COURSEWARE

AWS Network Access Control Lists (NACLs) CLI

Contents

Overview

Network **A**ccess **C**ontrol **L**ists **(NACLs)** are an optional layer of security for your VPC that act as a firewall for controlling traffic that enters your subnets. An NACL is a **Network** level firewall, so it has the same principles as a **security group**, where you allow certain IP Address to have access to a port running an application.

Network ACL Basics

- By default, VPCs have **NACLs** that allow all inbound and outbound IPv4 and (if applicable) IPv6 traffic. These default NACLs can be modified.
- You can create your own NACL and associate it to a VPC. By default, the NACLs will deny all inbound and outbound until you add rules.
- Each subnet in a VPC you create will have to be associated with a NACL. If you do not specify, then it will be associated with the default NACL.
- You can have multiple subnets associated with a single NACL. However, you cannot have multiple NACLs associated to a single subnet. When you attempt to associate more than one NACL to a single subnet, the previous NACL will be replaced by the new NACL.

Network ACL Rules

- You can add or remove rules from the default network ACL, or create additional network ACLs for your VPC. When you add or remove rules from a network ACL, the changes are automatically applied to the subnets that it's associated with.

Ingress / Egress

This configuration sets whether the rule created is for incoming / outgoing traffic

Rule Number

This sets the priority level of the rules attached to the network access control list. The lower the rule number
the higher the priority.

Protocol

There are only a couple of protocols that you need to concern yourself about, TCP and UDP. Most of the
time you will be using TCP

Port Range

This defines the ports through which you want to allow network traffic. For example, port 80 would allow incoming HTTP traffic.

Cidr Block

This defines the block of IP addresses that traffic can come from or go to depending on whether it is an ingress or an egress rule. For example, `10.0.0/24` is the IP range `10.0.0.0 - 10.0.0.255`.

Rule Action

This is important, it defines whether the rule was created to allow or deny traffic.
So there are options where you can explicitly deny if you want to.

Only options are **allow** or **deny**.

Tutorial

In this tutorial, we will create our first Network Access Control list. The best practice is to create an NACL for each VPC. By default there is already an NACL associated with the VPC, so we will create our own and replace the default NACL.

1. Create a VPC by running this command:

```
# Creating VPC
aws ec2 create-vpc --cidr-block 155.124.0.0/16
```

2. Get the VPC ID for your new VPC. Run the following command:

```
# Getting a list of VPC IDs
aws ec2 describe-vpcs --output text --query "Vpcs[].VpcId"
```

You must identify which VPC ID you want to use and create an NACL for. The short VPC ID is usually the Default VPC that already has an existing NACL.

3. Create your NACl by running the following command:

```
# Create NACLs for your new VPC
aws ec2 create-network-acl --vpc-id (your vpc id)
```

When you created your VPC, an NACL was automatically created for it. The above command was to demonstrate how to create your own NACL. There are now two NACLs associated with your VPC, the default one and the one you just created.

4. Let's get the NACL id. Run the following command:

```
# Get NACLs ID
aws ec2 describe-network-acls --filters "Name=vpc-id,Values=(your vpc id)"
```

Copy the NACL ID which you want to add rules to. I would suggest copying the ID for the default NACL. This is where the property "IsDefault" is "true".

5. Let's add a simple rule to your NACL. Run the following command:

```
# Adding NACLs rule
aws ec2 create-network-acl-entry --network-acl-id (your nacls id) --ingress --
rule-number 50 --protocol tcp --port-range From=8080,To=8080 --cidr-block
0.0.0.0/0 --rule-action allow
```

The above command created a rule that allows incoming traffic into port 8080 from any IP address using the TCP protocol. Rule number 50 implies that it would override any contradicting rules with a higher rule number.

6. You can navigate to your NACLs in the Web Console which can be found under VPC and view the rules you add.

We need to clean up our AWS Environment.

7. First, let's remove the NACL that we created. Make sure you get the NACL id of the non-default one. Run the following command:

```
# deleting nacls
aws ec2 delete-network-acl --network-acl-id (your nacl id)
```

8. Delete our VPC we created for this section. Run the following command:

```
# delete VPC
aws ec2 delete-vpc --vpc-id (your vpc id)
```

Exercises

1. Create your own VPC, Subnets and NACLs
2. Launch an EC2 instance in the VPC with your own NACL, make sure you are able to SSH into your Instance
3. Create a Rule in your NACL that will prevent you from connecting to your instance via SSH. Please do not set these rules in any of the first 20 numbers.
4. Create a rule that will allow you to connect back into your instance through SSH without removing the previous rule.