AWS-3

01-12-2019

Networking - VPC

1

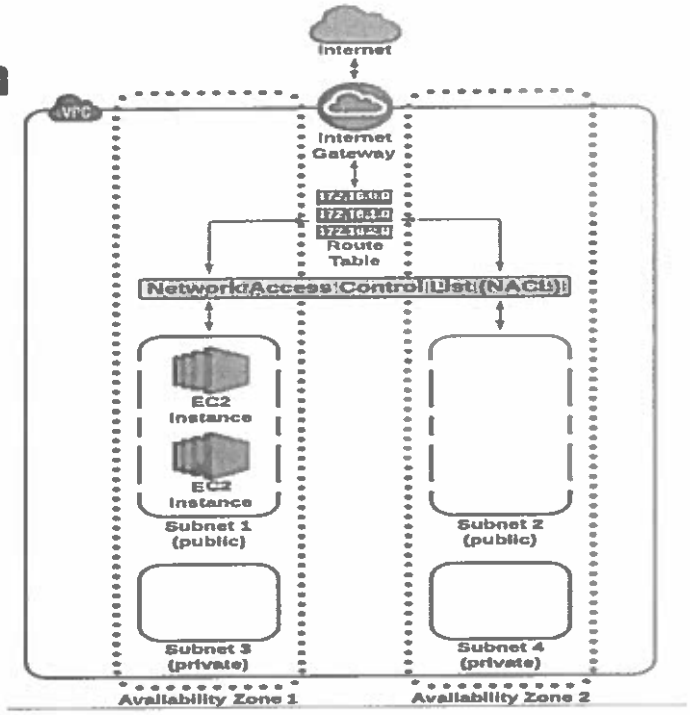
What is a VPC?

- A private sub-section of AWS that we control, in which we can place AWS resources (such as EC2 instances and databases).

- We have FULL control over who has access to the AWS resources that you place inside your VPC.

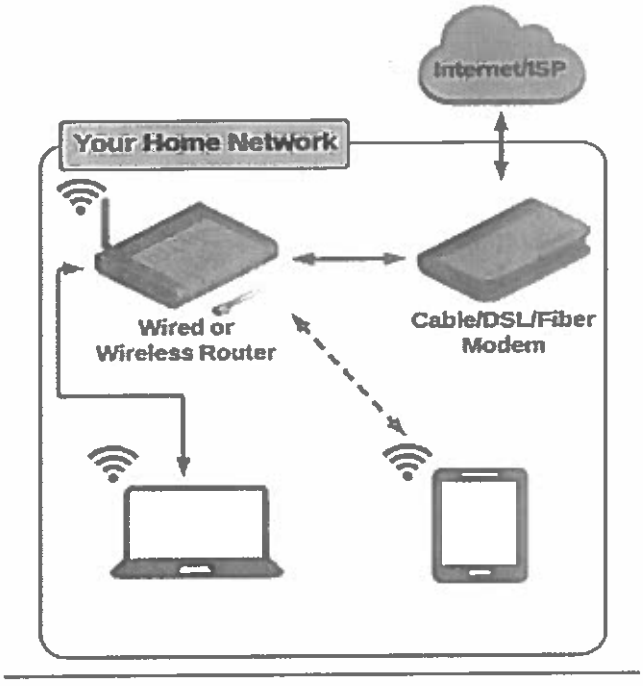
2

VPC Diagran

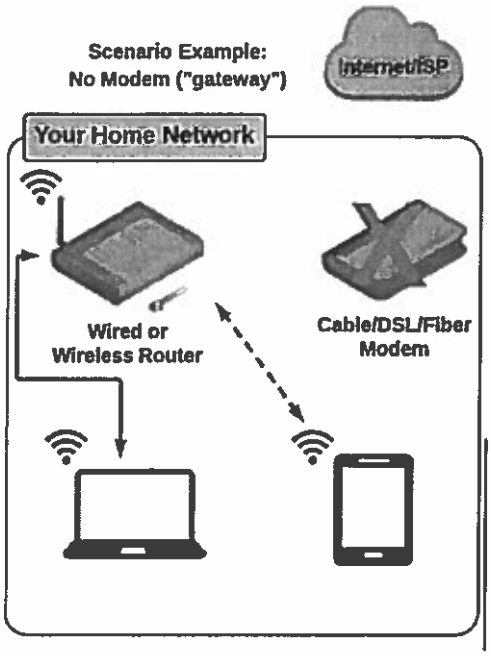


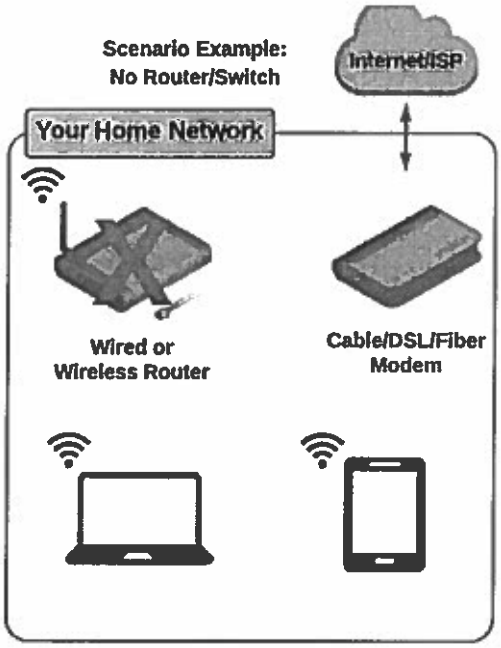
3

Home Network

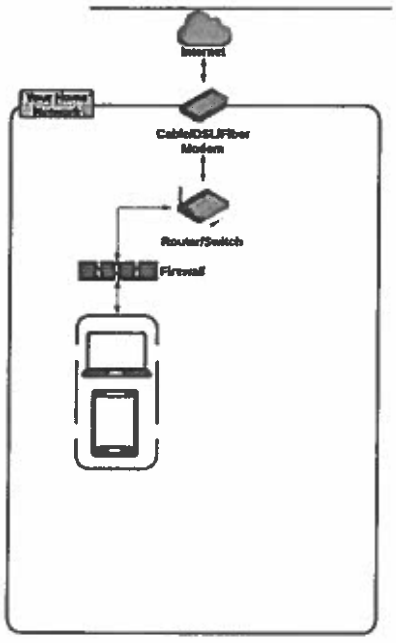


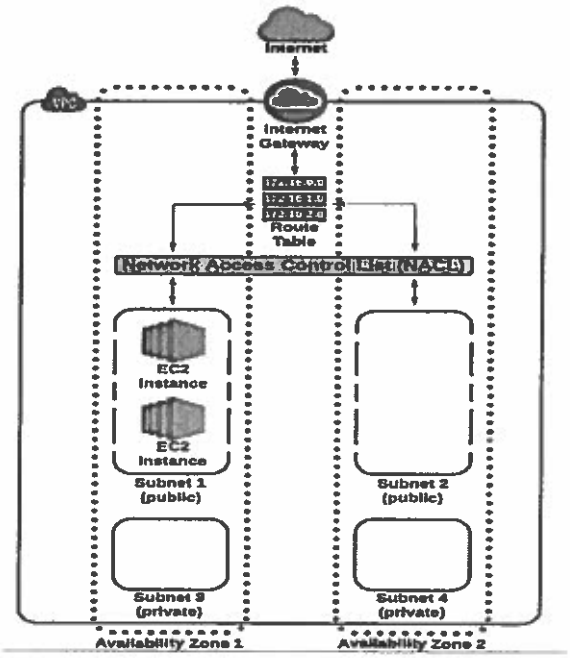
4


Scenario Example:
No Modem ("gateway")
Internet/ISP
Your Home Network
Wired or
Wireless Router
Cable/DSL/Fiber
Modem


Scenario Example:
No Router/Switch
Internet/ISP
Your Home Network
Wired or
Wireless Router
Cable/DSL/Fiber
Modem

5

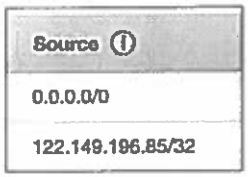

Internet
Cable/DSL/Fiber
Modem
Router/Switch
Firewall


Internet
Internet
Gateway
Route
Table
Network Access Control List (NACL)
EC2
Instance
EC2
Instance
Subnet 1
(public)
Subnet 2
(public)
Subnet 3
(private)
Subnet 4
(private)
Availability Zone 1
Availability Zone 2

6

Understanding CIDR - IPv4 (Classless Inter-Domain Routing)

- CIDR are used for Security Groups rules, or AWS networking in general



- They help to define an IP address range
  - WW.XX.YY.ZZ/32 == one IP
  - 0.0.0.0/0 == all IPs
  - But we can define for ex: 192.168.0.0/26:
    192.168.0.0 – 192.168.0.63 (64 IP)

7

Understanding CIDR

- A CIDR has two components:
  - The base IP (XX.XX.XX.XX)
  - The Subnet Mask (/26)

- The base IP represents an IP contained in the range
- The subnet masks defines how many bits can change in the IP

- The subnet mask can take two forms. Examples:
  - 255.255.255.0 (less common)
  - /24 (more common)

8

Understanding CIDRs Subnet Masks

- The subnet masks basically allows part of the underlying IP to get additional next values from the base IP
  - /32 allows for 1 IP = 2^0
  - /31 allows for 2 IP = 2^1
  - /30 allows for 4 IP = 2^2
  - /29 allows for 8 IP = 2^3
  - /28 allows for 16 IP = 2^4
  - /27 allows for 32 IP = 2^5
  - /26 allows for 64 IP = 2^6
  - /25 allows for 128 IP = 2^7
  - /24 allows for 256 IP = 2^8
  - /16 allows for 65,536 IP = 2^16
  - /0 allows for all IPs = 2^32

- Quick memo:
- /32 – no IP number can change
- /24 - last IP number can change
- /16 – last IP two numbers can change
- /8 – last IP three numbers can change
- /0 – all IP numbers can change

9

Understanding CIDRs Little exercise

- 192.168.0.0/24 = … ?
  - 192.168.0.0 – 192.168.0.255 (256 IP)
- 192.168.0.0/16 = … ?
  - 192.168.0.0 – 192.168.255.255 (65,536 IP)
- 134.56.78.123/32 = … ?
  - Just 134.56.78.123
- 0.0.0.0/0
  - All IP!
- When in doubt, use this website: https://www.ipaddressguide.com/cidr

10

Private vs Public IP (IPv4) Allowed ranges

- The Internet Assigned Numbers Authority (IANA) established certain blocks of IPV4 addresses for the use of private (LAN) and public (Internet) addresses.

- Private IP can only allow certain values
  - 10.0.0.0 – 10.255.255.255 (10.0.0.0/8) <= in big networks
  - 172.16.0.0 – 172.31.255.255 (172.16.0.0/12) <= default AWS one
  - 192.168.0.0 – 192.168.255.255 (192.168.0.0/16) <= example: home networks

- All the rest of the IP on the internet are public IP

11

Default VPC Walkthrough

- All new accounts have a default VPC

- New instances are launched into default VPC if no subnet is specified

- Default VPC have internet connectivity and all instances have public IP

- We also get a public and a private DNS name

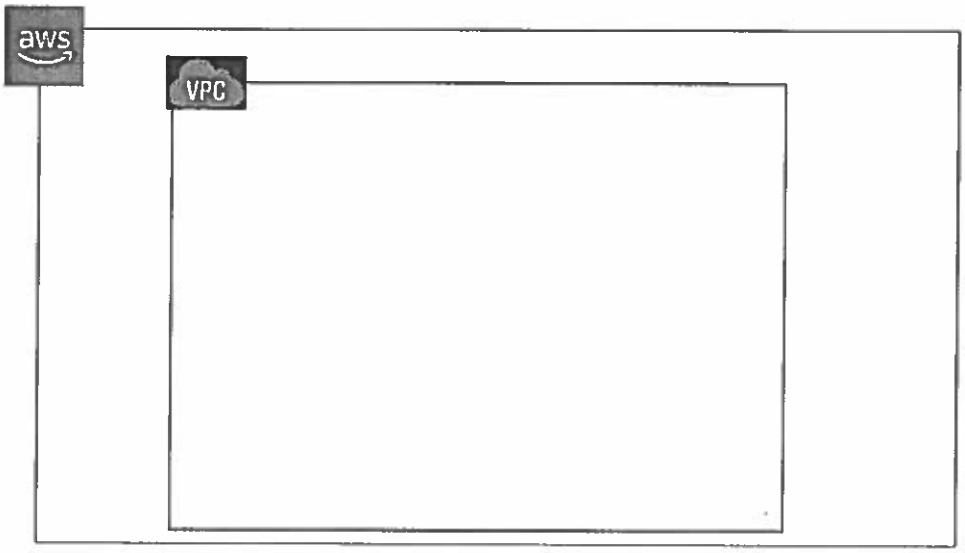
12

VPC in AWS – IPv4

- VPC = Virtual Private Cloud
- You can have multiple VPCs in a region (max 5 per region – soft limit)
- Max CIDR per VPC is 5. For each CIDR:
  - Min size is /28 = 16 IP Addresses
  - Max size is /16 = 65536 IP Addresses
- Because VPC is private, only the Private IP ranges are allowed:
  - 10.0.0.0 – 10.255.255.255 (10.0.0.0/8)
  - 172.16.0.0 – 172.31.255.255 (172.16.0.0/12)
  - 192.168.0.0 – 192.168.255.255 (192.168.0.0/16)
- Your VPC CIDR should not overlap with your other networks (ex: corporate)

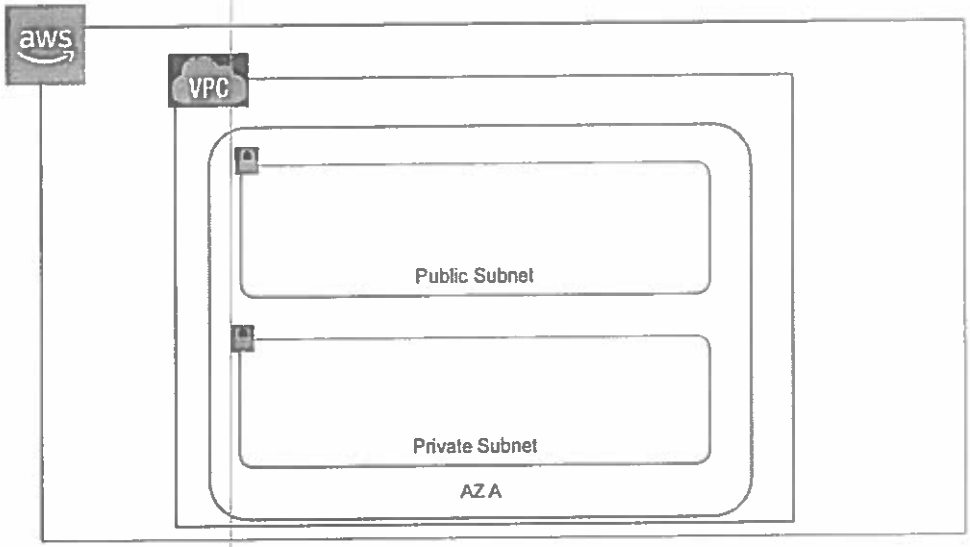
13

State of Hands On



14

Adding Subnets



15

Subnets - IPv4

- AWS reserves 5 IPs address (first 4 and last 1 IP address) in each Subnet
- These 5 IPs are not available for use and cannot be assigned to an instance
- Ex, if CIDR block 10.0.0.0/24, reserved IP are:
  - 10.0.0.0: Network address
  - 10.0.0.1: Reserved by AWS for the VPC router
  - 10.0.0.2: Reserved by AWS for mapping to Amazon-provided DNS
  - 10.0.0.3: Reserved by AWS for future use
  - 10.0.0.255: Network broadcast address. AWS does not support broadcast in a VPC, therefore the address is reserved
- Tip:
  - If you need 29 IP addresses for EC2 instances, you can't choose a Subnet of size /27 (32 IP)

16

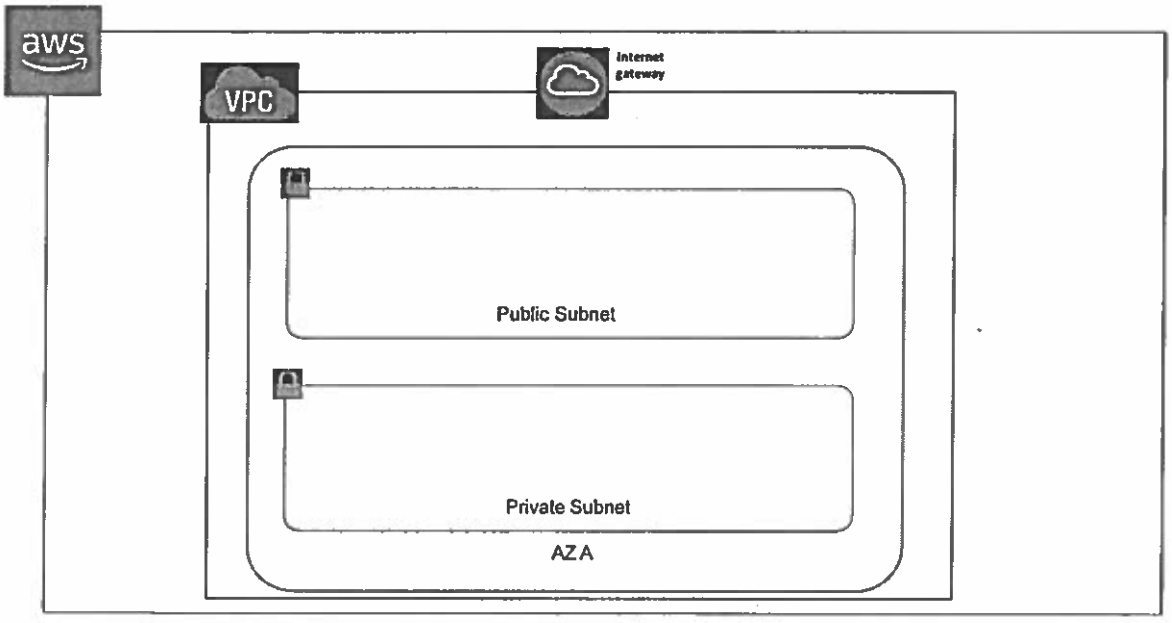
Internet Gateways

- Internet gateways helps our VPC instances connect with the internet
- It scales horizontally and is HA and redundant
- Must be created separately from VPC
- One VPC can only be attached to one IGW and vice versa
- Internet Gateway is also a NAT for the instances that have a public IPv4

- Internet Gateways on their own do not allow internet access…
- Route tables must also be edited!

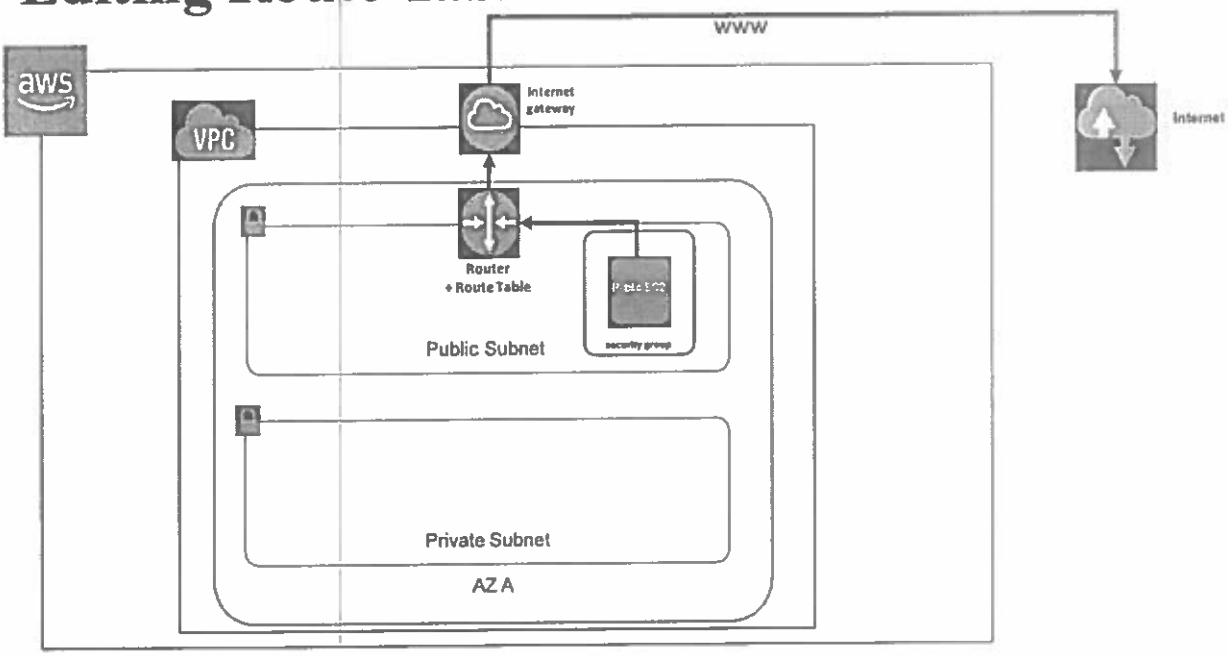
17

Adding IGW



18

Editing Route Tables



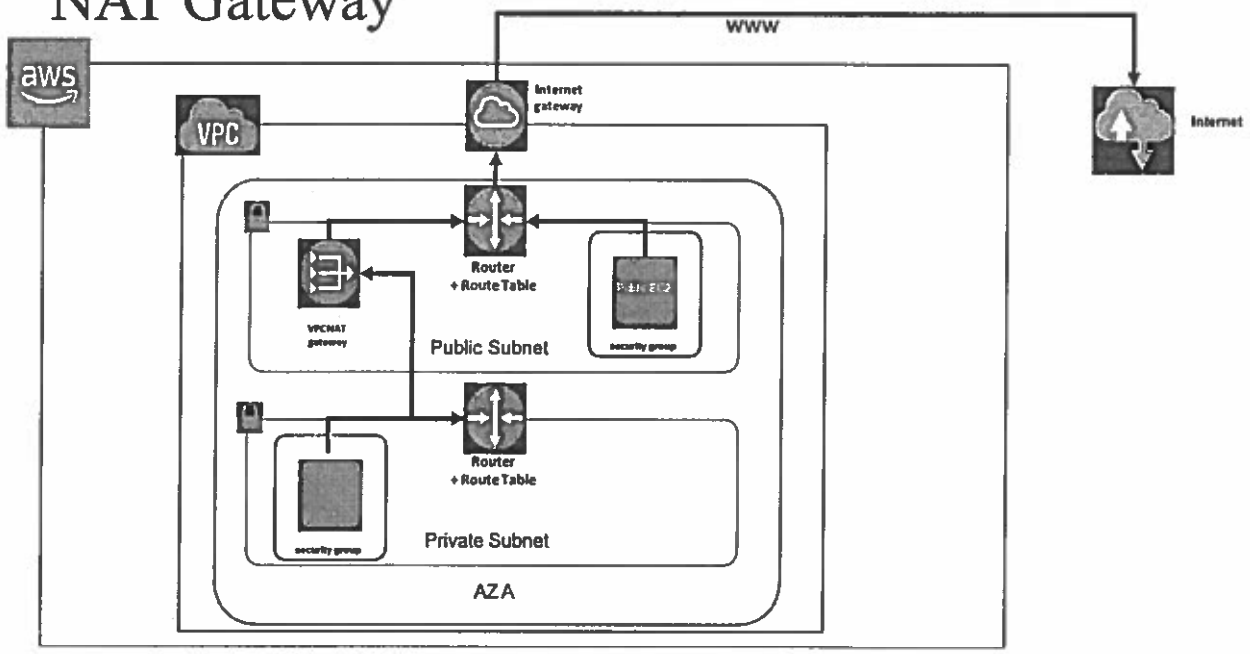
19

NAT Gateway

- AWS managed NAT, higher bandwidth, better availability, no admin
- Pay by the hour for usage and bandwidth
- NAT is created in a specific AZ, uses an EIP
- Cannot be used by an instance in that subnet (only from other subnets)
- Requires an IGW (Private Subnet => NAT => IGW)
- 5 Gbps of bandwidth with automatic scaling up to 45 Gbps

20

NAT Gateway



21

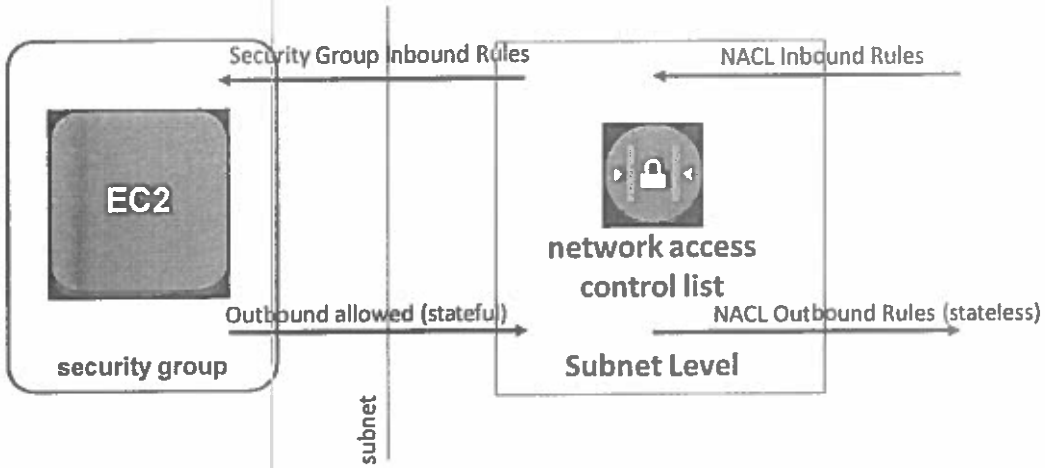
DNS Resolution in VPC

- enableDnsSupport: (= DNS Resolution setting)
  - Default True
  - Helps decide if DNS resolution is supported for the VPC
  - If True, queries the AWS DNS server at 169.254.169.253

- enableDnsHostname: (= DNS Hostname setting)
  - False by default for newly created VPC,True by default for Default VPC
  - Won't do anything unless enableDnsSupport=true
  - If True, Assign public hostname to EC2 instance if it has apublic

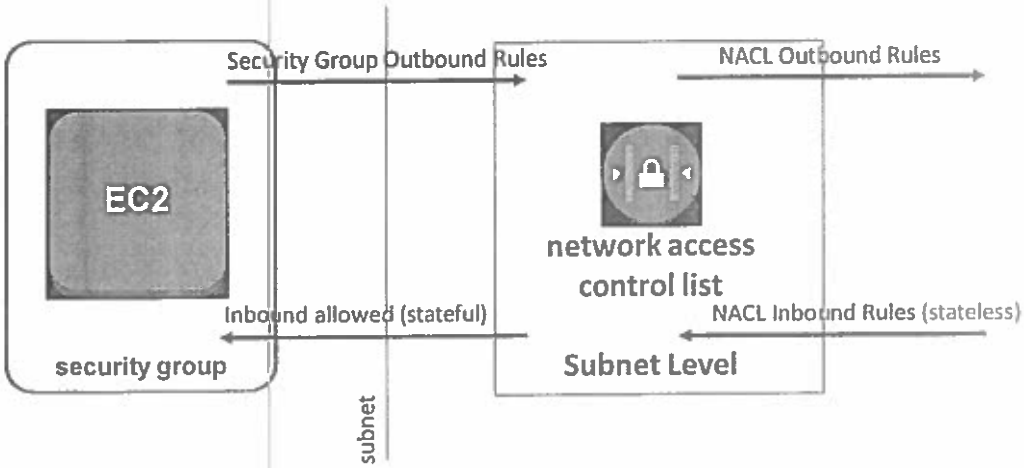
22

Network ACLs & SG Incoming Request



23

Network ACLs & SG Outgoing Request



24

Network ACLs

- NACL are like a firewall which control traffic from and to subnet
- Default NACL allows everything outbound and everything inbound
- One NACL per Subnet, new Subnets are assigned the Default NACL
- Define NACL rules:
  - Rules have a number (1-32766) and higher precedence with a lower number
  - E.g. If you define #100 ALLOW <IP> and #200 DENY <IP>, IP will be allowed
  - Last rule is an asterisk (*) and denies a request in case of no rule match
  - AWS recommends adding rules by increment of 100
- Newly created NACL will deny everything
- NACL are a great way of blocking a specific IP at the subnet level

25

Network ACLs vs Security Groups

Security Group	Network ACL
Operates at the instance level	Operates at the subnet level
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in number order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (therefore, you don't have to rely on users to specify the security group)

26