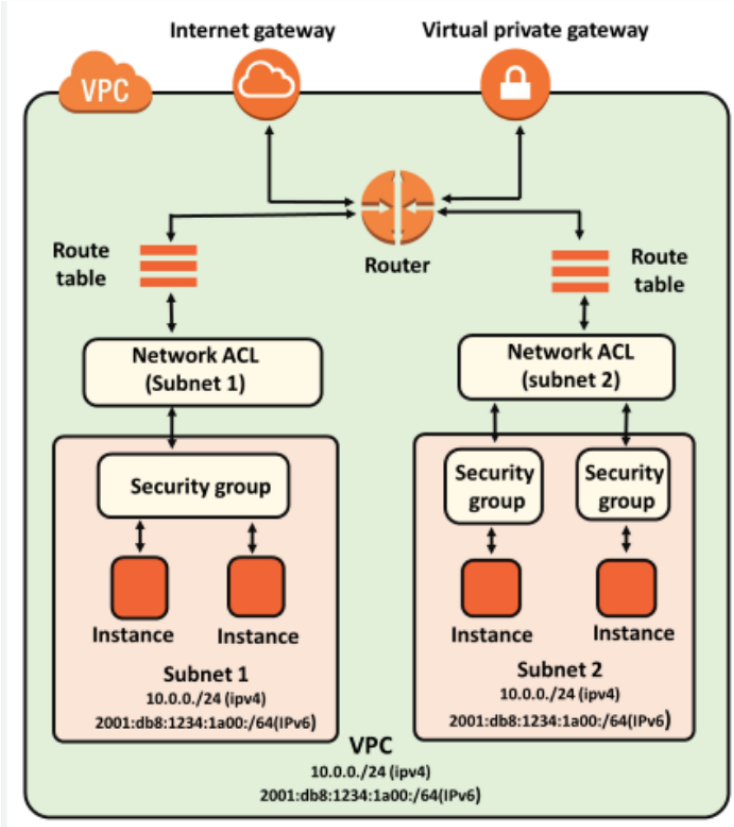
How do Security Groups and Network ACLs differ?



Feature	Security Groups	Network ACLs (NACLs)
Level	Instance level (ENI)	Subnet level

	Security groups are attached directly to **Elastic Network Interfaces (ENIs)**, which are associated with EC2 instances.	NACLs are applied at the **subnet level**, meaning they affect all resources (instances) within that subnet.
Rules Type	**Allow rules only**	**Allow and Deny rules**
	You can only define what traffic is **allowed**. All other traffic is implicitly denied.	You can explicitly define both **allow** and **deny** rules, giving more granular control.
State	**Stateful**	**Stateless**
	If an inbound rule allows traffic, the **response traffic is automatically allowed** out, even if there is no outbound rule. The reverse is also true.	Each rule is **evaluated separately** for inbound and outbound traffic. Return traffic **must be explicitly allowed** with a separate rule.
Return Traffic	**Automatically allowed**	**Must be explicitly allowed**
	No need to write rules for return traffic; handled automatically.	If you allow inbound traffic, you must separately allow the corresponding outbound traffic.

How do Security Groups and Network ACLs differ in AWS?

A. Security Groups are applied at the subnet level, while Network ACLs are applied at the instance level

B. Security Groups support both allow and deny rules, while Network ACLs support only allow rules

C. Security Groups are stateful, while Network ACLs are stateless

D. Network ACLs are used only for internet-facing applications, while Security Groups are used for internal traffic only

Correct Answer: ✅ **C. Security Groups are stateful, while Network ACLs are stateless**