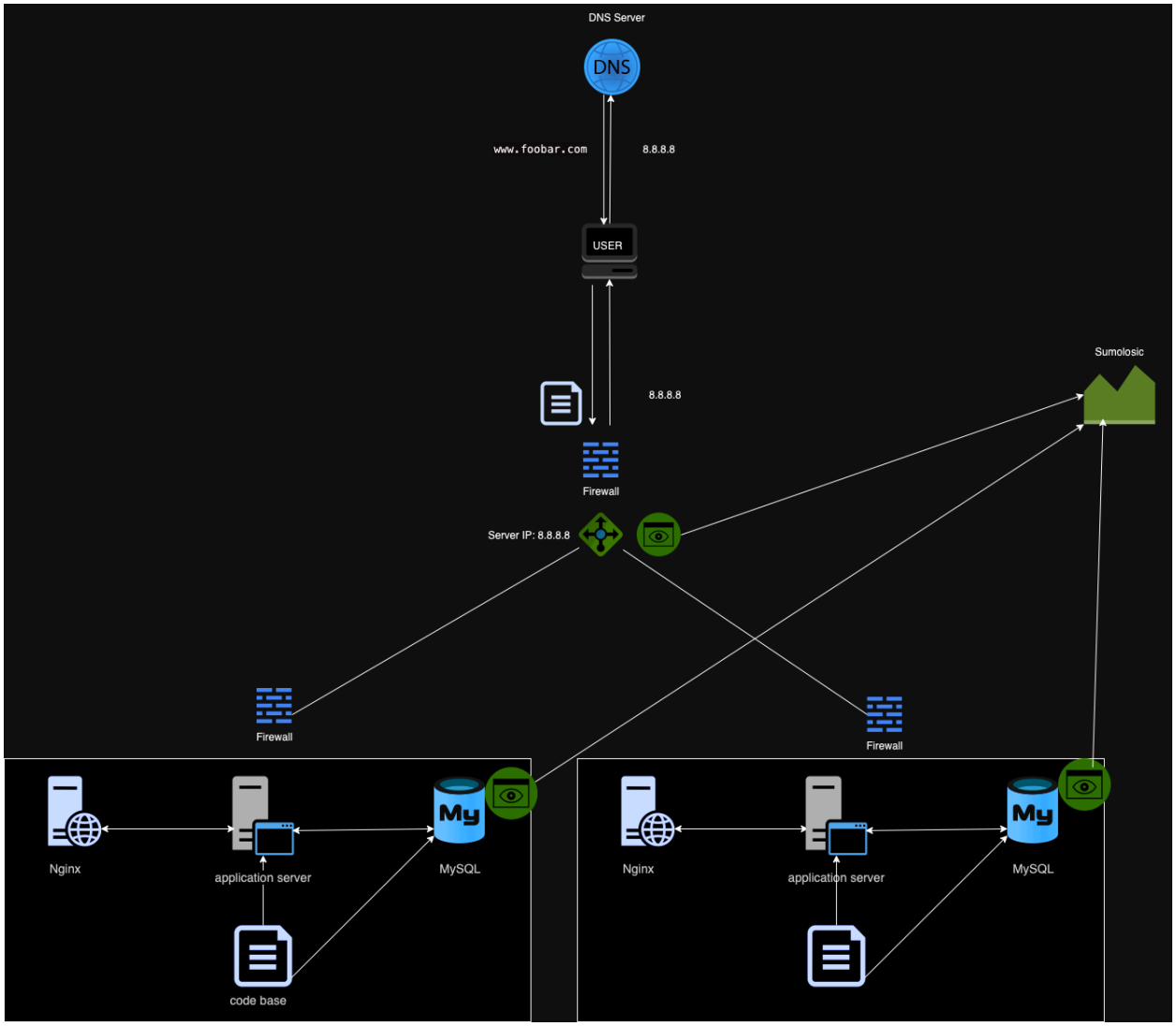

Components of the Infrastructure:

- Web Servers (Nginx): Responsible for serving web pages and handling incoming HTTP requests. Nginx will be configured to terminate SSL connections and serve encrypted traffic over HTTPS.
- Application Servers: Execute server-side code and handle dynamic content generation.
- Database Servers (MySQL): Store and manage the website's data, including user information and content.

- Firewalls: Deployed to control and monitor incoming and outgoing network traffic, ensuring the security of the infrastructure.
- SSL Certificate: Used to encrypt data transmitted between clients and servers, providing secure communication over the internet.
- Monitoring Clients: Collect data related to server performance, resource usage, and application health for analysis and troubleshooting.

Specifics of the Infrastructure:

- Firewalls: Added to enforce security policies, restrict unauthorized access, and protect the servers from potential threats. Firewalls monitor and filter incoming and outgoing traffic based on predefined rules.
- SSL Certificate: Implemented to serve www.foobar.com over HTTPS, ensuring data confidentiality, integrity, and authenticity. SSL/TLS encryption secures the communication between clients and servers, preventing eavesdropping and tampering of data.
- Monitoring: Utilized to track server performance metrics, detect anomalies, and troubleshoot issues proactively. Monitoring tools collect data from servers, analyze trends, and generate alerts for potential problems.
- Data Collection: Monitoring clients collect various data metrics, including CPU usage, memory utilization, network traffic, response times, and error rates. This data is sent to a centralized monitoring system, such as Sumo Logic, for storage, analysis, and visualization.
- Monitoring Web Server QPS: To monitor web server QPS (Queries Per Second), metrics such as incoming request count, response times, and server throughput are tracked. Alerts can be configured based on predefined thresholds to notify administrators of abnormal QPS levels.

Issues with the Infrastructure:

Terminating SSL at the Load Balancer Level:

- Terminating SSL at the load balancer exposes decrypted traffic within the internal network, increasing the risk of data interception. It's recommended to terminate SSL at the web server level to maintain end-to-end encryption.

Single MySQL Server for Writes:

- Having only one MySQL server capable of accepting writes introduces a single point of failure. Implementing a primary-replica (master-slave) replication setup would enhance fault tolerance and data redundancy.

Uniformity of Server Components:

- Deploying servers with identical components (database, web server, application server) may lead to a lack of diversity in the infrastructure. It's advisable to introduce diversity in server components to minimize the impact of potential vulnerabilities or failures.