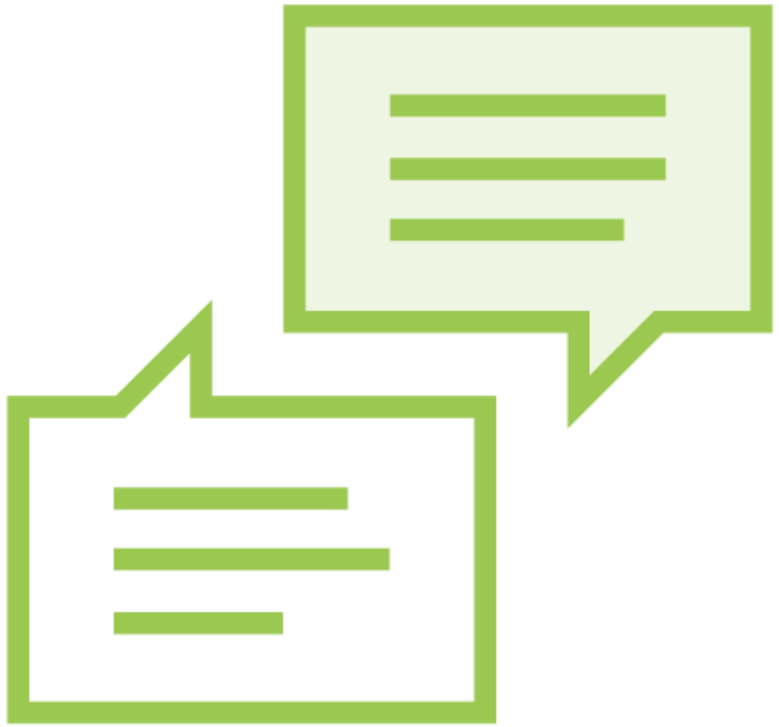
Protecting Data in Transit

Ben Piper
AWS CERTIFIED SOLUTIONS ARCHITECT

https://benpiper.com

Transport Layer Security (TLS)



People sometimes incorrectly call this SSL (secure sockets layer)

HTTPS uses TLS

Encrypting Data in Transit

Configure application to use TLS

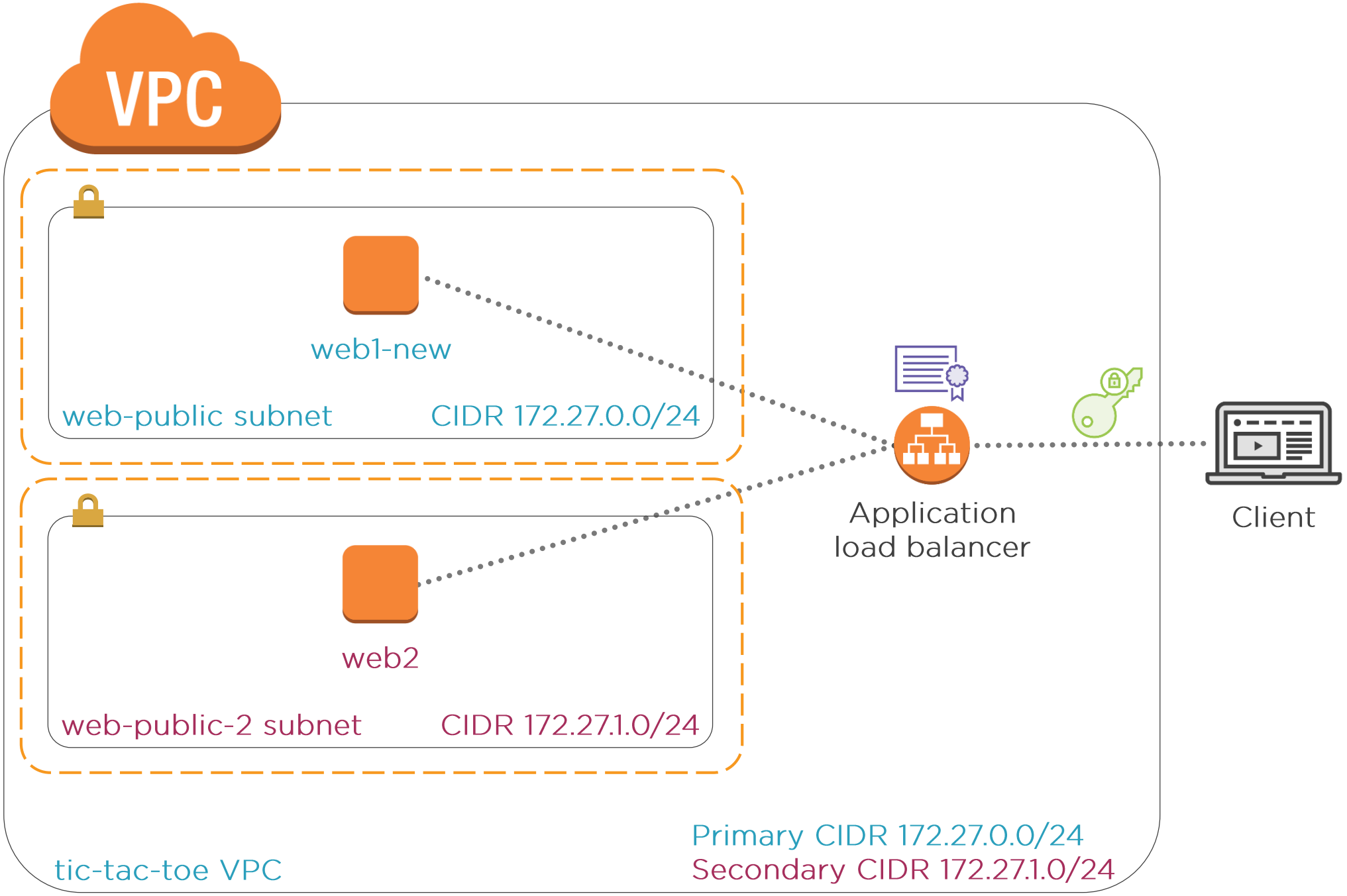
Application-dependent configuration

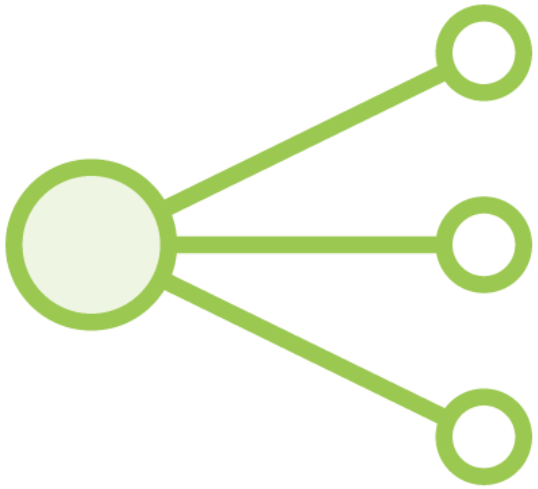
Independent of AWS

Application Load Balancer

Configure AWS Application Load Balancer to use TLS

Force all clients through the load balancer


VPC
web1-new
web-public subnet
CIDR 172.27.0.0/24
web2
web-public-2 subnet
CIDR 172.27.1.0/24
Application
load balancer
Client
tic-tac-toe VPC
Primary CIDR 172.27.0.0/24
Secondary CIDR 172.27.1.0/24



AWS Networking Deep Dive: Elastic Load Balancing (ELB)

- *Securing Web Applications with HTTPS*

Module Overview

Prepare the infrastructure to support an Application Load Balancer

Create a secure Application Load Balancer

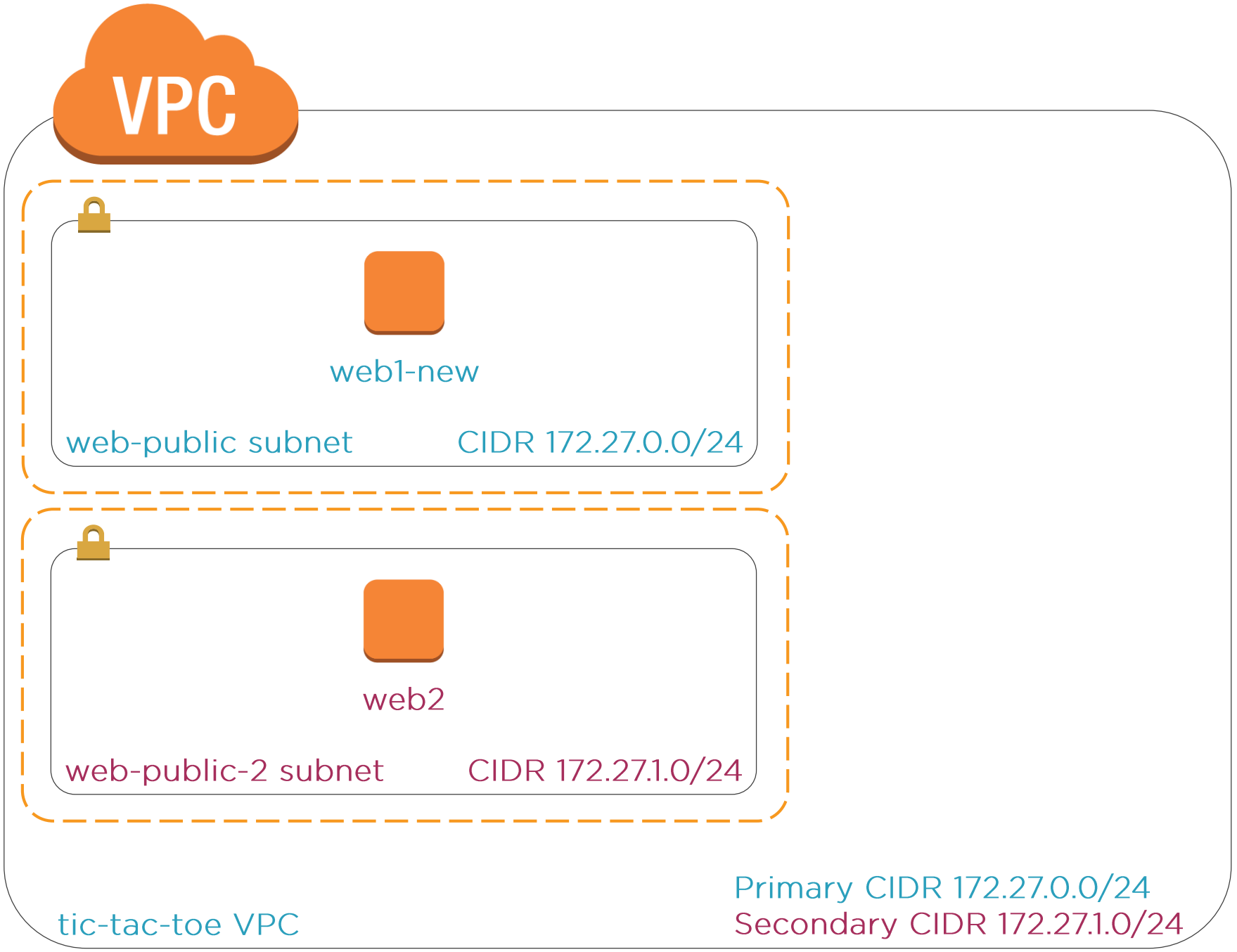
Demo

Create a new subnet in a different zone

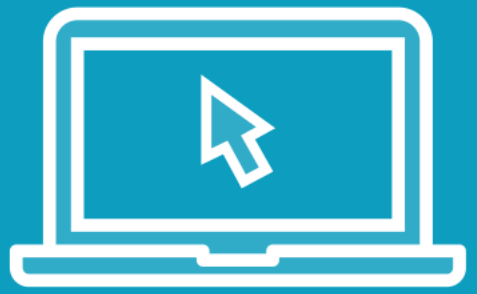
Bring up an instance named web2

Launch the application

Reconfigure security group


VPC
web1-new
web-public subnet
CIDR 172.27.0.0/24
web2
web-public-2 subnet
CIDR 172.27.1.0/24
tic-tac-toe VPC
Primary CIDR 172.27.0.0/24
Secondary CIDR 172.27.1.0/24

Demo

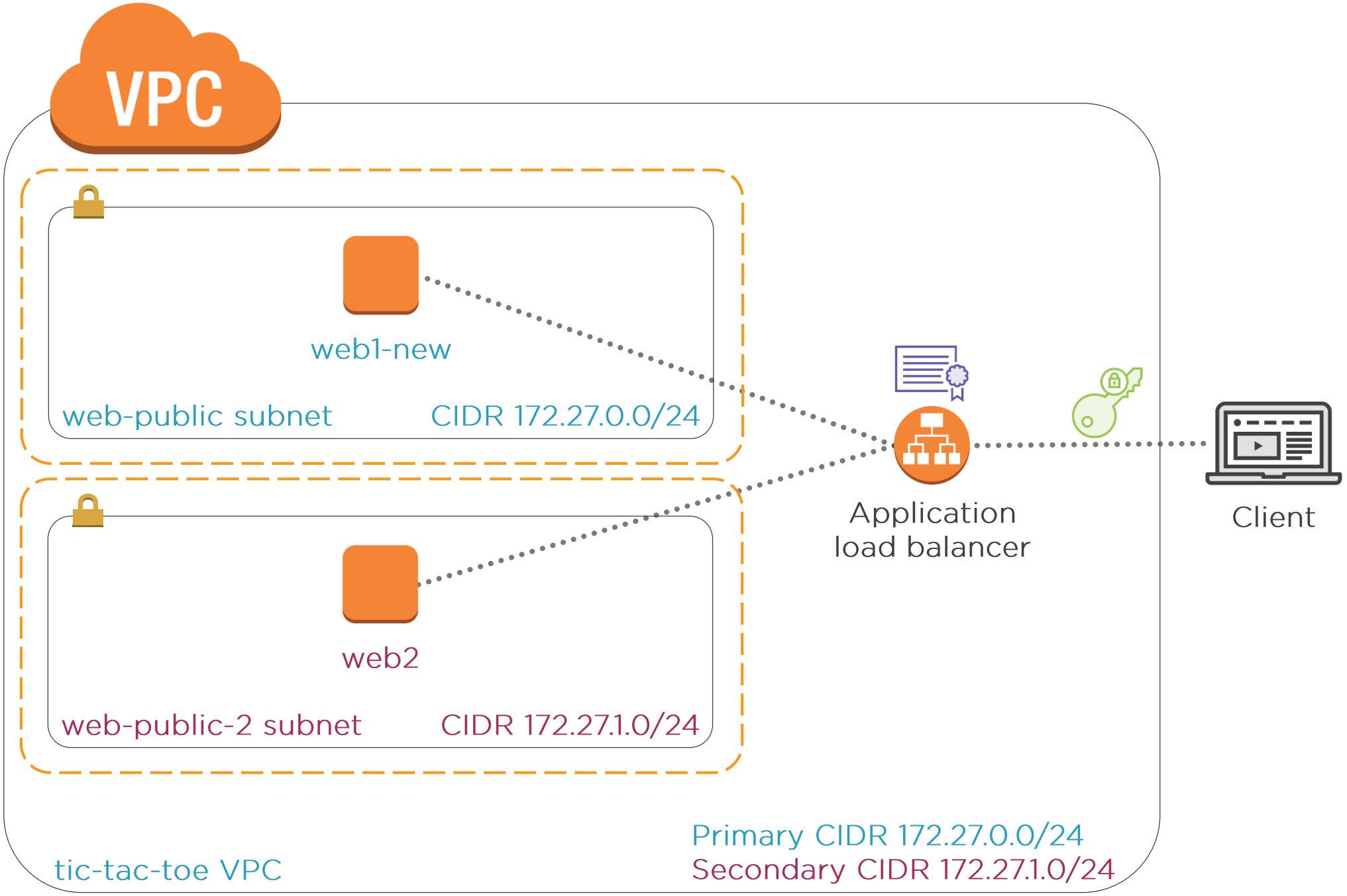


Use the AWS Certificate Manager to create a TLS certificate

Create an Application Load Balancer

Create a DNS record for the application

Browse to the application using HTTPS


VPC
web1-new
web-public subnet
CIDR 172.27.0.0/24
web2
web-public-2 subnet
CIDR 172.27.1.0/24
Application
load balancer
Client
tic-tac-toe VPC
Primary CIDR 172.27.0.0/24
Secondary CIDR 172.27.1.0/24

Summary

Choose where to terminate the TLS connection

- Individual instances
- Application Load Balancer

ALB requires two availability zones

ACM requires you to verify control of the domain name in the certificate

For private network connectivity, see *AWS Networking Deep Dive: Virtual Private Cloud (VPC)*

Coming up Next

Configuring data backup, replication, and recovery