What is NACL?

NACL also adds an additional layer of security associated with subnets that control both inbound and outbound traffic at the subnet level.

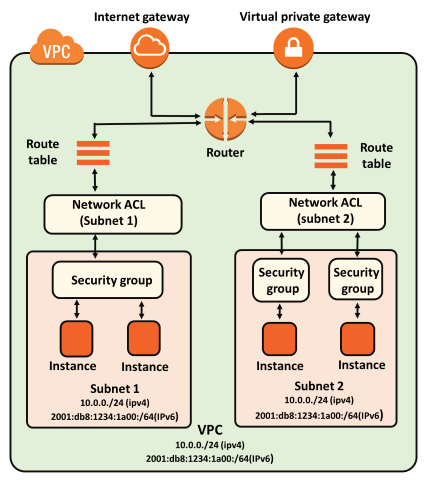
A network access control list (NACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

Combining Security Group and NACL

Maximum number of rules that exist per NACL: 20

Maximum number of rules that can exist per Security Group: 50

Differences b/w Security Group and NACL



|  |  |  |
| --- | --- | --- |
| **Security Group** | **NACL (Network Access Control List)** | |
| It supports only **allow** rules, and by default, all the rules are denied. You cannot deny the rule for establishing a connection. | | It supports both **allow and deny** rules, and by default, all the rules are denied. You need to add the rule which you can either allow or deny it. |
| It is a **stateful** means that any changes made in the inbound rule will be automatically reflected in the outbound rule. For example, If you are allowing an incoming port 80, then you also have to add the outbound rule explicitly. | | It is a **stateless** means that any changes made in the inbound rule will not reflect the outbound rule, i.e., you need to add the outbound rule separately. For example, if you add an inbound rule port number 80, then you also have to explicitly add the outbound rule. |
| It is associated with an EC2 instance. | | It is associated with a subnet. |
| All the rules are evaluated before deciding whether to allow the traffic. | | Rules are evaluated in order, starting from the lowest number. |
| Security Group is applied to an instance only when you specify a security group while launching an instance. | | NACL has applied automatically to all the instances which are associated with an instance. |
| It is the first layer of defense. | | It is the second layer of defense. |

**Step 1: Create VPC**

Services - VPC - Create VPC -vpn only - Name (my-vpc) - 10.0.0.0/16 - create VPC.

**Step 2: Create public Subnet (public-subnet)**

Subnet -Create Subnet - Name (public-subnet) - VPC (my-vpc) - Availability Zone (2a) - IPv4 CIDR Block (10.0.0.0/24) - Create subnet.

**Step 3: Create Internet Gateway**

Click on Internet Gateways – Create Internet Gateway – Name Tag (my-igw) – create Internet gateway – Action – Attach to VPC – Available VPC’s (my-vpc) – Attach Internet Gateway.

**Step 4: Routing Tables for public-subnet01**

Click on Route Tables – Create Route Table – Name (public-routing) – VPC (my-igw) –create route table - Subnet associations – edit subnet associations – select public-subnet01 – save association – routes – edit routes – add route – 0.0.0.0/0 – select internet gateway – save changes

**Step 5: Create NACL**

Service – VPC – Security – Network ACLs – Create Network ACL – Name (my-nacl) – VPC (my-vpc) - Create.

Now, Select create NACL –Inbound Rule – Edit Inbound Rule – Add Rule –

Rule# (100) – Type (RDP (3389)) – Protocol (TCP) – Port Range (3389) – Source (0.0.0.0) – Allow/Deny (ALLOW) – Save.

**Now click on Outbound Rules -**

Rule# (100) – Type (HTTP (80)) – Protocol (TCP) – Port Range (80) – Source (0.0.0.0) – Allow/Deny (ALLOW) – Save.

Rule# (200) – Type (HTTPS (443)) – Protocol (TCP) – Port Range (443) – Source (0.0.0.0) – Allow/Deny (ALLOW) – Save.

Attach New created NACL with public subnet

Select created nacl (my-nacl) – action – edit subnet association – select “public-subnet” – save.

**Note: we just add RDP in inbound not for outbound**

**Step 6: Now Instance Windows Server 2016**

Same step to create regular windows instance.

Services – EC2 – Launch Instance – Win-server2016 – my-vpc - public-subnet – security group (all traffic allow) – Launch.

Access it using RDP

**It failure due to RDP outbound Not enabled in NACL.**

**Step7: Allow RDP outbound through NACL**

Service – VPC – Network ACL – select my-nacl – outbound Rules – Edit outbound Rules – Add rule

Rule# (250) – Type (Custom TCP Rule) – Protocol (TCP) – Port Range (1024-65535) – Source (0.0.0.0) – Allow/Deny (ALLOW) – Save.

Now Try RDP Access Again, I will work properly.

Now try to Access Internet from windows server 2016,

It Failure Again Cause of Not allow inbound and outbound internet traffic both rule. So check http,https allowed in inbound and outbound.

Go NACL again Edit inbound rules, add rules-

Rule# (200) – Type (Custom TCP Rule) – Protocol (TCP) – Port Range (1024-65535) – Source (0.0.0.0) – Allow/Deny (ALLOW) – Save.

Now Try to Access Internet again through windows server 2016