**Network ACL (NACL)**

----------------------------

Security group will provide security at instance level

NACL will provide security at subnet level.

**Creating NACL**

------------------------

Select Network ACL ---- We have two default NACL

One for default VPC

One for MyVPC

(So, whenever we create new VPC, by default NACL is created automatically)

We will create a new NACL and attach to public subnet

----------------------------------------------------------------

Create Network ACL -- Name Tag: PublicNACL

VPC: MyVPC

Create

Subnet Associations -- Edit subnet associations --select public subnet

Edit

------------

Now, try to access the webserver

We cannot get the webpage !!! No

We need to open ports at NACL

Inbound rules ---- Edit inbound rules --Add rule

Rule# Type Source

100 SSH 49.204.176.51/32 (My laptop IP,we can get it from bastion security group)

200 HTTP 0.0.0.0/0 (HTTP open to all)

Save.

Now, try to access the webserver

We cannot get the webpage !!! No

We need to know about stateful and stateless

---------------------------------------

Let’s select webSecurity group -- Inbound tab -- edit

Did we add ports in outbound tab?

In security group, when we open inbound port, by default outbound port is open to all.

This status is called stateful.

So, we have opened HTTP incoming, by default outbound port is open to all.

Hence, we are able to access webserver.

This status is called stateful. **Security Groups are stateful**.

For NACL, The case is different.

We need to open outbound port to NACL explicitly.

So, **NACL is stateless**

Select NACL -- Outbound Rules --- Edit Outbound Rules --- Add Rule

Rule Type Destination

100 SSH 183.83.38.112/32 (MY IP)

200 HTTP 0.0.0.0/0

Save

Now, can we able to access webserver

No!!!

**Ephemeral ports**

-----------------------

Total Range of ports: 0 to 65535

Range 1024 - 65535 are the range of ephemeral ports

search in google "ephemeral ports in AWS", we can see the range

Assume in public subnet, we have 100 webservers

All are connected to load balancer.

If hacker blocks any http port on 1 webserver

Will it be a problem?

No!!

As load balancer will send the request to other servers.

If hacker blocks any http port on NACL level (subnet level)

Entire website is down.

To avoid this problem, AWS is providing range of ports (1024 - 65535)

We need to open this range in NACL level,

So, when hacker blocks a particular port (HTTP), AWS uses a random port from the range.

AWS will replace the random as HTTP port.

So that website will never go down.

Note: Ephemeral ports are mandatory at NACL level

++++++++++++++++++

Select -- PublicNACL --- Inbound -- Edit inboud rules -- Add rule

Rule Type port range

300 Custom TCP Rule 1024-65535

Save.

Now, can we able to access webserver?

No!!

NACL are stateless. We need to open ports in outbound level also.

Select -- PublicNACL --- Outbound -- Edit outboud rules -- Add rule

Rule Type port range

300 Custom TCP Rule 1024-65535

Save.

++++++++++++++++++

Now, can we able to access webserver?

Yes!!

++++++++++++++++++++

**What is the use of NACL?**

Select our NACL -- inbound rules

Rule Type

200 HTTP we have opened to all.

Add Rule

Rule# Type Allow/ Deny

201 HTTP Deny

Save.

Similarly

Select our NACL -- outbound rules

Rule Type

200 HTTP we have opened to all.

Add Rule Type Allow/ Deny

201 HTTP Deny

Save.

Now, Are we able to access webserver?

Yes!!!

Conclusion, Lowest rule# will have highest priority.

Now, in inbound rules

Rule# -- 201 change to 199.

Save.

goto outboud rules

Rule# -- 201 change to 199.

Save.

Now, Lowest rule# is 199 which is deny.

so, we cannot access the webserver.

No!!

Usecase:

-------------

Hacker is continuous accessing the webserver.

We want to block his IP, but other customers should be able to access the webserver.

How can we do it.

Let’s Assume, I am the hacker

Now, in inbound rules, change the source

Rule# Source

199 49.204.176.51/32 (My laptop IP)

Save.

(Network team will give us incoming request IP address)

Similarly, in outboud rules also

Rule# Source

199 106.217.195.229/32 (My laptop IP)

Save.

Now, Are we able to access webserver

No! (As it is blocked to my machine)

But, others can able to access the webserver.

Implementing Usecase: By using NACL, we can block specific IP address

Now,

Let’s delete Rule# 199 from inbound and outbound level.

Save.

Now, Are we able to access webserver

Yes!!!

NACL is not recommended to use for private subnet.

++++++++++++++++++++++++++++++

Deletion process

-------------------

Step 1: Delete NAT

Step 2: Delete all Ec2 Machines

Step 3: Delete VPC

Step 4: Release Elastic IP