ALX PROJECT: Web Infrastructure Design

Task 2: Secured and Monitored Web Infrastructure

1. Rationale Behind Additional Elements:

   Three essential components have been introduced to bolster the security and oversight of our web infrastructure. These enhancements encompass individual firewalls for each server to fortify against potential threats, the implementation of SSL certificates on servers to guarantee secure HTTPS communication, and the integration of monitoring clients tasked with diligently collecting and transmitting logs to our central data collector, Sumologic.
2. Role of Firewalls:

   Firewalls serve as a paramount network security measure, meticulously scrutinizing both inbound and outbound network traffic in accordance with pre-established security protocols. Their deployment establishes a protective barrier delineating trusted from untrusted network domains.
3. Significance of HTTPS Traffic:

   The adoption of HTTPS encryption ensures the secure transmission of data over the internet by employing Transport Layer Security (TLS). This cryptographic protocol safeguards sensitive information during transit, markedly contrasting with the vulnerability inherent in unencrypted HTTP transmissions.
4. Importance of Monitoring:

   Monitoring serves as a proactive mechanism for detecting and diagnosing potential performance anomalies within web applications. By continuously monitoring system metrics and behaviors, deviations from expected norms can be promptly identified and rectified, thereby optimizing overall system performance and reliability.
5. Methodology of Data Collection by Monitoring Tools:

   Monitoring tools systematically gather and analyze logs originating from various system components, including the application server, MySQL database, and Nginx web server. These logs serve as a comprehensive record of system activities, facilitating in-depth analysis and troubleshooting.
6. Monitoring Web Server QPS:

Monitoring the Query Per Second (QPS) metric of the web server entails a comprehensive assessment of its performance across both network and application layers. This meticulous observation enables timely intervention and optimization, particularly in scenarios where the server contends with high query loads.

Issues:

A. **SSL Termination at Load Balancer Level:** The practice of terminating SSL at the load balancer level entails the decryption of incoming SSL traffic before onward transmission to backend servers over an unencrypted connection, thus exposing potential security vulnerabilities.

B. **Single MySQL Server for Writes:** Relying solely on a single MySQL server to handle write operations introduces inherent risks, including potential performance bottlenecks and susceptibility to system downtime, thereby compromising data availability and integrity.

C. **Uniformity of Server Components:** The uniformity of server components across the infrastructure presents the risk of widespread system vulnerabilities in the event of a bug or security breach. Introducing diversity in component configurations can mitigate the impact of such incidents and enhance overall system resilience.