Getting Started with VPC

Sanchit Jain
16th May, Monday
10:00 AM to 12:00 PM

Speakers

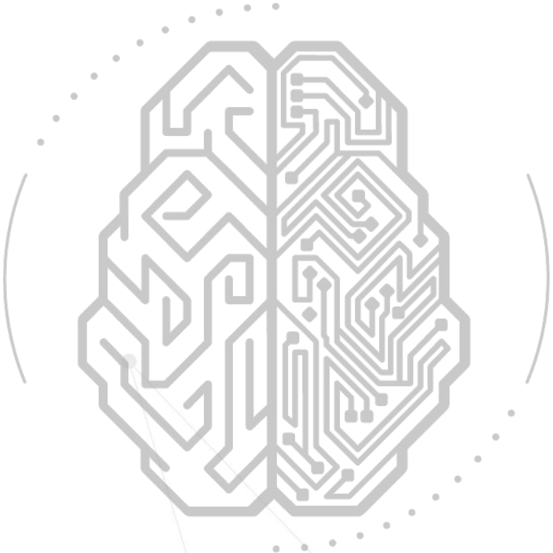
Sanchit Jain

Lead Architect - AWS at Quantiphi
AWS APN Ambassador & AWS UG Mumbai Lead

FOLLOW ME

in

AWS Services - VPC

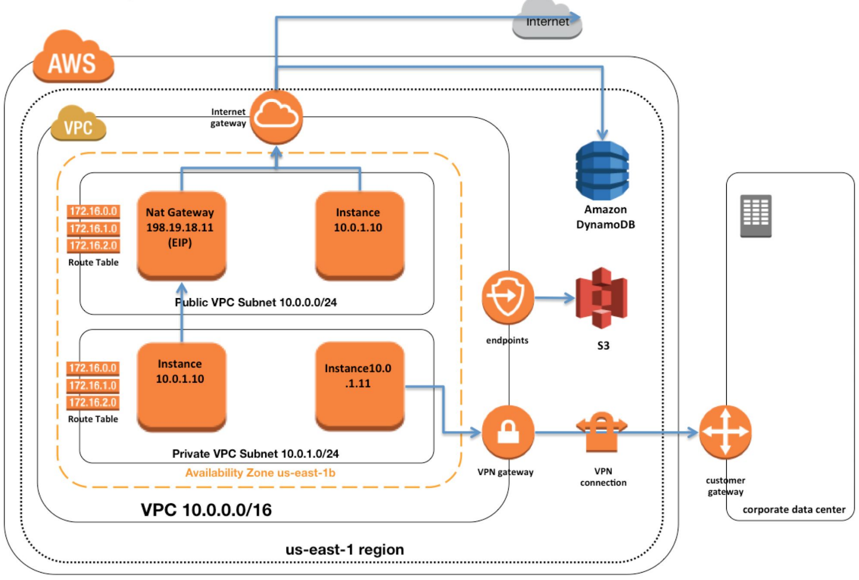


AWS Services - VPC: Introduction

- Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined.
- It is logically isolated from other virtual networks in the AWS Cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC.

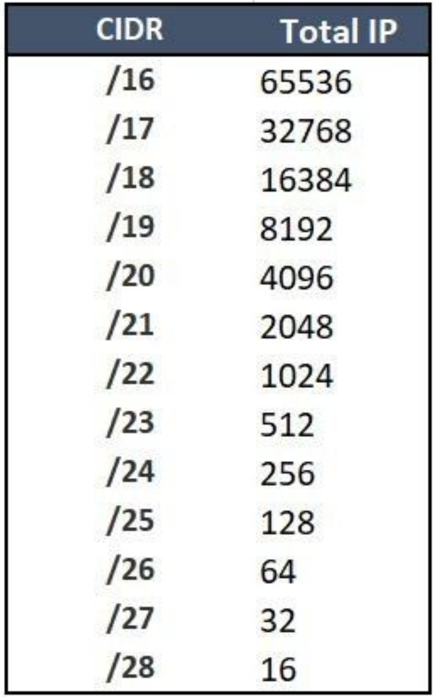
- Your account comes with a default VPC that has a default subnet in each Availability Zone. A default VPC has the benefits of the advanced features provided by EC2-VPC, and is ready for you to use.
- When you create a VPC, you must specify an IPv4 CIDR block for the VPC. The allowed block size is between a **/16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses)**

AWS VPC Components



What is CIDR?

- CIDR (Classless Inter-Domain Routing) is a method for allocating IP addresses and for IP routing.
- In 1993, the Internet Engineering Task Force (IETF) introduced the Classless Inter-Domain Routing (CIDR) protocol to replace the previous classful network addressing architecture on the Internet.



CIDR	Total IP
/16	65536
/17	32768
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16

If you work your way down the list from the top, all you have to do is divide the total number of IP addresses by 2 to get the next CIDR total IP address.

In above table /16 = 65536

What is the best way to get /17 IP rage?

= /16 Total IP divided by 2

= 65536 divided by 2 equals 32768

The total number of IP addresses for the next CIDR /17 is 32768.

AWS Services - VPC: Components

- **Internet Gateway** - An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.
- **Subnet** - Subnet is logical Isolation of your network i.e dividing your VPC into smaller network . Each subnet must be associated with a route table, which specifies the allowed routes for outbound traffic leaving the subnet. Security groups control inbound and outbound traffic for your instances, and network ACLs control inbound and outbound traffic for your subnets.
- **Route Tables** - A route table tells network packets which way they need to go to get to their destination. There are certain rules defined within this table. You can choose which subnets to be associated with a single route table. One subnet can be associated with only one RT, unlike RTs which can be associated with multiple subnets.
- **NAT Gateway** - NAT is a networking technique commonly used to give an entire private network access to the internet without assigning each host a public IPv4 address. When a host in the private network initiates an internet-bound connection, the NAT device public IP address becomes the source IP address for the outbound traffic. The response traffic from the internet therefore uses that public IP address as the destination IP address. The NAT device then routes the response to the host in the private network that initiated the connection

AWS Services - VPC: Components

- **Egress only Internet Gateway** - An egress-only internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows outbound communication over IPv6 from instances in your VPC to the internet, and prevents the internet from initiating an IPv6 connection with your instances.
- **Elastic IP** - When an EC2 instance is launched, it is associated with a public IP address. When that instance is stopped and started again, a new IP address gets attached to that. Now comes Elastic IP into the picture. When an elastic IP is created and is associated with an EC2 instance, even if the instance is stopped and started again, same IP address retains. We can disassociate elastic ip of a terminated/stopped instance and associate with another instance until the former one is started again

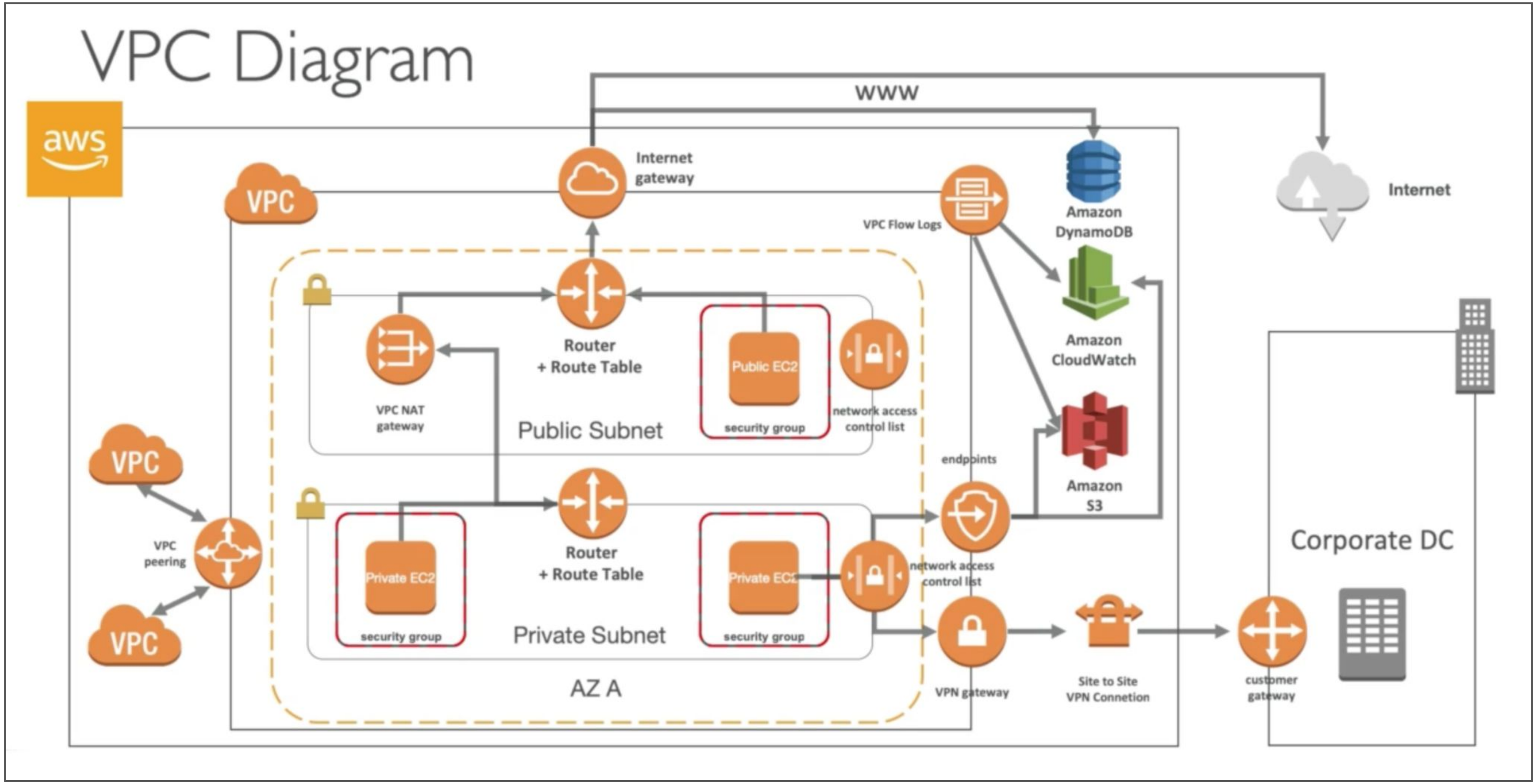
AWS Services - VPC: Components

- **Security Groups** - Automatically default security group is created when a VPC is created, Instance-level security, Default security group, Custom security group, Second line of defense, and Stateful
- **NACL** - Automatically default NACL is created when a VPC is created, Subnet-level security, Default NACL, Custom NACL, First line of defense, and Stateless
- **VPC Endpoints** - To prevent data from being unnecessarily exposed to the internet. VPC endpoint enables creation of a private connection between VPC to supported VPC Gateway (AWS services) and VPC endpoint services powered by PrivateLink using its private IP address.
- **VPC Peering** - A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. You cannot create a VPC peering connection between VPCs that have matching or overlapping IPv4 or IPv6 CIDR blocks

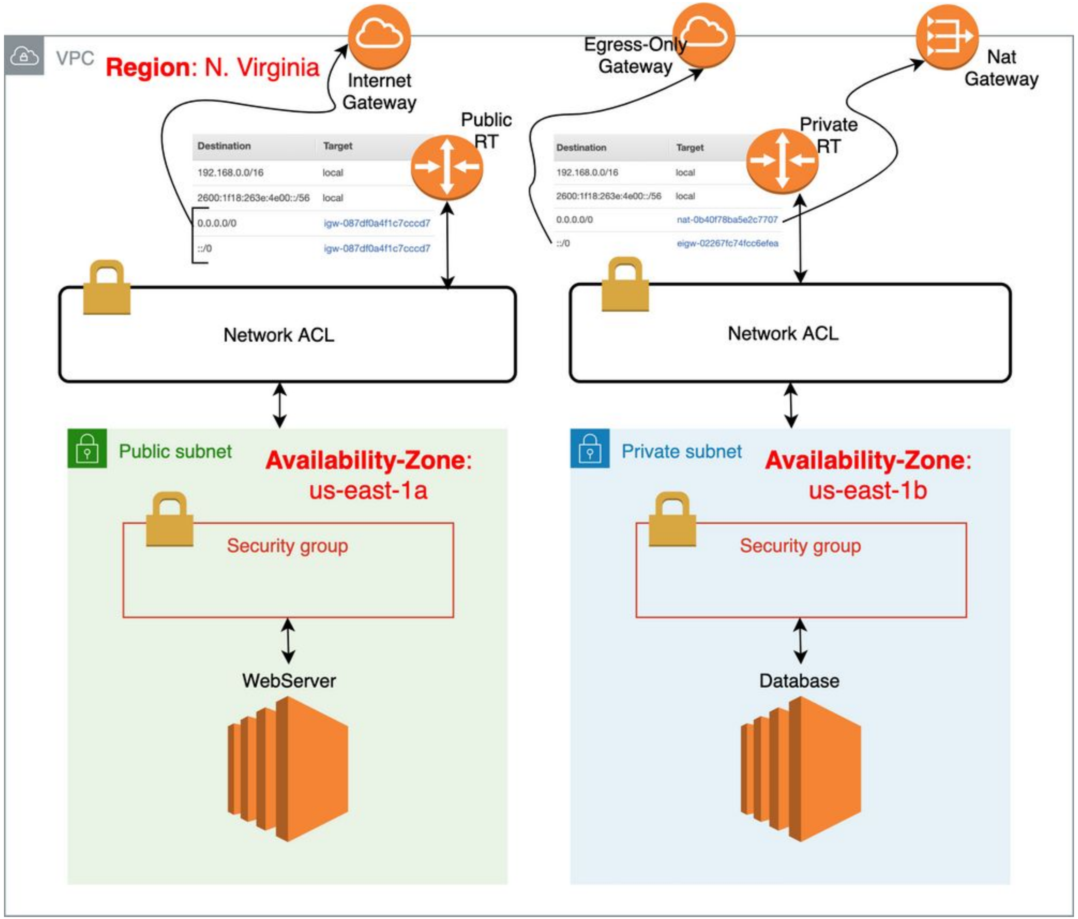
AWS Services - VPC: Components

- **Security and Best Practices** -
  - Always try to use custom VPC over default VPC
  - Launch EC2, RDS, etc resources in Private Subnet Only
  - For Connecting to Instances in Private Subnet use Bastion Host / Jump Server
  - Use NAT Gateway for Internet connection of EC2 in Private Subnet
  - Always try to use restricted IP address in Security Group Inbound
  - Do not Open port 22 to 0.0.0.0/0

AWS Services - VPC: End to End



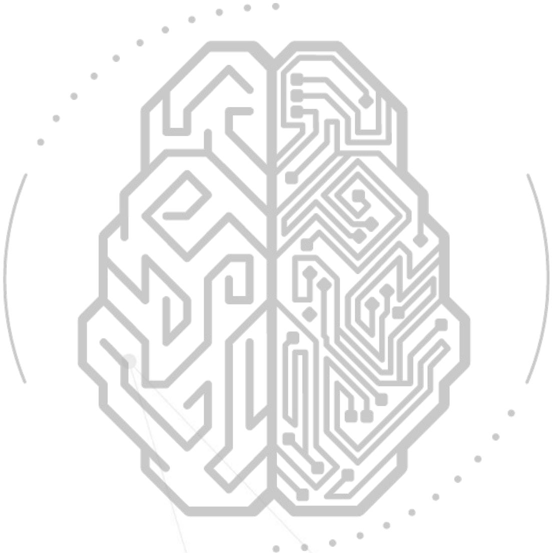
AWS Services - VPC: Traffic View



Destination	Target
192.168.0.0/16	local
2600:1f18:263e:4e00::/56	local
0.0.0.0/0	igw-087df0a4f1c7cccd7
::/0	igw-087df0a4f1c7cccd7

Destination	Target
192.168.0.0/16	local
2600:1f18:263e:4e00::/56	local
0.0.0.0/0	nat-0b40f78ba5e2c7707
::/0	eigw-02267fc74fcc6efea

Demo



Demo

- Install Nginx server
  - sudo amazon-linux-extras install nginx1
  - sudo systemctl enable nginx
  - sudo systemctl start nginx
  - sudo systemctl status nginx

- Deploy HTML file
  - Replace index.html store at this location with the server - /usr/share/nginx/html
  - Refresh your browser

- Nginx Config Example - link

THANK YOU