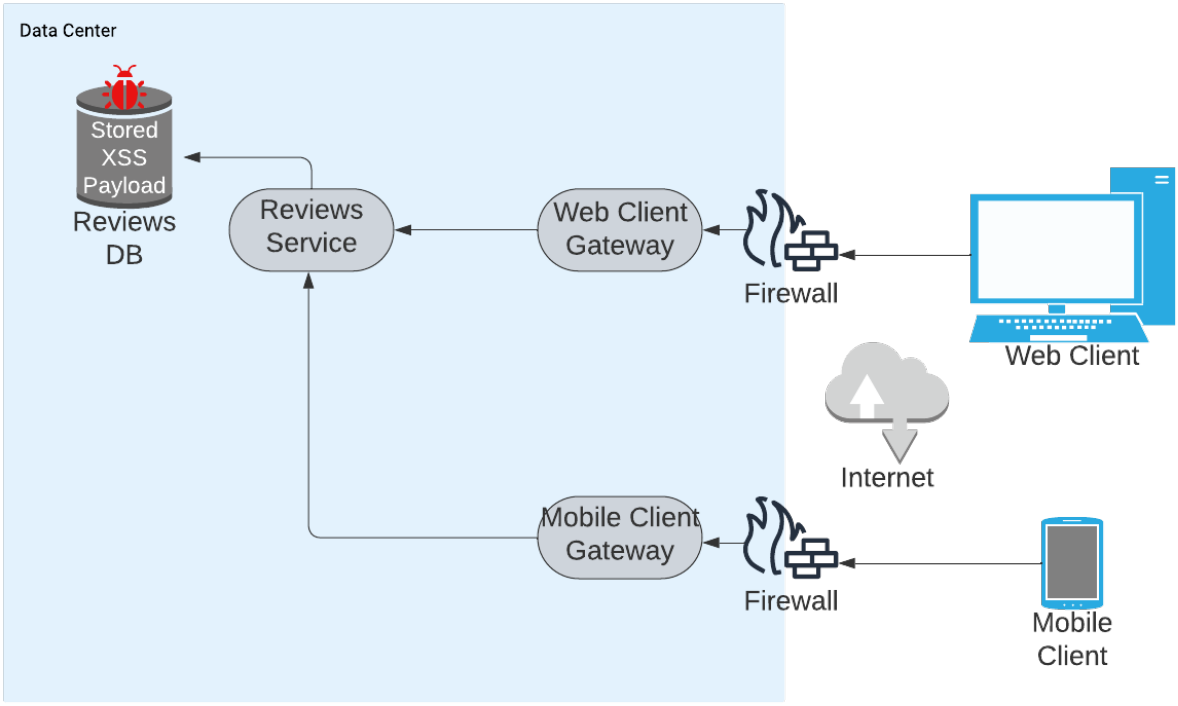
Exercise

1) The diagram below shows a simplified design for a consumer product reviews service. This architecture uses the API Gateways pattern. Assume that authentication and authorization are implemented appropriately according to this pattern, and that these flows are not depicted.



There is a Stored Cross-Site Scripting (XSS) vulnerability somewhere in this architecture.

- Where can the payload come from?
- Where can the payload execute?
- Which component likely houses the code that needs remediation?

After presenting your case to your management, they have made the risk decision to implement a web application firewall (WAF) to mitigate the risk associated with this vulnerability.

- What considerations do you need to present to your management regarding this approach?
- Does the WAF mitigate the XSS risk to any degree?
- What other activities do you think may need to occur here?

2) The diagram below shows a high-level architecture for an application that serves user-specific content. Assume there is a regulatory environment that requires any user-specific data can only be accessed by the user that owns that data.

   Create and document a brief threat model for this application.