ALX Project

Web infrastructure design

Additional Elements:

1. **Three Firewalls:**

- *Why:* Firewalls are added to enhance the security of the infrastructure. Placing them between the client and the internet (client-side firewall), between the internet and the load balancer (network firewall), and between the load balancer and the application servers provides layers of protection against unauthorized access and cyber threats.

2. **SSL Certificate for www.foobar.com:**

- *Why:* SSL certificates are crucial for securing communication between clients and the server. Serving www.foobar.com over HTTPS ensures encrypted and authenticated data transmission, protecting sensitive information from interception or tampering.

3. **Three Monitoring Clients (Data Collectors):**

- *Why:* Monitoring is essential for ensuring the health, performance, and security of the web infrastructure. By monitoring clients, data is collected and sent to monitoring services like Sumo Logic. This enables real-time analysis, alerting, and proactive issue resolution.

Specifics about the Infrastructure:

- **Why Firewalls:**

- Firewalls control and monitor incoming and outgoing traffic, preventing unauthorized access and enhancing overall network security.

- **Why HTTPS:**

- HTTPS encrypts data in transit, ensuring confidentiality and preventing unauthorized access during communication between clients and servers.

- **Why Monitoring:**

- Monitoring is used to track the health, performance, and security of the infrastructure, enabling proactive issue identification and resolution.

- **How Monitoring Tool Collects Data:**

- Monitoring clients act as data collectors, gathering information on server performance, error rates, and other relevant metrics. This data is then sent to monitoring services like Sumo Logic for analysis.

- **Monitoring Web Server QPS:**

- To monitor the web server QPS (Queries Per Second), set up monitoring tools to track incoming HTTP

requests. Analyze the data to identify patterns, peak times, and potential issues affecting the server's performance.

Issues with the Infrastructure:

- **Terminating SSL at the Load Balancer:**

- ***Issue:*** Terminating SSL at the load balancer means that the data between the load balancer and the application servers is transmitted in an unencrypted format. This creates a potential security risk, especially if the communication traverses untrusted networks.

- **Having Only One MySQL Server Accepting Writes:**

- ***Issue:*** If the single MySQL server accepting writes fails, it leads to a single point of failure and downtime. Additionally, it can become a performance bottleneck, affecting the scalability and reliability of the database system.

- **Servers with All the Same Components:**

- ***Issue:* Uniformity in server components poses a risk in terms of diversity.** If a vulnerability affects one type of component, it could potentially impact all servers. Diversifying components can enhance resilience against certain types of failures or attacks.