maintaining high network performance. This work offers practical guidance for enterprises aiming to strengthen Wi-Fi infrastructure against modern cyber threats.**

Keywords— ***Captive Portal, LDAP, Multi-Factor Authentication (MFA), Wi-Fi security, RADIUS, Role-Based Access Control (RBAC).***

I. INTRODUCTION

Network security is a fundamental aspect in ensuring the continuity of company operations [1], especially in the digital era where wireless connectivity is heavily relied upon. PT XYZ, as a satellite service provider and ISP collaborating with Starlink, faces significant challenges in maintaining data integrity and controlling access to internal networks.

With the increasing dependence on Wireless Fidelity (Wi-Fi) technology, cybersecurity threats such as credential theft, brute force attacks, and Man-in-the-Middle (MitM) attacks have become more prominent [2]. Previous studies indicate that more than 80% of security incidents stem from weak passwords and poor access management [3], [4]. Therefore, a robust authentication system is essential to ensure that only authorized users can access company networks [5].

One proposed solution is the implementation of Multi-Factor Authentication (MFA) [6], integrating Remote Authentication Dial-In User Service (RADIUS) [7], Lightweight Directory Access Protocol (LDAP), and Captive Portal [8], [9], managed through SOPHOS XGS 3100 firewall. RADIUS records and controls real-time access, while LDAP provides structured user identity management [10]. Captive Portal acts as an initial barrier directing authentication processes according to access policies, supporting Role-Based Access Control (RBAC) [11], [12].

This study aims to develop and test an integrated Wi-Fi security system in a real-world work environment, assessing its effectiveness against various cybersecurity threats. With this approach, companies are expected to enhance network security without compromising operational performance.

II. METHOD

This study employs an engineering-based research approach focused on developing a layered Wi-Fi security system within a corporate network environment. The methodology follows a systematic process comprising system design, implementation, and evaluation of a Multi-Factor Authentication (MFA)-based security architecture to enhance network authentication and access control mechanisms.

The proposed system integrates Remote Authentication Dial-In User Service (RADIUS), Lightweight Directory Access Protocol (LDAP), and Captive Portal technologies to establish multiple authentication layers. RADIUS manages device-level authentication and accounting, LDAP functions as centralized user identity management, and the Captive Portal enforces user authentication and role-based access policies. The system is implemented within the SOPHOS XGS firewall environment and evaluated through functional testing, Quality of Service (QoS) analysis, authentication load testing, and penetration testing to ensure security effectiveness without degrading network performance.

The research is structured into nine key stages, as outlined in Fig. 1, each playing a crucial role in ensuring the successful development, implementation, and evaluation of the proposed system.

1) Start: Gathering requirements and use cases to define the system scope.
2) Identification: Identifying core system needs, focusing on enhanced Wi-Fi security through multi-factor authentication, integrating RADIUS, SOPHOS XGS 3100 firewall, and LDAP.

*Corresponding author

3) Analysis: Conducting technical and non-technical analysis via literature review and interviews with PT XYZ's IT team.
4) System Design: Developing technical designs, including network architecture, system block diagrams (Fig.2), and workflow designs (Fig.3).
5) Testing: Performing authentication tests, Role-Based Access Control (RBAC) validation, and penetration testing using de-authentication attack and brute-force methods to evaluate system security.
6) Implementation: System development and configuration on physical devices, including integrating captive portal with RADIUS and LDAP through SOPHOS firewall.
7) Evaluation: Assessing test results and user feedback to measure system effectiveness.
8) Results and Discussion: Full-scale system deployment within the company's network to observe performance and security impacts.
9) End: Finalizing reports and documentation as the ultimate research output.

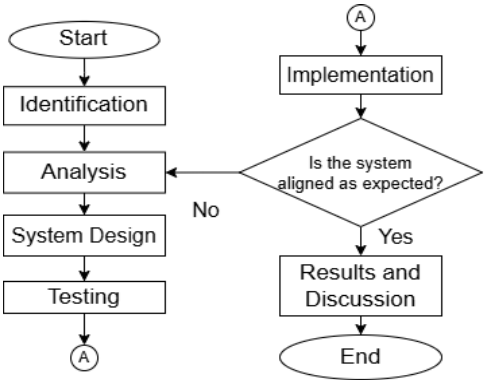


Figure 1. Research method

A. System Block Diagram

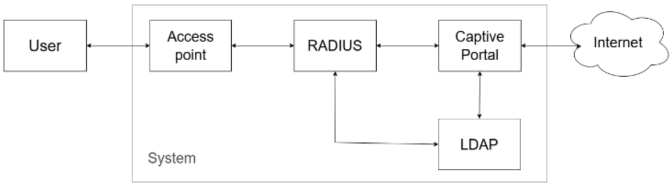


Figure 2. System Block Diagram

The system block diagram in Fig. 2 represents the authentication process as follows:

- The user connects to an Access Point (AP) and is prompted to enter a 12-character WPA2-PSK password. If the password is incorrect, the user must retry. If correct, the AP forwards the authentication request to the RADIUS server for further verification.
- The AP sends the request to the RADIUS server, where authentication continues with MAC address verification. If the received MAC address does not match the one stored in the RADIUS database, access is denied, and the user receives an Access Reject message. If authentication data is valid, the RADIUS server initiates the user session and proceeds with accounting to monitor network activity [2].
- After successful RADIUS authentication, the user is redirected to the Captive Portal within the SOPHOS firewall. At this stage, the user must enter their Employee Identification Number (NIK) and LDAP password, serving as the third authentication layer. LDAP authentication ensures that only authorized users can access the company's servers and internal data.

B. Activity System Diagram

The System Activity Diagram illustrates the user authentication flow, starting from the access request to the verification process via the RADIUS server and LDAP directory.

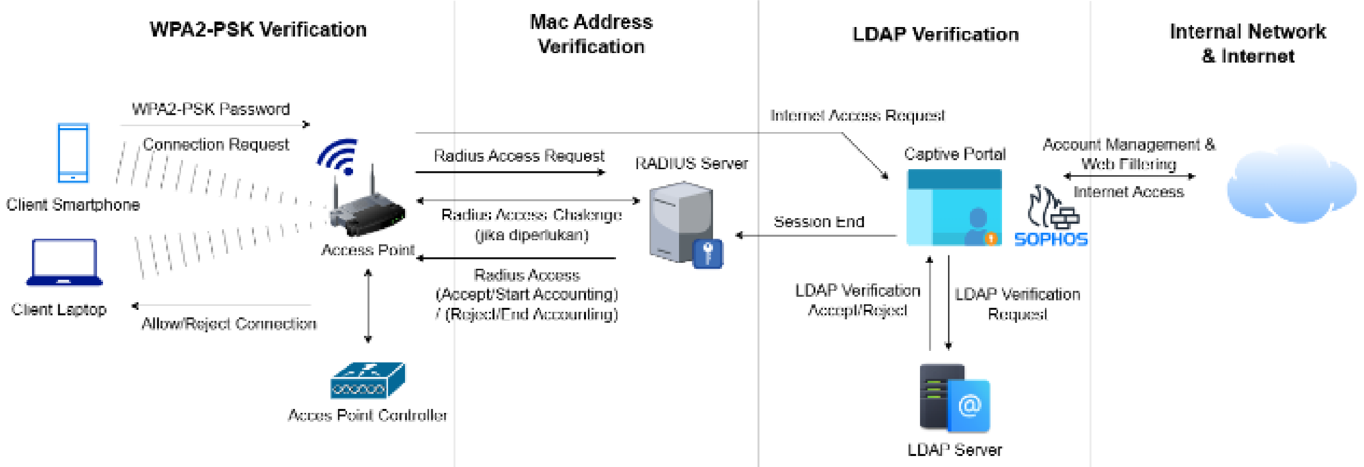


Figure 3. Activity system diagram

The network authentication system in the design of Fig.3 utilizes WPA2-PSK, RADIUS, and LDAP to ensure secure user access. Users initiate the connection by entering a 12-character WPA2-PSK password into the Access Point (AP). If valid, the AP forwards the request to the RADIUS server, which authenticates based on the MAC address. If required, an access challenge is prompted for additional verification [7]. If the MAC address does not match, RADIUS denies access, and the AP displays a "Can’t Connect to This Network" message. If validated, the session begins, and accounting is activated for monitoring.

Next, the user is redirected to the SOPHOS Captive Portal, where they must enter their Employee Identification Number (NIK) and LDAP password.

The LDAP account is linked to firewall rules in SOPHOS, restricting access to only authorized users who can enter the internal server farm, including databases and production APIs. LDAP serves as the third authentication layer, following WPA2-PSK and RADIUS, with a security measure requiring password renewal every three months. If repeated login failures occur, the account status changes to "change password required," which must be updated by the IT team before further access.

Successfully authenticated users are directed to the landing page, granting network access for an 8-hour session, after which reauthentication is required. SOPHOS Captive Portal implements access controls [13], restricting URL and application usage while securing the server farm from unauthorized access [14].

Monitoring is conducted through integrated logging with security systems, enabling the security team to respond instantly to suspicious activities via notifications and automated blocking [15], [16].

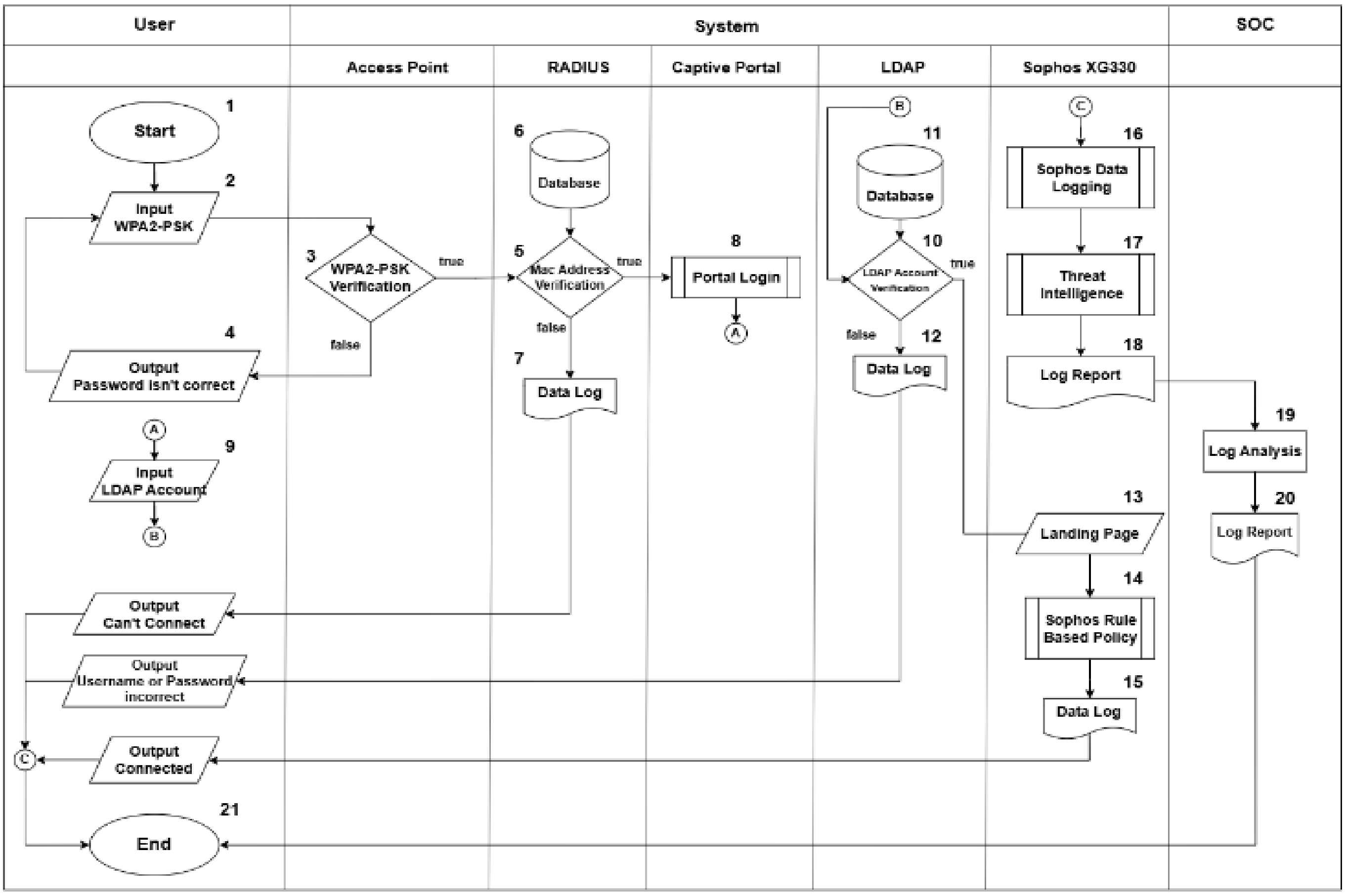


Figure 4. System Flow Diagram

C. System Flow Diagram

Fig.4 illustrates the system flow design that will be developed, with the following explanation:

1) Start*:* The user attempts to connect to the Wi-Fi network.
2) WPA2-PSK Input: The user is prompted to enter a password to gain network access
3) WPA2-PSK Verification: The Access Point (AP) verifies the password entered by the user. If incorrect, a password error prompt is displayed. If correct, the request is forwarded to the RADIUS server for further authentication.
4) Displaying the "Password isn’t correct" Message: If the password entered is incorrect, the user sees a "Password isn’t correct" message on the Wi-Fi connection screen and is prompted to re-enter the password.
5) Request Connection to RADIUS Server: The request received from the AP is processed by the RADIUS server, which queries the database. The RADIUS server retrieves

the user’s MAC address and makes an access decision based on the MAC address.

6) MAC Address Verification: The RADIUS server authenticates the user’s MAC address. If additional verification is needed, the RADIUS server requests an access challenge. This occurs when the MAC address cannot be verified or if the user has enabled random MAC address generation, leading to authentication failure. If the MAC address does not match the database, RADIUS rejects access and notifies the AP. If recognized, RADIUS grants access and initiates session accounting.
7) Data Log – Access Reject: Access rejections from RADIUS are logged and forwarded to the Sophos firewall log system as records. The user sees a "Can’t connect" message due to an unrecognized MAC address.
8) Portal Login: Once RADIUS grants access, the user is redirected to the Sophos captive portal, where all requests are temporarily rerouted. Users must authenticate using LDAP credentials to gain internet and internal application access.
9) LDAP Account Input: Users are prompted to enter their username and password to pass through the captive portal and access the internet.
10) LDAP Server Request: The captive portal forwards the authentication request to the LDAP server, which retrieves user data from its database for validation.
11) LDAP User Verification: The LDAP server verifies the user credentials against its stored database records. If the username or password is incorrect, authentication fails, and an error message is displayed. Successful authentication only occurs if the credentials match existing database records and the user account status is normal [17], [18].
12) Data Log – Access Reject: Failed authentication attempts in LDAP are logged and forwarded to the Sophos firewall system. Users receive a "Username or password incorrect" message when credentials do not match database records or if the account status is abnormal.
13) Landing Page: Successfully authenticated users are redirected to a landing page, granting internet and network access.
14) Sophos Rule-Based Policy: Internet and network traffic pass through Sophos firewall policies, enforcing restrictions based on user roles and access privileges.
15) Data Logging: Sophos firewall continuously monitors all network activity and data traffic in real time, storing it in log archives.
16) Sophos Data Logging: Security Operations Center (SOC) teams can monitor logs in real time, enabling them to query logs for suspicious activities or security incidents.
17) Threat Intelligence: Sophos firewall employs Threat Intelligence to detect malicious IPs, URLs, and applications, preventing data exchange with harmful entities. It also maintains a malware and virus database, ensuring updated security protection [14].
18) Log Report: Sophos firewall supports log export, allowing manual or automated analysis via integrated security systems [13].
19) Log Analysis: The SOC team performs log analysis using an external monitoring system, retrieving real-time traffic logs from the Sophos firewall.
20) Log Analysis Results: Processed log data generates insights, which are shared via WhatsApp groups, enabling SOC teams to take immediate security actions.
21) Completion: Logs and analysis results are used for advanced security evaluations and to improve future system efficiency. Real-time log reporting enhances network security, ensuring continuous protection for the company’s infrastructure.

D. Tools and Materials

Here are the tools and materials used in conducting this research.

TABLE I
TOOLS AND MATERIALS

Name	Description
Laptop	Used for configuration and report creation with the following specifications: Model : Lenovo LOQ 15IRX9 Processor : 12th Gen Intel® Core™ i5-12450HX (12 CPUs), ~2.4GHz RAM : 28 GB OS : Windows 11 Home
Access Point	Used for wirelees access point with the following specifications: Model : Unifi UAP AC-HD Frequency : 2.4 GHz & 5 GHz Antenna : 1x Dual band antenna
Access Point Controller	Used for AP Management and push Configuration with the following specifications: Model : Unifi US-48-750W Port : 48 GbE & 4 SFP PoE Total : 750W
RADIUS Server (Virtual)	Used for system integration and storing user MAC address data, with the following specifications: Model : RADIUSdesk Processor : 16 VCPUs RAM : 8 GB OS : Ubuntu 12 LTS
Firewall Sophos (*Appliance*)	Used for user management and access control, with the following specifications: Model : Sophos XGS 3100 (*Appliance*) Firewall Throughput : 47,000 Mbps Port : 8x GE copper, 2x SFP fiber, 2x SFP+ & 10 GE fiber
LDAP Server (*Appliance*)	Used for storing employee ID (NIK) and personal user data, with the following specifications: Model : Synology Rack Station RS3618xs Build : DSM 7.2.1-69057 Update 6 CPU : Intel Xeon D-1521 RAM : 48 GB Storage : 35 TB
Wi-Fi *dongle* TP-LINK	Used for penetration testing, with the following specifications: Model : TP-LINK TL-WN722N V1 *Interface* : USB 2.0 *Chipset* : Atheros AR9002U *Wireless Standart* : 802.11b/g/n *Operating Frequency* : 2.4 GHz

E. Testing Parameters

The system testing focuses on the following aspects:

- Quality of Service (QoS): Testing internet speed and latency before and after implementation.
- Authentication: Testing the maximum number of users that can log in simultaneously.
- RBAC (Role-Based Access Control): Testing access restrictions based on user roles.
- Web Filtering: Testing blocking mechanisms for unauthorized websites.
- MFA Security: Testing system resilience using de-authentication attacks and brute-force methods.

III. RESULT AND DISCUSSION

A. Research Location and Time

The research was conducted within the network environment of PT XYZ. The implementation and data collection process took place from January to April 2025, with testing primarily focused between February and March 2025.

B. Implementation Result

The Wi-Fi security system implemented integrates Captive Portal, RADIUS, and LDAP through the SOPHOS XGS 3100 firewall, ensuring multi-layer authentication and access control. The authentication process begins when a user connects to the Wi-Fi network, where their credentials are first verified through the Captive Portal, requiring WPA2-PSK authentication before granting access.

Once authenticated, the system enforces Role-Based Access Control (RBAC), ensuring that users are granted permissions according to their predefined roles. The RADIUS server further enhances security by verifying each device's MAC address, rejecting unauthorized connections and logging failed attempts for security audits. Users who pass RADIUS authentication are then redirected to the LDAP authentication stage, where they must enter their Employee Identification Number (NIK) and LDAP password.

Each user device must be registered in the system before gaining full network access, preventing unauthorized users from bypassing security protocols. The integration SOPHOS firewall policies further strengthen security by filtering web access, restricting unauthorized applications, and logging real-time network activity for security monitoring.

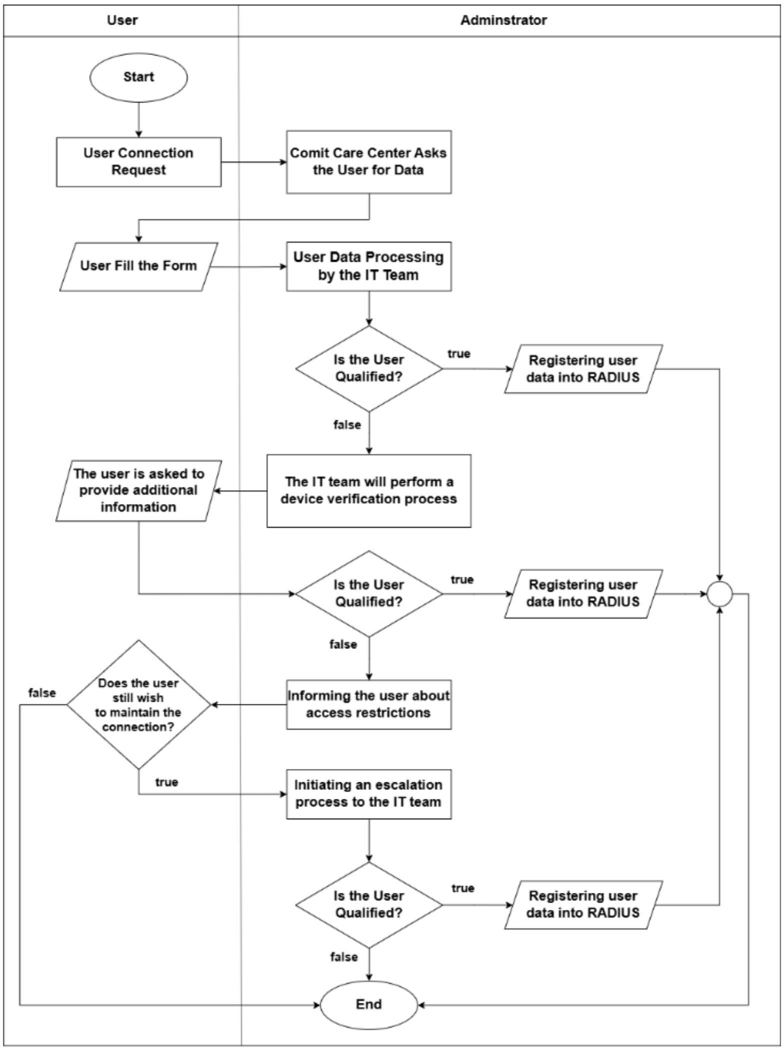

User
Adminstrator
Start
User Connection Request
Comit Care Center Asks the User for Data
User Fill the Form
User Data Processing by the IT Team
Is the User Qualified?
true
Registering user data into RADIUS
false
The user is asked to provide additional information
The IT team will perform a device verification process
Is the User Qualified?
true
Registering user data into RADIUS
false
Does the user still wish to maintain the connection?
false
Informing the user about access restrictions
true
Initiating an escalation process to the IT team
Is the User Qualified?
true
Registering user data into RADIUS
false
End

Figure 5. Early Access and Complaint Handling Diagram

C. Quality of Service (QoS)

Following the successful deployment of the system, a comprehensive performance evaluation will be conducted to assess its effectiveness across key operational parameters, including service quality, system reliability, and security resilience. The quality assessment will encompass multiple technical indicators, such as download and upload speeds, ensuring that data transmission rates remain optimal under varying network loads. Additionally, the evaluation will measure ping rate success over 100 trials, providing insights into the system's responsiveness and its ability to maintain stable connectivity. Latency stability will also be analyzed, with acceptable values ranging between 20ms and 100ms, as this range is recognized as the benchmark for efficient network performance under both typical and peak usage conditions. This analysis aims to validate the system's robustness, ensuring that its implementation does not introduce performance degradation while effectively supporting operational requirements.

Data collection will occur in two phases: before and after system deployment, to evaluate its impact on network performance. Peak hours represent periods of highest user activity within a 24-hour service cycle, where the number of active users reaches its maximum threshold. The comparative analysis aims to identify network stability variations and assess the efficiency of the system after implementation.

TABLE II
QoS BEFORE SYSTEM IMPLEMENTATION

Time*	Download**	Upload**	Avg. Ping 100x	Avg. Latency
06.00	140	85	98%	21 ms
08.00	126	76	99%	38 ms
10.00	126	106	97%	36 ms
12.00	82	51	98%	30 ms
14.00	101	81	99%	43 ms
16.00	138	108	100%	36 ms
18.00	140	100	99%	33 ms
20.00	137	107	100%	30 ms
22.00	124	88	99%	33 ms
24.00	142	60	97%	30 ms

*UTC+7 **Mbps □ Peak Hours

Table II presents the internet speed test results before system implementation, recorded between 06:00 and 24:00 WIB. The data indicates that during peak hours (10:00–14:00 WIB), download and upload speeds tend to decrease, while ping success rate and latency increase, signaling a decline in network quality. At 12:00, the lowest performance was recorded, with download speeds at 82 Mbps and upload speeds at 51 Mbps. Conversely, the best performance occurred at 06:00, showing 140 Mbps download, 85 Mbps upload, 98% ping success rate, and only 21ms latency. These findings highlight the significant impact of traffic density on overall network performance.

TABLE III
QoS AFTER SYSTEM IMPLEMENTATION

Time*	Download**	Upload**	Avg. Ping 100x	Avg. Latency
06.00	143	153	100%	19 ms
08.00	145	89	100%	56 ms
10.00	141	135	100%	68 ms
12.00	98	90	99%	51 ms
14.00	89	84	99%	49 ms
16.00	97	95	99 %	23 ms
18.00	100	91	100%	72 ms
20.00	172	90	100%	24 ms
22.00	142	60	99%	23 ms
24.00	151	73	99%	19 ms

*UTC+7 **Mbps □ Peak Hours

Table III shows that after the new system was implemented, network performance remained stable, even under high-traffic conditions. Download and upload speeds improved consistently, maintaining stability even during peak hours (10:00–14:00 WIB UTC+7). The average ping rate remained steady at 99–100%, while latency stabilized, particularly outside peak hours, with values below 30ms. A comparison of Tables II and III confirms that service quality remained intact after system implementation, with no decline in network performance.

D. Server Utilization

This testing focuses on the authentication system's capacity through large-scale login simulations, both during and outside working hours, to evaluate its resilience against authentication traffic spikes. The testing specifically targets RADIUSdesk server and SOPHOS firewall, which serve as the primary authentication gateways, ensuring that the system maintains stability, security, and controlled access, especially under high-load conditions that could affect service quality.

TABLE VI
SOPHOS FIREWALL UTILIZATION DATA

Time*	CPU	Memory	Firewall Traffic
06.00	12,58%	46%	8.263 Mbps
08.00	29,09%	47%	25.192 Mbps
10.00	22,41%	48%	123.779 Mbps
12.00	25,23%	47%	84.877 Mbps
14.00	28,47%	47%	153.004 Mbps
16.00	23,80%	47%	70.8 Mbps
18.00	21,90%	47%	52.849 Mbps
20.00	13,10%	47%	18,841 Mbps
22.00	09,08%	46%	18,121 Mbps
24.00	15,58%	46%	17,546 Mbps

*UTC+7 □ Peak Hours

The 24-hour system utilization testing, conducted at 2-hour intervals, confirms that the SOPHOS firewall has sufficient resources to support network operations without bottlenecks.

Table IV records CPU usage, memory consumption, and firewall traffic (FW traffic) from 06:00 to 24:00 WIB, where FW traffic represents the total data passing through the firewall in Mbps, reflecting the network load handled by the system.

During peak hours (08:00–20:00 WIB UTC+7), CPU utilization peaked at 28.47% at 14:00 WIB, coinciding with a traffic surge reaching 153,004 Mbps. Outside peak hours, the system load was lower, with CPU usage at 9.08% and traffic at 18,121 Mbps at 22:00 WIB.

Maximum recorded CPU usage reached 29.09%, while memory consumption peaked at 48%, remaining within safe operational limits. The SOPHOS firewall effectively managed traffic spikes, security policy enforcement, monitoring rule modifications, and cyber threat mitigation without significant performance degradation.

TABLE V
RADIUS SERVER UTILIZATION DATA

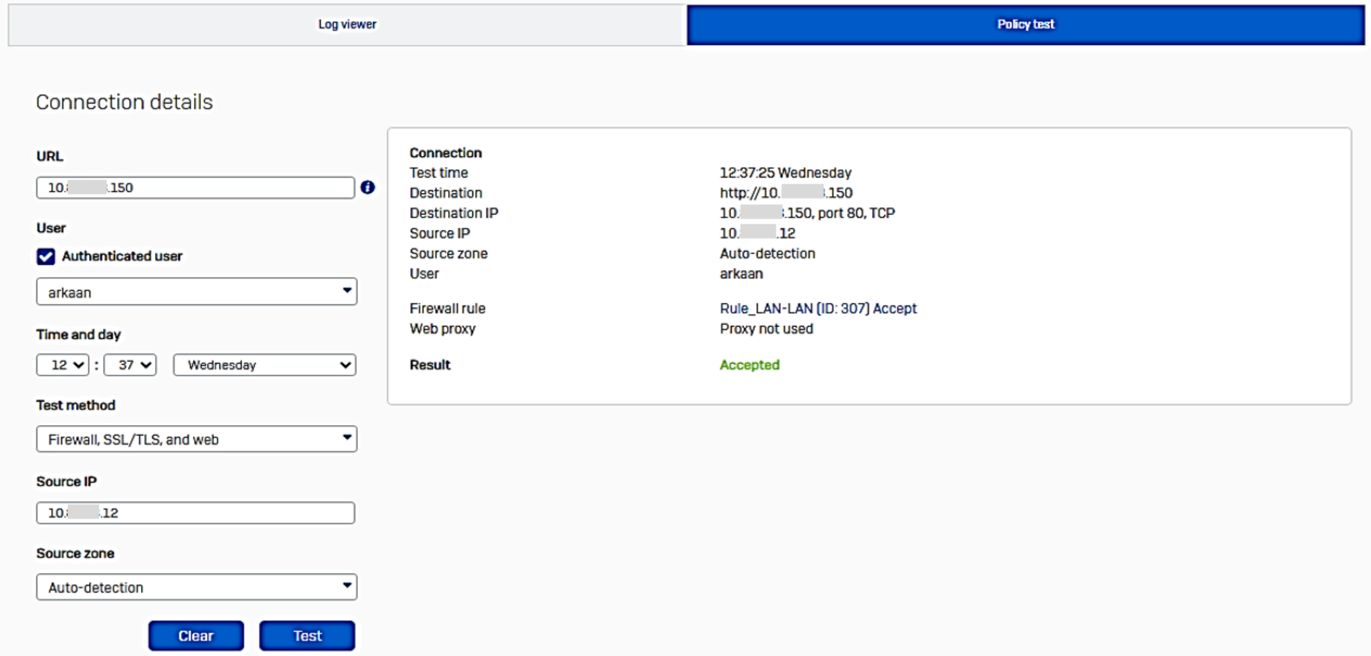
Time*	CPU	Memory	Network
06.00	0.041%	67,5%	228 byte
08.00	0.051%	67,5%	250 byte
10.00	0.093%	72.5%	417 byte
12.00	0.061%	72.25%	306 byte
14.00	0.077%	72.38%	377 byte
16.00	0.085%	72.5%	1,23 kb
18.00	0.076%	73.38%	273 byte
20.00	0.041%	73.13%	219 byte
22.00	0.039%	72.5%	208 byte
24.00	0.038%	72.38%	212 byte

*UTC+7 □ Peak Hours

From Table V, it can be observed that the RADIUS server demonstrates excellent performance in handling user authentication. With minimal CPU utilization, memory usage remaining within safe limits below 90%, and light network traffic—primarily due to its dedicated role in AAA (Authentication, Authorization, and Accounting) processes—the system maintains ample available resources to accommodate an increase in user volume or higher traffic loads.

E. Role-Based Access Control (RBAC)

In the implemented network security system, Role-Based Access Control (RBAC) restrictions are applied to ensure that only authorized users can access administrative resources. Each user registered within the Captive Portal of the SOPHOS firewall is granted access privileges based on their role, with strict limitations on administrative page access.



Connection details

URL: 10.[redacted].150

User
☑ Authenticated user
arkaan

Time and day: 12 : 37 Wednesday

Test method: Firewall, SSL/TLS, and web

Source IP: 10.[redacted].12

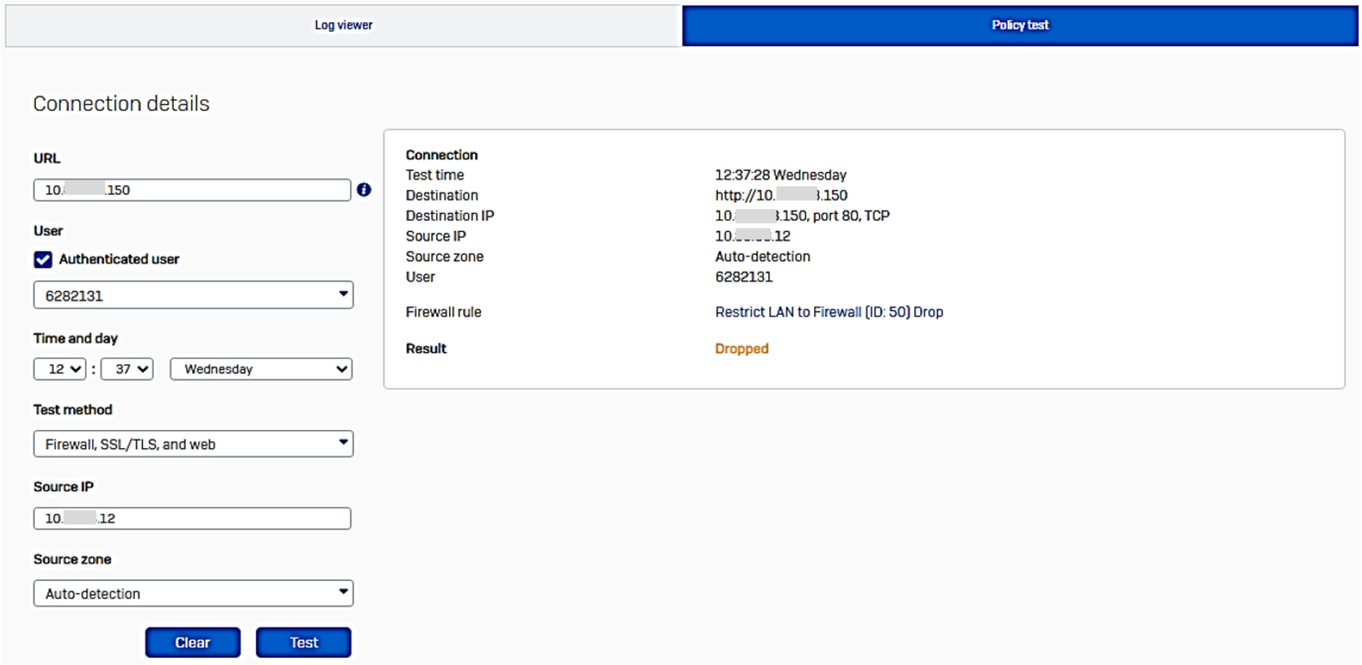
Source zone: Auto-detection

Connection
Test time 12:37:25 Wednesday
Destination http://10.[redacted].150
Destination IP 10.[redacted].150, port 80, TCP
Source IP 10.[redacted].12
Source zone Auto-detection
User arkaan

Firewall rule Rule_LAN-LAN (ID: 307) Accept
Web proxy Proxy not used

Result Accepted

Figure 6. Policy test accepted



Connection details

URL: 10.[redacted].150

User
☑ Authenticated user
6282131

Time and day: 12 : 37 Wednesday

Test method: Firewall, SSL/TLS, and web

Source IP: 10.[redacted].12

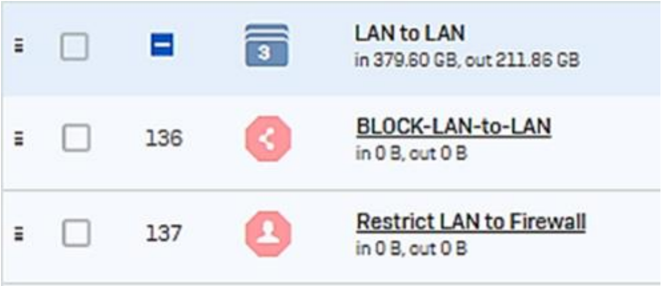
Source zone: Auto-detection

Connection	
Test time	12:37:28 Wednesday
Destination	http://10.[redacted].150
Destination IP	10.[redacted].150, port 80, TCP
Source IP	10.[redacted].12
Source zone	Auto-detection
User	6282131
Firewall rule	Restrict LAN to Firewall (ID: 50) Drop
Result	Dropped

Figure 7. Policy test dropped

Testing with the same destination address but different users shows that the user "arkaan", designated as an administrator, has full access to the internal server, in accordance with the Role-Based Access Control (RBAC) policy implemented. In this configuration, administrators registered in the SOPHOS Captive Portal are granted unrestricted access to the company's production server infrastructure.

Conversely, the user "628131", who lacks a designated role, does not have access to the internal server. Every connection attempt made by this user is denied by the system with a "dropped" status, ensuring that only authorized users can access sensitive information under the established security policy. Access restrictions are enforced through SOPHOS firewall rules, as illustrated in the image below.



□		3	LAN to LAN in 379.60 GB, out 211.86 GB
□	136		BLOCK-LAN-to-LAN in 0 B, out 0 B
□	137		Restrict LAN to Firewall in 0 B, out 0 B

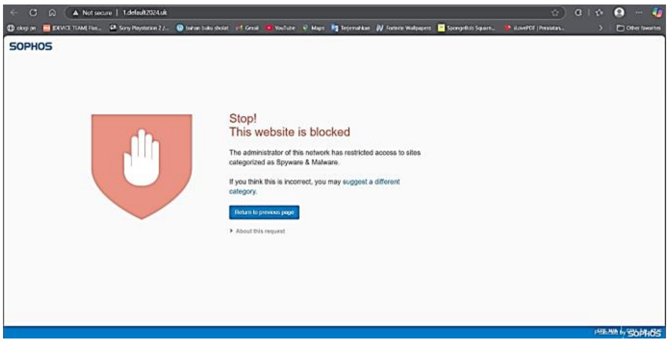
Figure 8. Rule "Restrict LAN to Firewall"

A total inbound and outbound value of "0" confirms that the applied rule aligns with the research objective, ensuring no data traffic occurs under that specific rule. This validation supports the system's access control measures, demonstrating that the intended restrictions are effectively enforced without unexpected network activity.

F. Web Filtering

This test aims to evaluate the effectiveness of the web filtering mechanism in restricting user access to content that supports company operations. By implementing this filtering system, the company can control and prevent access to websites that pose potential security threats, while also minimizing disruptions to workplace productivity.

Beyond protecting the system from threats like malware and phishing, this mechanism plays a crucial role in optimizing IT resource efficiency, ensuring that bandwidth and network devices are allocated appropriately for business needs. The evaluation is conducted by analyzing user access patterns and assessing the effectiveness of blocking high-risk website categories. Fig.9 illustrates an example of a blocked website display via the SOPHOS firewall.



Stop!
This website is blocked

The administrator of this network has restricted access to sites categorized as Spyware & Malware.

If you think this is incorrect, you may suggest a different category.

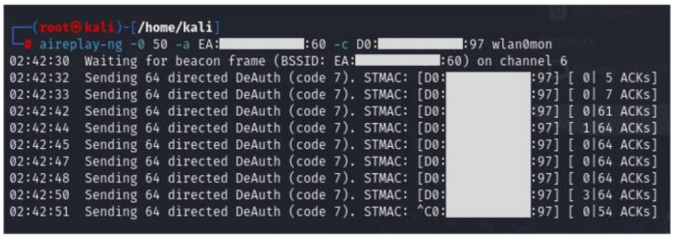
Figure 9. Blocked site warning page from SOPHOS firewall

G. Multi-Factor Authentication (MFA)

System security evaluation is conducted through penetration testing, serving as a means to assess the resilience of Multi-

Factor Authentication (MFA) against various attack methods. This testing aims to simulate direct threat scenarios that may occur, ensuring the system's ability to withstand exploitation attempts by unauthorized entities.

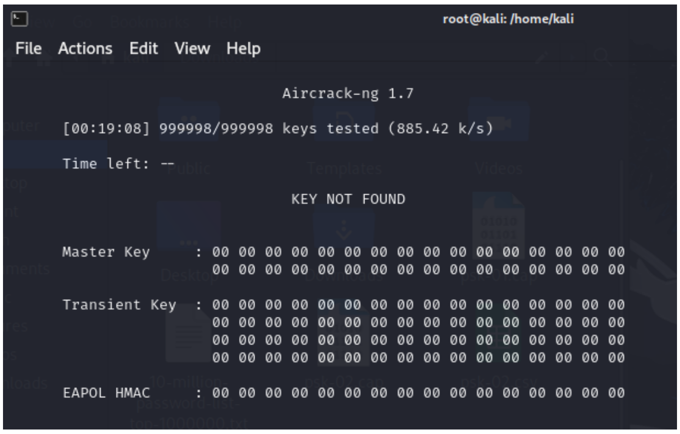
1) De-authentication and Dictionary Brute force Attack: This research evaluates the security of authentication systems by testing various penetration techniques to identify potential vulnerabilities that attackers could exploit [19]. One such method is the De-authentication Attack, which aims to disconnect users from the network, assessing the system's response to unauthorized access disruptions [20], [21]. If weaknesses exist within the security framework, attackers may intercept authentication data exchanged by victims during network communication [22], [23]. Additionally, Dictionary Brute force Attack is employed to examine the system's resilience against credential-based attacks, where an adversary attempts to crack authentication credentials using extensive precompiled wordlists.



```
┌──(root㉿kali)-[/home/kali]
└─# aireplay-ng -0 50 -a EA:[redacted]:60 -c D0:[redacted]:97 wlan0mon
02:42:30  Waiting for beacon frame (BSSID: EA:[redacted]:60) on channel 6
02:42:32  Sending 64 directed DeAuth (code 7). STMAC: [D0:[redacted]:97] [ 0| 5 ACKs]
02:42:33  Sending 64 directed DeAuth (code 7). STMAC: [D0:          :97] [ 0| 7 ACKs]
02:42:42  Sending 64 directed DeAuth (code 7). STMAC: [D0:          :97] [ 0|61 ACKs]
02:42:44  Sending 64 directed DeAuth (code 7). STMAC: [D0:          :97] [ 1|64 ACKs]
02:42:45  Sending 64 directed DeAuth (code 7). STMAC: [D0:          :97] [ 0|64 ACKs]
02:42:47  Sending 64 directed DeAuth (code 7). STMAC: [D0:          :97] [ 0|64 ACKs]
02:42:48  Sending 64 directed DeAuth (code 7). STMAC: [D0:          :97] [ 0|64 ACKs]
02:42:50  Sending 64 directed DeAuth (code 7). STMAC: [D0:          :97] [ 3|64 ACKs]
02:42:51  Sending 64 directed DeAuth (code 7). STMAC: ^C0:          :97] [ 0|54 ACKs]
```

Figure 10. De-authentication attack process

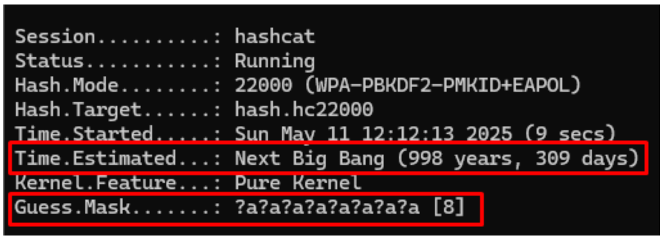
After the data was obtained, password cracking was conducted to evaluate credential resilience against brute force methods [24]. The effectiveness of the brute force process depends on the number of keywords within the dictionary file and the complexity of the characters being guessed [25]. The results of this test indicate that the dictionary brute force attack failed to retrieve the system's latest password, confirming the strength of the authentication mechanism against this attack method.



```
                              Aircrack-ng 1.7

      [00:19:08] 999998/999998 keys tested (885.42 k/s)

      Time left: --

                               KEY NOT FOUND


      Master Key     : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Figure 11. Dictionary brute force process

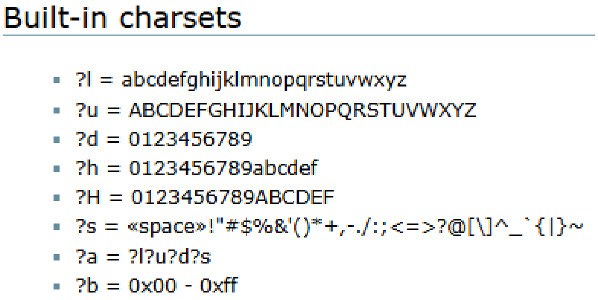
2) Pure Brute force Attack Method: On the other hand, pure brute force attack is a method used to decrypt a captured handshake, though it requires significantly more time for decryption. This is due to its guessing-based process, which involves repeated iterations and exhaustive attempts to determine the correct credentials. Below is an example of a pure brute force method applied by the author during password strength testing using the Hashcat application.



```
Session..........: hashcat
Status...........: Running
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: hash.hc22000
Time.Started.....: Sun May 11 12:12:13 2025 (9 secs)
Time.Estimated...: Next Big Bang (998 years, 309 days)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?a?a?a?a?a?a?a?a [8]
```

Figure 12. Pure brute force process

As shown in Fig.12, upon initiating the decryption process, the system estimates that cracking an 8-character password would take approximately 998 years and 309 days. This test assumes that the attacker has no prior knowledge of the target's password, thus incorporating all possible characters using full ASCII exploration via the "?a" parameter in the brute force attack. Due to this extensive search space, the tester was unable to proceed with the attack. Below is the detailed masking configuration used during the testing process.



Built-in charsets

- ?l = abcdefghijklmnopqrstuvwxyz
- ?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
- ?d = 0123456789
- ?h = 0123456789abcdef
- ?H = 0123456789ABCDEF
- ?s = «space»!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
- ?a = ?l?u?d?s
- ?b = 0x00 - 0xff

Figure 13. Masking parameter in hashcat

IV. Conclusion

The testing results demonstrate that the implementation of the authentication system does not degrade overall network service quality. Download speeds increased from 126 Mbps to 141 Mbps, while upload speeds improved from 85 Mbps to 153 Mbps after system deployment. Although latency slightly increased from 30ms to 51ms during peak hours, this change is attributed to additional authentication processes and traffic filtering mechanisms and remains within acceptable operational limits.

Furthermore, the SOPHOS XGS 3100 firewall proved capable of managing multiple active users simultaneously without experiencing performance bottlenecks. During peak usage, the system maintained a maximum CPU utilization of 29.09%, while memory usage remained stable at 47–48%, indicating sufficient processing capacity to handle high traffic loads. The implementation of Role-Based Access Control (RBAC) effectively restricted access to internal resources, ensuring that only authorized users could access sensitive systems. Unauthorized access attempts were successfully blocked, with zero traffic recorded under the "Restrict LAN to

Firewall" rule. In addition, penetration testing confirmed the system's resilience against De-authentication and Brute force attacks, with an estimated decryption time of 998 years for an 8-character mixed password. To further enhance security, the authentication policy was strengthened by implementing a 20-character complex password requirement.

REFERENCES

[1] A. R. Raharja, *Keamanan Jaringan*, 1st ed., vol. 1. Penerbit KBM Indonesia, 2024.

[2] A. D. Yudhistira and R. Harwahyu, "Implementation strategy analysis of network security using dalo RADIUS and Pi-hole DNS server to enhance computer network security, case study: XYZ as a fintech company," *Journal of Social Technology*, vol. 5, no. 10, p. 4364, 2024.

[3] S. Wibawa, S. Suryanto, and R. Ningsih, "Perlindungan data digital dengan time-based one-time password (TOTP)," *INSANtek*, vol. 5, no. 1, pp. 30–36, May 2024.

[4] R. P. Azhari, "Metodologi penelitian dalam pengembangan keamanan data untuk sistem informasi," Universitas Komputer Indonesia, 2024. [Online]. Available: https://www.researchgate.net/publication/383145632

[5] F. Hasibuan, "Jaringan komputer berbasis radius server untuk meningkatkan pemanfaatan internet di Madrasah Aliyah Al-Azhaar Ummu Suwanah," *Jurnal Teknik Informatika*, vol. 7, no. 1, pp. 30–39, 2021.

[6] M. Rusdan and M. Sabar, "Analisis dan perancangan jaringan wireless dengan wireless distribution system menggunakan user authentication berbasis multi-factor authentication," *Journal of Information Technology*, vol. 2, no. 1, pp. 17–24, Mar. 2020.

[7] L. Galchynsky and A. Murtazina, "Vulnerability detection in the network traffic flow of the RADIUS protocol based on the object-oriented model," *Theoretical and Applied Cybersecurity*, vol. 4, no. 1, Feb. 2023.

[8] F. A. Mustika, F. P. Sulistyo, and C. A. Tanof, "Implementasi system captive portal dengan otentikasi RADIUS," *Jurnal Ilmiah FIFO*, vol. 12, no. 1, p. 49, Jul. 2020.

[9] A. D. Yudhistira and R. Harwahyu, "Implementation strategy analysis of network security using dalo RADIUS and Pi-hole DNS server to enhance computer network security," *Jurnal Indonesia Sosial Teknologi*, vol. 5, no. 10, pp. 4364–4379, Oct. 2024.

[10] C. A. O. Villanueva and A. Roman-Gonzalez, "Implementation of a RADIUS server for access control through authentication in wireless networks," *International Journal of Advanced and Applied Sciences*, vol. 10, no. 3, pp. 183–188, 2023.

[11] Herpendi, F. Fathurrahmani, and K. A. Hafizd, "Pemanfaatan cloud identity sebagai sumber data pengguna dalam penerapan otorisasi dan otentikasi layanan aplikasi berbasis web menggunakan LDAP dan RADIUS (studi kasus: Politeknik Negeri Tanah Laut)," *SEMINASTIKA*, vol. 3, no. 1, pp. 156–160, Nov. 2021.

[12] Y. Yuricha and I. K. Phan, "Penerapan role based access control dalam sistem supply chain management berbasis cloud," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 3, no. 2, pp. 339–348, Nov. 2023.

[13] A. Eluwa, "Trends in wireless network security," *Open Access Library Journal*, vol. 11, no. 11, pp. 1–17, Nov. 2024.

[14] Y. S. Tomar and N. Bhile, "First line of defense: Firewall," *Asian Journal of Research in Computer Science*, pp. 25–32, Nov. 2021.

[15] U. e. Khadija and I. Saqib, "Comparison of different firewalls performance in a virtual for cloud data center," *Journal of Advancement in Computing*, vol. 1, no. 1, pp. 21–28, Mar. 2023.

[16] S. N. Adzimi, H. A. Alfasih, F. N. G. Ramadhan, S. N. Neyman, and A. Setiawan, "Implementasi konfigurasi firewall dan sistem deteksi intrusi menggunakan Debian," *Journal of Internet and Software Engineering*, vol. 1, no. 4, p. 12, Jun. 2024.

[17] J. Yang *et al.*, "A model study on collaborative learning and exploration of RBAC roles," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, Jan. 2021.

[18] Fathurrahmani, Herpendi, and K. A. Hafizd, "Perancangan single sign on (SSO) pada aplikasi web menggunakan cloud identity," *Antivirus: Jurnal Ilmiah Teknik Informatika*, vol. 15, no. 2, pp. 242–251, Nov. 2021.

[19] M. Hasibuan and A. M. Elhanafi, "Penetration testing sistem jaringan komputer menggunakan Kali Linux untuk mengetahui kerentanan keamanan server dengan metode black box," *sudo Jurnal Teknik Informatika*, vol. 1, no. 4, pp. 171–177, Dec. 2022.

[20] S. A. Maherza, B. Hananto, and I. W. W. Pradnyana, "Penetration testing terhadap website sekolah menengah atas ABC dengan metode NIST SP 800-115," *Informatik: Jurnal Ilmu Komputer*, vol. 19, no. 1, pp. 11–27, May 2023.

[21] P. Janardhan and B. Jagadeesh, "Accurate deauthentication attack detection using linear discriminant analysis in comparison with multilayer perceptron," *Journal of Pharmaceutical Negative Results*, vol. 13, no. SO4, Jan. 2022.

[22] H. Amnur, Rasyidah, and F. Setyawan, "Keamanan jaringan wireless dengan Kali Linux," *JITSI: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 3, no. 1, pp. 16–22, Mar. 2022.

[23] A. P. Armadhani, D. Nofriansyah, and K. Ibnutama, "Analisis keamanan untuk mengetahui vulnerability pada DVWA lab esting menggunakan penetration testing standart OWASP," *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)*, vol. 21, no. 2, p. 80, Aug. 2022.

[24] D. A. Putra *et al.*, “Analisa perbandingan tools CEWL, CRUNCH, CUPP dalam pengujian password cracking,” *Jurnal Teknik Mesin, Elektro dan Ilmu Komputer*, vol. 3, no. 1, pp. 15–22, Mar. 2023.

[25] M. A. Adiguna and B. W. Widagdo, “Analisis keamanan jaringan WPA2-PSK menggunakan metode penetration testing (studi kasus: Router Tp-Link Mercusys Mw302r),” *Jurnal SISKOM-KB (Sistem Komputer dan Kecerdasan Buatan)*, vol. 5, no. 2, pp. 1–8, Mar. 2022.