Infrastructure Overview:

We will implement a three-server web infrastructure to host www.foobar.com with a focus on security, encryption, and monitoring. The infrastructure includes three servers, three firewalls, SSL certificate for HTTPS, and monitoring clients for data collection.

Components:

1. **Web Servers (Server1, Server2, Server3):**
    - Purpose: Hosts the website www.foobar.com.
    - Rationale: Distributing the workload among multiple servers ensures redundancy and improved performance.
2. **Load Balancer:**
    - Purpose: Distributes incoming traffic across the three web servers.
    - Rationale: Enhances availability, fault tolerance, and scalability by efficiently managing incoming requests.
3. **Firewalls (Firewall1, Firewall2, Firewall3):**
    - Purpose: Controls and monitors incoming and outgoing network traffic based on predetermined security rules.
    - Rationale: Protects the infrastructure from unauthorized access, potential attacks, and ensures network security.
4. **SSL Certificate:**
    - Purpose: Enables HTTPS for secure communication between clients and web servers.
    - Rationale: Encrypts data in transit, safeguarding sensitive information and providing a secure browsing experience.
5. **Monitoring Clients (MonitoringClient1, MonitoringClient2, MonitoringClient3):**
    - Purpose: Collects data on system performance, traffic, and potential issues.
    - Rationale: Proactive monitoring allows for early detection of anomalies, performance bottlenecks, and security threats.

Specifics and Explanation:

- **Why Firewalls:**
    - Firewalls act as a barrier between a secure internal network and untrusted external networks, preventing unauthorized access and ensuring the confidentiality and integrity of data.
- **Why HTTPS:**

    - HTTPS encrypts data during transit, protecting it from interception and manipulation. It establishes a secure channel between clients and servers, crucial for safeguarding sensitive information.

- **Why Monitoring:**
    - Monitoring provides real-time insights into system performance, identifies potential issues, and ensures the overall health of the infrastructure.
- **Monitoring Data Collection:**
    - Monitoring tools like Sumo Logic collect data through agents (Monitoring Clients) deployed on servers. These agents gather information on system metrics, logs, and events.
- **Monitoring Web Server QPS:**
    - To monitor Web Server Query Per Second (QPS), set up monitoring clients to collect performance metrics, analyze server logs, and use tools like Sumo Logic to visualize and alert on QPS trends.

Issues with the Infrastructure:

- **SSL Termination at Load Balancer:**
    - Issue: SSL termination at the load balancer exposes unencrypted traffic within the internal network. To resolve, implement end-to-end encryption by enabling SSL on web servers.
- **Single MySQL Server for Writes:**
    - Issue: A single point of failure for write operations. Implement database replication or clustering for redundancy and fault tolerance.
- **Identical Components Across Servers:**
    - Issue: Uniformity across servers poses a risk if a flaw is discovered. Introduce diversity in software versions, configurations, and update schedules to minimize vulnerabilities.