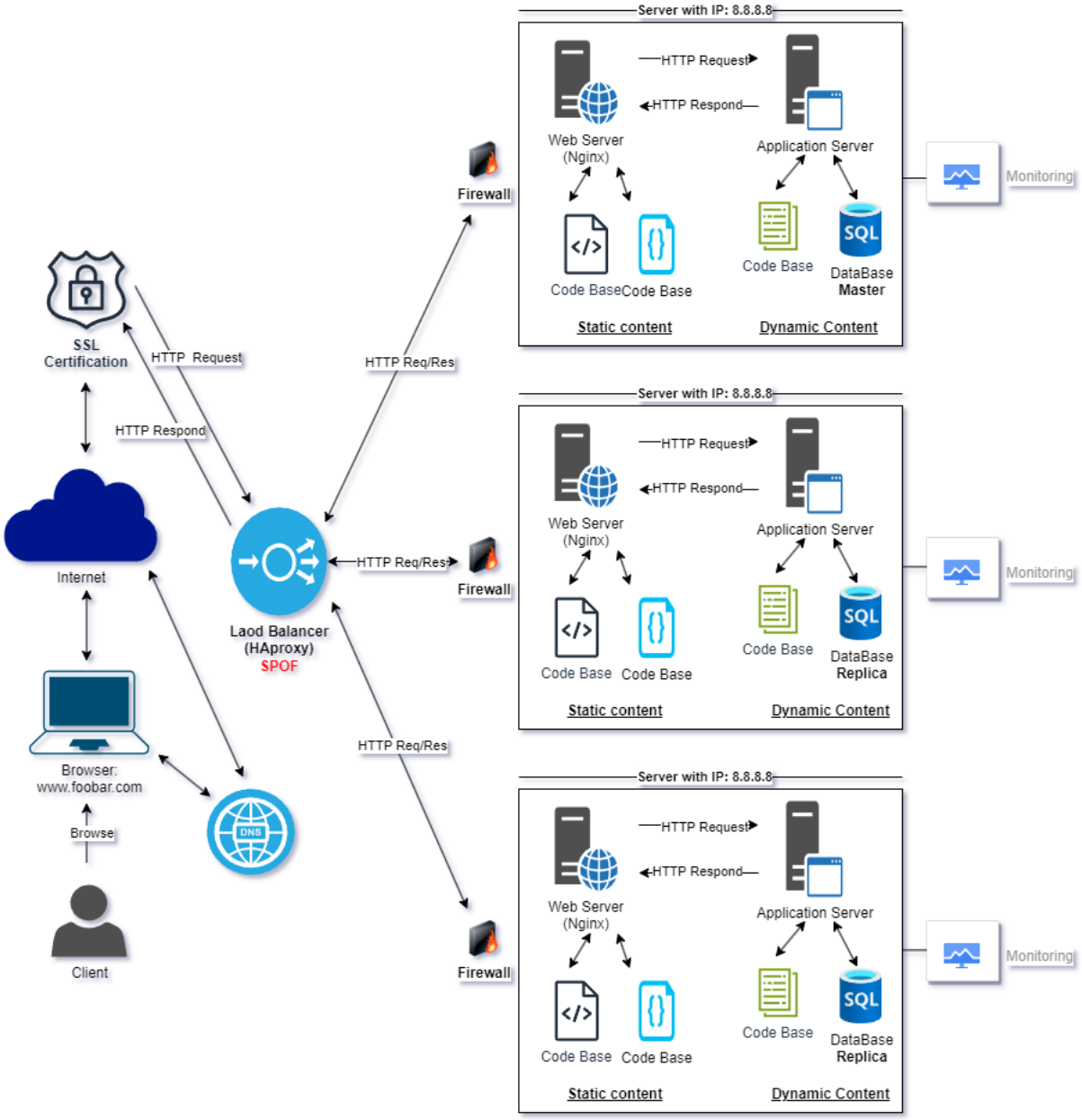
Secured and Monitored Three-Server Web Infrastructure Design

Whiteboard Diagram



Explanation

<u>Scenario</u>:
A user wants to access the secured website www.foobar.com, and the infrastructure is designed to be secured, serve encrypted traffic, and be monitored.

Components:

1. Load Balancer (HAproxy):

- Purpose: Distributes incoming traffic across multiple servers.
- Security: Acts as a point of entry where incoming traffic is filtered and monitored.
- HTTPS Termination: SSL termination is performed at the load balancer to encrypt and decrypt traffic, enhancing security.

2. Web Server (Nginx):

- Purpose: Handles HTTP requests, serving static content and forwarding dynamic content requests to the application server.
- Security: Nginx ensures secure communication and serves as a middle layer between the load balancer and the application server.

3. Application Server:

- Purpose: Executes the application logic, handling dynamic content generation.
- Security: Contains the core application logic, isolated from direct external access.

4. Database (MySQL):

- Purpose: Stores and manages website data.
- Security: Database server is protected from direct external access by placing it behind firewalls.

5. Firewalls (3):

- Purpose: Enhance security by controlling incoming and outgoing network traffic.
- Placement: Positioned to control access to the web server, application server, and database, restricting unauthorised access.

6. SSL Certificate:

- Purpose: Enables HTTPS to encrypt communication between users and the website.
- Termination: SSL termination at the load balancer ensures encrypted traffic until it reaches the load balancer.

7. Monitoring Clients (3):

- Purpose: Collect data on the performance and health of the infrastructure.
- Sumologic: Chosen as the monitoring service for collecting, analysing, and visualising log data for comprehensive monitoring.
- Data Collection: Monitoring clients collect data on server performance, application health, and database status.

Issues with the Infrastructure:

1. SSL Termination at Load Balancer:

- Issue: Terminating SSL at the load balancer means that traffic between the load balancer and internal servers is unencrypted. Internal communication could be susceptible to attacks if compromised.
- Solution: Use end-to-end encryption or re-encrypt traffic between the load balancer and internal servers.

2. Single MySQL Server for Writes:

- Issue: Having only one MySQL server capable of accepting writes introduces a single point of failure for write operations.
- Solution: Implement a Primary-Replica (Master-Slave) setup to distribute write operations and ensure high availability.

3. Uniform Servers:

- Issue: Servers with identical components might lead to uniform vulnerabilities. If one server is compromised, all others are potentially vulnerable.
- Solution: Introduce diversity in the configuration and components of servers to minimise the impact of a potential breach.