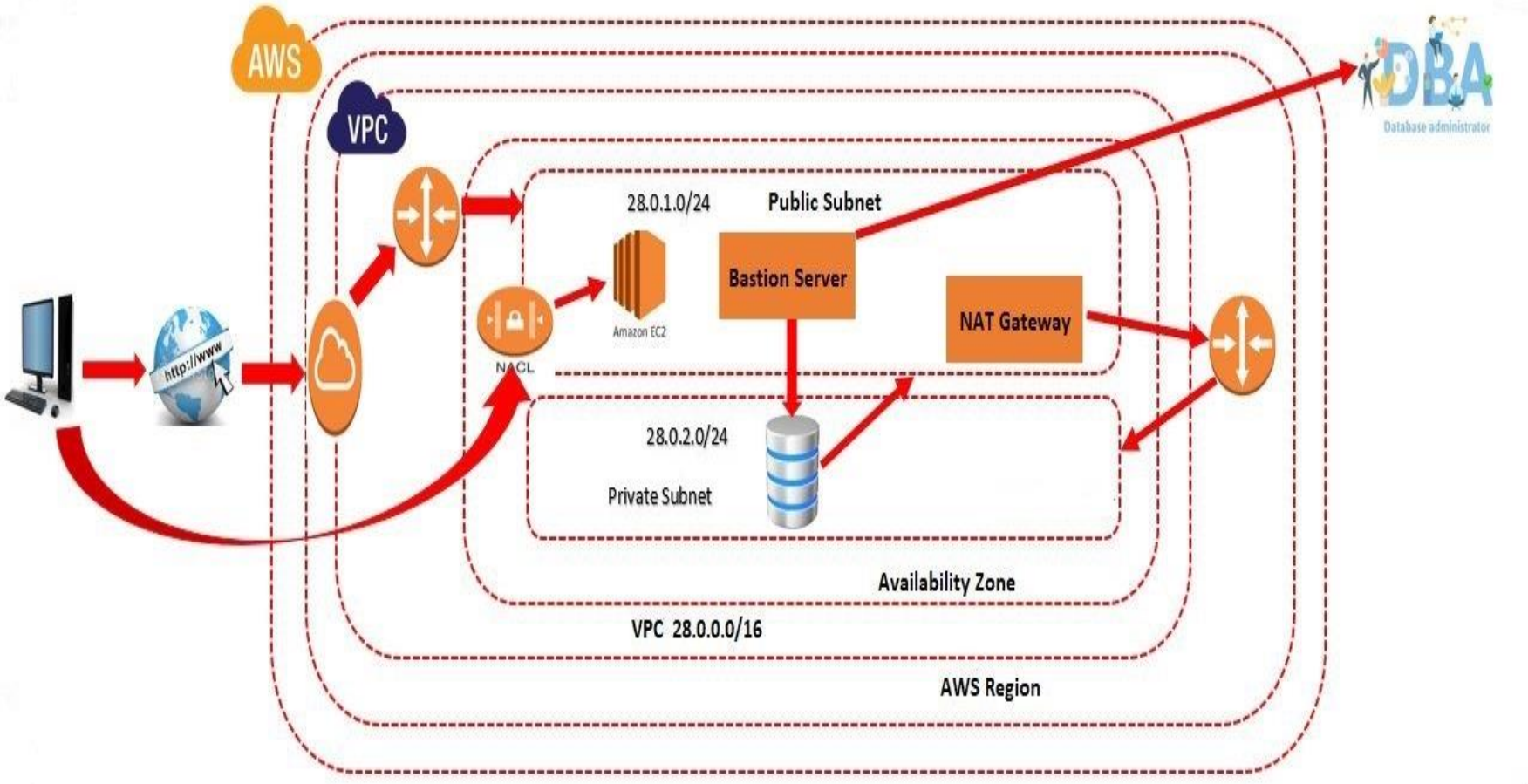
Amazon Web Services

Network Access Control Lists

ankitnarula1991@gmail.com

Network Access Control Lists - NACL

- It is a security layer for our VPC that controls the traffic in and out of one or more subnets. It is an optional layer for our VPC.



NACL - Important

- Our custom VPC automatically comes with the default Network ACL which includes all inbound and outbound ipv4 traffic.
- We can also create a custom network ACL and associates with a subnet. By default, a custom Network ACL denies all the inbound and outbound ipv4 traffic until you add rules.
- Network ACL is associated with both inbound and outbound rules that can either deny or allow the rules.
- A Network ACL contains numbered lists of rules that are evaluated in order, starting from the lowest numbered rule, to determine whether the traffic goes in or out of the subnet associated with the Network ACL. The highest numbered rule can be 32766. It is recommended to create new rules with increments (For example, increments of 10 or 100) so that you can easily add new rules where you need later on.

NACL

- Click on Network ACL
- Click on Create Network ACL
- Enter the name
- Select Our VPC
- Click on Create Network ACL
- No subnet attach to our NACL

NACL

- Attach Subnet to our NACL

Actions → Edit Subnet Associations

- Select public subnet
- Click on save changes
- Now, try to access the webserver
- Open ports in NACL at Inbound rules

Actions → Edit Inbound Rules

NACL

- Click on Add new rule
- Enter the Rule Number (100)
- Select Type as SSH
- In the Source enter our IP Address
- Click on Add New Rule
- Enter the Rule Number 200
- Select type as HTTP (80)
- Enter Source as 0.0.0.0/0
- Click on save changes

NACL

- Add the Rules in outbound rules

Actions → Edit Outbound rules

- Enter the Rule Number (100)
- Select Type as SSH
- In the Source enter our IP Address
- Click on Add New Rule
- Enter the Rule Number 200
- Select type as HTTP (80)
- Enter Source as 0.0.0.0/0
- Click on save changes

NACL - Ephemeral Ports

- An ephemeral port is a temporary communication hub used for Internet Protocol (IP) communications.

- Total Number of Ports are 0 to 65535 in networking but NAT gateway uses ports 1024-65535.

- For Example: Assume in public subnet, we have 100 webservers. All are connected to load balancer. If hacker blocks any http port on 1 webserver. There is will be no problem for us because all other 99 webservers are working fine. As load balancer will send the request to other servers.

- But 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**

NACL - Ephemeral Ports

- Enable at Inbound rules
- Click on Add Rule
- Enter Rule Number 300
- Enter Port range (1024-65535)
- Enable at Outbound rules
- Click on Add Rule
- Enter rule number 300
- Enter Port range (1024-65535)

NACL - Deny Rules

- Create one more rule in inbound rules
- Enter Rule Number as 201
- Select type as HTTP(80)
- Enter Source as 0.0.0.0/0
- Select Allow/Deny as Deny
- Create Same rule in Outbound also

NACL - Deny Rules

- Now Change the rule number 201 to 199 in inbound rule
- Now Change the rule number 201 to 199 in outbound rule
- **Use cases:** Hacker is continuous accessing the webserver. We want to block his IP, but other customers should be able to access the webserver.
- For Better understand Enter the our own IP Address in Source
- Change rule in Inbound & outbound rules
- **Imp Use case**: By using NACL, we can block specific IP address & Network team will give us incoming request IP address.

NACL - Deletion process

- Step 1: Delete NAT
- Step 2: Delete all Ec2 Machines
- Step 3: Delete VPC
- Step 4: Release Elastic IP

NACL - D/B Security Group & NACL

Security Group	Network Access Control List
Operates at the Instance Level	Operates at Subnet Level
Support Allow rules Only	Support Allow rules and Deny Rules
State-full: return traffic is automatically allowed, regardless of any rules	Stateless: return traffic must be explicitly allowed by rules (think of ephemeral ports)
All Rules are evaluated before deciding whether to allow traffic	Rules are evaluated in order (Lowest to highest) when decided whether to allow traffic , first match wins
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.

ankitnarula1991@gmail.com