AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 3(2026)

FIREWALL INSTRUCTION DETECTION SYSTEM AND MONITORING SYSTEM

[1] Dr.B Ravi Kumar, [2] P Bhanu Chander, [3]B Vamshi, [4]N Manoj
[1]Associate Professor, [234]Students
Department of Computer Science and Engineering,
Siddhartha Institute of Technology and Sciences, Narapally, Korremula Road,
Ghatkesar, Medchal-Malkajgiri, Hyderabad, Telangana - 500088. INDIA
dr.brkou@siddhartha.org.in, 23TQ1A6210@siddhartha.co.in,
23TQ1A6228@siddhartha.co.in, 23TQ1A6220@siddhartha.co.in

Abstract

Firewalls are an important component of network security because they control and monitor traffic flowing between trusted and untrusted network environments. With the increasing number of network services, devices, and applications, manually monitoring firewall activity can become difficult. Suspicious traffic patterns, repeated connection attempts, policy violations, and abnormal network behavior may be overlooked without an effective monitoring and detection mechanism.

The proposed Firewall Instruction Detection System and Monitoring System is designed as a defensive platform for monitoring firewall events and identifying potentially suspicious or unauthorized network activity. The system collects permitted firewall logs and analyzes information such as source and destination addresses, ports, protocols, timestamps, connection status, and rule actions. The collected information is processed using predefined security rules and detection criteria.

The detection engine analyzes firewall events to identify patterns that may indicate suspicious activity, such as repeated denied connections, unusual traffic volumes, policy violations, or unexpected access attempts. Detected events can be categorized according to severity and assigned appropriate risk levels. This helps security administrators focus their attention on events that require further investigation.

A centralized dashboard provides security teams with a visual representation of firewall activity, including allowed and blocked traffic, detected events, source and destination information, protocol distribution, and risk trends. The system can maintain historical firewall records and provide alerts for important events. It can also generate structured security reports containing detection results, event information, risk classification, and recommended defensive actions.

The primary objective of the system is to improve firewall visibility, event detection, monitoring, and security analysis. By combining firewall-log collection, rule-based detection, event correlation, risk assessment, visualization, alerting, and reporting, the platform provides a centralized defensive monitoring solution.

I. Introduction

Modern organizations depend heavily on computer networks for communication, applications, databases, cloud services, and business operations. As network infrastructure becomes larger and more complex, organizations face an increasing

number of security threats. Unauthorized connection attempts, abnormal traffic, configuration errors, and policy violations can create security risks. Firewalls provide an important security layer by controlling network traffic according to predefined security policies.

A firewall typically evaluates network connections based on rules involving addresses, ports, protocols, interfaces, and other traffic characteristics. Depending on the configured policy, traffic can be allowed, denied, or logged for further analysis. Although firewall rules provide an important preventive mechanism, the large volume of generated events can make manual monitoring difficult for security administrators.

Firewall monitoring involves collecting and analyzing firewall events to understand network activity and identify potentially suspicious behavior. Repeated blocked connections, unusual traffic patterns, unexpected access attempts, and changes in firewall behavior can provide useful security indicators. Effective monitoring can therefore help administrators investigate potential security incidents and verify whether firewall policies are operating as intended.

The proposed system provides a centralized platform for collecting and analyzing authorized firewall events. It processes firewall logs and applies predefined detection rules to identify suspicious activity. The platform can classify events according to severity, correlate related events, and provide security alerts to authorized administrators. A dashboard can provide real-time or near-real-time visibility into network traffic and firewall decisions.

The main objective of the proposed system is to improve network security monitoring by providing a structured mechanism for firewall event analysis. It helps administrators understand traffic behavior, identify potential policy violations, prioritize security events, and maintain historical records. By combining monitoring, detection, analytics, and reporting, the system can support a more effective defensive security-management process.

II. Literature Survey

Firewall technology has been extensively studied as a fundamental component of network security. Traditional firewalls primarily focus on controlling network traffic according to predefined security policies. They can restrict connections based on parameters such as source address, destination address, port, protocol, and network interface. Although these mechanisms provide important preventive protection, they require appropriate configuration and continuous monitoring.

Network intrusion detection research has investigated methods for identifying suspicious traffic and abnormal network behavior. Signature-based approaches compare observed events with known patterns, while anomaly-based approaches attempt to identify deviations from expected behavior. Signature-based detection can provide efficient identification of known patterns, whereas anomaly detection may help identify unusual activity that does not exactly match predefined signatures.

Firewall log analysis is another important area of cybersecurity research. Firewall logs can contain information about allowed and denied connections, source and destination

addresses, ports, protocols, timestamps, and rule actions. Analyzing this information can help security teams understand network activity and identify recurring patterns. However, large organizations can generate substantial volumes of log data, making automated processing increasingly important.

Security Information and Event Management systems provide centralized mechanisms for collecting and correlating security events from different infrastructure components. Firewall logs can be integrated with authentication events, endpoint alerts, server logs, and other security information. Correlation provides additional context and can help security analysts identify relationships between individual events.

Machine-learning and behavioral-analysis approaches have also been explored for network-security monitoring. These approaches can examine traffic characteristics and event patterns to identify potentially abnormal behavior. However, machine-learning-based systems require suitable training data, regular model maintenance, and appropriate methods for reducing false positives. Explainability is also important because security analysts need to understand why an event was classified as suspicious.

Existing firewall-monitoring and intrusion-detection platforms demonstrate the value of centralized logging, event analysis, alerting, visualization, and reporting. However, organizations may still require multiple systems to manage firewall policies, analyze logs, correlate events, and generate reports.

III. System Analysis

System analysis for the proposed firewall monitoring platform focuses on identifying the requirements for effective defensive event detection. The system should provide authenticated access to authorized network administrators and security analysts. It should collect permitted firewall logs and security events from configured firewall sources. The collection layer should normalize events from different firewall formats into a common structure. The detection engine should analyze events using predefined security rules and configurable detection criteria. Suspicious events should be identified based on characteristics such as repeated denials, unusual traffic, or policy violations. The system should correlate related events to provide additional context for security investigation. A risk-assessment module should classify detected events according to severity and potential impact. The database should securely maintain firewall events, alerts, findings, and historical records. A dashboard should display traffic statistics, blocked events, detected threats, and risk trends. Alerting mechanisms should notify authorized personnel about important security events. Finally, the reporting module should generate structured firewall security-monitoring reports.

Existing System

Traditional firewall monitoring commonly depends on firewall administration consoles, log viewers, network-monitoring tools, and separate intrusion-detection systems. Administrators may manually inspect firewall logs to identify unusual traffic and repeated blocked connections. Large networks can generate thousands or millions of firewall events, making manual analysis impractical. Different firewall products

may also generate logs in different formats. Security teams may therefore require additional tools to normalize and correlate events. Basic firewall interfaces may provide limited historical analysis and visualization. Risk classification can also require manual interpretation of individual events. Security analysts may need to switch between multiple systems to investigate suspicious traffic. Alert configurations can vary between firewall products and may generate excessive notifications. Report generation may require manual collection of statistics and findings. These limitations can reduce monitoring efficiency and delay investigation of important security events. A centralized firewall monitoring platform can address these challenges through automated collection, analysis, correlation, visualization, and reporting.

Disadvantages of Existing System

- Large volumes of firewall logs are difficult to analyze manually.
- Different firewall products may use different log formats.
- Limited centralized event correlation.
- Manual investigation can consume significant time.
- Excessive alerts can create alert fatigue.
- Basic firewall consoles may provide limited analytics.
- Historical event comparison can be difficult.
- Risk classification may require manual analysis.
- Multiple security tools may be required for complete monitoring.

Proposed System

The proposed Firewall Instruction Detection and Monitoring System provides a centralized platform for analyzing authorized firewall events and identifying potentially suspicious activity. The system collects permitted firewall logs from configured network-security sources. A preprocessing module validates, filters, and normalizes events into a common format. The detection engine evaluates firewall events using predefined security rules and configurable monitoring criteria. Suspicious patterns such as repeated blocked connections, unusual traffic behavior, unexpected access attempts, and policy violations can be flagged for investigation. An event-correlation module groups related events to provide additional security context. The risk-assessment engine evaluates detected events and assigns appropriate severity and priority levels. A centralized database stores firewall events, alerts, findings, and historical monitoring information. The dashboard presents traffic statistics, allowed and blocked events, detected suspicious activity, and risk distributions. Authorized analysts can investigate individual events and review related information. The alerting module can notify security personnel when important events are detected. The reporting module generates structured security reports containing event details, risk classifications, trends, and recommended defensive actions. Overall, the proposed platform provides a systematic workflow for firewall monitoring, event detection, analysis, alerting, and reporting.

Advantages of Proposed System

- Provides centralized firewall-event monitoring.
- Automates processing of large volumes of firewall logs.
- Supports configurable detection rules.

- Identifies potentially suspicious traffic patterns.
- Provides event correlation for better investigation.
- Supports risk-based event prioritization.
- Provides centralized dashboards and analytics.
- Maintains historical firewall-event records.
- Can be extended with anomaly detection and machine-learning techniques.

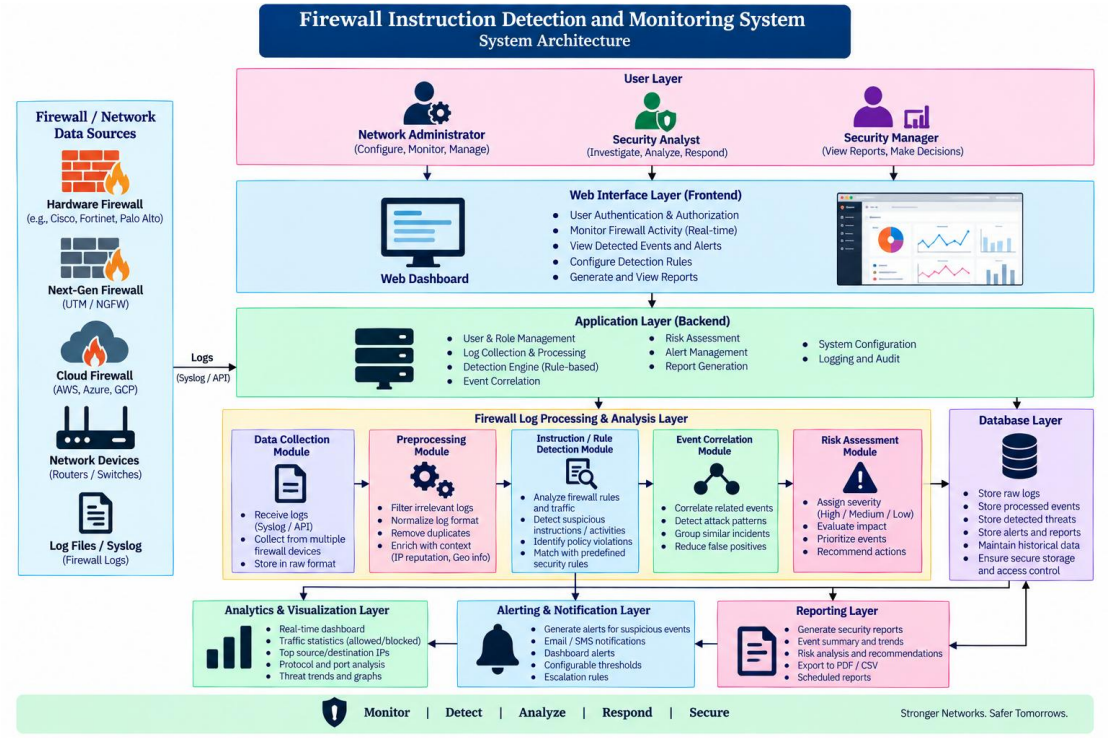
IV. Methodology

The methodology begins with authentication of the authorized network administrator or security analyst. The administrator configures the permitted firewall-log sources and monitoring parameters. Firewall events are collected from approved network-security devices and transferred to the monitoring platform. The preprocessing module validates and normalizes the collected events. Irrelevant or duplicate records can be filtered according to configured policies. The detection engine analyzes events against predefined firewall-security rules and detection criteria. Potentially suspicious events are classified according to their observed characteristics. Related events are correlated using information such as source, destination, timestamp, port, protocol, and rule action. The risk engine evaluates the detected activity and assigns an appropriate severity level. Important events can generate alerts for authorized security personnel. The database stores events, alerts, analysis results, and historical records for future investigation. The dashboard presents firewall activity, blocked traffic, detected events, and risk trends. Finally, the reporting module generates structured security reports containing findings and recommended defensive measures.

System Architecture

The system architecture consists of multiple interconnected layers designed to provide centralized firewall security monitoring and event detection. The User Layer contains authorized network administrators, security analysts, and security managers who access the platform according to their assigned roles. The Web Interface Layer provides authentication, monitoring configuration, dashboards, event investigation, alert management, and report access. The Application Layer manages users, roles, monitoring workflows, configuration, validation, logging, and communication between system components. The Firewall Data Collection Layer receives permitted logs and security events from configured firewall devices and monitoring sources. The Preprocessing Layer validates, filters, normalizes, and enriches firewall events before analysis. The Instruction/Rule Detection Layer evaluates events using predefined security rules and configurable detection criteria to identify potentially suspicious activity. The Event Correlation Layer groups related events to provide additional context for investigation. The Risk Assessment Layer evaluates detected events according to severity, potential impact, and organizational priorities. The Database Layer securely stores firewall events, alerts, detection results, risk scores, configurations, and historical records. The Analytics and Visualization Layer presents allowed and blocked traffic, event trends, protocol distributions, detected activity, and risk statistics. The Alerting Layer generates notifications for important security events and high-priority findings. The Reporting Layer generates structured firewall monitoring and security-assessment reports containing event summaries, findings, risk classifications, and recommendations. Access control, audit logging, secure data handling, and retention policies protect the monitoring platform. The overall

architecture provides a controlled flow from firewall-event collection through preprocessing, rule-based detection, event correlation, risk assessment, visualization, alerting, and reporting.



V. Result and Output

VI. Conclusion

The Firewall Instruction Detection and Monitoring System provides a centralized and structured approach for monitoring firewall activity and identifying potentially suspicious network events. By collecting firewall logs and analyzing information such as source and destination addresses, ports, protocols, timestamps, and rule actions, the system helps security administrators gain better visibility into network traffic.

The proposed system improves traditional firewall monitoring by automating log processing, applying configurable detection rules, correlating related events, and assigning risk levels. The centralized dashboard provides clear information about allowed and blocked traffic, suspicious events, alerts, firewall-rule activity, and security trends, making investigation more efficient.

The system also supports historical event storage, alert generation, analytics, and security reporting. These capabilities help administrators identify recurring patterns, investigate important events, evaluate firewall-policy effectiveness, and prioritize security incidents that require attention.

Overall, the Firewall Instruction Detection and Monitoring System can serve as a useful platform for network security monitoring, cybersecurity education, firewall administration, and authorized security operations. Future enhancements can include machine-learning-based anomaly detection, automated threat correlation, SIEM integration, improved real-time alerting, and advanced behavioral analysis. When combined with properly configured firewall policies and other security controls, the system can contribute to stronger network protection and faster detection of suspicious activity.

References

[1] Kumar, R. D., Prudhviraj, G., Vijay, K., Kumar, P. S., & Plugmann, P. (2024). Exploring COVID-19 through intensive investigation with supervised machine learning algorithm. In Handbook of Artificial Intelligence and Wearables (pp. 145-158). CRC Press.
[2] Swathi, B., Vijay, K., Sushanth Babu, M., & Dinesh Kumar, R. (2024, November). Machine Learning Techniques in Cloud Based Intrusion Detection. In The International Conference on Artificial Intelligence and Smart Environment (pp. 557-564). Cham: Springer Nature Switzerland.
[3] Sv satyakrishna, shirisha rangu ,bhargavi nalacheruve.(2024) Prospective investigation on colorectal cancer with SMOTE on machine learning Algorithm
[4] Dr.G.Vishnu Murthy, BhargaviNalacheruve 1Professor, Department of computer Science & engineering, Anurag University, TS, India. 2Student, Department of computer Science & engineering, Anurag University, TS, India.
[5] V. N. S. Manaswini, K. K, C. Nigam, S. S. Ali, R. Niranjana, and Suman, “Real-Time Object Detection in Drone Surveillance Using YOLOv5,” in Proc. 2025 3rd Int. Conf. IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2025, pp. 1–6, doi: 10.1109/ICICAT68430.2025.11414670.
[6] B. Soundarya, V. N. S. Manaswini, M. Ayyakrishnan, R. D. Kumar, “Contextual Analysis of Big Data Analytics in Intelligent Transportation Frameworks,” in

Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment, Lecture Notes in Networks and Systems, vol. 1353, Cham: Springer, 2025, doi: 10.1007/978-3-031-88304-0_79.
[7] R. D. Kumar, V. N. S.Manaswini, "Applications of blockchain in smart cities: detecting fake documents from land records using blockchain technology," in Blockchain for Smart Cities, Elsevier, 2021, pp. 105–117, doi: 10.1016/B978-0-12-824446-3.00017-X.
[8] Tejavath Veeramma, Badarla Anil, Guguloth Ravinder, "An advanced movie recommender using collaborative filtering and sentiment analysis," International Research Journal of Modernization in Engineering Technology and Science, vol. 7, no. 7, July 2025, doi: 10.56726/IRJMETS81618.
[9] Ravi Kumar Banoth, Ramana Murthy B V, "Automatic crop recommendation system using LightGBM and decision tree machine learning models," Journal of Machine and Computing, vol. 5, no. 1, pp. 343, Jan. 2025, doi: 10.53759/7669/jmc202505026.
[10] Ravi Kumar Banoth, Dr. B.V. Ramana Murthy, "Smart agriculture through IoT and machine learning for analyzing carbon footprints," in Proc. Int. Conf. Computer Science and Communication Engineering (ICCSCE), Apr. 2025.
[11] Ravi Kumar Banoth, B. V. Ramana Murthy, "Soil image classification using transfer learning approach: MobileNetV2 with CNN," SN Computer Science, vol. 5, art. no. 199, 2024, doi: 10.1007/s42979-023-02500-x.