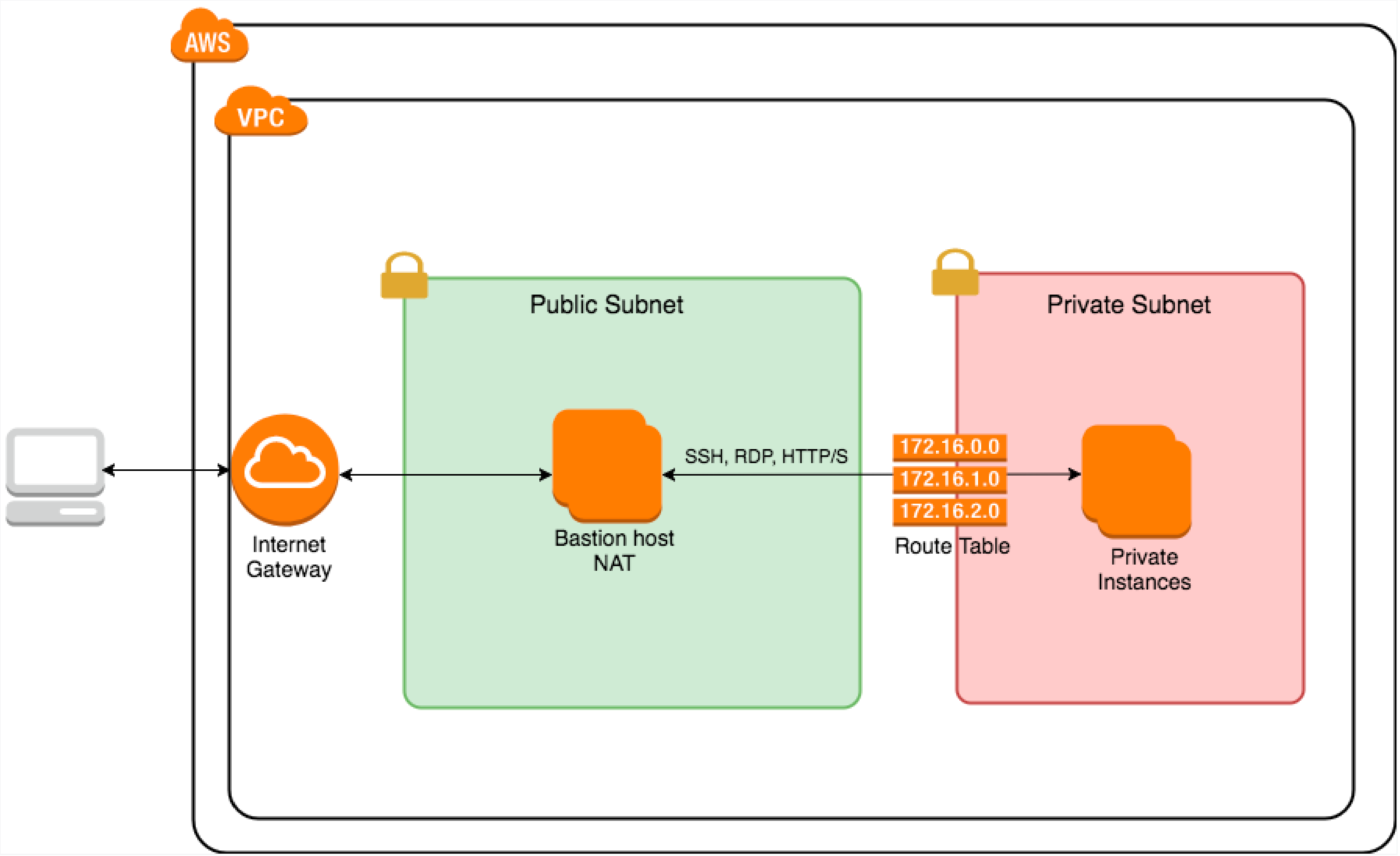
Let's look at the high-level lab environment diagram again, and go over some key points to tie this Lab together. Time and interest permitting, use the AWS Management Console to look up and/or confirm various settings as you read through this lab step. Realize that different organizations might configure things differently in accord with their security goals and policies. For example, increased or relaxed security on various inbound or outbound rules, etc.



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 device (gateway or instance).

Each instance launched in either subnet has its 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 device 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 priority order. They are set up 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 device was in place. The private route table sends the traffic from the instances in the private subnet to the NAT device in the public subnet. The NAT device sends the traffic to the Internet gateway for the VPC. The traffic is attributed to the Elastic IP address of the NAT device.