Designing a Secured and Monitored Three-Server Web Infrastructure for www.foobar.com

1. User Wants to Access www.foobar.com:
- A user opens their web browser and enters the URL www.foobar.com.

2. Domain Name and DNS:
- The domain name, www.foobar.com, is resolved to the IP addresses of the load balancer (e.g., 8.8.8.1 and 8.8.8.2) using DNS. DNS is configured to point to the load balancer, which distributes requests among the servers.

3. Firewalls:
- Three firewalls are deployed to control incoming and outgoing traffic. Firewalls act as a security barrier, blocking unauthorized access and potential attacks. They are configured to allow only necessary traffic, enhancing the overall security posture of the infrastructure.

4. Load Balancer with SSL Termination:
- The load balancer handles SSL termination, decrypting HTTPS traffic and forwarding it to the web servers as plain HTTP. SSL termination at the load balancer level allows for efficient use of server resources, as decryption is a CPU-intensive process. It also simplifies SSL certificate management since certificates are installed only on the load balancer.

5. Web Servers (Nginx):
- The web servers handle HTTP requests from users' browsers. They serve static content directly and forward dynamic requests to the application servers. Nginx efficiently manages connections, improving performance and security.

6. Application Servers:
- Application servers execute dynamic content, processing requests, executing code, and generating web pages. Having multiple application servers ensures redundancy and fault tolerance. If one server fails, others can handle incoming requests, minimizing downtime.

7. Database (MySQL Primary-Replica Cluster):
- The database operates as a Primary-Replica (Master-Slave) cluster. The primary node handles write operations, while replica nodes replicate data from the primary and handle read operations. This setup enhances data redundancy, fault tolerance, and read scalability.

8. SSL Certificate for HTTPS:
- An SSL certificate is installed on the load balancer to enable HTTPS. HTTPS encrypts data transmitted between the user's browser and the web servers, ensuring confidentiality and integrity. It is crucial for securing sensitive information, such as user credentials and payment details.

9. Monitoring Clients (Data Collectors for Sumo Logic or Other Monitoring Services):
- Three monitoring clients are deployed on the servers to collect data for Sumo Logic or other monitoring services. Monitoring tools track server performance, identify issues, and provide insights into the infrastructure's health and security. They collect data on various metrics such as CPU usage, memory usage, network traffic, and application performance.

Issues with the Infrastructure:

a. Terminating SSL at the Load Balancer Level
- Terminating SSL at the load balancer means that traffic between the load balancer and web servers is unencrypted. If an attacker gains access to the internal network, they can intercept sensitive data. To mitigate this, internal network traffic should be encrypted using protocols like IPsec.

b. Single MySQL Server Accepting Writes:
- Having only one MySQL server capable of accepting writes creates a single point of failure. If this server fails, write operations will be disrupted, impacting the application's functionality. Implementing a multi-master replication setup with automatic failover can address this issue, ensuring continuous availability of the database.

c. Servers with Identical Components:
- Servers with identical components might pose a problem if there are vulnerabilities affecting those components. A uniform setup means that a single vulnerability could potentially impact all servers simultaneously. Implementing diversity in software versions, libraries, or configurations across servers can enhance security by reducing the likelihood of a widespread compromise.