AWS SG & NACL

As before we learned about AWS VPC. VPC is a very crucial service of AWS, because it connects the idea of public cloud with private cloud. Now, from before we know that when a user or internet tries to connect to an application deployed in AWS VPC's EC2 instance, NAT translates the private IP to public to keep the IP safe, and even the user passess through multiple systems to reach the application. If passess through VPC's internet gateway, then ELB, then to the application. This means we can add security and authentication at multiple levels to restrict traffic and access.

Addition of security at subnet level is NACL and at application level is SG.

So, both SG and NACL are network firewalls, which control the traffic from inbound and outbound of the resources.

What are Security Groups?

Security groups are virtual shields or protectors of EC2 instances. Unless specifically allowed by default, all inbound traffic is blocked where as all outbound traffic is allowed from the Instance.

In SG you can have specific ALLOW rules but no specific DENY rules

What is NACL?

NACL is a virtual firewalls for subnets which controls the inbound and outbound traffic of subnets. After a VPC is created a default NACL will be associated and allow all inbound and outbound traffic.

NACL has both specific ALLOW & DENY rules.

Combining SG & NACL

Imagine a situation where you have a setup:

1. Web Server: An EC2 instance hosting a public-facing web application.
2. Database Server: An EC2 instance hosting a database, accessible only by web server.
3. VPC: Contains two subnets - one for public for webserver, one private for database server.

NACL Configuration:

Inbound rules:

1. Allow HTTP (port 80) req. from any IP
2. Allow HTTP (port 443) from any IP
3. Allow SSH (port 22) from a specific IP range (eg: 16.0.0.0/24)
4. Deny all other inbounds

SG Configuration

Inbound:

1. Allow HTTP port 80 from all IP
2. Allow HTTP port 443 from all IP
3. Allow SSH (port 22) from all IP

Outbound:

1. Allow MySQL port 3306 to DB server's IP
2. Allow all other outbounds

In this concrete example:

① NACL provide the first layer of security by allowing or denying traffic at subnet level. Inbound traffic to the public subnet is restricted to HTTP, HTTPS and SSH from specific IP ranges, while all other traffics are denied. The private subnet only allows MySQL traffic from the webserver's IP range. denying all other inbound traffic.

② Security Groups provide a second layer of security by allowing or denying traffic at the instance level. The webservers allow HTTP, HTTPS and SSH traffic, and it can send MySQL traffic to the database server. The DB server only accepts MySQL traffic from the web server's SG, enhancing the security by ensuring only the web server can communicate with it.

Summary

NACL only works at broader level, therefore within a same subnet, there might by public and private server, so each of them need security. Thus, both are important.