11. Server SSL Certificates

The Application Load Balancer (ALB) provides a flexible set of features for apps using HTTP or HTTPs.

You can add **Listeners** to listen for either type of request. Since HTTPS sets up an **encrypted** communication channel between the client and the ALB, it requres additional configuration.

The ALB needs a **server certificate** and **security policy** to receive this encrypted traffic.

SSL stands for **Secure Sockets Layer**. It is a **cryptographic protocol**, and TLS (**Transport Layer Security**) is an improved version of SSL. These are used interchangeably in the context of ALB certificates.

The ALB uses an **X.509 certificate.** This is a digital ID provisioned by a Certificate Authority such as the AWS Certificate Manager (ACM).

- In regions supported by ACM, choose a certificate provisioned by ACM.
- In regions not supported by ACM, you can use a **third party certificate with IAM (Identity and Access Management) as the certificate manager**.

The certificate is used to terminate the encrypted connection from the remote client, then the request is decrypted and forwarded to the resources in the ELB target group.