**Project Documentation: FortiAnalyzer-like Application Using ELK Stack**

**Project Overview**

The objective of this project is to develop an open-source platform similar to FortiAnalyzer using the ELK (Elasticsearch, Logstash, Kibana) stack. The focus is on integrating logs from FortiGate devices into Logstash and creating a FortiAnalyzer-like dashboard in Kibana.

**Project Phases**

**Phase 1**: Integrate firewall logs from FortiGate devices and develop a custom dashboard in Kibana.

**Timeline**

* **Start Date**: 7th August, 2024
* **Current Phase**: Testing ELK Stack setup on Windows.

**Progress (7th August – 9th August, 2024)**

**1. Elasticsearch Installation and Configuration**

* **Purpose**: Store and search logs from FortiGate devices.
* **Tasks Completed**:
  + Installed Elasticsearch on Windows.
  + Configured Elasticsearch for initial testing purposes.

**2. Logstash Installation and Configuration**

* **Purpose**: Collect and process logs from FortiGate devices.
* **Tasks Completed**:
  + Installed Logstash on Windows.
  + Configured Logstash to receive logs from FortiGate devices.

**3. Kibana Installation and Configuration**

* **Purpose**: Visualize logs and create dashboards similar to FortiAnalyzer.
* **Tasks Completed**:
  + Installed Kibana on Windows.
  + Configured Kibana and began creating dashboards for testing.

**Next Steps**

* Continue refining the Kibana dashboard to closely resemble FortiAnalyzer.
* Begin testing log ingestion from FortiGate devices into Logstash.
* Iterate on the dashboard design based on log data and visualization requirements.



