Mr. Satheeshkumar S, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science,
Engineering and Technology
An Open Access Journal

Design and Implementation of Secure Wireless Network

Mr. Satheeshkumar S , Mrs.Thendral K, Madhan Kumar S, Madhan R, Mukesh Pandian A, Ravivarma R

Department of Electronics and Communication Engineering,
Paavai Engineering college,
Namakkal,India

Abstract — Wireless networking has become a fundamental component of modern organizations and educational institutions, enabling users to access the internet and communicate efficiently. However, these networks are often vulnerable to several security challenges, including unauthorized device access and the presence of rogue access points. This work focuses on the design and deployment of a secure wireless network using Juniper networking technologies such as the SRX300 firewall, EX series switches, and Mist AP32/AP63 wireless access points. Network segmentation is implemented using Virtual Local Area Networks (VLANs) to separate traffic and enhance overall network security and management. A dedicated guest wireless network is also configured through the Juniper Mist Cloud platform using a captive portal authentication mechanism, which provides controlled access for external users. The SRX300 firewall is used to enforce security policies that regulate network traffic and restrict unauthorized activities. Furthermore, advanced security features including rogue access point detection is integrated to identify and analyze potential wireless threats. The developed system demonstrates an effective solution for establishing a secure, scalable, and well-managed enterprise wireless network environment.

Keywords— Secure Wireless Networking, Firewall, VLAN, Captive Portal Authentication, Rogue Access Point Detection.

I. INTRODUCTION

Wireless networks are widely used in enterprises and educational institutions because they provide flexible and convenient connectivity. However, the open nature of wireless communication makes these networks vulnerable to security threats such as rogue access points, unauthorized access, and authentication attacks. Traditional security mechanisms that rely only on encryption standards such as WPA2 and WPA3 are not sufficient to address modern security challenges.

To improve wireless network security, this project proposes a secure architecture that integrates multiple protection mechanisms, including VLAN-based traffic segmentation, firewall policy enforcement, captive portal authentication for guest access, and continuous monitoring for rogue access points. The system is implemented using Juniper networking technologies such as the SRX300 firewall, EX series switches, and Mist AP32/AP63 wireless access points. The proposed design aims to provide a scalable, manageable, and secure wireless networking environment suitable for modern enterprise networks.

II. LITERATURE SURVEY

Wireless network security has received significant attention in recent years due to the growing number of cyber threats targeting wireless infrastructures. Many studies have focused on improving authentication methods, access control mechanisms, and threat detection techniques to strengthen wireless network protection.

The study in [1] examines improvements in captive portal authentication to reduce the risk of phishing attacks. Traditional captive portals typically rely on web-based login pages, which attackers may replicate to obtain user credentials. To address this issue, the

research proposes the use of hardware-based security tokens and stronger authentication mechanisms. The findings indicate that integrating secure authentication methods can significantly reduce the chances of credential theft. This approach supports the secure guest onboarding mechanism used in the proposed wireless network architecture.

In [2], the authors investigate the use of OAuth-based authentication for wireless network environments. Conventional authentication methods that rely on passwords are often vulnerable to security threats such as brute-force attacks and credential reuse. The study highlights that OAuth enables users to authenticate through trusted identity providers, which enhances both security and user convenience. The use of Single Sign-On (SSO) in this approach is closely related to the social login-based captive portal authentication mechanism implemented in the proposed wireless network system.

The study in [3] explores techniques for detecting rogue Wi-Fi access points in real time using behavioral analysis. Rogue access points can imitate legitimate wireless networks and capture user traffic, which may lead to serious security risks. To address this issue, the research proposes monitoring and anomaly detection methods that analyze wireless signals and traffic patterns continuously to identify unauthorized devices within the network. The findings emphasize the importance of proactive rogue access point detection, which is also incorporated in the proposed wireless network deployment.

The research presented in [4] examines the role of IEEE 802.1X authentication in securing enterprise networks. This mechanism provides port-based access control by verifying user or device credentials before granting network connectivity. The study explains how authentication servers such as RADIUS are used to validate identities and enforce access policies. By implementing identity-based authentication, the framework ensures that only authorized users and devices are allowed to connect to the network. Although the proposed system primarily utilizes captive portal authentication, the concepts of IEEE 802.1X offer a strong basis for enhancing secure access control in future network deployments.

The study in [5] examines security risks introduced by rogue access points in wireless local area networks. Unauthorized access points can imitate legitimate network devices and may be used to launch attacks such as traffic interception, man-in-the-middle attacks, and potential data leakage. The research emphasizes the need for continuous monitoring and detection mechanisms to identify suspicious wireless devices operating within the network environment. These findings highlight the importance of implementing rogue access point detection features as part of a secure wireless network deployment.

The study in [6] explores the application of the Zero Trust Security Model in wireless networking environments. This security approach assumes that no user or device should be automatically trusted, even if it is connected within the network perimeter. Instead, every access request must be verified and continuously monitored before granting permission. The research highlights the importance of identity verification, strict access policies, and proper network segmentation to strengthen overall security. These principles are reflected in the proposed wireless network architecture through the use of VLAN-based traffic isolation and firewall-based access control mechanisms.

The research in [7] examines enterprise network design using VLAN-based segmentation and hierarchical network architecture. By organizing networks into logical segments, organizations can improve scalability, minimize broadcast traffic, and strengthen overall network security. The study also discusses the role of inter-VLAN routing in enabling controlled communication between different network segments. These concepts support the VLAN segmentation strategy implemented in the proposed secure wireless network system.

The study in [8] analyzes the use of VLAN technology in campus network environments and demonstrates how network segmentation can improve both traffic management and security. By dividing the network into separate logical segments, VLANs allow different user groups—such as administrative staff, students, and guest users—to operate within isolated network spaces. This approach helps reduce the risk of unauthorized internal access while also improving network efficiency and performance. These findings support the VLAN-based wireless segmentation strategy implemented in the proposed network architecture

The study in [9] investigates the use of honeypot systems combined with machine learning techniques to detect unauthorized access attempts within network environments. Honeypots function as decoy systems designed to attract potential attackers, allowing administrators to observe and analyze malicious activities. By examining the interactions between attackers and these decoy systems, security frameworks can identify suspicious behavior and possible threats. This concept influenced the honeypot-based monitoring mechanism incorporated in the proposed secure wireless network deployment.
The study in [10] presents a security analysis of the WPA3 authentication protocol. Although WPA3 offers stronger encryption and improved authentication compared to earlier wireless security standards, the research identifies certain weaknesses in the SAE (Simultaneous Authentication of Equals) handshake process. The findings suggest that depending only on encryption mechanisms cannot fully protect wireless networks from emerging threats. Therefore, the study recommends adopting a layered security strategy that combines authentication, continuous monitoring, and network segmentation. This observation supports the multi-layered security approach implemented in the proposed wireless network architecture.

III. PROPOSED SYSTEM

The proposed system aims to deploy a secure wireless network infrastructure using Juniper networking technologies. The architecture includes a Juniper SRX300 firewall, EX series switches, and AP32/AP63 wireless access points. The wireless access points deliver network connectivity to users, while the SRX300 firewall applies security policies and continuously monitors network traffic.

Wireless traffic is organized using Virtual Local Area Networks (VLANs) to separate guest users from internal network users. This segmentation enhances network protection and helps prevent unauthorized communication between different network segments. The system also incorporates a captive portal authentication mechanism through the Juniper Mist Cloud platform to manage and control guest Wi-Fi access.

Firewall filters are implemented on the SRX300 firewall to limit access to certain applications and domains. In addition, the system incorporates rogue access point detection to identify suspicious or unauthorized devices operating within the wireless network.

IV. SYSTEM ARCHITECTURE

The proposed system architecture integrates enterprise-level networking components to establish a secure wireless networking environment. The architecture includes an Internet Service Provider (ISP) connection, a Juniper SRX300 firewall router, EX-series switches, and Juniper Mist-managed wireless access points.

The ISP delivers external network connectivity, which is first directed through the SRX300 firewall. The firewall functions as the main security gateway and is responsible for packet filtering, network address translation (NAT), and enforcement of security policies. The SRX300 is connected to an EX4100 core switch that distributes network traffic to several access-layer switches such as the EX2300.

Multiple wireless access points, including AP32 and AP63, are connected to these switches to provide wireless coverage throughout the network. These

access points broadcast multiple SSIDs corresponding to different VLANs, such as administrative, student, and guest networks. Each SSID is associated with a specific VLAN to maintain proper traffic segmentation and network isolation.

The guest wireless network is configured with a captive portal authentication mechanism using the Juniper Mist Cloud platform. This feature enables users to authenticate through social login services before obtaining access to the network.

To further enhance wireless security, rogue access point detection is implemented. These security features continuously observe the wireless environment to identify unauthorized access points attempting to imitate legitimate networks.

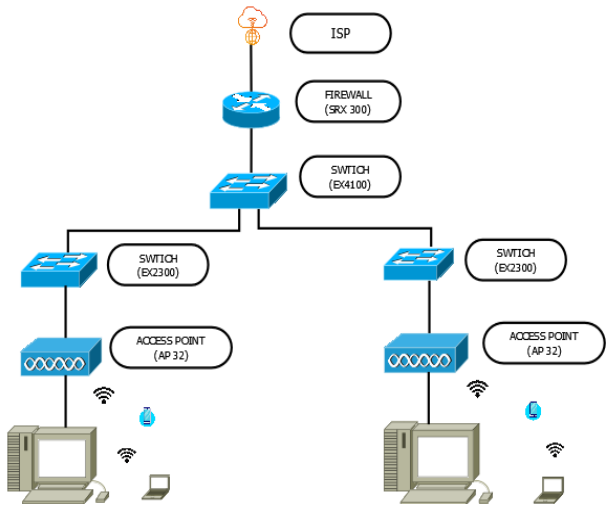

Fig 1. Block Diagram of the Proposed Secure Wireless Network Architecture.

Fig. 1 shows the proposed secure wireless network architecture where the ISP connects to the SRX300 firewall responsible for enforcing network security policies. The firewall links to EX-series switches that distribute network traffic to several AP32 and AP63 access points. Wireless users connect through SSIDs mapped to VLANs, while captive portal authentication, rogue access point detection, and firewall filtering maintain secure network access.

V. NETWORK IMPLEMENTATION

The implementation of the secure wireless architecture is performed using Juniper networking devices integrated with cloud-based management. The SRX300 firewall is configured to create logical VLAN interfaces that divide network traffic into different security zones. Each VLAN is allocated a unique subnet and DHCP configuration to enable automatic IP address assignment for connected devices.

Juniper EX-series switches provide Layer-2 connectivity and support VLAN trunking between the firewall and wireless access points. These switches ensure efficient traffic distribution while maintaining VLAN isolation across the network infrastructure.

The wireless network is deployed using Juniper Mist AP32 and AP63 access points. These access points broadcast multiple SSIDs mapped to corresponding VLAN identifiers. The guest SSID is configured with captive portal authentication through the Mist Cloud platform.

Security policies are applied on the Juniper SRX300 Firewall to enforce access control rules. These policies allow guest users to access only the internet while blocking communication with internal enterprise resources.

Application filtering and domain blocking mechanisms are implemented to restrict certain websites and services. Rogue access point detection mechanisms continuously monitor nearby wireless networks to identify unauthorized access points attempting to imitate legitimate SSIDs.

VI. RESULTS AND DISCUSSION

The implemented secure wireless network architecture was evaluated by verifying captive portal authentication, VLAN segmentation, DHCP address allocation, and internet connectivity for guest users. The experimental results show that the proposed system effectively provides secure access control while maintaining appropriate network isolation.

Fig. 2. Captive Portal Authentication Page for Guest Wireless Network Access using Juniper Mist Cloud.

The guest wireless network is secured through a captive portal authentication mechanism provided by Juniper Mist Cloud. When a user connects to the Juniper_Guest SSID, the device is automatically redirected to the captive portal login page as illustrated in Fig. 2. Users must enter required details such as name, email, and organization before receiving internet access. This authentication process restricts unauthorized access and allows administrators to monitor guest user activity within the network.

```
mist@PIF_Juniper> show configuration vlans
guest {
    vlan-id 40;
    l3-interface irb.40;
}
```

Fig. 3. VLAN Configuration for Guest Network (VLAN ID 40) Configured on SRX300 Firewall.

Network segmentation is achieved using VLAN technology to separate guest traffic from internal enterprise networks. As illustrated in Fig. 3, the guest wireless network is assigned to VLAN ID 40 and linked with the logical interface irb.40 on the Juniper SRX300 Firewall. This configuration ensures that guest users remain in an isolated network segment and blocks unauthorized access to internal organizational resources.

```
mist@PIF_Juniper> show dhcp server binding
IP address      Session Id  Hardware address   Expires   State   Interface
10.10.10.21     12          06:bd:5b:e1:dc:a2  86095     BOUND   irb.0
10.10.10.16     7           08:f9:7e:b6:12:03  84858     BOUND   irb.0
10.10.10.23     14          08:f9:7e:dc:38:a3  78879     BOUND   irb.0
10.10.10.36     35          08:f9:7e:dc:39:93  86006     BOUND   irb.0
10.10.10.22     13          28:c5:d2:28:d8:04  86368     BOUND   irb.0
10.10.40.14     21          28:c5:d2:28:d8:04  71887     BOUND   irb.40
10.10.40.17     32          2a:68:3c:45:18:e1  82635     BOUND   irb.40
10.10.40.15     29          34:1c:f0:7f:dd:8d  85780     BOUND   irb.40
10.10.10.14     5           54:33:c6:13:0a:47  79380     BOUND   irb.0
10.10.10.24     15          56:61:66:f6:8c:ae  65433     BOUND   irb.0
10.10.10.26     22          6e:02:97:4f:2d:8c  79704     BOUND   irb.0
10.10.10.15     6           70:90:41:91:a4:0f  62096     BOUND   irb.0
10.10.10.10     1           70:90:41:94:70:5e  86312     BOUND   irb.0
10.10.10.20     11          84:1b:77:f1:52:a2  81425     BOUND   irb.0
10.10.10.25     19          9e:9a:76:6f:66:12  86279     BOUND   irb.0
10.10.10.31     27          a0:d3:65:67:72:3f  84792     BOUND   irb.0
10.10.10.35     34          a2:a2:0c:1b:05:23  84150     BOUND   irb.0
10.10.10.34     33          b6:3d:96:fd:b0:1b  85856     BOUND   irb.0
10.10.10.19     10          ba:12:fd:34:bc:f3  84656     BOUND   irb.0
10.10.40.16     31          bc:6a:d1:70:b5:d9  86019     BOUND   irb.40
10.10.40.13     20          be:9b:0a:f1:b7:aa  80470     BOUND   irb.40
```

Fig. 4. DHCP Server Binding Table Showing Dynamic IP Assignment for Guest Wireless Clients.

Dynamic Host Configuration Protocol (DHCP) is configured on the Juniper SRX300 Firewall to automatically allocate IP addresses to devices connected to the wireless network. Fig. 4 displays the DHCP binding table where several client devices obtain IP addresses dynamically. The highlighted entries represent devices associated with VLAN 40, confirming that guest clients receive IP addresses within the designated guest subnet.

```
C:\WINDOWS\system32\cmd.
Microsoft Windows [Version 10.0.26100.7840]
(c) Microsoft Corporation. All rights reserved.

C:\Users\krishnaveni>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=283ms TTL=119
Reply from 8.8.8.8: bytes=32 time=293ms TTL=119
Reply from 8.8.8.8: bytes=32 time=404ms TTL=119
Reply from 8.8.8.8: bytes=32 time=305ms TTL=119

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 283ms, Maximum = 404ms, Average = 321ms
```

Fig. 5. Internet Connectivity Test from Guest Wireless Client using ICMP Ping.

Connectivity testing was conducted to confirm internet access for authenticated guest users. As illustrated in Fig. 5, the client device successfully transmits ICMP echo requests to the external server 8.8.8.8 and receives responses without packet loss. This result verifies that firewall policies permit guest users to access the

internet while maintaining isolation from internal network resources

VI.CONCLUSION

This paper presented the design and implementation of a secure wireless network architecture that integrates VLAN segmentation, firewall-based policy enforcement, captive portal authentication, and rogue access point detection mechanisms. By combining identity-based access control, Zero Trust principles, and layered defense techniques, the proposed system reduces common wireless threats such as unauthorized access, phishing attacks, and rogue infrastructure.

The implementation shows that enterprise-level firewall integration improves wireless network security while preserving scalability and usability. The proposed architecture offers a strong foundation for secure wireless deployments in campus and enterprise environments and can be further improved with advanced authentication frameworks and AI-based anomaly detection systems

REFERENCES

1. D. P. Mishra and P. K. Sahu, "Adapting a Captive Portal for Phishing-Resistant Network Authentication Using Security Keys," IEEE JNIC, 2023. DOI: 10.23919/JNIC58574.2023.10205713.
2. "Enhancing WiFi Authentication: Leveraging OAuth for Secure and User-Friendly Wireless Networks," IEEE CCWC, 2025. DOI: 10.1109/CCWC62904.2025.10903952.
3. "Real-Time Identification of Rogue WiFi Connections in the Wild," IEEE Internet of Things Journal, 2022. DOI: 10.1109/JIOT.2022.3223682.
4. "IEEE 802.1X Authentication and Security Mechanisms in Modern Networks," IEEE Access, 2025. DOI: 10.1109/ACCESS65134.2025.11135604.
5. "Rogue Access Point: The WLAN Threat," IEEE ICCCIS, 2022. DOI: 10.1109/ICCCIS56430.2022.10037591.
6. "Guest Editorial: Zero Trust Security Methods for Wireless Networks," IEEE Wireless Communications Magazine, 2024. DOI: 10.1109/MWC.2024.10495912.
7. "Design and Simulation of a VLAN-Based Hierarchical Enterprise Network with MSTP and Inter-VLAN Routing," IEEE CSITSS, 2025. DOI: 10.1109/CSITSS67709.2025.11294144
8. "Implementation and Optimization of VLANs in a Campus Network," IEEE ICCCT, 2025. DOI: 10.1109/ICCCT63501.2025.11019580.
9. "Unauthorized Access Detection System Using Machine Learning with Honeypot Integration," IEEE ICSTSDG, 2024. DOI: 10.1109/ICSTSDG61998.2024.11026180.
10. M. Vanhoef and E. Ronen, "Dragonblood: A Security Analysis of WPA3's SAE Handshake," IEEE Symposium on Security and Privacy, 2020. DOI: 10.1109/SP40000.2020.00076.
11. "IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients," IEEE ICON, 2004. DOI: 10.1109/ICON.2004.1409151.
12. "Next Generation IEEE 802.11 Wireless LANs: Current Status and Open Challenges," arXiv preprint, 2021. DOI: 10.48550/arXiv.2109.11770.
13. "Strategic Honeypot Deployment in Ultra-Dense Beyond 5G Networks: A Reinforcement Learning Approach," IEEE Transactions on Emerging Topics in Computing, 2022. DOI: 10.1109/TETC.2022.3184112.
14. "Application and Practice of Wireless LAN Security Enhancement Technology Based on WAPI," IEEE ICICCE, 2023. DOI: 10.1109/ICICCE61720.2023.00013.
15. "Measuring Public Wi-Fi Security Awareness via Captive Portal Connections Using a Microcontroller," IEEE WCNPS, 2024. DOI: 10.1109/WCNPS65035.2024.10814259.