"How do you secure your cloud network with Security Groups and NACLs?”

What are security Groups?

Security groups are what we call the safeguards in the AWS that controls the incoming and outgoing traffic from EC2 instance depending upon a pre-defined set of rules. The major key point of the security groups is that they work at the instance level of the Virtual Private Cloud. And because of this, the security groups can be enforced on multiple instances, whereas an instance can also relate to multiple security groups. The security groups are automatically created when AWS creates Virtual Private Cloud. Moreover, while the rules of the security groups can be updated, the security groups cannot be permanently eradicated.

What are NACLs?

NACLs are the same as security groups in a way that both control the incoming and outgoing traffic depending on the pre-defined set of rules but the difference comes from the fact that NACLs work on the subnet instead of the EC2 instance. Therefore, NACLs usually relate to network-level security. As NACLs work at the subnet level of the Virtual Private Cloud, a single NACL can be associated with multiple subnets, however, a subnet can only have one single NACL related to it. Same as the security groups, NACLs are automatically created when AWS creates Virtual Private Cloud and while rules governing NACLs can be updated, NACLs individually cannot be deleted.

How do Both secure the cloud network?

While a cloud network can be secured just by using NACL or a security group, it is recommended that both are used to create the most protection. The main job of both of them is to act as a virtual firewall that filters out the incoming and outgoing traffic. In the could network, NACLs filter out the traffic first and after that, it is filtered by the security groups. They both work at different levels, NACL at the subnet level and security groups at the instance level, so they do complement each other. However, security groups are considered as required for instance protection as each EC2 instance must have at least one security group associated with it. Whereas the NACL is referred to as more of a side option for instance protection.

Security groups work based on the rules they are set up with, so the more strict the rules are, the more the EC2 instances be secured. On contrary, NACLs are processed on individual bases as each of its rule are given a number and AWS started in ascending order as soon as the traffic matches any of those rules, it is allowed to pass, whereas if it doesn’t next rule is applied.

The best way to secure the cloud network is by NACLs as are the first level of protection and then having security groups defined to increase the security.

Diagram

Description automatically generated

Photo retrieved from: https://www.javatpoint.com/aws-nacl-vs-security-group.

References

Wright, D. (n.d.). *Cloud network security 101: AWS Security groups VS nacls*. Fugue. Retrieved April 14, 2022, from https://www.fugue.co/blog/cloud-network-security-101-aws-security-groups-vs-nacls