**Lecture Notes:**

**Load Balancer:**  
  
A load balancer is a device that acts as a reverse proxy and is responsible for distributing network traffic across multiple servers. Load balancers smooth out the concurrent user experience of the application and improve reliability. An evenly distributed load means that each server will be better able to service application/network requests.

Round-robin   
Weighted round-robin   
Least response time   
Least connections

**Proxy Server:**  
  
A proxy server is an intermediate piece of software or hardware that sits between the client and the server. Clients connect to a proxy to make a request for a service like a web page, file, or connection from the server. Essentially, a proxy server (aka the forward proxy) is a piece of software or hardware that facilitates the request for resources from other servers on behalf of clients, thus anonymizing the client from the server.  
  
  
  
  
**SSL Passthrough:**  
  
‘SSL passthrough’ passes encrypted HTTPS traffics directly to the backend servers without decrypting the traffics on the load balancer (the proxy server). So any nodes (either network or proxy server instances) can’t read the contents in the traffic and pass through them all the way to the destination.

**SSL Termination:**  
  
SSL termination (a.k.a. SSL Offloading) decrypts all HTTPS traffics when it arrives at the load balancer (or Proxy server), and the data is sent to the destination server as plain HTTP traffic. When the traffic is decrypted, it usually reaches the company (or virtual/private network) and the traffic will be sent to the private network. (like internal end-point, private IP addresses)

**SSL Bridging:**  
  
SSL bridging is for checking the data to ensure that there is no malware in the traffic. Hackers envelop the hacking tools or malware software/codes into the encrypted traffic. Once the traffic gets to the server, the malware is exposed in the server and starts to breach the server. So SSL Bridging will offload the traffic and protect the backend server from being compromised.

**When do we need to use which one?**   
  
You can use the Passthrough if you don’t decrypt the traffic in any 7 layers, no access rules, no blocking, no cookie on the session. But if you need to decrypt the traffic to see what inside for any purpose, it needs to be offloaded once. In certain cases, the contents in the traffic are not very important then we want to load less burden to the application server by terminating the SSL and send HTTP traffic to the server from the load balancer. But SSL offloading is the most unrecommended way to ship the traffic, so we can add another step of encrypting the traffic back once it is offloaded and confirmed no (e.g.) security issue, called SSL bridging

The interview gave a scenario for Google docs and multiple users can access the same document, and google docs uses a Round Robin load balancing approach. Do you see any issues with using such an approach.