**Network Access Control Lists vs Security Groups**

**Exam tips – Network ACLs:**

* Your VPC automatically comes with a default network ACL, and by default it allows all outbound and inbound traffic.
* You can create custom network ACLs. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
* Each subnet in your VPC must be associated with a network ACL. If you don’t explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL.
* You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACLL at a time. When you associate a network ACL with a subnet, the previous association is removed.
* Network ACLs contain a numbered list of rules that is evaluated in order, starting with the lowest numbered rule.
* Network ACLs have separate inbound and outbound rules, and each rule can either allow or deny traffic.
* Network ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).
* Block IP addresses using network ACLs not security groups.