## Option 1: Build a VPC with Public and Private Subnets

Your VPC will need to include:

1. An Internet Gateway
2. Two Subnets:
   1. One Public Subnet (called Subnet A) associated with a route table that contains a Default Route to an Internet Gateway
   2. One Private Subnet (called Subnet B) associated with a route table that contains a Default Route to the NAT server
3. Two Route Tables:
   1. A Route Table with a default route to the Internet Gateway
   2. A Route Table with a default route to the NAT Server
4. A NAT Server and NAT Security Group
   1. Use AMI: ami-69ae8259
   2. Make sure to Disable “Source/Destination” Checks
   3. Security Group Allows HTTP in from batch-processing
5. An ssh Bastion Host
   1. Security Group Allows ssh in from 0.0.0.0/0
6. A Batch Processing Host
   1. Security Group Allows ssh Bastion Host in

Your VPC will be designed as follows:



## Option 2: Build a VPC Containing two Public Subnets and Web Servers, *optionally locking down with Network ACL*

Your VPC will need to include:

1. An Internet Gateway
2. Two Public Subnets:
   1. Both Subnets should be associated with a route table that contains a Default Route to an Internet Gateway
3. One Route Table:
   1. A Route Table with a default route to the Internet Gateway
4. Two Web Servers:
   1. Both will be members of the “www” Security Group
5. Optional:
   1. Lock down outbound using a Network ACL:
      1. *Only allow inbound traffic on ports 22, 80*
      2. *Only allow outbound traffic on ephemeral ports*

Your VPC will be designed as follows:

