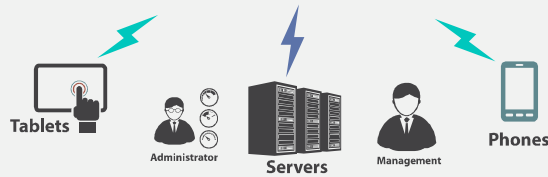
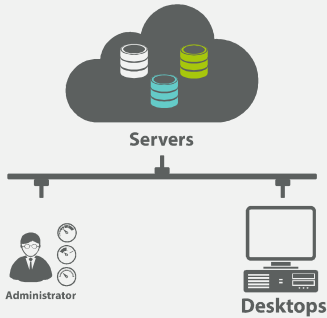




# 클라우드 아키텍처 구조

AWS 가상 사설 클라우드(VPC) Service





Servers

Administrator

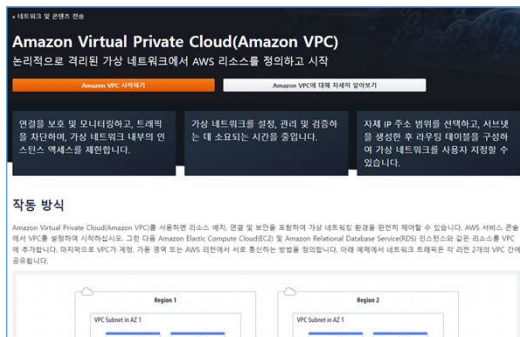
Desktops

## Index

01. 수업 목표
02. VPC CIDR Block
03. VPC(Virtual Private Cloud)
04. Subnet
05. Ability Zones
06. Elastic Network Interfaces
07. Gateways
08. Route Tables
09. Security Groups & Network ACL
10. Public IP Address & Elastic IP Address

## 수업 목표

### 개요

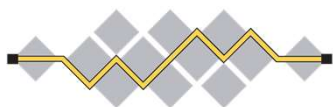


- VPC CIDR에 대한 이해
- VPC, Subnet, AZ에 대한 이해
- AWS Cloud Networking을 위한 다양한 서비스 이해

# VPC CIDR Block

## VPC CIDR Block

### What's CIDR



**I E T F**®

[https://en.wikipedia.org/wiki/Internet\\_Engineering\\_Task\\_Force/](https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force/)

- Classless Inter-Domain Routing
- /ˈsaɪdər, ˈsɪ-/
- Is a method for allocating IP addresses and for IP routing.
- **IETF**(The Internet Engineering Task Force) introduced CIDR in 1993 to replace the previous classful network addressing architecture on the Internet.

## VPC CIDR Block

### Classful Network

Classes

Class	Leading bits	Size of network number bit field	Size of rest bit field	Number of networks	Addresses per network	Total addresses in class	Start address	End address	Default subnet mask in dot-decimal notation	CIDR notation
Class A	0	8	24	128 ( $2^7$ )	16,777,216 ( $2^{24}$ )	2,147,483,648 ( $2^{31}$ )	0.0.0.0	127.255.255.255 <sup>[6]</sup>	255.0.0.0	/8
Class B	10	16	16	16,384 ( $2^{14}$ )	65,536 ( $2^{16}$ )	1,073,741,824 ( $2^{30}$ )	128.0.0.0	191.255.255.255	255.255.0.0	/16
Class C	110	24	8	2,097,152 ( $2^{21}$ )	256 ( $2^8$ )	536,870,912 ( $2^{29}$ )	192.0.0.0	223.255.255.255	255.255.255.0	/24
Class D (multicast)	1110	not defined	not defined	not defined	not defined	268,435,456 ( $2^{28}$ )	224.0.0.0	239.255.255.255	not defined	/4 <sup>[7]</sup>
Class E (reserved)	1111	not defined	not defined	not defined	not defined	268,435,456 ( $2^{28}$ )	240.0.0.0	255.255.255.255 <sup>[8]</sup>	not defined	not defined

- **Reserved**

- In A class, 0.0.0.0/8(Anywhere address) and 127.0.0.1/8 ~ 127.255.255.255(Loopback address).
- In B class, 128.0.0.0/16 and 191.255.0.0/16.
- In C class, 192.0.0.0/24 and 223.255.255.0/24.
- 255.255.255.255(Broadcast address).

[https://en.wikipedia.org/wiki/Classful\\_network](https://en.wikipedia.org/wiki/Classful_network)

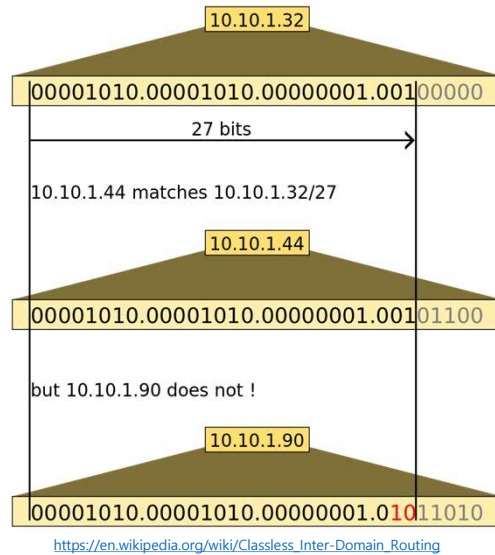
## VPC CIDR Block

### CIDR Notation

- Is a compact representation of an IP address and its associated network mask.
- Specifies an IP address, a slash ('/') character, and a decimal number.
- The decimal number is the count of consecutive leading 1-bits (*from left to right*) in the network mask.
- The number can be thought of as the width (in bits) of the *network prefix*.

## VPC CIDR Block

### CIDR Notation



## VPC CIDR Block

### Private Address

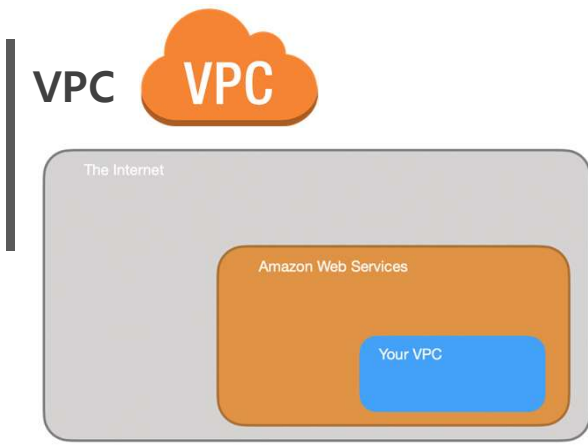
- [RFC 1918](#)
- Is commonly used for local area networks (LANs) in residential, office, and enterprise environments.

RFC 1918 name	IP address range	Number of addresses	Largest CIDR block (subnet mask)	Host ID size	Mask bits	<i>Classful description</i> <sup>[Note 1]</sup>
24-bit block	10.0.0.0 – 10.255.255.255	16 777 216	10.0.0.0/8 (255.0.0.0)	24 bits	8 bits	single class A network
20-bit block	172.16.0.0 – 172.31.255.255	1 048 576	172.16.0.0/12 (255.240.0.0)	20 bits	12 bits	16 contiguous class B networks
16-bit block	192.168.0.0 – 192.168.255.255	65 536	192.168.0.0/16 (255.255.0.0)	16 bits	16 bits	256 contiguous class C networks

[https://en.wikipedia.org/wiki/Private\\_network](https://en.wikipedia.org/wiki/Private_network)

# VPC(Virtual Private Cloud)

## AWS VPC

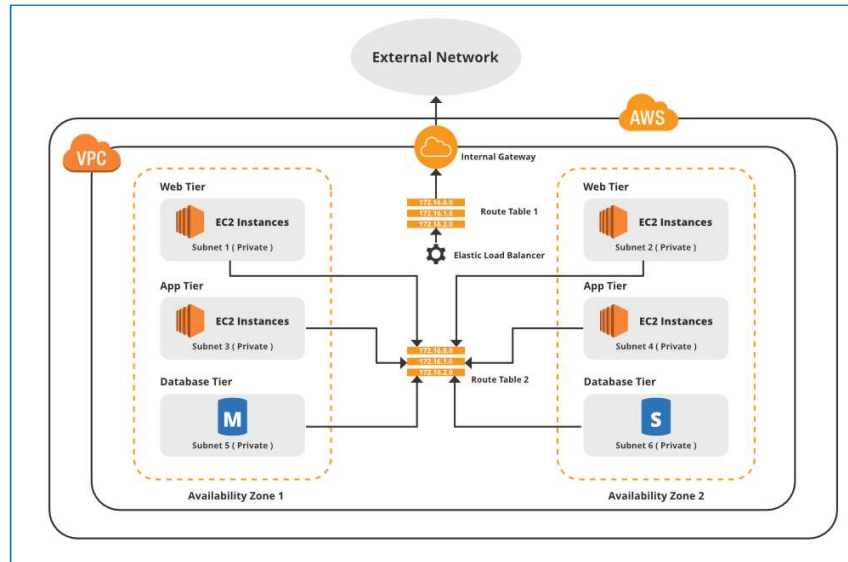


<https://grapeup.com/blog/the-path-towards-enterprise-level-aws-infrastructure-architecture-scaffolding/#>

- Allows to create a virtual network in which can launch resources.
- Allows to have logically isolated from other VPCs and the outside world.
- Within the VPC resources have private IP addresses.
- Can control the access to all those resources inside the VPC and route outgoing traffic.

## AWS VPC

## VPC



<https://www.geeksforgeeks.org/amazon-vpc-introduction-to-amazon-virtual-cloud/>

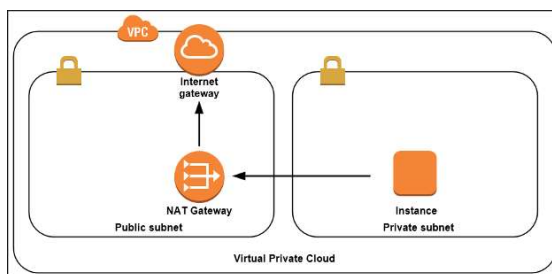


## Lab1. Create a New AWS VPC

# Subnet

## Subnet

### Subnet



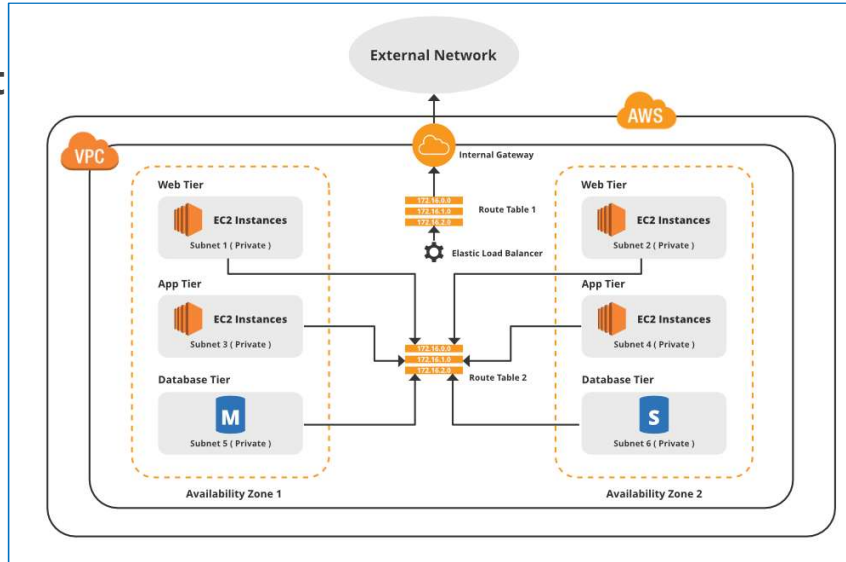
<https://aws.amazon.com/ko/blogs/security/how-to-patch-inspect-and-protect-microsoft-windows-workloads-on-aws-part-1/>

- Is a logical container within a VPC that holds VPC resources, including EC2 instances.
- A subnet lets isolate instances from each other.
- Every instance must exist within a subnet.
- After create an instance in a subnet, can't move the instance.



# Subnet

## Subnet



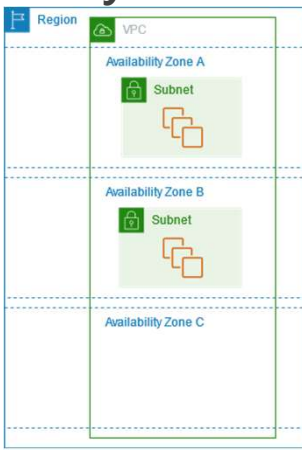
<https://www.geeksforgeeks.org/amazon-vpc-introduction-to-amazon-virtual-cloud/>



## Lab2. Create a Net Subnet

# Availability Zones

## Availability Zones



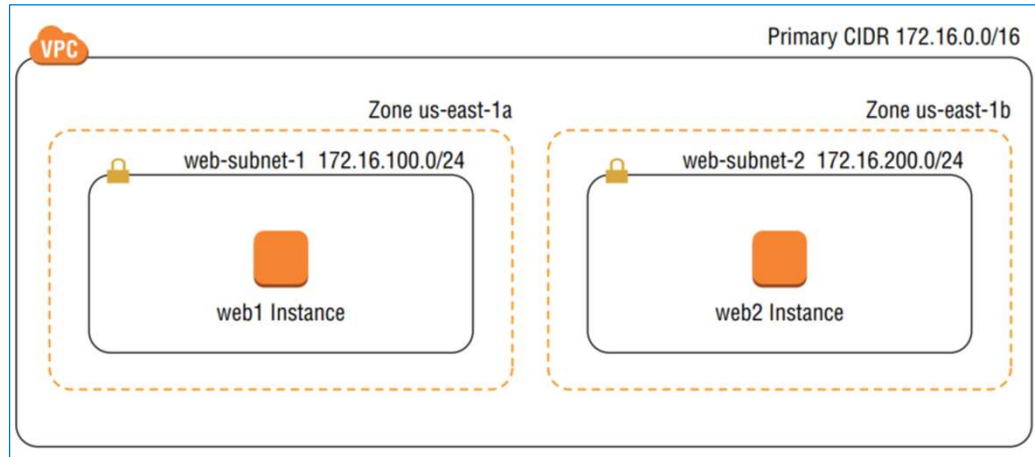
The diagram illustrates the hierarchy of AWS resources. A large blue box labeled 'Region' contains a green box labeled 'VPC'. Inside the VPC, there are three horizontal dashed lines representing 'Availability Zone A', 'Availability Zone B', and 'Availability Zone C'. Each availability zone contains a green box labeled 'Subnet' and three orange server icons. This shows that subnets are isolated to specific availability zones within a region.

- A subnet can exist within only one AZ.
- Is roughly analogous to a relatively small geographic location such as a data center.
- Although availability zones in an AWS region are connected, they are designed so that a failure in one zone doesn't cause a failure in another.

[https://docs.aws.amazon.com/ko\\_kr/AWSEC2/latest/UserGuide/using-regions-availability-zones.html](https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/using-regions-availability-zones.html)

## Availability Zones

AZ

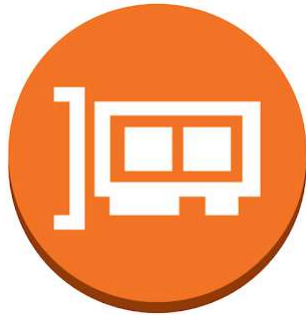


"AWS 공인 솔루션스 아키텍트 스테디 가이드-여소시에이트 3/e", 벤 파이퍼, 데이비드 클린턴 공저, 동준상 역, 에이콘 출판사, 2022, p155

## Elastic Network Interfaces

## Elastic Network Interfaces

### ENI

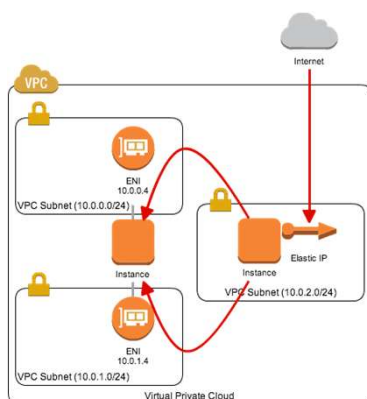


<https://freshers.in/certification/aws/elastic-network-interfaces-quick-reference-and-cheat-sheet/>

- Allows an instance to communicate with other network resources.
- Makes it possible to use SSH or RDP to connect to the OS running on instance to manage it.
- Every instance must have a the primary ENI which is connected to only one subnet.
- Can't remove the primary ENI from an instance, and can't change its subnet.

## Elastic Network Interfaces

### Attaching ENI

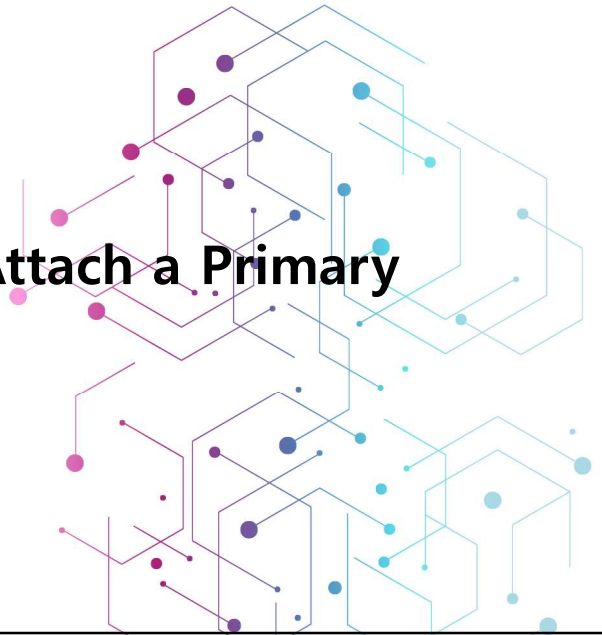


<https://cloudpack.media/138>

- Can exist *independently* of an instance.
- Can create an ENI first and then attach it to an instance later.
  - i.e. You can create an ENI in one subnet and then attach it to an instance in the same subnet as the primary ENI when you launch the instance.
  - If You disable the Delete On Termination attribute of the ENI, you can terminate the instance without deleting the ENI.
  - You can then associate the ENI with another instance.



## Lab3. Create and Attach a Primary ENI

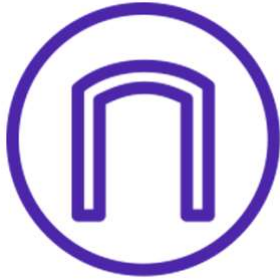


## Gateways



## Gateways

### Internet Gateways



<https://pyongwonlee.com/2020/10/14/aws-vpc-igw-nat/>

- Are a VPC component allows communication between resources in the VPC and the internet.
- Are horizontally scaled, redundant, and highly available.
- The default VPC has an IGW attached by default.
- But when create a custom VPC, it does not have an IGW associated with it.
- Must create an IGW and associate it with a VPC manually.

## Gateways

### NAT Gateways

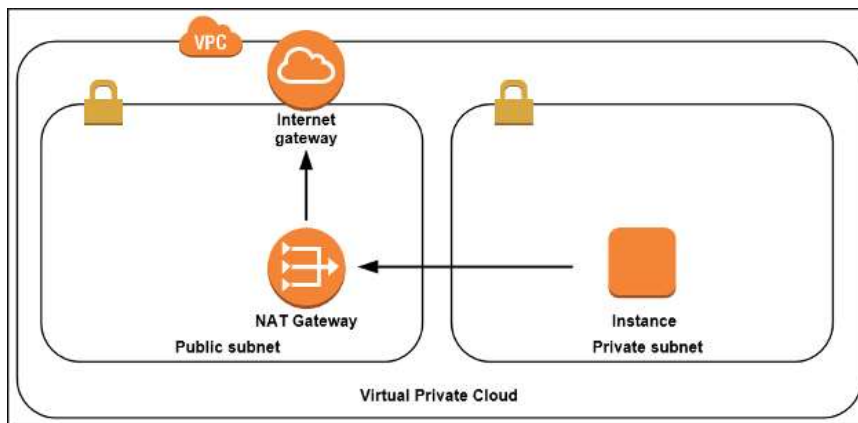


<https://vecta.io/symbols/9/aws-compute/27/vpc-nat-gateway>

- Are used to enable instances located in private subnets to connect to the Internet or other AWS services.
- AWS provides a NAT gateway managed service which requires very little administrative effort. We will use it while setting up our infrastructure.

## Gateways

### NAT Gateways



<https://aws.amazon.com/ko/blogs/security/how-to-patch-inspect-and-protect-microsoft-windows-workloads-on-aws-part-1/>

## Route Tables



## Route Tables



### Route Tables

- To control how traffic ingresses, egresses, and moves within VPC, need to use routes stored in route tables.
- Rather than using physical or virtual routers that configure, the VPC architecture implements IP routing as a software function.
- Each route table consists of one or more routes and at least one subnet association.
- When create a VPC, AWS automatically creates a default route table called the main route table and associates it with every subnet in that VPC.
- A subnet cannot exist without a route table association.

## Route Tables



### Routes

- Determine how to forward traffic *to* or *from* resources within the subnets associated with the route table.
- IP routing is destination-based, meaning that routing decisions are based only on the destination IP prefix, not the source IP address.
- When create a route, must provide the following elements:
  - Destination IP prefix
  - Target resource
- The destination must be an IPv4 or IPv6 prefix in CIDR notation.
- The target must be an AWS network resource such as an IGW or an ENI.
- It cannot be an IP prefix.



## Route Tables

### Routes

- Every route table contains a local route that allows instances in different subnets to communicate with each other.

The local route	
Destination	Target
172.31.0.0/16	Local

- The local route is the only mandatory route that exists in every route table.
- It's what allows communication between instances in the same VPC.
- Because there are no routes for any other IP prefixes, any traffic destined for an address outside of the VPC CIDR range will get dropped.

## Route Tables

### The Default Route

- To enable Internet access for instances, must create a default route pointing to the IGW.

Route table with default route	
Destination	Target
172.31.0.0/16	Local
0.0.0.0/0	igw-0e538022a0fddc318

- The 0.0.0.0/0 prefix encompasses all IP addresses, including those of hosts on the Internet.
- Public Subnet means that is associated with a route table containing a route pointing to an IGW.
- Contrast, a private subnet does not have a route with an IGW as a target.



## Lab4. Create an Internet Gateway and Default Route

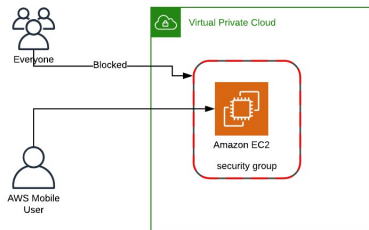


## Security Groups



## Security Groups

### Security Groups



<https://aws-blog.de/2019/10/defenders-caller-based-ec2-security-with-cdk.html>

- Function as a firewall that controls traffic **to** and **from** an instance by permitting traffic to ingress or egress that instance's ENI.
- Every ENI must have at least one security group associated with it.
- One ENI **can** have multiple security groups attached, and the same security group **can** be attached to multiple ENIs.

## Security Groups

### Inbound Rules

Edit inbound rules

Inbound rules control the incoming traffic that's allowed to reach the instance.

Type	Protocol	Port Range	Source	Description
Custom ...	TCP	22	Custom	Set to my CIDR (SSH)
Custom ...	TCP	443	Custom	Set to my CIDR (UI access)
Custom ...	TCP	9443	Custom	Set to CDP CIDR
Custom ...	TCP	0-65535	Custom	Open to internal commun...
Custom ...	UDP	0-65535	Custom	Open to internal commun...

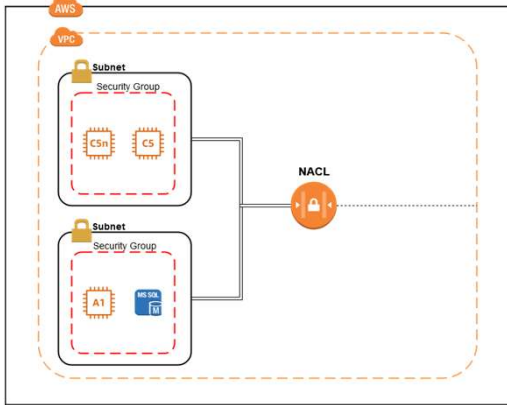
Add Rule

<https://docs.cloudera.com/cdp/latest/requirements-aws/topics/mc-aws-req-security-groups.html>

# Network Access Control Lists

## Network Access Control Lists

### NACL

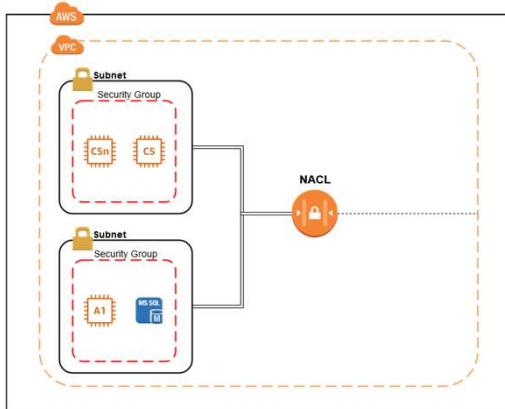


<https://medium.com/kernel-space/when-to-use-security-groups-and-nacl-in-aws-e6a320ca0734>

- **Security Group**
  - Is a stateful firewall to the instances.
  - Stateful means, keeps a track of the State.
  - Operates at the instance level.
- **Network Access Control List**
  - Is stateless.
  - Won't keep any track of the state.
  - Operates at Subnet level.

## Network Access Control Lists

### NACL

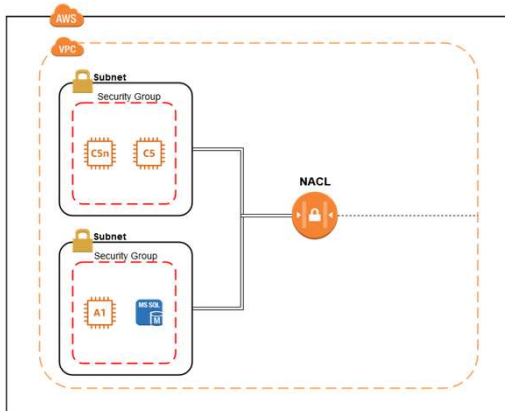


<https://medium.com/kernel-space/when-to-use-security-groups-and-nacl-in-aws-e6a320ca0734>

- A default NACL **allows** everything both Inbound and Outbound Traffic.
- Unlike Security Groups, in NACLs have to explicitly tell what to deny in Inbound and Outbound Rules.
- There's **no** Implicit Deny in NACL.

## Network Access Control Lists

### NACL & SG Default Quota



<https://medium.com/kernel-space/when-to-use-security-groups-and-nacl-in-aws-e6a320ca0734>

- NACL
  - NACLs Per VPC — 200
  - Rules per NACL — 20
- Security Groups
  - VPC Security Groups per Region — 2500
  - Rules Per Security Group — 60 Inbound and 60 Outbound.



## Lab5. Create an Additional Security Group & NACL



## Public IP Addresses & Elastic IP Addresses



## Public IP Addresses & Elastic IP Addresses

### Public IP Addresses

Instance: i-0d7cfe2af7f494d95 (Remove-IP)

Details	Security	Networking	Storage	Status Checks	Monitoring	Tags
▼ Instance summary <a href="#">Info</a>						
Instance ID i-0d7cfe2af7f494d95 (Remove-IP)	Public IPv4 address 3.115.9.36 <a href="#">open address</a>		Private IPv4 addresses 172.31.9.224			
Instance state Running	Public IPv4 DNS ec2-3-115-9-36.ap-northeast-1.compute.amazonaws.com   <a href="#">open address</a>		Private IPv4 DNS ip-172-31-9-224.ap-northeast-1.compute.internal			
Instance type t3.nano	Elastic IP addresses -		VPC ID vpc-9f217bf8			

<https://ystatit.medium.com/remove-aws-ec2-auto-assigned-public-ip-address-9649d13ee536>

## Public IP Addresses & Elastic IP Addresses

### Public IP Addresses

- Are reachable over the public Internet.
- Need if want others to directly connect to it via the Internet.
- Naturally, this requires an IGW attached to the VPC that the instance resides in.
- When launch an instance into a subnet, can choose to automatically assign it a public IP.
- Automatically assigned public IP addresses aren't persistent.
- When stop or terminate the instance, will lose the public IP address.
- If you stop and restart the instance, it will receive a different public IP address.

## Public IP Addresses & Elastic IP Addresses

### Elastic IP Addresses



<https://www.pinterest.co.kr/pin/737675613942412136/>

- Is a type of public IP address that AWS allocates to *your* account when you request it.
- After AWS allocates an EIP to *your* account, you have exclusive use of that address until you manually release it.
- When initially allocate an EIP, it is not bound to any instance.
- Instead, must associate it with an ENI.



### Lab6. Create a EC2 Instance with Apache Web Server & Allocate Elastic IP Address





## Lab7. Create Private Subnet, NAT Gateway and Network Connection Test

