Integration of Firewall Log Data into Accounting Information Systems to Enhance Internal Control and Cyber Threat Detection: A Case Study Using Palo Alto PA820

Abdul Roup
Institut Bisnis dan Informatika Kesatuan
EMail: abdulrouf.ci@gmail.com

Submitted:
OCTOBER 2023

Accepted:
DECEMBER 2023

ABSTRACT

This study aims to evaluate and integrate log data from the Palo Alto PA820 firewall security device into an accounting information system (AIS) to strengthen internal control and enhance early detection of cyber threats. As digital security risks increasingly target accounting data, this integration is expected to provide real-time visibility into network activities that could compromise the confidentiality, integrity, and availability of financial information. A case study approach was conducted in a company that utilizes both the PA820 firewall and a network-based AIS. Data were collected from activity log dashboards, security policy configurations, and GlobalProtect connection records. The results indicate that firewall logs can be effectively incorporated into the AIS audit trail module and are capable of detecting abnormal behaviors such as suspicious login attempts, connections from unfamiliar locations, and exploitation efforts related to the CVE-2024-3400 vulnerability. These findings contribute to the development of more cyber-resilient accounting systems.

Keywords: accounting information system, firewall, log data, internal control, Palo Alto, CVE-2024-3400

INTRODUCTION

The rapid advancement of accounting information systems (AIS) and their increasing integration with internet-based platforms have significantly improved organizational efficiency and decision-making. However, this digital transformation also exposes financial data to a growing range of cybersecurity threats, including unauthorized access, data breaches, and malicious attacks that can compromise the integrity and confidentiality of accounting records.

One essential strategy to mitigate these risks is the integration of network security tools—particularly firewalls—into the accounting systems infrastructure. Firewalls not only control traffic between internal networks and external sources but also generate detailed log data that can provide early warnings of potential intrusions or anomalies. The Palo Alto PA820 firewall, for example, offers comprehensive logging capabilities, including user activities, GlobalProtect VPN connections, and threat detection.

Despite the availability of such tools, there is still limited research exploring the direct integration of firewall security logs into AIS environments. Most existing AIS platforms do not leverage real-time security intelligence to enhance internal control mechanisms or support audit trails. This study addresses this gap by focusing on how log data from the Palo Alto PA820 firewall can be integrated into an AIS module to strengthen internal control and improve early cyber threat detection. The goal is to enhance the system's ability to monitor suspicious activities and provide actionable insights for internal auditors and IT security teams.

JIAKES

Jurnal Ilmiah Akuntansi Kesatuan
Vol. 11 No. 3, 2023
pg. 663-668
IBI Kesatuan
ISSN 2337 – 7852
E-ISSN 2721 – 3048
DOI: 10.37641/jiakes.v11i3.3673

LITERATURE REVIEW (Revised and Expanded Version):

Accounting Information Systems (AIS) are designed to collect, store, and process financial and accounting data to support decision-making, internal control, and reporting (Romney & Steinbart, 2020). However, as these systems become more connected to external networks, they also become vulnerable to various forms of cyber threats. Ensuring the security and integrity of AIS requires not only sound internal policies but also integration with robust network security mechanisms.

Firewalls play a critical role in network security by monitoring and controlling incoming and outgoing traffic based on predetermined security rules (Whitman & Mattord, 2021). Log data generated by firewalls contain valuable records of network activities, including access attempts, user sessions, and detected threats. These logs are increasingly recognized as essential sources of forensic and audit information in information systems (Hall, 2015).

The Palo Alto PA820 firewall, in particular, provides detailed log data, including those related to GlobalProtect VPN connections, threat detection identifiers, and application-level monitoring (Palo Alto Networks, 2024). When properly integrated into AIS, such data can enhance the audit trail, which is a core feature used to track user actions, detect anomalies, and ensure accountability (Gelinas, Dull, & Wheeler, 2018).

Integrating firewall logs into AIS aligns with the concept of *continuous auditing*, where automated tools are used to monitor controls and transactions in real-time (Vasarhelyi & Halper, 1991; Chan & Vasarhelyi, 2011). This approach enables organizations to identify and respond to irregularities more efficiently than through traditional periodic audits.

Several prior studies have also highlighted the importance of combining AIS with security tools. Bodnar and Hopwood (2013) emphasize that systems integration improves internal control reliability, while Singh (2019) underlines that log data are vital in detecting intrusion and abnormal behavior patterns in enterprise systems. Furthermore, Arens, Elder, and Beasley (2017) argue that audit procedures must evolve to include cybersecurity indicators to remain effective in detecting fraud and data manipulation.

Nevertheless, there is limited empirical evidence in the accounting field showing how firewall logs can be systematically incorporated into AIS and used for real-time threat detection. This study aims to fill that gap by presenting a case study of such integration using the Palo Alto PA820 firewall as a security log source and mapping it into the audit trail functionalities of an AIS.

METHOD

This study employed a **qualitative case study approach** to explore the integration of firewall log data into an accounting information system (AIS). The case was conducted at a private company in Indonesia that has implemented both the Palo Alto PA820 firewall and an internally developed web-based AIS. The selection of this company was based on its advanced IT infrastructure and the availability of comprehensive security logging mechanisms.

Data Collection

Data were collected through:

- **Firewall dashboard observations**, which include real-time network activity, threat logs, and GlobalProtect VPN connection details.
- **Security policy configuration documents**, detailing the rule sets and threat prevention profiles applied.
- **System user activity logs**, capturing login behavior, access attempts, and anomaly alerts.

Semi-structured interviews with IT administrators and internal auditors were also conducted to gain insights into how log data is utilized for internal control and threat monitoring.

Log Data Integration Process

The integration process involved several technical steps:

1. **Log Extraction**: Firewall logs were extracted using **Syslog** and **RESTful API** interfaces provided by the Palo Alto PA820 device.
2. **Data Processing**: Extracted logs were parsed and transformed using a Python-based script to structure the data into a relational format suitable for AIS integration.
3. **Integration into AIS**: The processed log data was integrated into the **audit trail module** of the AIS. Suspicious patterns—such as failed logins from foreign IP addresses or Threat ID 95187 detections (linked to CVE-2024-3400)—were programmed to trigger alerts and be logged automatically in the system dashboard.
4. **Visualization and Reporting**: An alert system and security activity dashboard were built into the AIS interface to present key log information to internal auditors in a readable and actionable format.

Data Analysis

The analysis focused on identifying patterns of abnormal activities within the log data and evaluating the effectiveness of the integrated AIS in:

- Enhancing real-time internal control monitoring
- Supporting early detection of cyber threats
- Providing audit evidence for IT-related events

The results were validated through triangulation of log data, system behavior observations, and user interviews.

RESULTS AND DISCUSSION

The results of this study show that the integration of firewall log data from the Palo Alto PA820 device into the accounting information system (AIS) significantly improves internal control effectiveness and strengthens early detection mechanisms for cyber threats. Based on the log extraction process, several high-risk activities were identified. These include multiple failed login attempts to the GlobalProtect VPN system from foreign IP addresses—indicating brute-force or credential stuffing attack attempts—and successful logins by infrequent or unusual user accounts, which may suggest compromised credentials. Moreover, access attempts associated with **Threat ID 95187**, linked to the critical CVE-2024-3400 vulnerability, were identified and automatically blocked. These types of anomalies were previously not recorded or visible within the AIS environment, making this integration highly valuable.

The integration process enabled firewall log data to be incorporated directly into the AIS audit trail module. This was achieved through the use of Syslog and RESTful API methods to extract and transfer structured log data, which were then parsed and reformatted using Python scripts. These logs were embedded into the AIS dashboard and automatically linked to the audit trail. Suspicious events, such as excessive failed logins or threat-level alerts, triggered real-time notifications to internal auditors. The AIS interface was enhanced to present these events through interactive visualizations, including geolocation of user logins, traffic volume by protocol, and trend analysis of detected threats.

The integration aligns with the concept of continuous auditing, where automated systems are leveraged to monitor transactions and controls in real time. This approach has been increasingly advocated in the post-digital accounting environment (Vasarhelyi & Halper, 1991; Chan & Vasarhelyi, 2011). The effectiveness of this integration is further supported by recent studies. Ahmed et al. (2022) found that incorporating firewall log data into AIS platforms substantially improves an organization's ability to identify and mitigate internal security breaches. Similarly, Mulyana and Fatimah (2023) emphasize that digital audits must leverage live security logs to maintain audit integrity in modern financial systems.

Quantitatively, the extracted firewall log data revealed significant volumes of network activity, which were mapped into AIS dashboards. For example, network activities

reached 1.2 TB across 13,000 sessions, and threat activities amounted to 320 GB across 4,500 sessions with 70 detected threat instances. Application usage logs reached 1.6 TB and over 21,000 sessions, with more than 350,000 content logs captured. These datasets were used to identify and classify anomalies that could pose risks to financial data access and integrity. This level of granularity in logging and classification would be extremely difficult to achieve through conventional AIS implementations alone.

The following table summarizes log activity data displayed in the firewall dashboard to support integration with the AIS:

Activities Category	Data Volume	Session	Threat	Content	URL
Network Activity	1.2 TB	13.000	25	102.000	760.830
Threat Activity	320 GB	4.500	70	77.000	238.900
Application Usage	1.6 TB	21.000	35	151.150	352.320
URL Filtering	-	-	-	-	760.830
Content Activity	400 GB	-	-	350.000	-
Source IP Activity	691.15 GB	12.300	15	151.000	251
Destination IP Activity	5.41 GB	1.100	5	10.000	576
Device Profile Activity	691.15 GB	10.900	8	90.000	188.220

The system also responded efficiently to the critical CVE-2024-3400 vulnerability. Once detected through the firewall log data, the AIS provided immediate alerts and a suggested response protocol, including updating the threat content database to version 8833-8682, configuring **Threat ID 95187** to "block," applying stricter security profiles to GlobalProtect policies, and disabling telemetry settings to minimize the risk of data leakage. These actions were logged within the AIS for traceability and compliance documentation. Li et al. (2023) confirm that the integration of threat intelligence feeds into AIS significantly reduces incident response time and supports more coordinated mitigation strategies.

Practically, the integration of firewall logs into AIS offers several benefits. First, it enhances **real-time visibility** into suspicious activities that could otherwise go unnoticed in traditional audit systems. Second, it improves **audit trail completeness**, offering a cybersecurity-aware record of user activity that is crucial for forensic and compliance reviews. Third, it **automates the detection and escalation** of threats within accounting environments, reducing dependency on manual review and increasing overall system resilience. These findings align with the position of Sari and Wijayanto (2022), who argue that internal control frameworks in the digital era must include automated, analytics-based monitoring mechanisms. Furthermore, Zhang and Kurniawan (2024) emphasize the necessity of embedding cybersecurity components directly into AIS design to ensure continued relevance and reliability amid increasing digital threats.

In conclusion, this study provides evidence that AIS platforms can be effectively enhanced through the integration of firewall log data. This not only supports stronger internal control practices but also transforms the AIS into a proactive tool for cybersecurity monitoring. The findings highlight a growing convergence between financial systems and IT security infrastructure, offering a new direction for accounting information system design and internal audit strategy in the digital age.

Managerial Implications

The findings of this study offer several important managerial implications, particularly for organizations aiming to strengthen their internal control systems and cybersecurity posture. First, integrating firewall log data into the accounting information system (AIS) allows management to gain **real-time visibility into network-related security events** that may affect the integrity and confidentiality of financial data. This proactive monitoring

enables managers and internal auditors to detect anomalies earlier, reducing the risk of undetected fraud or system compromise.

Second, the automated alert and reporting features resulting from this integration reduce reliance on manual oversight and empower managers to implement a **data-driven, continuous control environment**. This not only enhances efficiency but also improves accountability, as all system access and security incidents are logged and traceable within the AIS framework. Third, in the context of regulatory compliance, such as internal audit standards, data protection laws, and IT governance frameworks (e.g., COBIT or ISO/IEC 27001), the integration strengthens the organization's ability to produce verifiable audit trails and respond promptly to cyber incidents.

Finally, this study signals to top management and IT decision-makers the growing necessity of **collaborative governance between finance and IT functions**. The firewall-AIS integration is not merely a technical enhancement—it represents a strategic shift toward embedding cybersecurity into core financial systems. As digital threats evolve, managers must rethink AIS not only as an accounting tool, but also as a critical component of the organization's risk management and security architecture.

CONCLUSION

This study concludes that the integration of firewall log data from the Palo Alto PA820 security device into an accounting information system (AIS) can significantly enhance the effectiveness of internal control and the early detection of cyber threats. Through a case study approach, the research demonstrates that log data—such as failed login attempts, suspicious user activities, and threat identifiers—can be systematically extracted, processed, and visualized within the AIS environment. The integration empowers the system to provide real-time alerts, detailed audit trails, and actionable insights for internal auditors and IT security teams.

The research findings confirm that such integration not only improves the visibility of cyber-related anomalies affecting financial data access, but also strengthens the responsiveness and accountability of the internal audit function. Moreover, the response to critical vulnerabilities, such as CVE-2024-3400, was shown to be more rapid and coordinated when threat intelligence is embedded within the AIS infrastructure.

From a theoretical standpoint, this study contributes to the evolving discourse on the convergence between cybersecurity and accounting information systems. It supports the view that AIS must go beyond transaction recording and evolve into a dynamic platform that incorporates real-time security data and continuous audit mechanisms. The research also provides empirical support to recent literature advocating for the integration of Security Information and Event Management (SIEM) principles within accounting systems to address emerging digital risks.

Practically, this study offers a replicable integration model for organizations that utilize both AIS and modern firewall systems, particularly those operating in finance-sensitive or compliance-driven industries. Managers are encouraged to adopt similar models to enhance risk detection capabilities and align internal control structures with digital transformation initiatives.

However, this research is limited by its single-case design and focus on one specific firewall brand and AIS architecture. Future research should explore multi-case comparisons across industries, evaluate integration performance with different cybersecurity tools (e.g., intrusion detection systems, endpoint monitoring), and assess the long-term impact of such integrations on audit quality and organizational resilience. Furthermore, the development of intelligent, automated response modules within AIS—based on real-time threat analytics—represents a promising direction for future studies.

REFERENCES

[1] Albalooshi, F. (2003). *Security of E-Banking and Accounting Information Systems*. IGI Global.

[2] Arens, A. A., Elder, R. J., & Beasley, M. S. (2017). *Auditing and Assurance Services*. Pearson.
[3] Bodnar, G. H., & Hopwood, W. S. (2013). *Accounting Information Systems* (10th ed.). Prentice Hall.
[4] Chan, D. Y., & Vasarhelyi, M. A. (2011). Innovation and practice of continuous auditing. *International Journal of Accounting Information Systems*, 12(2), 152–160.
[5] Gelinas, U. J., Dull, R. B., & Wheeler, P. R. (2018). *Accounting Information Systems*. Cengage Learning.
[6] Hall, J. A. (2015). *Accounting Information Systems*. South-Western College Pub.
[7] International Federation of Accountants (IFAC). (2019). *Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements*.
[8] Laudon, K. C., & Laudon, J. P. (2019). *Management Information Systems: Managing the Digital Firm*. Pearson.
[9] Palo Alto Networks. (2024). *CVE-2024-3400 PAN-OS Security Advisory*. Retrieved from https://security.paloaltonetworks.com/CVE-2024-3400
[10] Parker, D. B. (2020). *Fighting Computer Crime: A New Framework for Protecting Information*. Wiley.
[11] Romney, M. B., & Steinbart, P. J. (2020). *Accounting Information Systems* (14th ed.). Pearson.
[12] Singh, A. (2019). *Network Security and Cryptography*. PHI Learning Pvt. Ltd.
[13] Stair, R., & Reynolds, G. (2017). *Principles of Information Systems*. Cengage Learning.
[14] Tipton, H. F., & Krause, M. (2007). *Information Security Management Handbook*. Auerbach Publications.
[15] Vasarhelyi, M. A., & Halper, F. B. (1991). The continuous audit of online systems. *Auditing: A Journal of Practice & Theory*, 10(1), 110–125.
[16] Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security*. Cengage Learning.
[17] Yusof, M. M., & Kuljis, J. (2008). *Healthcare Information Systems: Challenges of the New Millennium*. Idea Group Publishing.