SSL OFFLOADING ISHIKA

Self-Signed Certificate V/S Third Party SSL Certificate

A self-signed certificate is a public key certificate that is signed and validated by the same person. It means that the certificate is signed with its own private key and is not relevant to the organization or person identity that does sign process. Such certificate is ideally for testing servers.

A reputable third-party certificate authority (CA) issues a certificate that requires verification of domain ownership, legal business documents, and other essential technical perspectives. To establish certificate chain, certificate authority also itself issues a certificate that is named trusted root certificate.

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.

SSL termination is particularly useful when used with clusters of SSL VPNs, because it greatly increases the number of connections a cluster can handle.