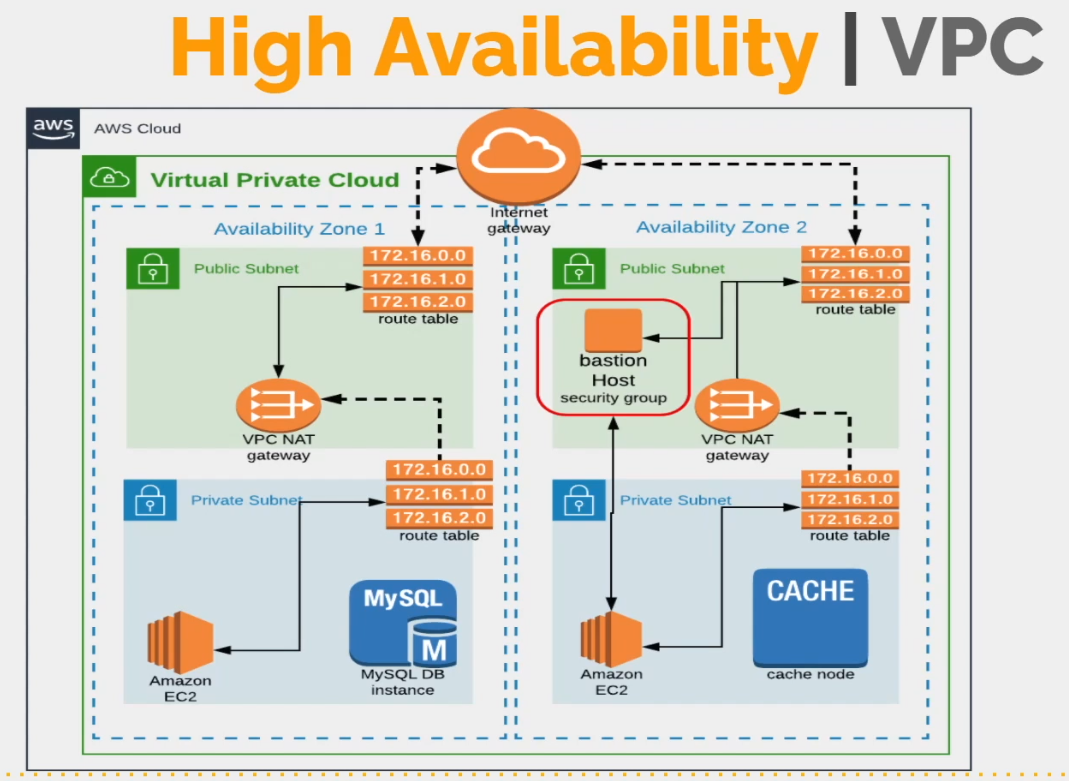
VPC project - 01. High availability with the security provision.



Region: us-west-1

VPC Range 172.20.0.0/16

4 subnets: 2 pub sub, 2 priv sub

2 zones: us-west-1a, us-west-1b

172.20.1.0/24 => pub-sub-1 [us-west-1a]

172.20.2.0/24 => pub-sub-2 [us-west-1c]

172.20.3.0/24 => priv-sub-1 [us-west-1a]

172.20.4.0/24 => priv-sub-2 [us-west-1c]

1 Internet GW

2 NAT Gateway

1 EIP

2 Route Tables : 1 Pub Sub RT, 1 Pub Sub RT

1 Bastion host in Pub subnet

NACL

1 more VPC => VPC Peering

* Be perfect to create High Availability & Secure VPC
  + High availability = at least 2 regions
  + secure VPC = pub subnet, priv subnet, SG, NACL
  + NAT GW, EIP, IG, LB
* Create VPC = VProfile-VPC
* Create 2 pub & 2 priv subnets
* Create IG (internet gateway) = VPR-RT
* Create pub-RT for pub subnets
  + Create route 0.0.0.0/0 -> IG
* Create NAT-GW -> pub subnet + EIP
* Create priv-RT for priv subnets
  + Create route 0.0.0.0/0 -> NAT-GW
* Install for pub subnets to get auto public IPs
* Enable DNS hostnames in VPC settings
* Create web EC2 and attach to priv subnet, web-sg, wave-key,
* Create basteon/jumpserver, basteon-sg, basteon-key, pub-subnet1, ssh access
* Web server -> allow ssh for basteon ip
* Copy wave-key to basteon and make chmod 400
  + scp -i Downloads/basteon.pem Downloads/wave.pem [ec2-user@13.56.11.203:/home/ec2-user/](mailto:ec2-user@13.56.11.203:/home/ec2-user/)
* create classic Load balancer (LB), vpr-lb
* web01 SG -> allow access for LB-SG port 80
* WEBSAIT is now available via LB link
  + <http://vpr-lb-628481761.us-west-1.elb.amazonaws.com/>
* VPC peering – allows instances from different regions to communicate
* create new VPC, Oregon region, – 172.16.0.0/16, DR-VPC
* VPR-VPC, Create new peering connection to DR-VPC
* DR-VPC, accept peering connection from VPR-VPC
* VPR-VPC, add Route table, pub-RT, 172.16.0.0/16 –> peering connection
* DR-VPC, add RT, 172.20.0.0/16 –> peering connection
* SG for instance. SG is statefull.
* Network ACL for subnet. NACL is stateless.
* VPR-VPC, create NACL as pub-sub-NACL. Add pub-subnet1, pub-subnet1/2. Allow 80, 22 inbound, outbound. Deny all inbound, outbound.
* Cleaning - LB (vpr-LB). EC2s (web01, bastion). NAT GW (vpr-NAT-GW).

IG(vpr-RT). Peering connection. VPCs (VPR-VPC). EIP