Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th June 2025. Vol. 4. No. 3; e-ISSN: 2808-4519

Analysis of Firewall Policy Effectiveness in Filtering Network Traffic Using Elastic Stack

Dewa Ayu Rai Sudarma Putri[1]*, Lilik Widyawati[2], Husain[3], I Made Yadi Dharma[4]

[1,2,3,4] *Universitas Bumigora*
2101020047@universitasbumigora.ac.id[1]*, lilikwidya@universitasbumigora.ac.id[2], husain@universitasbumigora.ac.id[3], yadi_dharma@universitasbumigora.ac.id[4]

Abstract

This research is motivated by the increasing importance of network security in the digital age, particularly for organizations like Company X, given the rise in cyber threats that compromise data and system integrity. The study aims to analyze the effectiveness of the firewall policy in filtering network traffic using the Elastic Stack and to provide recommendations for improvement. The research methodology involves processing and analyzing firewall log data over one month using the Elastic Stack. The results demonstrate that the Elastic Stack successfully identified normal and suspicious traffic patterns, as well as the effectiveness of the firewall in blocking threats. The research also found connections with an "incomplete" status, indicating potential network communication issues. It is concluded that the firewall policy at Company X is generally effective, but there is room for improvement. This research recommends adjusting filtering rules, improving network segmentation, and implementing an intrusion detection system.

Keywords: *Firewall, Elastic Stack, Network Traffic, Network Security, Log Analysis*

1. Introduction

In the era of digital transformation, network security has become one of the greatest challenges for organizations, both in the private and public sectors. With the increasing complexity of technology, the number of cyber threats such as Distributed Denial of Service (DDoS) attacks, phishing, malware, and ransomware continues to rise[1]. These attacks not only cause financial losses but also threaten the confidentiality of critical data, which often becomes a strategic target for cyber attackers.
The firewall, as a core component of network security systems, functions to control the flow of data entering and leaving the network by filtering traffic based on predefined policies[2]. Appropriate firewall policies are essential to ensure that only legitimate and necessary traffic is allowed to access the network, while harmful traffic can be blocked. However, the implemented firewall policies are not always optimal. Overly strict policies can hinder communication and network operations, whereas overly lenient policies may create vulnerabilities that cyber attackers can exploit[3]. Therefore, it is crucial to evaluate the implemented firewall policies to ensure their effectiveness in securing the network without disrupting operational continuity.

Currently, the firewall policies implemented in Company X function to maintain network security. However, the effectiveness of these policies in filtering network traffic and addressing various cyber threats still requires more in-depth analysis. With the increasing sophistication of cyberattacks[4], it is essential for Company X to evaluate and improve its firewall policies to minimize potential threats to the information systems they manage.

One way to evaluate firewall policies is by using log data generated by the firewall itself[5]. This log data records every activity on the firewall, including accepted and denied traffic. However, processing and analyzing large and complex log data often presents a significant challenge[6]. Therefore, an effective and efficient tool is needed to process such log data. Elastic Stack is one of the most suitable solutions for processing, analyzing, and visualizing log data quickly and accurately[1]. Elastic Stack has the capability to filter and index large volumes of log data, enabling in-depth analysis of network traffic patterns and detecting anomalies that may indicate potential threats[5].
Through this study, an analysis will be conducted on the effectiveness of the firewall policies implemented in Company X by utilizing Elastic Stack to process the firewall's log data. This method is expected to identify traffic patterns that do not comply with the implemented firewall policies and to detect potential gaps that could be exploited by malicious actors. Furthermore, this research will provide recommendations to improve firewall policies to enhance their effectiveness in securing the network and ensuring smooth network operations at Company X.

2. Research Methodology

The research methodology used consists of a literature review and the application of an approach based on specific stages of the Network Development Life Cycle (NDLC). This study specifically adopts the stages of firewall log data collection, analysis, and policy evaluation, using relevant tools and methods to achieve the research objectives.

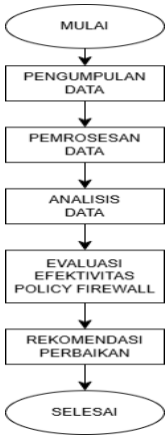

Fig. 1: Research Flowchart

2.1. Data Collection

The firewall log data collection phase aims to provide a comprehensive understanding of network traffic within Company X. The collected data will serve as the foundation for evaluating the effectiveness of the implemented firewall policies. Log data will be gathered over a one-month period, from October 1 to October 31, 2024. This timeframe was selected to capture variations in traffic patterns that may occur throughout the month, ensuring a more representative and comprehensive dataset.

The log data will be extracted directly from the active firewall device deployed at Company X. The specific type of firewall and its logging configuration will be documented in detail. If a Palo Alto Networks firewall is used, syslog and log forwarding configurations will be applied to facilitate data collection. The data collection process is designed to be non-intrusive and will not interfere with ongoing network operations. The logs will contain detailed information about each network connection traversing the firewall, which is essential for identifying traffic characteristics, detecting potential threats, and evaluating the effectiveness of firewall policies.

2.2. Initial Network Topology

The data collection process will adhere strictly to Company X security protocols. Access to firewall devices will be restricted to authorized personnel only, and log transmission to the analysis server will utilize secure, encrypted channels. Structured collection will involve defining specific rules to determine which source log files should be processed.

The network topology at Company X highlights significant changes introduced following the implementation of updated firewall policies. These changes were crucial in enhancing the overall security posture of the network. Prior to this implementation, the network operated under a highly permissive configuration, commonly referred to as a “Default Any-to-Any” rule. This configuration allowed unrestricted traffic, making it difficult to distinguish between legitimate and suspicious activity. Consequently, the generated log data was excessively voluminous and lacked focus, posing challenges for administrators in identifying security threats and responding promptly to incidents.

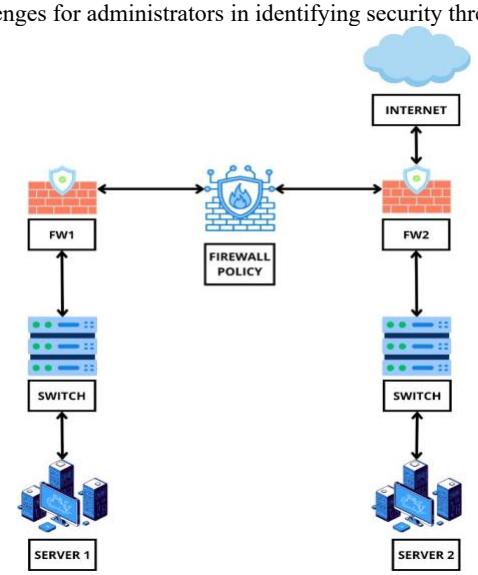

Fig. 2: Initial Network Topology

2.3. Data Processing with Elastic Stack

Once the firewall log data has been successfully collected and prepared, the next step is to process the data using the Elastic Stack. The data ingestion process begins with the use of Beats, a lightweight data shipper that collects data directly from the firewall device and forwards it to the Elastic Stack. After being collected by Beats, the data is sent to Logstash for further processing. Logstash serves as a powerful data processing pipeline, allowing for the formatting, filtering, and transformation of data according to the required specifications. Once processed, the data is stored in Elasticsearch, a distributed, open-source search and analytics engine. Elasticsearch organizes the data into structured indices, enabling rapid and efficient querying, aggregation, and analysis of large volumes of log data.

2.4. Data Analysis

After the firewall log data has undergone collection, cleansing, transformation, and storage in Elasticsearch, the analysis phase begins. This stage serves as the core of the research, where meaningful insights are extracted from the structured data. Kibana plays a central role in this phase by enabling the visualization and exploration of log data to uncover patterns, trends, anomalies, and potential indicators of threats that may not be evident in raw data alone.

Table 1: Data Log Tuning Policy

Zone	Source Ip	Dest Ip	Dest Port	Protokol	Application	Outcome	Ket.
	192.18.30.199	192.16.99.31	443	tcp	ssl	success	
	192.18.30.199	192.16.99.31	53	tcp	dns-base	success	
	192.18.30.199	192.16.99.31	53	udp	dns-base	success	
	192.18.30.199	192.16.99.31	443	tcp	ssl	success	
	192.18.30.199	192.16.99.31	443	tcp	incomplete	success	
	192.18.30.199	192.16.99.31	22	tcp	ssh	success	
	192.18.30.199	192.16.99.31	80	tcp	incomplete	success	
	192.18.30.199	192.18.1.14	443	tcp	ssl	success	
	192.18.30.199	192.18.1.14	443	tcp	incomplete	success	
	192.18.30.199	192.18.1.14	22	tcp	ssh	success	
	192.18.30.199	192.18.1.14	80	tcp	incomplete	success	
	192.18.30.199	192.18.16.11	53	udp	dns-base	success	
	192.18.30.199	192.18.16.11	53	tcp	dns-base	success	
	192.18.30.199	192.18.1.15	443	tcp	ssl	success	
	192.18.30.199	192.18.1.15	443	tcp	incomplete	success	
	192.18.30.199	192.18.1.15	22	tcp	ssh	success	
X	192.18.30.198	192.18.1.14	443	tcp	ssl	success	
	192.18.30.198	192.18.1.14	443	tcp	incomplete	success	
	192.18.30.198	192.18.1.14	80	tcp	incomplete	success	
	192.18.30.198	192.18.1.14	22	tcp	incomplete	success	
	192.18.30.198	192.18.16.11	53	udp	dns-base	success	
	192.18.30.198	192.18.16.11	53	tcp	dns-base	success	
	192.18.30.198	192.18.1.15	443	tcp	ssl	success	
	192.18.30.198	192.18.1.15	443	tcp	incomplete	success	
	192.18.30.198	192.18.1.15	80	tcp	incomplete	success	
	192.18.30.198	192.18.1.15	22	tcp	ssh	success	
	192.18.30.198	192.16.99.31	443	tcp	ssl	success	
	192.18.30.198	192.16.99.31	443	tcp	incomplete	success	
	192.18.30.198	192.16.99.31	80	tcp	incomplete	success	
	192.18.30.198	192.16.99.31	22	tcp	ssh	success	
	192.18.30.198	192.18.1.1	22	tcp	ssh	success	
	192.18.30.198	192.16.99.32	443	tcp	ssl	success	
	192.18.30.198	192.18.1.13	22	tcp	ssh	success	
	192.18.30.198	192.18.1.2	22	tcp	ssh	success	

3. Result and Discussion

The results of this study are derived from the analysis of firewall log data comprehensively collected over one month at Company X. The data was then processed and analyzed using Elastic Stack to understand network traffic characteristics and identify anomalies that may

pose security threats. The primary focus was on evaluating the effectiveness of the implemented firewall policies to ensure network security without disrupting operational processes.

Significant changes in the network topology at Company X were observed following the implementation of the new firewall policies. These changes were crucial in enhancing overall network security, replacing the previous overly permissive configuration that allowed unrestricted traffic, making threat identification difficult.

Data processing was carried out using Elastic Stack, starting with data collection via Beats, processing through Logstash, and storage and analysis in Elasticsearch. Data visualization using Kibana facilitated the discovery of patterns, trends, and anomalies that might be overlooked when examining raw data alone.

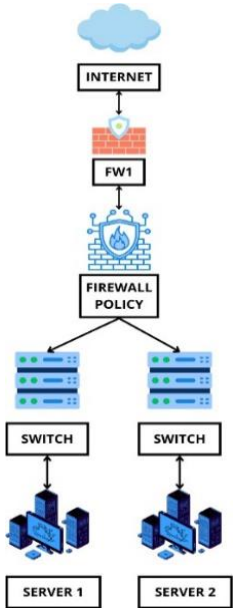

Fig. 3: Network Topology Results After Firewall Policy Implementation

The security evaluation was conducted to ensure the effectiveness of the firewall in protecting the network. This evaluation includes the firewall configuration, which currently shows successful connections for critical applications such as SSL (port 443), DNS (port 53), and SSH (port 22), although some "incomplete" connections indicate potential issues. Firewall policies must align with operational requirements, ensuring that all necessary ports (443, 53, 22, and 80) are allowed according to business needs.

Network segmentation was assessed to ensure that devices with similar functions are grouped together, with inter-segment access controlled by firewall policies. Firewall logs serve as records of traffic activity, where a "success" status indicates that necessary communications are permitted. The log entries include information such as IP addresses, ports, protocols, applications, and connection results, which are valuable for security analysis and performance monitoring.

Firewall policy rules should be tailored based on the log data, such as permitting access to port 443 for SSL and port 53 for DNS, as well as implementing preventive measures against "incomplete" connections. Real-time security monitoring using tools like Elastic Stack enables data analysis to detect anomalies or suspicious activities, allowing for rapid response to security incidents before causing further damage.

Based on the analysis of network traffic, several recommendations are proposed to enhance the effectiveness of firewall policies and overall network security: a comprehensive review and adjustment of firewall policies to ensure alignment with operational needs and identification of the causes behind "incomplete" connections; enhancement of network segmentation by separating devices based on function and implementing role-based access control (RBAC); regular monitoring and analysis of logs using tools such as Elastic Stack to detect anomalies and conducting log audits to identify unusual patterns; strengthening remote access security by using VPNs and implementing two-factor authentication (2FA) for SSH; conducting user training and awareness programs through cybersecurity training and periodic security awareness campaigns; and regular system updates and maintenance, including applying the latest patches and performing routine security assessments such as penetration testing.

4. Conclusion

Based on the results and discussion of this study, it can be concluded that the research successfully evaluated the effectiveness of the firewall policies implemented at Company X in filtering network traffic using Elastic Stack. By collecting and analyzing firewall log data, this study provides a clear understanding of how the existing policies function in protecting the network from threats. Elastic Stack has proven effective in processing, analyzing, and visualizing firewall log data. This capability enables the identification of traffic patterns that do not comply with the applied policies, as well as the detection of anomalies that may indicate potential attacks. The use of this tool offers an advantage in gaining deep insights into network traffic dynamics. The analysis using Elastic Stack helped identify potential security gaps and cyber threats that might have gone undetected previously. These findings indicate that, although the current firewall policies are fairly effective, there is still room for improvement in policy configuration and response to emerging threats. Evaluating firewall policies using this method provides valuable insights for enhancing network security at Company X. This study emphasizes the importance of continuous monitoring and policy adjustment to address the ever-evolving landscape of cyber threats.

References

[1] S. A. Indrarto And A. Basuki, "Penerapan Platform Visualisasi Dan Analisis Trafik Jaringan Menggunakan Elastic Stack," 2022. [Online]. Available: Http://J-Ptiik.Ub.Ac.Id

[2] A. Admi, A. Hakim, And N. Maulana, "Penerapan Elastic Stack Sebagai Tools Alternatif Pemantauan Traffic Jaringan Dan Host Pada Instansi Pemerintah Untuk Memperkuat Keamanan Dan Ketahanan Siber Indonesia".

[3] M. Rafi, F. Fathin, A. Basuki, And A. Bhawiyuga, "Penerapan Elastic Stack Sebagai Platform Visualisasi Dan Analisis Trafik Pada Jaringan Riset Dan Edukasi," 2022. [Online]. Available: Http://J-Ptiik.Ub.Ac.Id

[4] F. Riza, "Analisis Security Information And Event Management (Siem) Elastic Search Menggunakan Metode Nist 800-61 Rev2 Pada Datacenter Pt. Sembilan Pilar Semesta," 2023.

[5] A. Setiyawan, A. Pinandito, And W. Purnomo, "Pengembangan Sistem Informasi Log Management Server Monitoring Menggunakan Elk (Elastic Search, Logstash Dan Kibana) Stack Pada Aplikasi Padichain Di Pt. Bank Rakyat Indonesia," 2023. [Online]. Available: Http://J-Ptiik.Ub.Ac.Id

[6] P. Napoleon And K. Bayu, "Implementasi Server Log Monitoring System Menggunakan Elastic Stack," 2022. [Online]. Available: Http://J-Ptiik.Ub.Ac.Id