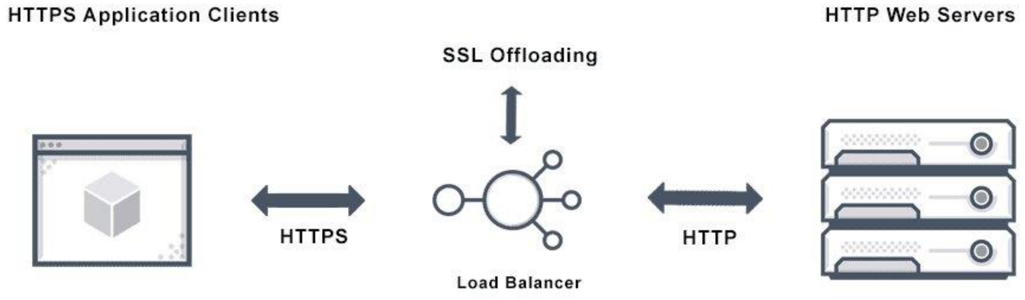
SSL Offloading:

SSL offloading is **the process of removing the SSL-based encryption from incoming traffic to relieve a web server of the processing burden of decrypting and/or encrypting traffic sent via SSL**. The processing is offloaded to a separate device designed specifically for SSL acceleration or SSL termination.

Client browse the website in secured mode using port 443, but internally webserver uses port 80 to communicate with different component of network like Load Balancer, Database, etc.



Load Balancer supports SSLOffloading.

Self-Signed Certificate V/S CA Signed Certificate:

Self-signed certificates are created, issued, and signed by the entities whose identities the certificates are meant to verify. This means that the individual developers or the companies who have created and/or own the website or software in question are, essentially, signing off on themselves. Furthermore, self-signed certificates are signed by their own private keys. This is yet another reason why they’re not publicly trusted certificates.

A CA-signed certificate, on the other hand, is signed by a third-party, publicly trusted certificate authority (CA). The popular CAs are Sectigo (formerly Comodo CA), Symantec, DigiCert, Thawte, GeoTrust, GlobalSign, GoDaddy, and Entrust. These entities are responsible for validating the person or organization that requests each certificate.

There are uses for Self-Signed certificates in testing environments, however, on the outward-facing Internet, they lead to browser warnings that dissuade potential visitors from coming to your website. While Self-Signed certificates do offer encryption, they offer no authentication and that’s going to be a problem with the browsers.

Trusted CA Signed SSL Certificates, on the other hand, do offer authentication and that, in turn, allows them to avoid those pesky browser warnings and work as an SSL Certificate should. So the choice is really a no-brainer. While it may seem like a good idea to try and save money and sign your own certificate, in the long run, you’re only hurting your website—go with a Trusted CA-Signed Certificate instead.