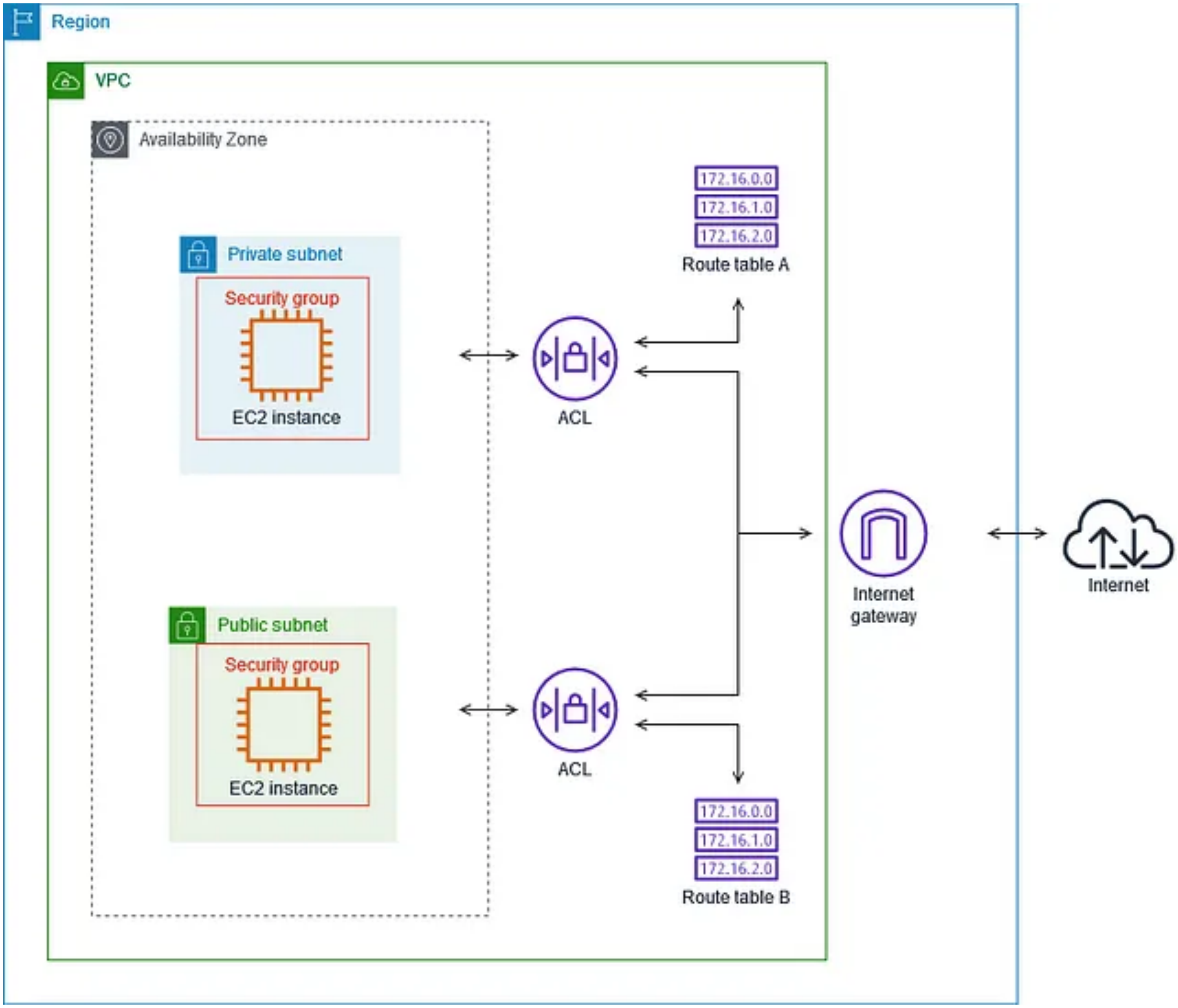
AWS — Difference between Security Groups and Network Access Control List (NACL)

Ashish Patel

Comparison: VPC Security Group vs NACL in AWS.



Awesome Cloud — Security Groups and Network ACLs

TL;DR:

Security group is the firewall of EC2 **Instances**.
Network ACL is the firewall of the VPC **Subnets**.

Key Differences: Security group vs NACL

Scope: Subnet or Instance (where to apply)

Security Groups operate at Instance (Network Interface) level. Security Group has to be assigned explicitly to the instance.

Network ACLs at the subnet level. Applies automatically to all instances deployed in the associated subnet.

State: Stateful or Stateless

Security groups are stateful. Return traffic is allowed, regardless of the rules.
e.g. If you allow an incoming traffic on port 80, the outgoing traffic on port 80 will be automatically allowed.

Network ACLs are stateless. Return traffic must be explicitly allowed by the rules. Meaning any changes applied to an incoming rule will not be applied to outgoing rule.
e.g. If you allow an incoming port 80, you would also need to apply the rule for outgoing traffic.

Rule Type: Allow or Deny

Security group supports allow rules only (everything else is denied implicitly). You can specify allow rules, but not deny rules.
e.g. You cannot deny a certain IP address from establishing a connection.

Network ACL supports allow and deny rules.
e.g. By deny rules, you could explicitly deny a certain IP address to establish a connection to an EC2 Instance.

Rule Process order

Security group evaluates all rules before deciding whether to allow traffic. (When you associate multiple security groups with a resource, the rules from each security group are aggregated to form a single set of rules that are used to determine whether to allow access.)

Network ACL evaluates rules in order, starting with the lowest numbered rule, when deciding whether to allow traffic.
If matching rule found during evaluation, remaining rules won't be evaluated.

Occurrence

Instance can have multiple Security groups.

Subnet can have only one NACL.

Rule Destination

Security group rule allows CIDR, IP, and Security Group as destinations.

Network ACL rule only allows CIDR as a destination.

Defense order

Security group first layer of defense, whereas Network ACL is the second layer of defense for outbound/egress traffic.

Network ACL first layer of defense, whereas the Security group is the second layer of defense for inbound/ingress traffic.

> *Consider creating Network ACLs with rules similar to your security groups, to add an additional layer of security to your VPC.*

View more from *Awesome Cloud*

- Difference between SQS and SNS
- Difference between Application load balancer and Network load balancer
- Difference between Amazon Aurora and Amazon RDS
- Difference between Internet Gateway and NAT Gateway
- Difference between Secrets Manager and Parameter Store
- Difference between EKS and ECS

Happy Clouding!!!