AWS VPC (Virtual Private Cloud)

It is related to Network and Security part

VPC provides isolated network for resources in AWS cloud

Is AWS a public or private cloud -> it is a public (anyone can access the AWS website, create acount, use resources)

Can anyone login and work with resources in AWS? Yes, then it is a public cloud

In that case, protecting my resources is very crucial. If I login into my account, can I access other accounts’ resources, answer is no

With my login, I shouldn’t access your resources and vice-versa. that’s called as isolated resources

With the help of VPC, we can protect our resources in AWS cloud

VPC provides flexible and secured network to maintain and manage our resources in AWS cloud

Can everyone access every resource available in your home? The answer is No. Mostly outsiders can access only up to front door

VPC is like our home, before creating the resources, first part is to create a VPC

Even though, we haven’t created our own VPC, still while creating other resources, we used the default VPC being created. Maximum we can create 65000 IPs, that many IPs we can allow within one VPC. Maximum approx 65000 IPs will be there in one VPC

VPC (approx 65000 IPs)

Subnet 1

Subnet 3 (public)

Subnet 2  
(private)

Internetworking Gateway

We can have any number of Subnets inside VPCs, we have something called as Public Subnet and Private Subnet

VPC terminology:

1. VPC
2. Subnet (Private or Public)
3. CIDR Block (IP ranges) -> VPC sizing
4. Route tables
5. Internet gateway
6. NAT gateway
7. VPC peering
8. Security groups --> at Resource level --> Rules (both Inbound [who can access] and Outbound [what we can access]) to allow who can access
9. NACL --> Subnet level --> but at Subnet level, we can have rules for allowing also and denying also

What’s one Subnet? Like a small network within VPC. We can allocate like 256 IPs in the subnet.

In Subnet SN2, we can allocate 124 IPs

Private Subnet is for the internal communication

Public subnet can be accessed through internetworking. Internetworking means outsiders can also access. Say if I attached an Internetworking Gateway (INW) to a public subnet, anyone can access. Any of the Subnet, if I attach Internet Gateway (INW), it becomes Public otherwise it is Private

Public subnet --> Internet Gateway, Private subnet --> NAT Gateway

IPs

There are several types of IPs (Internet Protocol) address used in a computer network. All devices like mobile phones, laptops, desktops etc all have IPs. If devices have to get connected over internet, IP address is a must

IPv4: 32 bits --> 4 sets of numbers

IPv4 ---> 32 bits numeric addresses written in four sets of numbers separated by periods: 192.168.1.1

It is most widely used IP version and supports approximately 4.3 billion unique addresses

IPv6: 128 bits, IPv6 is trying to solve the problem of IP shortage, which might occur in the future due to IPv4 --> 8 sets of four hexadecimal digits will be there

IPv6 uses hexadecimal notation with colons eg: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Supports 340 undecillion unique addresses

Public IP

Private IP

Static IP address

Dynamic IP

VPC Sizing: process of allocating IPs to VPC subnets. In general, allocating IPs is called as VPC sizing, within VPC how many IPs are required and within each subnet how many IPs are required. When we create a new VPC, that time we decide how many IPs we want --> Decision of allocating IPs to VPCs is only called as VPC sizing

IP Ranges we will be doing with CIDR --> Class less Inter domain Range

VPCs are regional-specific

Can VPCs interact? Yes that’s called as VPC peering

Any device, if it has to access resources of internet, is IP compusory? Yes

On a regular basis, number of new devices are rapidly increasing and are using internet, and any device if it has to use internet, then IP is mandatory and a must and there might be possibility of running out of IPs, which has to be unique. To overcome this issue, IPv6 was introduced

When we connect Internet Gateway to a Private Subnet, it becomes Public Subnet. Also Route Table (RT) will be there between INW and Public SN1 to make it public. Rules of routing, with the help of route tables, INW, outsiders can access resources within one Subnet

VPC sizing: Sizing will be calculated in 2 power or power of 2

**IPv4**

10.0.0.1/16 ==> means 2 power (32-16) ==> 2 power 16. 32 is the maximum . Maximum one VPC can have is 65,536

10.0.0.1/32 ==> 2 power (32-32) ==> 2 power 0 = 1 IPs address, not recommended to create VPC or Subnet with just one IP address

Therefore, AWS supports from 28

10.0.0.1/28 ==> 2 power (32-28) ==> 2 power 4 = 16. this is the minimum number of IPs AWS supports. AWS supports from 28 and less

AWS supports minimum 16 to maximum 65,536 IPs

Similarly, AWS does not support ==> 10.0.0.1/15 less than 16

Subnet ranges can be given from /16 to /28

Recommended to use /24

10.0.0.1/24 ==> 2 power (32-24) = 2 power 8 = 256 IPs that’s generally we use. In real-life scenario also 256 IP is more than enough for Subnets