AWS Default VPC

- In AWS, All new accounts have a default VPC
- All the New instances are launched into default VPC if no subnet is specified.
- Default VPC have internet connectivity and all EC2 instances have public IP.
- We also get a public and a private DNS name.

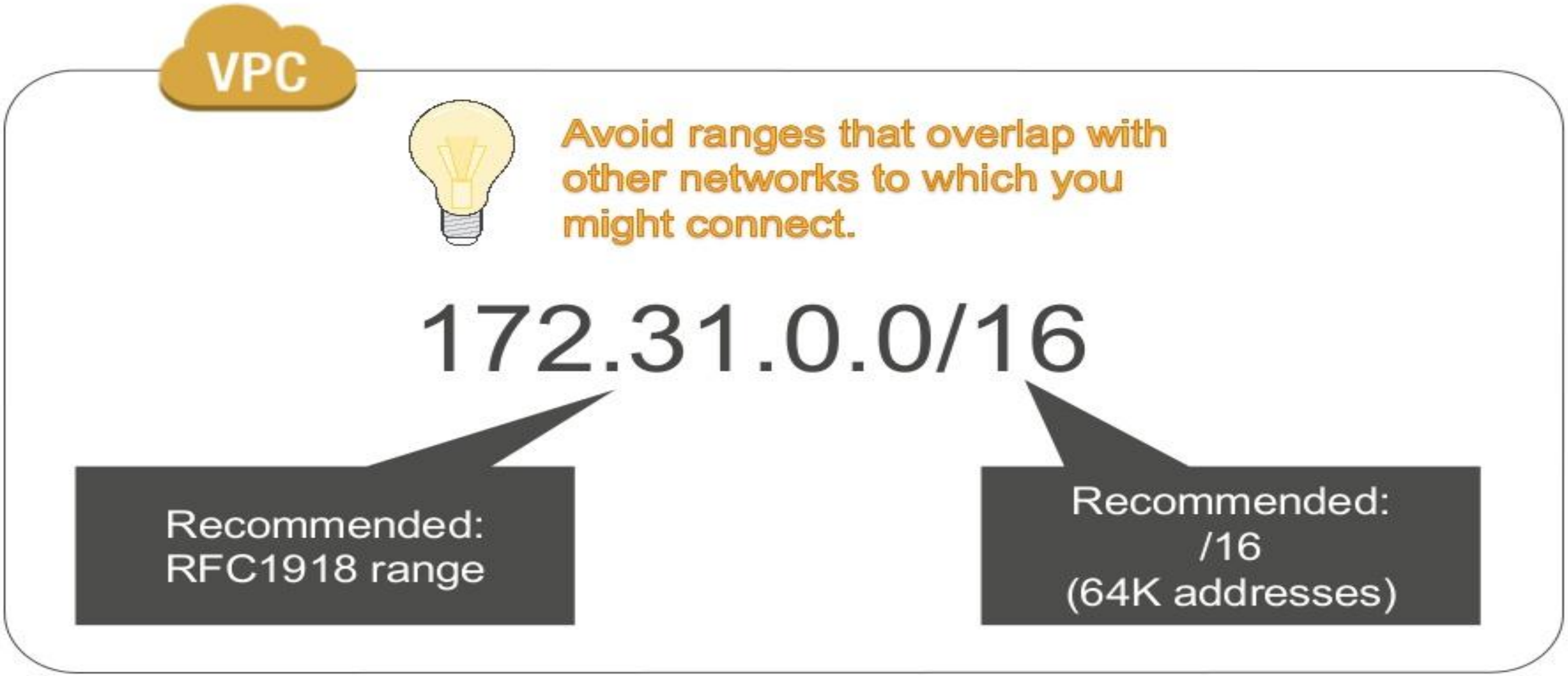
VPC in AWS – IPv4

- There is a Soft limit of 5 VPCs in a region.
- Each CIDR will be:
  - *Min size is /28 = 16 IP Addresses*
  - *Max size is /16 = 65536 IP Addresses*

- <u>What are the IP ranges allowed?</u>
- 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)

Choosing an IPv4 address for your VPC.



VPC

Avoid ranges that overlap with other networks to which you might connect.

172.31.0.0/16

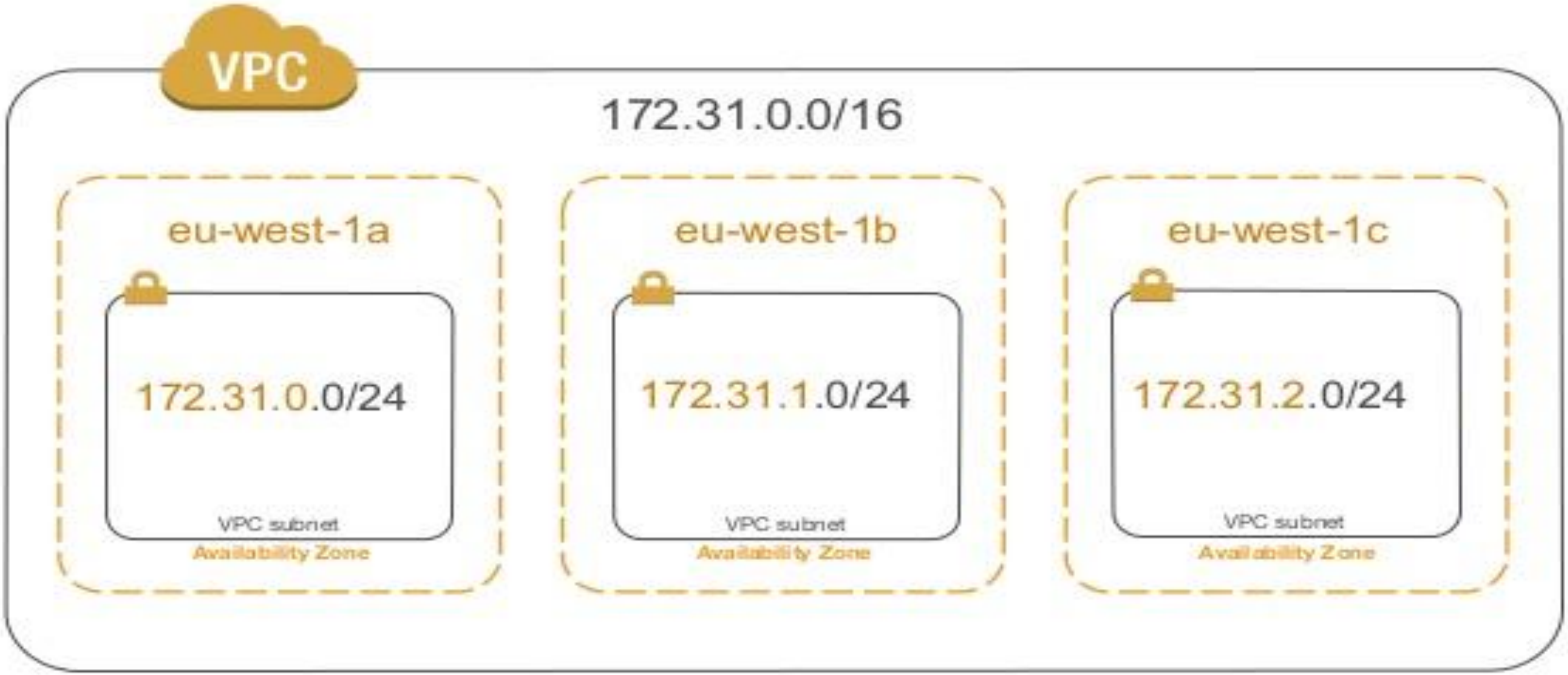
Recommended: RFC1918 range

Recommended: /16 (64K addresses)

VPC Subnets

- 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*

VPC Subnet and AZ



Internet Gateways

- Internet gateways(IG) 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…
- For this , Route tables must also be edited!

Security Group

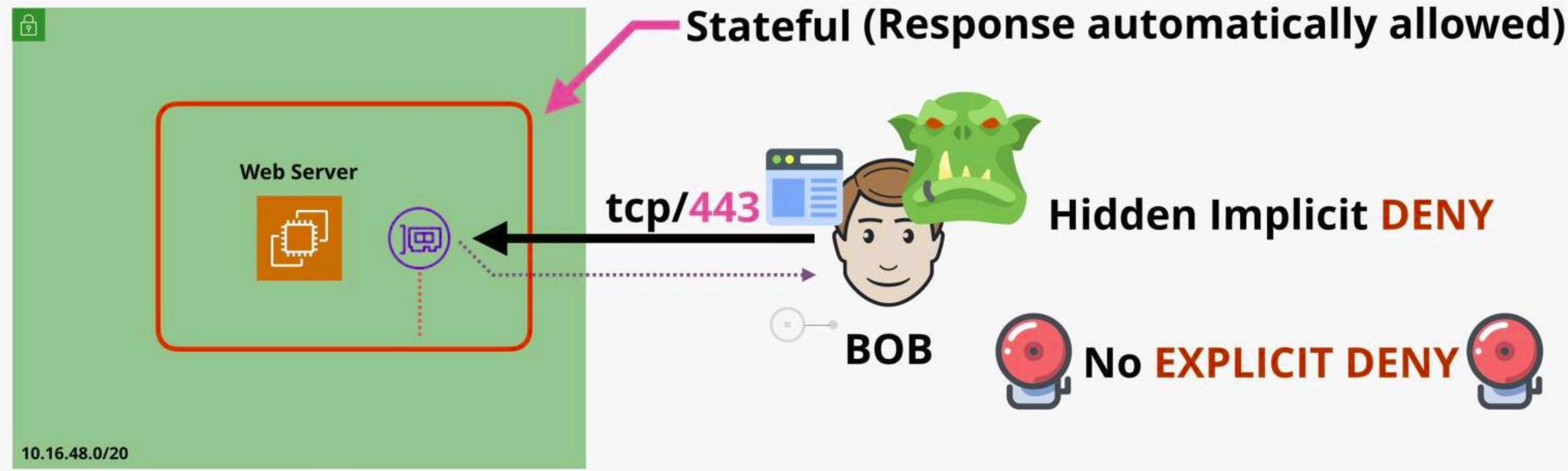
- A security group consists of a set of rules.

Each rule allows network traffic based on the following:

- *Direction (inbound or outbound)*
- *IP protocol (TCP, UDP, ICMP)*
- *Port*
- *Source/destination based on IP address, IP address range, or security group (works only within AWS)*

- You could define rules that allow traffic to enter and leave your EC2 instance virtual machine
- AWS won’t prevent you from doing so.
- But it’s best practice to define your rules so they are as restrictive as possible.

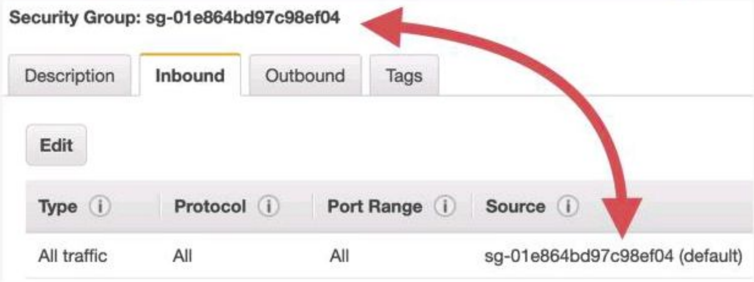
Security Group



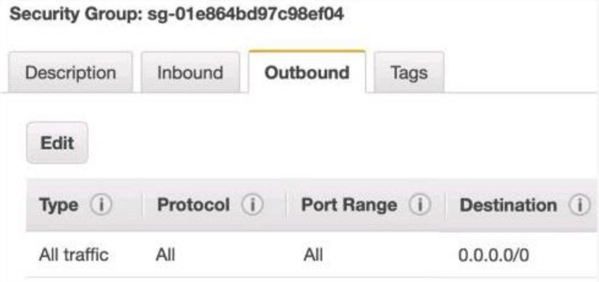
Stateful (Response automatically allowed)

Hidden Implicit DENY

No EXPLICIT DENY


Security Group: sg-01e864bd97c98ef04

Type	Protocol	Port Range	Source
All traffic	All	All	sg-01e864bd97c98ef04 (default)


Security Group: sg-01e864bd97c98ef04

Type	Protocol	Port Range	Destination
All traffic	All	All	0.0.0.0/0

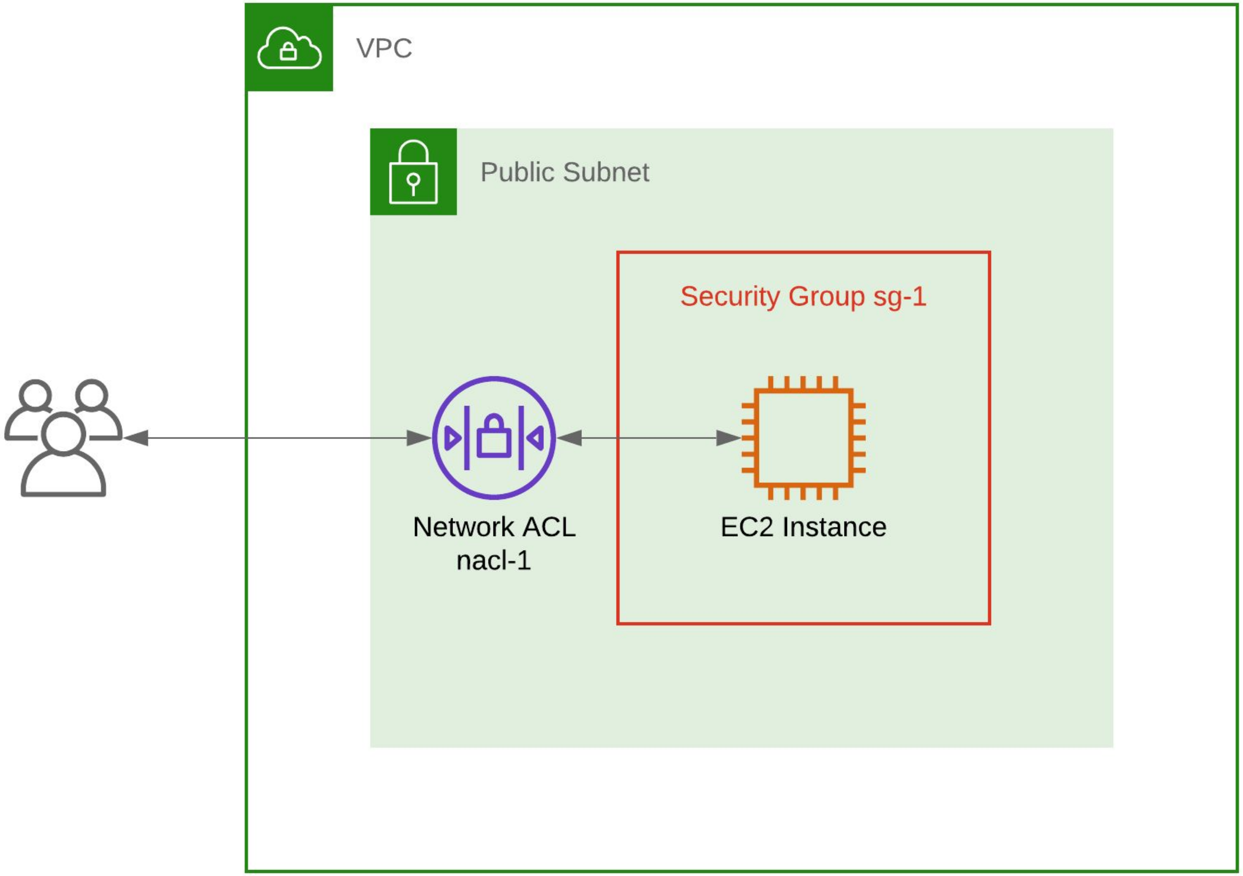
Network ACLs

- 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

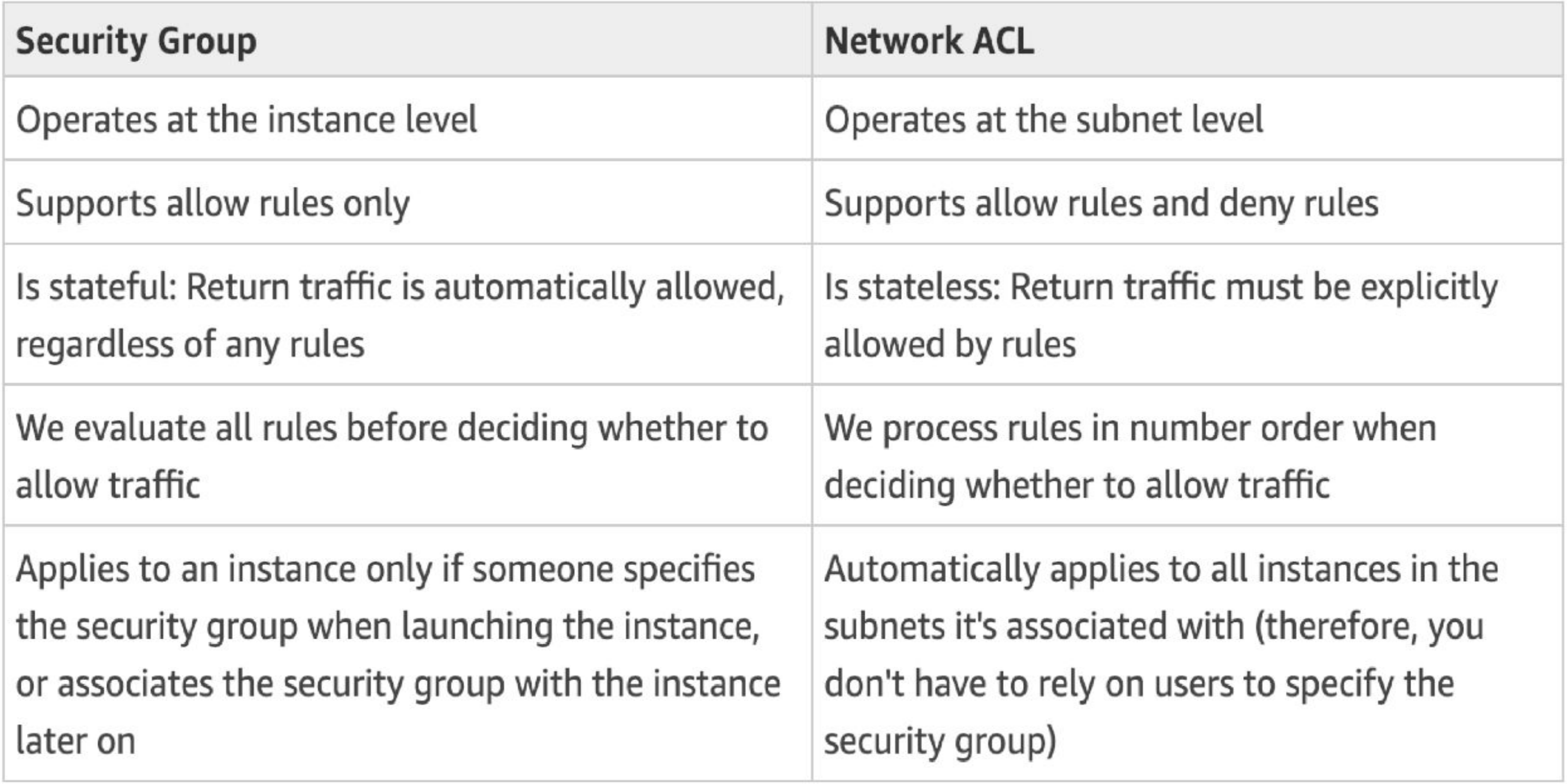
Define NACL rules:

- 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.

Network ACLs and Security Group

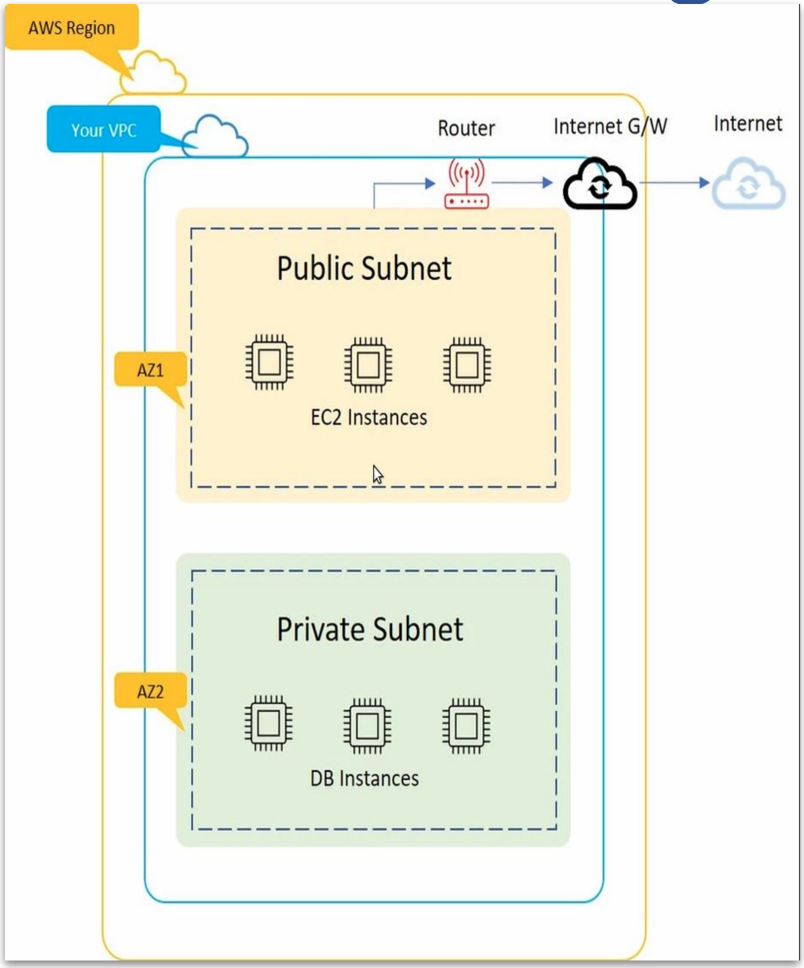


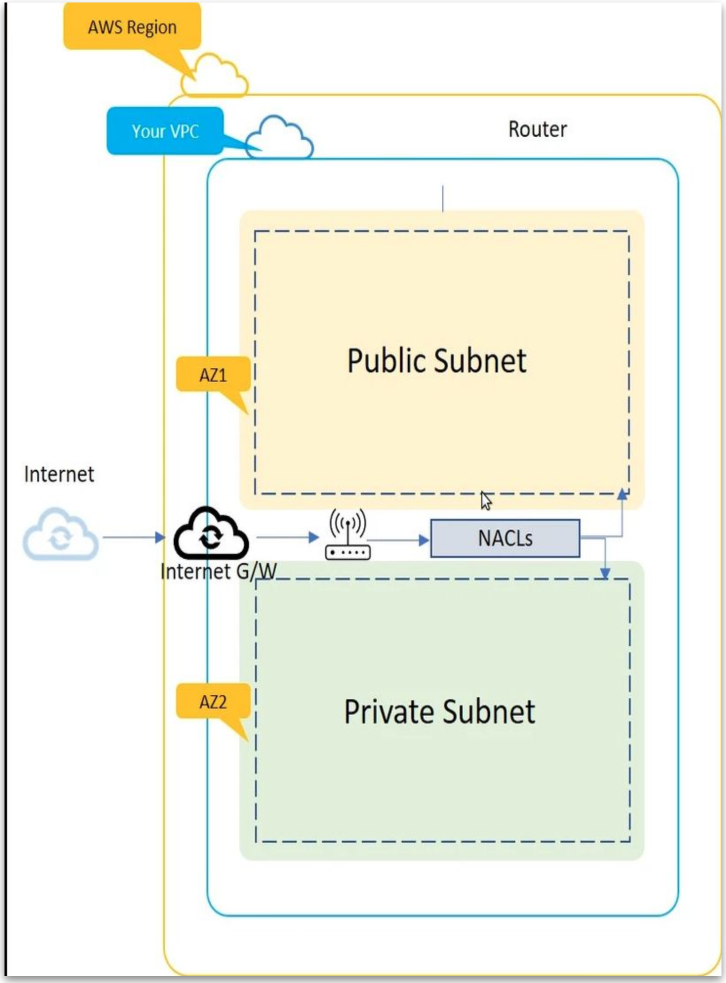
Using Security Group & Network ACLs



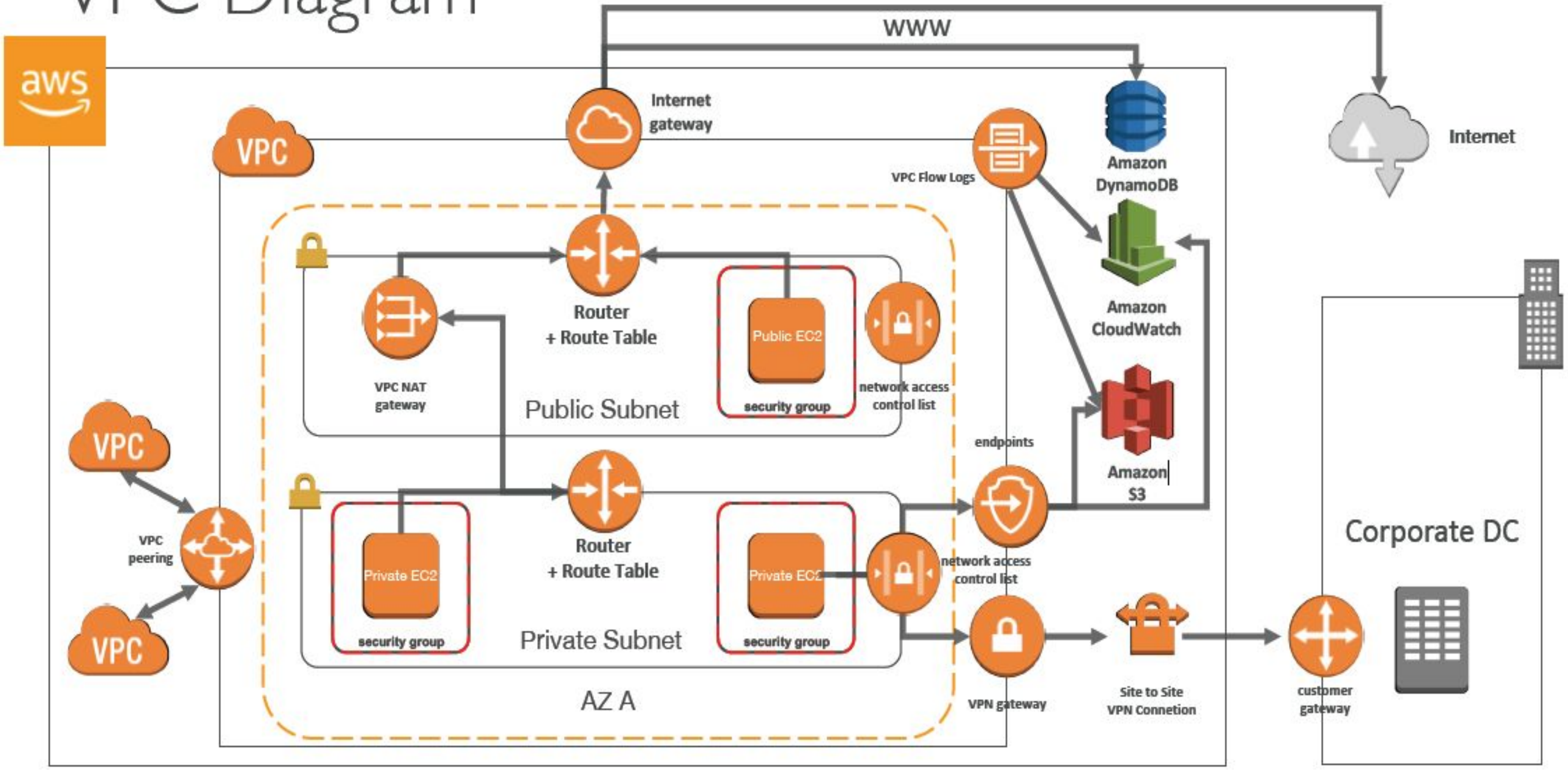
Security Group	Network ACL
Operates at the instance level	Operates at the subnet level
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate 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)

VPC High Level Overview





VPC Diagram


aws
WWW
VPC
Internet gateway
VPC Flow Logs
Amazon DynamoDB
Internet
Amazon CloudWatch
Router + Route Table
VPC NAT gateway
Public EC2
security group
network access control list
Public Subnet
Amazon S3
endpoints
VPC
VPC peering
VPC
Router + Route Table
Private EC2
security group
Private EC2
security group
network access control list
Private Subnet
VPN gateway
Site to Site VPN Connetion
customer gateway
Corporate DC
AZ A

ANY Questions?