Security groups vs Network ACLs - What is the Difference?

The differences between NACL and security groups have been discussed below:

NACL	Security Group
Network Access Control List that helps provide a layer of security to the amazon web services. There are two kinds of NACL- Customized and default.	A security group must be explicitly assigned to an instance; it doesn't associate itself to a subnet.
Multiple subnets can be bound with a single NACL, but one subnet can be bound with a single NACL only, at a time	Security groups are associated with an instance of a service. It can be associated with one or more security groups which has been created by the user.
NACL can be understood as the firewall or protection for the subnet.	Security group can be understood as a firewall to protect EC2 instances.
These are stateless, meaning any change applied to an incoming rule isn't automatically applied to an outgoing rule.	These are stateful, which means any changes which are applied to an incoming rule is automatically applied to a rule which is outgoing.
Example: If a request comes through port 80, it should be explicitly indicated that its outgoing response would be the same port 80.	Example: If the incoming port of a request is 80, the outgoing response of that request is also 80 (it is opened automatically) by default.
NACL can be used to support as well as deny rules. Denial of rules can be explicitly mentioned, so that when the layer sees a specific IP address, it blocks connecting to it.	They support rules only, and the default behaviour is denial of all rules. Every VPC can belong to different security groups.

NACL	Security Group
It is considered to be the second layer of defence, which helps protect AWS stack. It is an optional layer for VPC, which adds another security layer to the amazon service.	It is considered to be the first defence layer that helps protect the Amazon Web Services infrastructure.
In case of NACL, the rules are applied in the order of their priority, wherein priority is indicated by the number the rule is assigned.	In case of a security group, all the rules are applied to an instance.
This means every rule is evaluated based on the priority it has.	This means all rules are evaluated before they allow a traffic.