Security Groups vs NACL

Once we have set up our Virtual Private Cloud (VPC) environments with EC2 instances or other resources within them, ensuring their security and putting guardrails in place such that undesirable users do not access our VPCs automatically becomes a crucial task. AWS provides us with two ways of achieving this: **Network Access Control Lists (NACLs)** and **Security Groups**. Short descriptions of them are given below:

NACLs (Network Access Control Lists): These operate at the subnet level and control traffic for all the instances within that subnet. Unlike Security Groups, NACLs are stateless, meaning that rules need to be explicitly stated for both inbound and outbound traffic separately. Each NACL has numbered rules, and traffic is evaluated against these rules in ascending order, starting from the lowest number. The first rule that matches the traffic is applied, and the rest are ignored. This allows for both "allow" and "deny" rules, providing more flexibility for granular control over traffic.

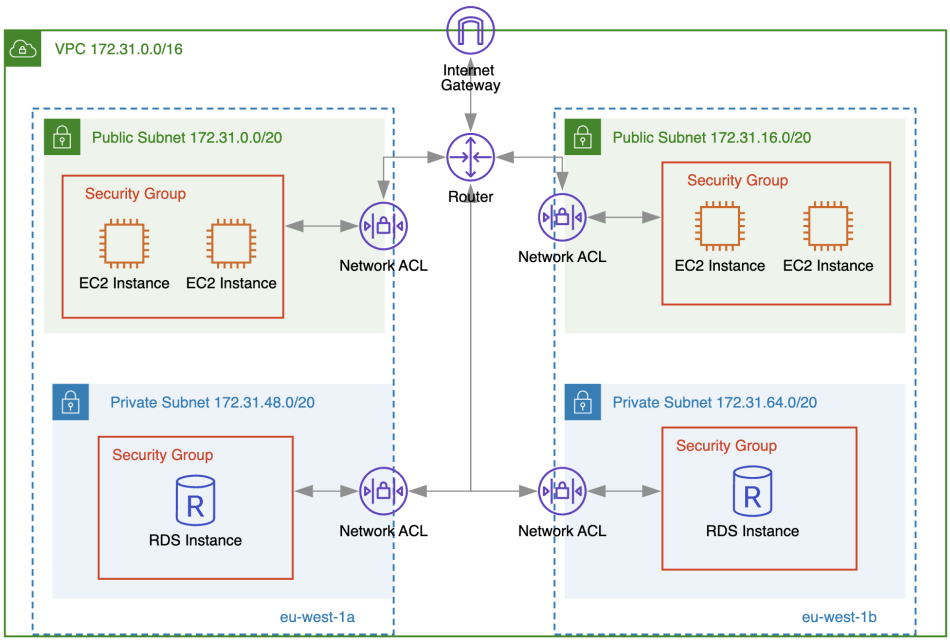
By default, NACLs have a rule that denies all inbound and outbound traffic unless otherwise specified. This makes NACLs useful for applying broad security controls to an entire subnet, as opposed to individual instances. However, their stateless nature means that we need to create separate rules for incoming and outgoing traffic, which can lead to more complex configurations compared to Security Groups. NACLs are often used in scenarios where subnet-level protection is needed, such as when managing public-facing resources that need additional security.

Security Groups: A more granular, EC2 instance focused offering, these act as firewalls at the instance level, controlling the traffic going in and out of individual

EC2 instances. Also, Security Groups are stateful, meaning that if we create a rule allowing an inbound request, the outbound response is automatically allowed, and vice versa. This simplifies configuration compared to NACLs, where each direction must be handled separately. Security Groups do not have an ordered rule set; instead, all rules are evaluated equally, and any traffic that matches an "allow" rule is permitted.

By default, Security Groups has a rule that denies all inbound traffic and allows all outbound traffic. However, they only support "allow" rules, meaning you cannot explicitly block traffic using a Security Group. This limitation is offset by their granular control over instance-level traffic. Security Groups are ideal for managing access to specific EC2 instances for example, allowing us to define precise security policies and protocols.

Furthermore, such that it becomes easier for the reader to visualize Network Access Control Lists (NACLs) and Security Groups, an architecture diagram showcasing the placement and bounds of both are given below:



Source: CloudViz

As the descriptions might have already betrayed, though they serve the same purpose, Security Groups and NACLs operate at different levels and have quite a few contrasting characteristics. These characteristics have been tabulated for the ease of the reader below:

Security Group	Network Access Control List
Acts as a firewall for associated Amazon EC2 instances and other specific resources	Acts as a firewall for associated subnets; Ambivalent to resources within the subnet
Controls both inbound and outbound traffic at the instance level	Controls both inbound and outbound traffic at the subnet level
You can secure your VPC instances using only security groups	Network ACLs are an additional layer of defense
Supports allow rules only	Supports both allow and deny rules
Stateful i.e. Return traffic is automatically allowed, regardless of any rules)	Stateless i.e. Return traffic must be explicitly allowed by rules
Evaluates all rules before deciding whether to allow traffic	Evaluates rules in number order when deciding whether to allow traffic, starting with the lowest numbered rule
Applies only to the instance that is associated to it	Applies to all instances in the subnet it is associated with
Has separate rules for inbound and outbound traffic	Has separate rules for inbound and outbound traffic
A newly created security group denies all inbound traffic by default	A newly created NACL denies all inbound traffic by default
A newly created security group has an outbound rule that allows all outbound traffic by default	A newly created NACL denies all outbound traffic by default
Instances associated with a security group can't talk to each other unless you add rules allowing it	Each subnet in your VPC must be associated with a network ACL. If none is associated, the default NACL is selected.
Security groups are associated with network interfaces	You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time