Design of a Three-Server Secure, Encrypted, and Monitored Web Infrastructure for www.foobar.com:

\*\*Components\*\*:

1. \*\*Web Servers (x3)\*\*:

- Hosting the website and serving as the entry point for user requests.

- Load balanced for distribution.

2. \*\*Application Servers (x3)\*\*:

- Hosting the website's dynamic codebase and processing application logic.

- Synchronized with the web servers.

3. \*\*Database Servers (x3)\*\*:

- Storing structured data and enabling read and write operations.

- Configured for high availability.

4. \*\*Load Balancer (HAproxy)\*\*:

- Distributing incoming traffic among web servers for load balancing and high availability.

5. \*\*Firewalls (x3)\*\*:

- Added to enhance security by controlling incoming and outgoing network traffic and preventing unauthorized access.

6. \*\*SSL Certificate\*\*:

- Installed to secure the website and serve encrypted traffic over HTTPS.

7. \*\*Monitoring Clients (Data Collectors)\*\*:

- Installed on servers to gather performance and security data for monitoring and alerting.

\*\*Specifics\*\*:

\*\*Additional Elements\*\*:

- \*\*Firewalls\*\*: Added for security to restrict access and protect the infrastructure from unauthorized connections, including DDoS attacks and other threats.

- \*\*SSL Certificate\*\*: Implemented to encrypt the communication between users and the web servers, ensuring data privacy and security.

- \*\*Monitoring Clients\*\*: Deployed to track server and application performance, security, and to detect issues proactively.

\*\*Firewalls\*\*:

- Firewalls are added to control network traffic. They act as a barrier between the internal network and external networks (e.g., the internet).

- Firewalls restrict access, filter traffic, and block unauthorized requests, enhancing security and safeguarding the infrastructure from cyber threats.

\*\*HTTPS Traffic\*\*:

- HTTPS is used to secure data in transit between users and the website. It encrypts the communication, protecting sensitive information such as login credentials and personal data from eavesdropping and interception.

\*\*Monitoring\*\*:

- Monitoring is essential for assessing server performance, identifying bottlenecks, and ensuring security.

- Monitoring tools collect data about server resources (CPU, memory, disk usage), network traffic, security events, and application performance.

\*\*Monitoring Data Collection\*\*:

- Monitoring tools (e.g., Sumo Logic, Prometheus, Grafana) are configured with monitoring clients on each server.

- These clients collect data about server health, application performance, and security incidents.

- Collected data is then sent to a centralized monitoring service for analysis and alerting.

\*\*Monitoring Web Server QPS\*\*:

- To monitor web server queries per second (QPS), set up monitoring clients to track incoming requests and responses.

- Use monitoring tools to aggregate and visualize the data, enabling you to analyze web server performance over time.

\*\*Issues\*\*:

1. \*\*Terminating SSL at the Load Balancer Level\*\*:

- Termination of SSL at the load balancer can expose sensitive data to potential threats on the internal network.

- To address this, SSL should be terminated on the web servers and re-encrypted for communication between the load balancer and web servers.

2. \*\*Single MySQL Server Accepting Writes\*\*:

- Relying on a single MySQL server for write operations introduces a single point of failure.

- Implement a Primary-Replica (Master-Slave) cluster configuration to ensure data consistency and high availability.

3. \*\*Servers with Identical Components\*\*:

- Using servers with the same components can create a uniform target for attackers. A vulnerability in one server can potentially affect all others.

- Implementing diversity in server components or services can add an extra layer of security.

By addressing these issues and optimizing the infrastructure, you can achieve a more secure, available, and performant web environment while ensuring sensitive data is encrypted and closely monitored for any anomalies.