**What is Amazon EC2 Security Groups**

Security groups is an AWS virtual firewall solution that filters the inbound and outbound traffic of an EC2 instance.

This means security groups acts as NACL (Network Access Control List).

Security groups has rules that allow defined types of traffic can only access the instance and same as defined type of traffic can only leave from instance.

**Note:** Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC can be assigned to a different set of security groups.

**Note:** you can assign up to 5 security groups to the instance. If you need to increase or decrease this limit, you can contact AWS Support.

For each security group, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.

You can have 50 inbound and 50 outbound rules per security group giving a total of 100 combined inbound and outbound.

**Note:** If you launch an instance using the Amazon EC2 API or a command line tool and you don't specify a security group, the instance is automatically assigned to the default security group for the VPC.

If you launch an instance using the Amazon EC2 console, you have an option to create a new security group for the instance.

**Difference b/w Security groups and NACL (Network access control list)**

| **Security group** | **Network ACL** |
| --- | --- |
| Operates at the instance level | Operates at the subnet level |
| Supports allow rules only | Supports allow rules and deny rules |
| Return traffic is automatically allowed, regardless of any rules. | Return traffic must be explicitly allowed by rules. |
| We evaluate all rules before deciding whether to allow traffic | We process rules in order, starting with the lowest numbered rule, when deciding whether to allow traffic |
| Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on | Automatically applies to all instances in the subnets that it's associated with (therefore, it provides an additional layer of defense if the security group rules are too permissive) |

The following diagram illustrates the layers of security provided by security groups and network ACLs.


        Traffic is controlled using security groups and network ACLs
      

Traffic from an internet gateway is routed to the appropriate subnet using the routes in the routing table.

The rules of the network ACL(NACL) that is associated with the subnet control which traffic is allowed to the subnet.

The rules of the security group that is associated with an instance control which traffic is allowed to the instance.

**Note:** By default, all types of traffics are allowed in outbound rules on an EC2 instance.

If you don’t want to allow all types of outbound traffic you can edit/change the outbound rules.