AWS Bastion Host

Bastion Host Overview

- Bastion means a structure for Fortification to protect things behind it
- In AWS, a Bastion host (also referred to as a Jump server) can be used to securely access instances in the private subnets.
- Bastion host launched in the Public subnets would act as a primary access point from the Internet and acts as a proxy to other instances.

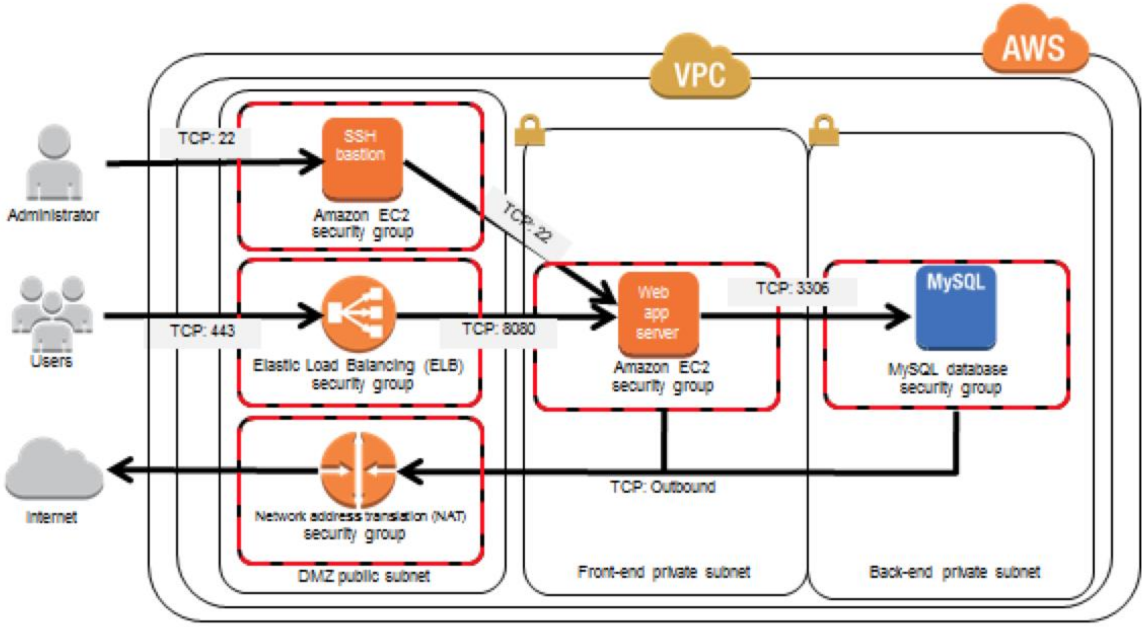

Figure 2. Reference architecture with Amazon VPC configuration

Key points

- Bastion host is deployed in the Public subnet and acts as a proxy or a gateway between you and your instances
- Bastion host is a security measure that helps to reduce attack on your infrastructure and you have to concentrate to hardening a single layer
- Bastion host allows you to login to instances in the Private subnet securely without having to store the private keys on the Bastion host (using ssh-agent forwarding or RDP gateways)
- Bastion host security can be further tightened to allow SSH/RDP access from specific trusted IPs or corporate IP ranges

- Bastion host for your AWS infrastructure shouldn’t be used for any other purpose, as that could open unnecessary security holes
- Security for all the Instances in the private subnet should be hardened to accept SSH/RDP connections only from the Bastion host
- Deploy a Bastion host within each Availability Zone for HA, cause if the Bastion instance or the AZ hosting the Bastion server goes down the ability to connect to your private instances is lost completely
-