VPC (Virtual Private Cloud)

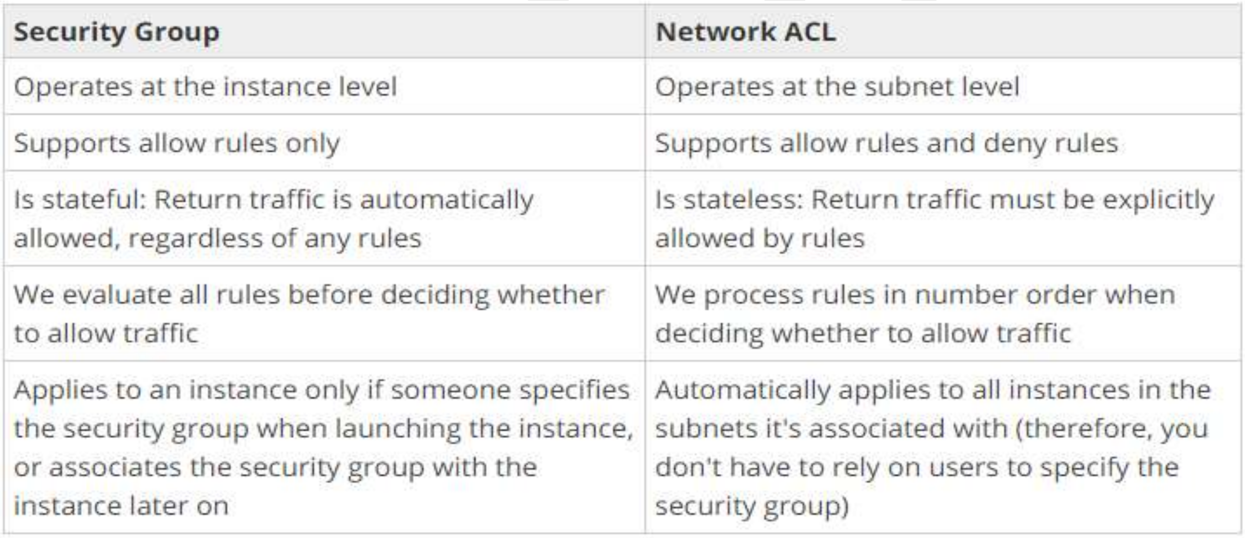
- VPC is a virtual data centre in the cloud
- VPC lets you provision a logically isolated section of the Amazon Web Services cloud where you can launch AWS resources in a virtual network that you define.

Important Points

- VPC consists of IGWs, Route Tables, NACL, Subnets and Security Groups
- 1 Subnet = 1 AZ
- Security Groups are Stateful
- NACLs are Stateless
- Your VPC automatically comes with a default network ACL and by default it allows all outbound and inbound traffic
- You can create a custom network ACL. 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 associated 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 ACL at a time. When you associate a network ACL with a subnet, the previous association is removed
- A network ACL contains a numbered list of rules that is evaluated in order, starting with the lowest numbers rule
- A network ACL has separate inbound and outbound rules, and each rule can be either allow or deny traffic.

Security Group vs Network ACL



Security Group	Network ACL
Operates at the instance level	Operates at the subnet level
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in number order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (therefore, you don't have to rely on users to specify the security group)