VPC & Networking

IP Addresses in AWS

- IP addresses are of two types - IPv4 and IPv6
- VPC supports both IPv4 and IPv6.
- Talking about EC2 instances, you always get a public IPv4 address and a private IPv4 address associated with it.
- Everytime an instance is stopped and started again, a new public IP address is allocated to it by default. The private IP address however stays the same even if you stop or start the instance a thousand times.

1. **Public IP Address:**
   - **Accessibility:** Public IP addresses are reachable over the internet. They allow communication between the EC2 instance and external networks, including the internet.
   - **Purpose:** Public IP addresses are typically used when you want your EC2 instance to be directly accessible from the internet. This is common for web servers, application servers, or any service that needs to be publicly available.
2. **Private IP Address:**
   - **Accessibility:** Private IP addresses are used for communication within a private network. They are not directly accessible from the internet.
   - **Purpose:** Private IP addresses are commonly used for internal communication between instances within the same Virtual Private Cloud (VPC) or a connected network. This is useful for database servers, internal APIs, and other components that don't need direct exposure to the internet.

- Now, **Elastic IP** comes into the picture. Elastic IP allows you to attach a fixed public IPv4 address to an EC2 instance.
- Elastic IP will incur costs if not attached to any instance. Whenever you stop an EC2 instance, the elastic IP service makes you pay for the fixed public IP address to keep it alive within the network.

VPC & Subnets Primer

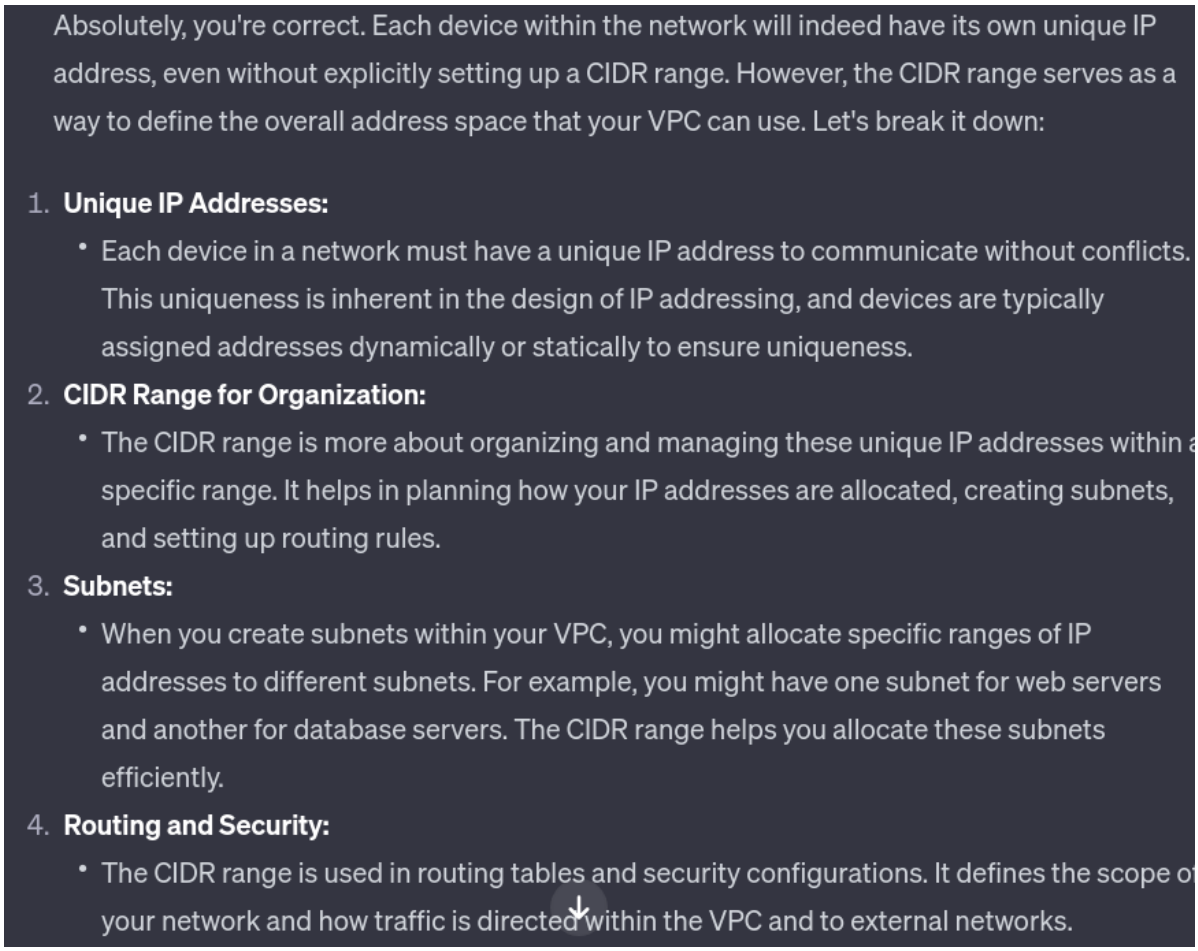
- **VPC or Virtual Private Cloud** is a private network to deploy your regional resources. A VPC is pinned down to one particular region.
- **Subnets** allow you to partition your network inside your VPC (mostly to AZs)
    - **Public subnet** is accessible from the internet - used to store web servers (ec2 instances) and stuff.
    - **Private subnet** is not accessible from the internet - you store things like the database of your application in the private subnet as they don't need direct internet access and this way, your data is more secure.
- Now, to define access to the internet and between these subnets within a VPC, we use **route tables**.
- **CIDR Range:**

CIDR, or Classless Inter-Domain Routing, is like a system for organizing and managing IP addresses (the unique addresses that devices use to communicate on a network). It's a set of rules that helps computers understand how to find and talk to each other over the Internet.

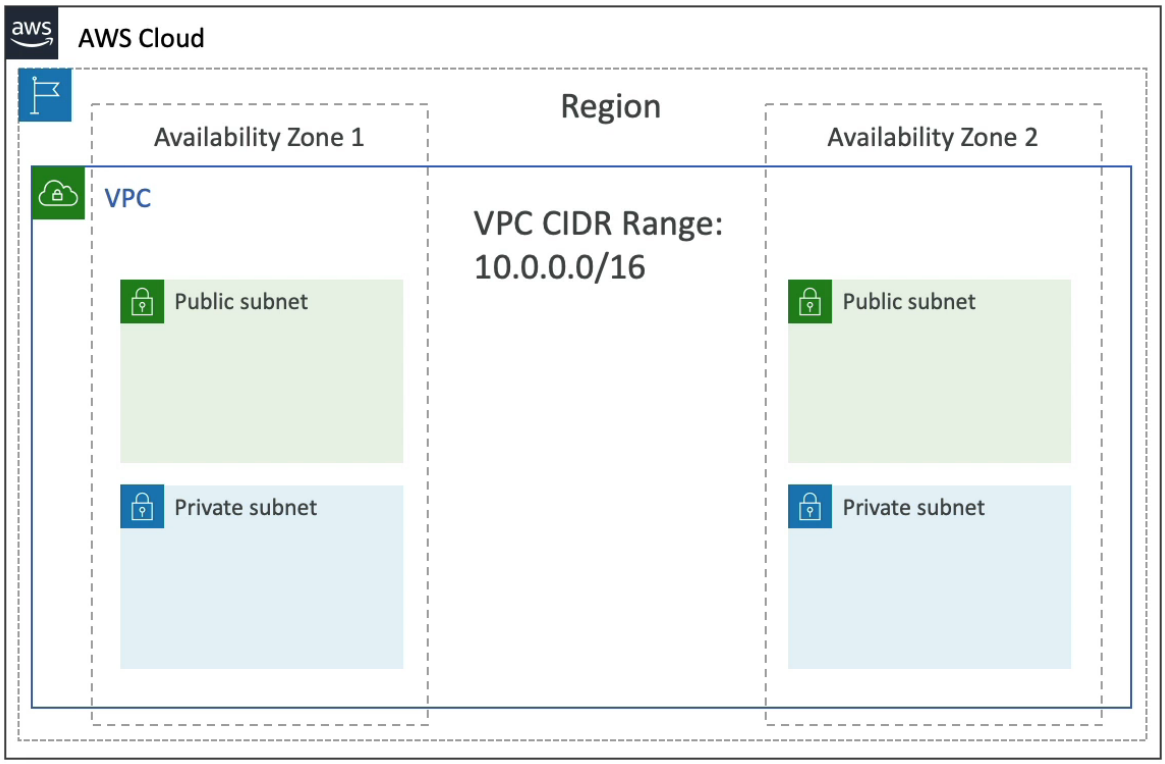
Imagine a large city with many streets. Each street has houses, and each house has a unique address. CIDR is like the system that helps organize and allocate these addresses so that devices, like computers or servers, know where to find each other.

CIDR uses a notation that looks like this: `**10.0.0.0/16**` or `**192.168.0.0/24**`. This notation specifies a range of addresses. For example, `**10.0.0.0/16**` means all addresses from `**10.0.0.0**` to `**10.255.255.255**`. It's like saying, "This neighborhood starts at 10.0.0.0, and it goes up to 10.255.255.255."

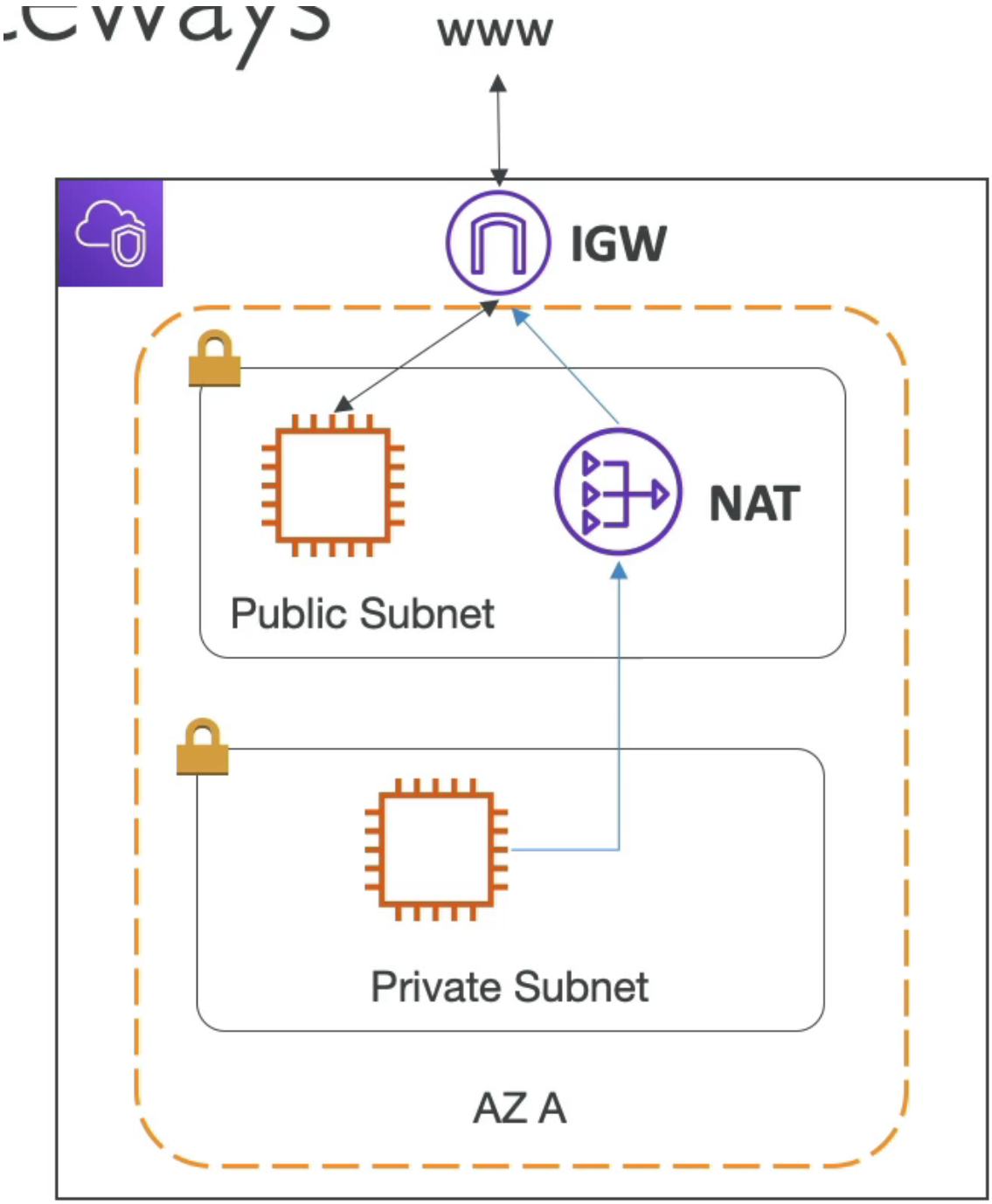
When you create a Virtual Private Cloud (VPC) in AWS and define its CIDR range, you're essentially setting up the address space for your virtual network, deciding which range of addresses your devices inside the network can use. This helps in organizing and managing communication within your virtual network and beyond.



- **VPC architecture**



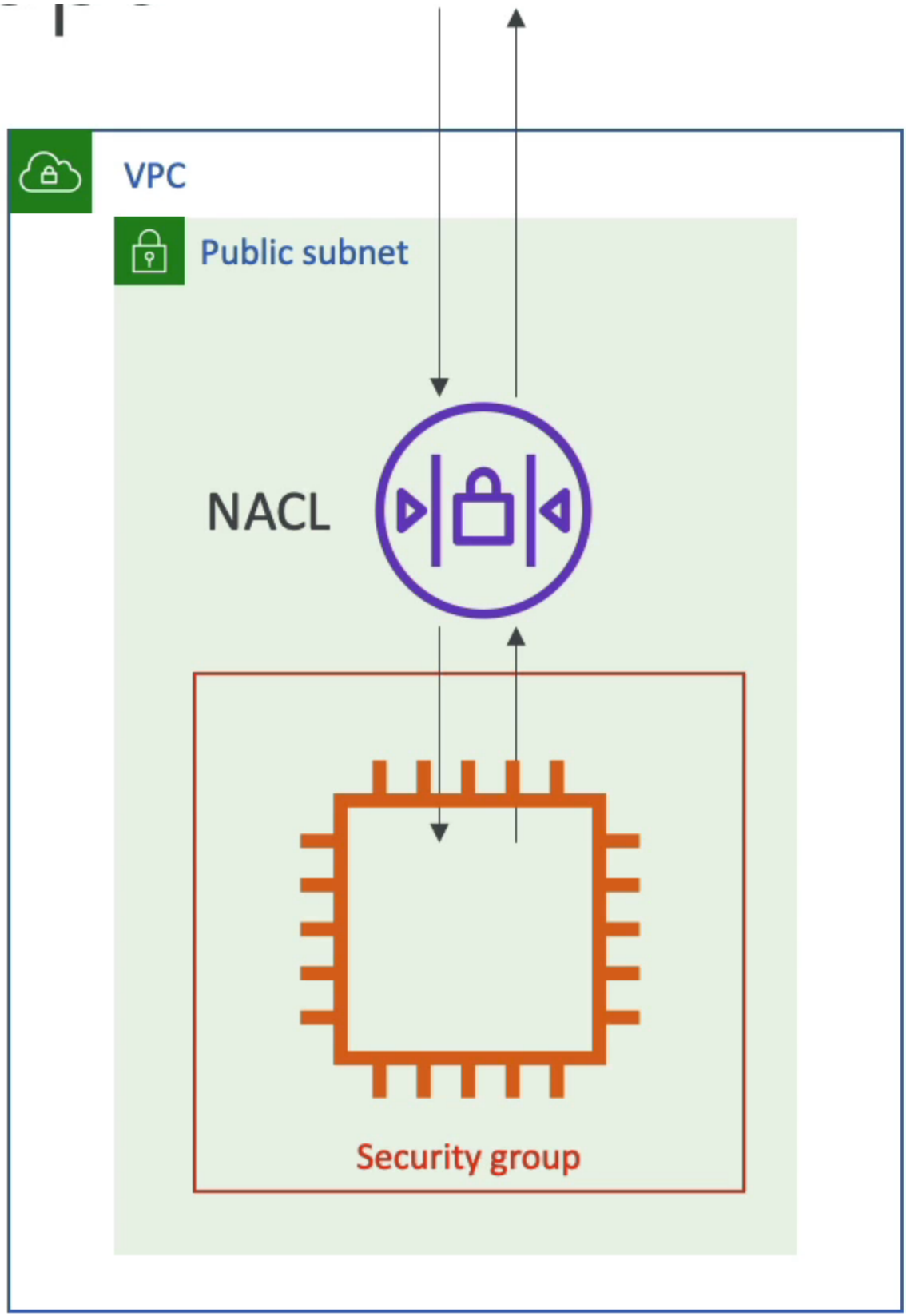
- **Internet Gateway and NAT gateways:**
  - For the public subnets to be able to access the internet, they need an internet gateway. Whenever a subnet has an IGW and a double-sided route to the IGW, it becomes a public subnet.
  - Also, sometimes you want to give your private subnets access to the internet but not from the internet. This could be to fetch information or software updates. So, a NAT gateway is created for the same.
  - NAT gateways (aws-managed) and NAT instances (self-managed) allow your instances within private subnets to access the internet while remaining private.
  - The NAT gateway is created within the public subnet.
  - **Public subnets = IGW = Internet gateway**
  - **Private subnets = NAT gateway = Network Address Translation gateway**



Network ACL & Security Groups

- Network security within our VPC
- EC2 instances exist in the public subnets within our VPC which need to have a controlled incoming traffic from the web (for safety) for which we have **NACL** and **Security Groups** as a firewalls.
- **NACL or Network Access Control List**
    - It is a firewall which controls traffic to and from the subnet (it is attached at the subnet level).
    - It has ALLOW and DENY rules which consist of IP addresses.
- **Security Groups**
    - A firewall that controls traffic to and from an ENI (Elastic Network Interface) / EC2 instance.
    - It has only ALLOW rules which consist of IP addresses and other security groups.

- Red border around the EC2 instance represents the security group.


VPC
Public subnet
NACL
Security group

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)

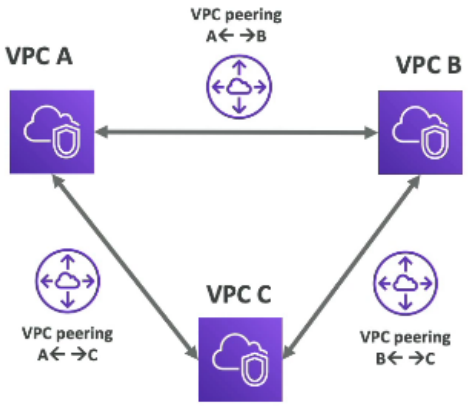
VPC Flow Logs

- A log (record) of all the IP traffic going in or out of the VPC.
- You can access
  - VPC Flow Logs
  - Subnet Flow Logs
  - Elastic Network Interface Logs
- This can help with monitoring and troubleshooting connectivity issues. For example
  - Subnet cannot connect to internet (check IPs and rules)
  - Subnet cannot connect to subnets
  - Internet cannot connect to subnets
- VPC Flow Logs can capture network information from other aws managed services as well like ELB, ElastiCache, RDS, Aurora, etc.

- These logs can go to S3, CloudWatch Logs, Kinesis Data Firehose, etc.

VPC Peering

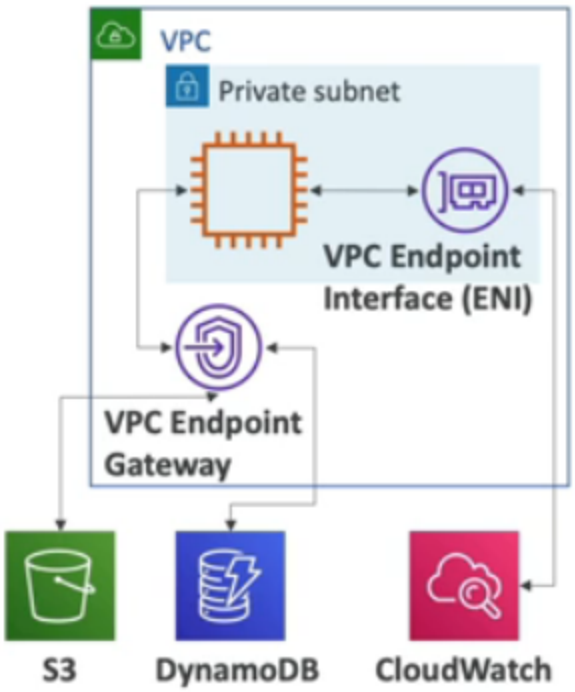
- Connect two VPC, privately using AWS' network
- Make them behave as if they were in the same network
- Must not have overlapping CIDR (IP address range)
- VPC Peering connection is **not transitive** (must be established for each VPC that need to communicate with one another)



VPC Endpoints

- All the AWS services we have been using are public — when we connect to them, we do it publically.
- But if we use a VPC endpoint, we can connect to these services using a private AWS network instead of the public internet network.
- This private network will enable better security and lower latency to access aws services.
- So, image you have an EC2 instance within a private subnet and you want to use VPC endpoints to connect that instance to other aws services. For this, you can use VPC Endpoints instead of the public network.
- Types of Endpoints:

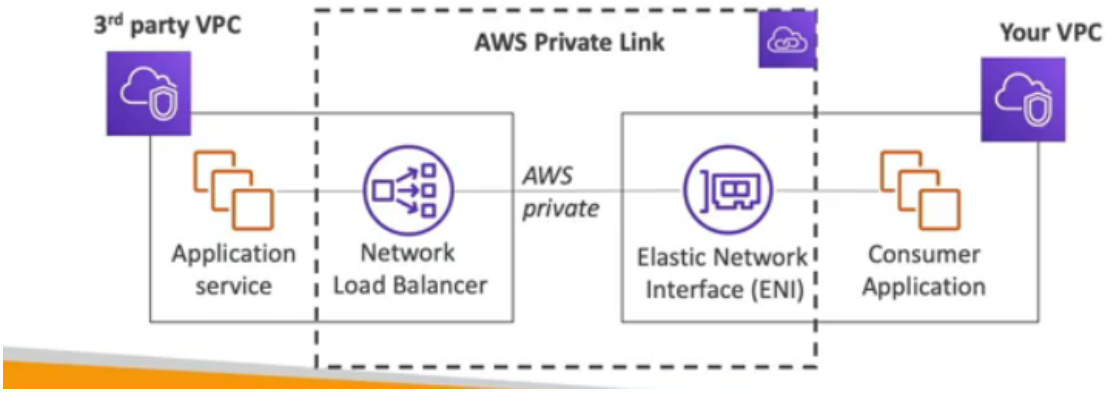
- **VPC Endpoint Gateway** is for S3 and DynamoDB.
- **VPC Endpoint Interface** is for rest of the services.



AWS PrivateLink (VPC Endpoint Services)

- Suppose you have an application running on your VPC that you want to expose to 1000s of services within other VPCs or vice-versa.
- For this, you can use aws PrivateLink. (you cannot use vpc peering as it is not scalable)
- When you use PrivateLink, it does not require internet gateway, NAT, route tables, anything of the sort.
- This is easily scalable and way more secure than the public network.
- To establish this PrivateLink, you will have to ask the vendor to create a Network Load Balancer (NLB) to expose their service and at your end you will

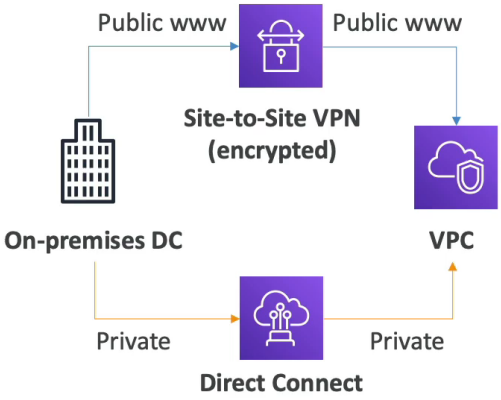
create an Elastic Network Interface (ENI) and then you will establish a private link between the two. This will give you access to their NLB privately and hence to their service.



Site to Site VPN & Direct Connect

- Hybrid cloud - to connect your on premises data centre to VPC.
- There are two ways to do so:
  1. Site to Site VPN
  2. Direct Connect (DX)

- Site to Site VPN
  - Connect an on-premises VPN to AWS
  - The connection is automatically encrypted
  - Goes over the public internet
- Direct Connect (DX)
  - Establish a physical connection between on-premises and AWS
  - The connection is private, secure and fast
  - Goes over a private network
  - Takes at least a month to establish

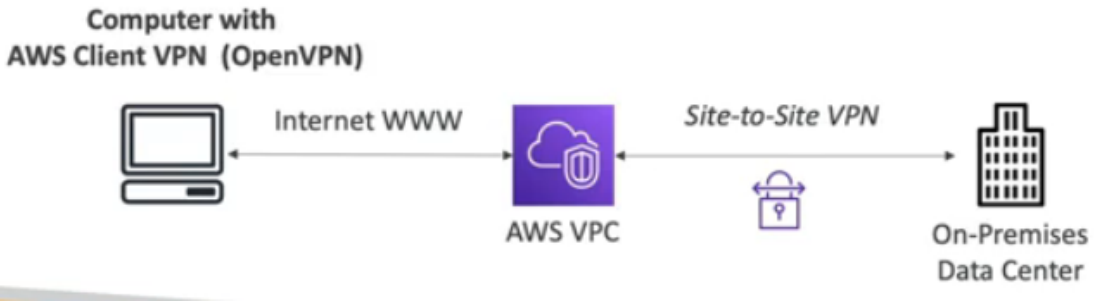


Site-to-Site VPN

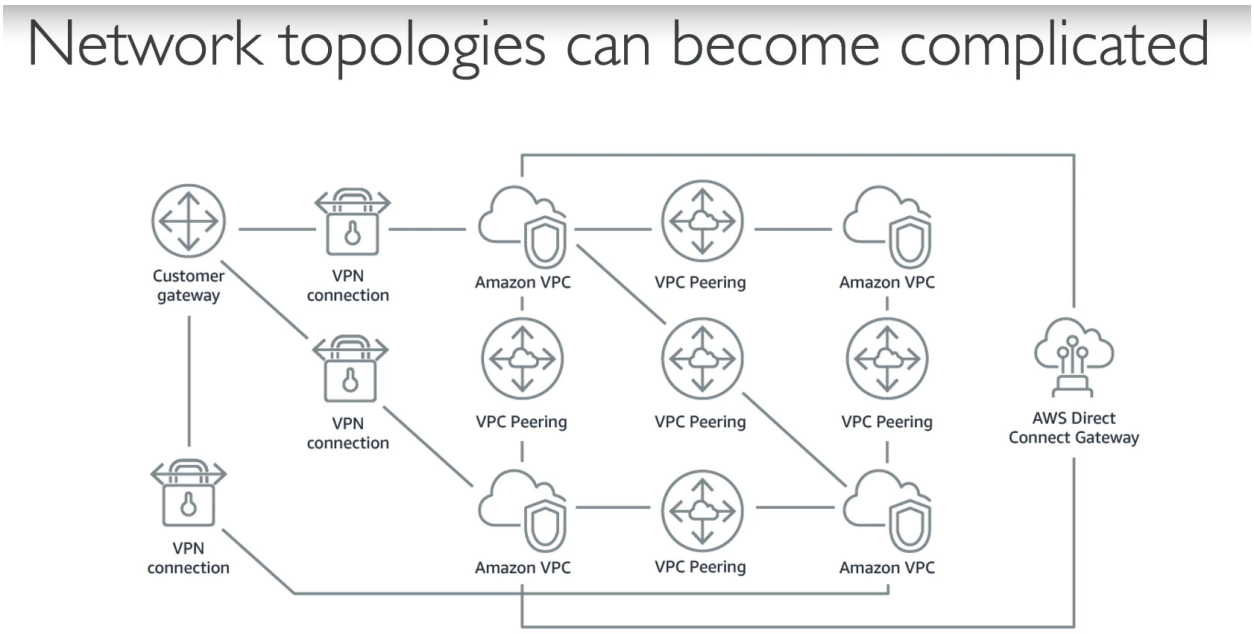
- On-premises: must use a Customer Gateway (CGW)
- AWS: must use a Virtual Private Gateway (VGW)

AWS Client VPN (OpenVPN)

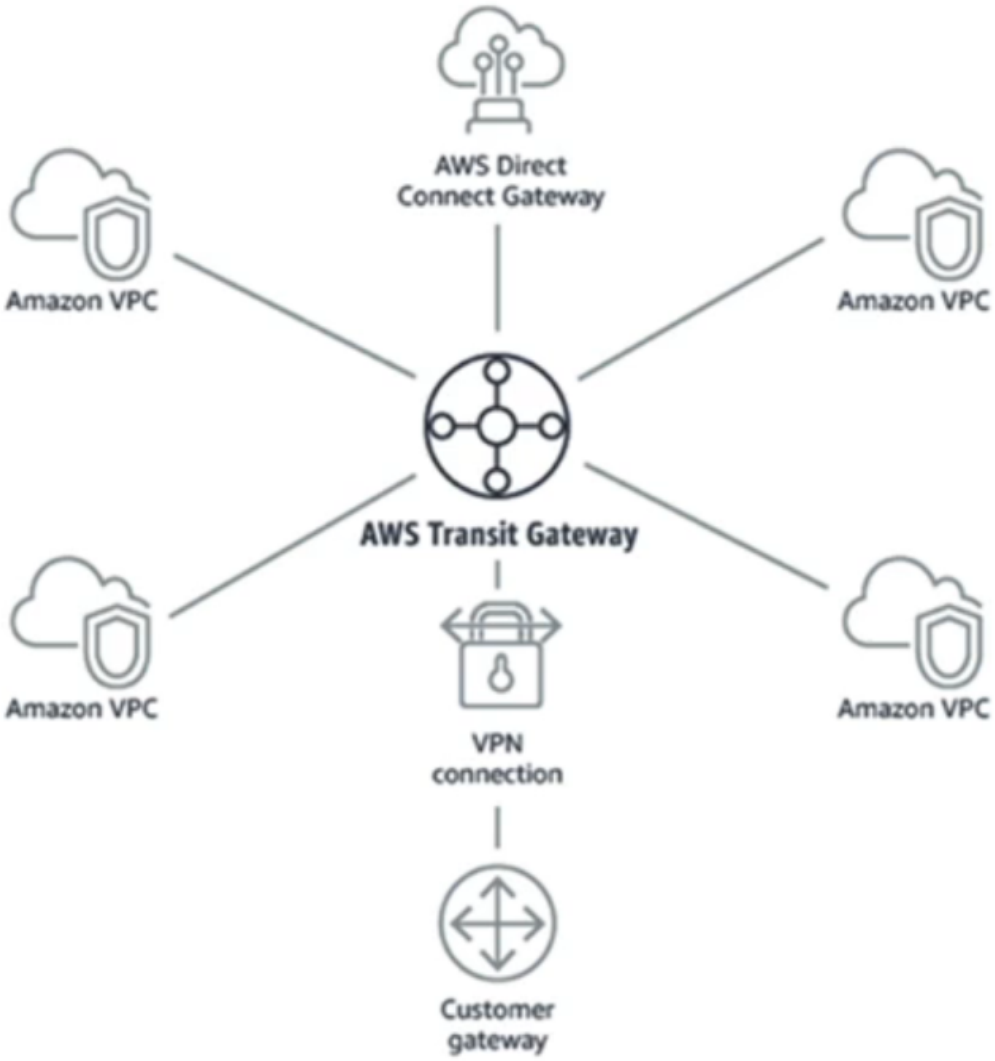
- If you want to access your EC2 instance deployed within a private subnet in a VPC (in aws or on-premises) from your system, you can use OpenVPN.
- It allows you to connect to your instances over a private IP almost as if you were in the private VPC network.
- This connection is established over the public internet.



Transit Gateway



- To solve this mess, transit gateway service was created.
- The Transit Gateway facilitates peering connections between thousands of VPCs and your on-premises system, organized in a hub-and-spoke star connection.
- In this architecture, the VPC Transit Gateway is positioned in the middle, acting as a centralized point of connectivity. All Amazon VPCs, Direct Connect gateways, and VPN connections are seamlessly linked through the Transit Gateway.
- This eliminates the need to establish direct peering connections between individual VPCs, streamlining the network architecture.
- There is no necessity for separate connections and routes for each VPC, Direct Connect, and site-to-site VPN. Instead, all of these connections and routing complexities are efficiently managed within a single gateway, simplifying network configuration and providing a unified solution for connectivity across your AWS infrastructure.


AWS Direct
Connect Gateway
Amazon VPC
Amazon VPC
AWS Transit Gateway
Amazon VPC
Amazon VPC
VPN
connection
Customer
gateway

Summary

- **VPC:** Virtual Private Cloud
- **Subnets:** Tied to an AZ, network partition of the VPC
- **Internet Gateway:** at the VPC level, provide Internet Access
- **NAT Gateway / Instances:** give internet access to private subnets
- **NACL:** Stateless, subnet rules for inbound and outbound
- **Security Groups:** Stateful, operate at the EC2 instance level or ENI
- **VPC Peering:** Connect two VPC with non overlapping IP ranges, nontransitive
- **Elastic IP** –fixed public IPv4, ongoing cost if not in-use

- **VPC Endpoints:** Provide private access to AWS Services within VPC
- **PrivateLink:** Privately connect to a service in a 3rd party VPC
- **VPC Flow Logs:** network traffic logs
- **Site to Site VPN:** VPN over public internet between on-premises DC and AWS
- **Client VPN:** OpenVPN connection from your computer into your VPC
- **Direct Connect:** direct private connection to AWS
- **Transit Gateway:** Connect thousands of VPC and on-premises networks together

Good job!
AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated private network connection from your premises to AWS.

Question 7:

A company needs to have a private, secure, and fast connection between its on-premises data centers and the AWS Cloud. Which connection should they use?

- ○ AWS Connect
- ○ Site-to-Site VPN
- ○ VPC Peering
- ◉ **AWS Direct Connect**

Good job!
A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. 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.

Question 6:

You need a logically isolated section of AWS, where you can launch AWS resources in a private network that you define. What should you use?

- ○ Subnets
- ○ Availability Zones
- ◉ **A VPC**
- ○ NAT Instances

Good job!
VPC Peering connection is a networking connection between two VPCs using AWS' network.

Question 5:

A company needs two VPCs to communicate with each other. What can they use?

- ○ VPC Endpoints
- ○ AWS Direct Connect
- ○ Internet Gateway
- ◉ **VPC Peering**