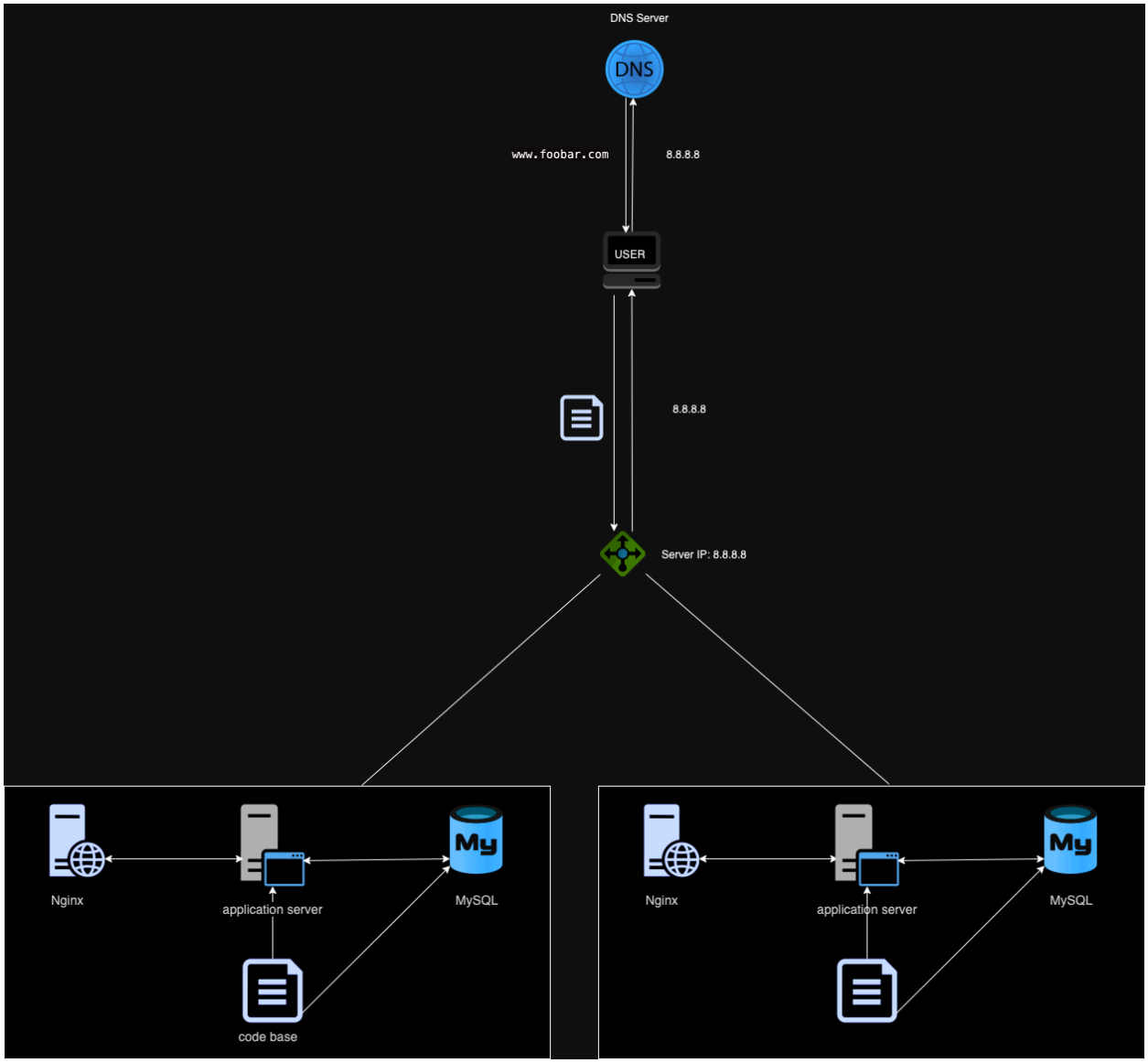
DNS Server
DNS
www.foobar.com
8.8.8.8
USER
8.8.8.8
Server IP: 8.8.8.8
Nginx
application server
MySQL
code base
Nginx
application server
MySQL

Specifics of the Infrastructure:

- Web Server (Nginx): Added to improve performance and handle static content delivery efficiently. Nginx acts as a reverse proxy to distribute incoming requests to the application servers.
- Application Servers: Introduced to handle dynamic content generation and user request processing. Multiple application servers are utilized for load balancing and redundancy.
- Load Balancer (HAproxy): Configured with a round-robin distribution algorithm to evenly distribute incoming requests among the application servers. This ensures optimal resource utilization and prevents overloading of any single server.
- Distribution Algorithm: HAproxy is configured with a round-robin algorithm, which sequentially routes incoming requests to each server in rotation. This evenly distributes the load across all available servers.
- Active-Active Setup: The load balancer enables an active-active setup, where all application servers actively serve user requests simultaneously. In this setup, each server is capable of handling traffic independently, providing redundancy and scalability.
- Database Primary-Replica Cluster: Implemented to ensure data redundancy and high availability. The primary-replica cluster consists of a primary (master) node and one or more replica (slave) nodes. The primary node handles write operations, while replica nodes replicate data from the primary node to serve read operations.
- Difference Between Primary and Replica Nodes: The primary node accepts write operations and maintains the authoritative copy of the data. On the other hand, replica nodes replicate data from the primary node and serve read operations. Replica nodes are read-only and cannot accept write operations directly.

Issues with the Infrastructure:

Single Points of Failure (SPOF):

- The load balancer and database may become single points of failure if not properly configured for redundancy.

Security Issues:

- Lack of firewall configurations may expose servers to security threats and unauthorized access.
- Absence of HTTPS encryption poses security risks, especially when transmitting sensitive data over the network.

No Monitoring:

- Without monitoring tools and systems in place, it becomes challenging to detect and troubleshoot issues, leading to potential downtime and performance degradation.