Project Report: Pfsense and Suricata integration with Splunk

=

Architecture Description

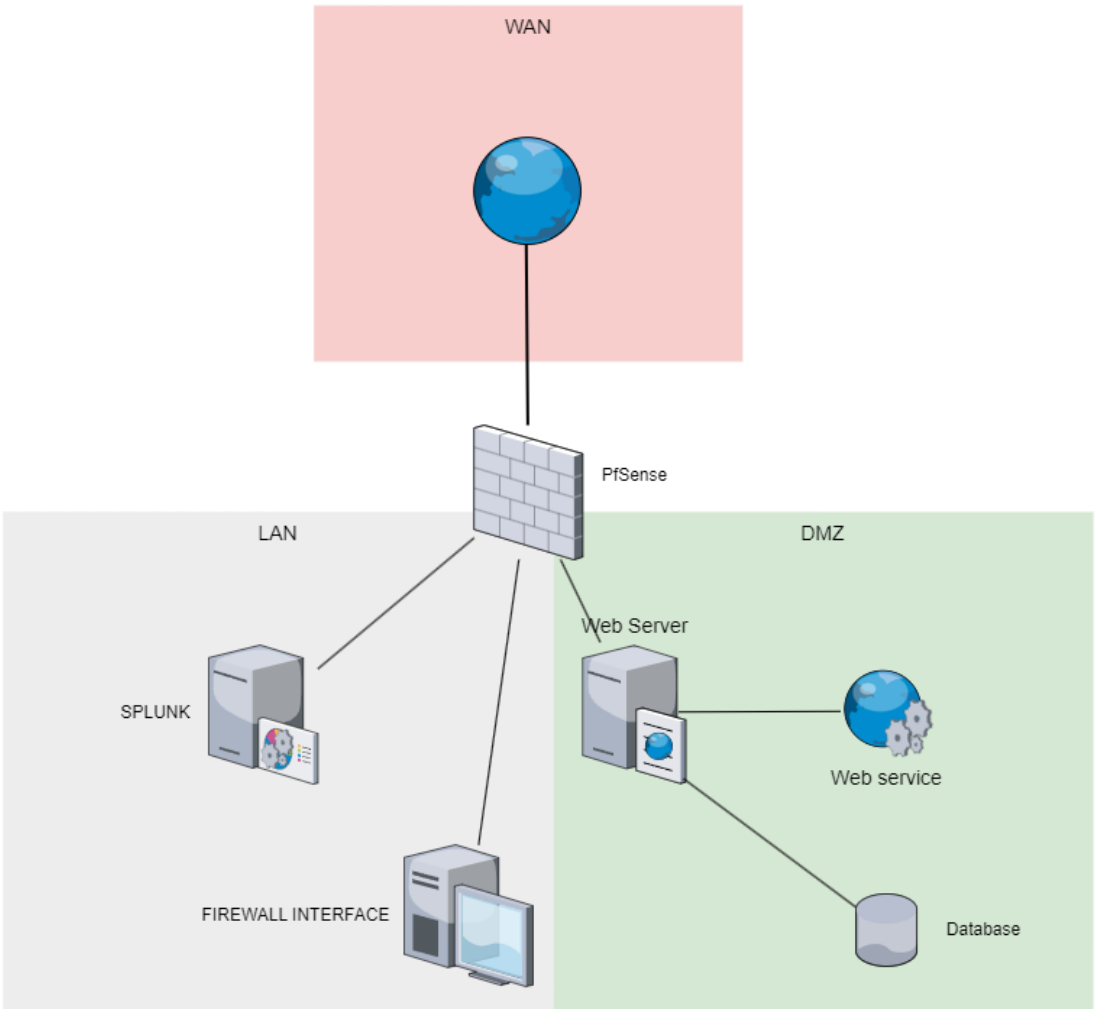
The cybersecurity solution is structured around the integration of Pfsense, Suricata IDS, and Splunk for network security monitoring and log analysis. The architecture encompasses the following components:

1. **Pfsense**: Utilized as the primary firewall and routing platform, responsible for traffic management, security rule enforcement, and logging.

2. **Suricata IDS**: Implemented for real-time intrusion detection and prevention, analysing network traffic for malicious patterns based on predefined rules or custom configurations.

3. **Splunk**: Used as the centralized log management and security information and event management (SIEM) tool, collecting, indexing, and correlating log data from Pfsense and Suricata to enable real-time monitoring, alerting, and analysis.

Pfsense Suricata integration with Splunk



Objectives

The primary project objectives encompass the following:

1. **Enhance Network Security**: Improve network security posture through real-time monitoring of network traffic for potential threats and vulnerabilities.
2. **Streamline Log Analysis**: Enable comprehensive log collection, analysis, and correlation for proactive threat detection and incident response.
3. **Implement Centralized Management**: Establish a centralized platform for monitoring and managing security events, logs, and alerts across the network infrastructure.

High-Level Features

The implemented solution offers the following key features:

1. **Real-Time Threat Detection**: Suricata IDS enables real-time monitoring of network traffic for detecting and preventing potential intrusions and cyber threats.
2. **Custom Logging**: Pfsense captures detailed network traffic logs, providing granular visibility into network activities and security events.
3. **Log Aggregation and Correlation**: Splunk serves as the central repository for aggregating and indexing log data from Pfsense and Suricata, allowing for the correlation of security events and logs.
4. **Alerting and Reporting**: Splunk enables the creation of custom alerts and reports based on predefined threat indicators and security events, facilitating proactive incident response and analysis.

5. **Dashboard Visualization**: Splunk dashboard provides interactive visualization of security events, logs, and network traffic, offering a holistic view of the network security posture.