**Building Architecture with a Bastion Host and NAT Gateway**

**Architecture:**

Customers 
(front end/public access) 
External Server 
(for software updates) 
Open Internet 
Web Browser 
(http) 
VPC 
Network Access 
Control List 
(ACLs) 
Subnet 1 
(public) 
Security 
Group 
Bastion Host 
Subnet 3 
(private) 
EC2 
(w/out Public IP) 
Availability Zone 
Internet 
Gateway 
ELB 
172.16.0.0 
172.16.1.0 
172.16.2.0, 
Route Table 
with IGW 
172.16.omo 
172.16.1.0 
172.16.2.0 
Route Table 
w/out IGW 
IAWS Users 
(back end/private access) 
SSH 
Terminal 
(sshlrdp) 
Network Access 
Control List 
(ACLs) 
Subnet 2 
(public) 
NAT Gateway 
Subnet 4 
(private) 
EC2 
(w/out Public IP) 
Availability Zone 

**Implementation:**

**Purpose:** 2 EC2 instances in private subnet which won't be able to directly connect to Internet, however we would still need a way to connect to EC2 instance and download software package from internet to the EC2 instance.

1. Create New VPC "Security-VPC" [10.0.0.0/16]
2. Create Internet Gateway "Security-IGW" -> attach it to VPC
3. Create Subnet "Public-1" [10.0.1.0/24] (AZ-1) , "Public-2" [10.0.2.0/24] (AZ-2) , "Private-1" [10.0.3.0/24] (AZ-1) , "Private-2" [10.0.4.0/24] (AZ-2) in VPC "Security-VPC"
4. Check NACL is properly configured to all either all or selected traffic
5. Create 2 Route Tables; a) Public Subnets "Security-PublicRT" ->Routes: Add IGW & associate 2 Public subnets ; b) Private Subnets "Security-PrivateRT" & associate 2 private subnets
6. Create 2 EC2 instances in private subnets. 1st one in "Web-1" subnet & 2nd one in "Web-2" subnet.
   1. Choose proper VPC & Private Subnets
   2. Do not need Public IP
   3. Add Storage, Add Tags
   4. Create Security Group with necessary inbound traffic

Inbound Rule:

1. RDP : Public-1 & Public-2 subnets Allow: 3389

1. Key-Pairs creation
2. Create Bastion Host to connect the instance which are in Private subnets.
   1. Launch New EC2 instance in Public "Public-1" subnet
   2. Enable Auto-assign Public IP
   3. Add Storage, Add Tags
   4. Create Security Group "Bastion-SG" with necessary inbound traffic
   5. Key-Pairs creation
3. Create NAT Gateway for Internet Access from EC2 instances.
   1. VPC -> NAT Gateways -> Create a NAT Gateway
   2. Select Public "Public-2" subnet
   3. Assign/Create Elastic IP
4. Associate NAT Gateway to Private Route Table.
   1. Edit "Security-PrivateRT" -> Routes
   2. Add another route: 0.0.0.0/0 -> NAT Gateway
5. Create Classic Load Balancer "Security-ELB" inside our "Security-VPC".
   1. ELB Name: "Security-ELB" & VPC: "Security-VPC"
   2. Select 2 subnets
   3. Create Security Group:
      1. Allow Internet on All ports.
   4. Configure Health Check: TCP -> 135 (or any open port on EC2)
   5. Add EC2 instances which are in Private Subnets.

**Explanation:**

The VPC has been configured with two subnets, a public subnet, and a private subnet. If a subnet's traffic is routed to an Internet gateway, the subnet is known as a public subnet. If a subnet doesn't have a route to the Internet gateway, the subnet is known as a private subnet. Instances launched in a private subnet do not have publicly routable internet addresses either.

Both subnets have a route table associated with them. Instances on the public subnet route internet traffic through the internet gateway. The private subnet routes internet traffic through the NAT instance.

Each instance launched in either subnet has it's own security group with inbound and outbound rules, to guarantee access is locked down to specific ports and protocols. For example, private instances on the private subnet allow any outbound traffic, but only allow SSH access from the bastion host. As another example, although the NAT instance is in the public subnet, it cannot be reached from the internet. It has an inbound rule that only grants instances from the private security group (private instances) access. Note that you might allow SSH access from your personal IP address or specific administrator's as well, or perhaps grant ICMP (ping) access during setup and troubleshooting efforts.

In addition to security groups, the private subnet also has a network access control list (NACL) as an added measure of security. NACL's allow for inbound and outbound rules, specified in a priority order. They are setup as implicit allow rules. If none of them are matched, all other traffic is denied. This private subnet NACL in this Lab allowed for SSH inbound traffic from the public subnet only. The outbound rules for the private NACL allowed for HTTP/S access to anywhere. This was proven to work in the Lab by performing operating system updates once the NAT instance was in place. The private route table sends the traffic from the instances in the private subnet to the NAT instance in the public subnet. The NAT instance sends the traffic to the Internet gateway for the VPC. The traffic is attributed to the Elastic IP address of the NAT instance.