Amazon Virtual Private Cloud Detailed summary

- Security groups are stateful**: This means any changes applied to an incoming rule will be automatically applied to the outgoing rule**.
- Incoming == out going (Stateful)
- If you allow an incoming port 22, the outgoing port 22 will be automatically opened.
- **Inspects packets in the context of their traffic flow, allows you to use more complex rules, and allows you to log network traffic and to log Network Firewall fire wall alerts on traffic.**
- **Stateful rules consider traffic direction**.

Components of VPC

1. IP address Range
2. Subnets

Difference b/n SG and Subnet

3. Route tables
4. Network gateways
5. Security Groups
6. NACL
7. VPC end points
8. Elastic Network interfaces
9. NATs
10. VPC peering

Connectivity options: VPC Peering, Software VPN, Software to AWS managed VPN, Direct connect, AWS private link

What is a VPC?

- VPC stands for Virtual Private Cloud.

- It's a custom-defined virtual network within the AWS Cloud.
- Users can logically create their personal network, designing and implementing a separate and independent network that would operate in the AWS Cloud.
- Primary components are : **Subnets**, **IP addresses**, **NAT Devices** (Instances & Gateways), **Route Tables**, Internet & Virtual Private Gateways, **Access Control Lists**, **Security groups**, VPC Endpoints.
- A subnet is a segment of the VPC IP address range, where we can launch EC2 Instances (Public) , RDS (Private) and other AWS resources.
- Subnet are further classified as Public and Private.
- Public subnets hold resources that can be accessed from the Internet.
- Common attributes for instances in Public Subnets to have are:
- **Elastic IP (EIP) address or Public IP address attached to the EC2 instance**.
- **IGW attached to the VPC**.
- **Internet Gateway (IGW) is a virtual router which helps a VPC connect to the Internet**.

- **The subnet must have a route table entry with destination as internet gateway (IGW) 0.0.0.0/0.**

- **Public subnets are associated with a route table that directs subnet traffic to the internet using an Internet Gateway**
- **Security groups and NACLs should not block remove access**.
- .
- Private subnets hold resources that can be accessed from within the VPC network.
- **Multiple subnets can be associated with a single route table**. However, a single subnet cannot be associated with multiple route tables. ****
- Route tables hold sets of rules, called **routes** that are used to determine where the traffic is directed.
- Every **subnet in a VPC is linked to the route table**.
- Primary or Main route tables are the ones that automatically come with your VPC. They control the routing for all subnets that are not explicitly associated with any other route table.
- The **default route table cannot be deleted**.
- **Custom route tables are the ones you create for your VPC, and you can add routes as needed**.
- **Custom route tables can be deleted when not required**.
- By default**, instances that are launched in a VPC cannot communicate with the Internet**. To enable Internet access, Internet gateway needed to be attached to the VPC.
- Public subnets gets connected to IGW through route tables to get accessed over the Internet.
- Internet Gateways are horizontally scalable, highly available and redundant.
- EIP, Elastic IP address is a static IPv4 address used by AWS to manage its dynamic cloud computing services.

- It is associated with an AWS Account, and you can use it to mask if an instance failure occurs i.e., if a server fails, we can map this IP address to another server and keep moving without any issues.
- NAT devices can be either an Instance / Gateway residing in Public subnet, (to which an EIP is assigned).
- **NAT devices help instances in Private subnets interact with the Internet**.
- Access Control List (ACL) is an optional layer of security that acts as a firewall for controlling network traffic in and out of the subnet.
- Rules are defined with **the ACL for allowing or denying network traffic either on ports / IP** addresses.

- Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically-isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including the selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.
- You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications.
- You can easily customize the network configuration of your Amazon VPC. For example, you can create a public-facing subnet for your web servers that have access to the internet.
- You can also place your backend systems, such as databases or application servers, in a private-facing subnet with no internet access. You can use multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet

What is NAT Gateways?

- NAT stands for Network Address Translation.
- A NAT Gateway is a device used to **enable instances in a private subnet ---to connect to --- the internet or other AWS services**.
- It prevents the internet from initiating connections with the instances present in the private subnet.
- It forwards traffic from the instance in the private subnet to the internet or other AWS services, and then sends the response back to the instances.
- Changes the instances IP address with the NAT device's address when the traffic goes to the Internet.
- We have 2 kinds of NAT devices:
    - NAT Instance
    - NAT Gateway

<u>What is an Egress only Internet Gateway?</u>

- An egress-only internet gateway is a horizontally scaled, redundant, and highly available VPC component.
- It 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.

- IPv6 addresses are globally unique, and are therefore public by default.
- If you want your instance to be able to access the internet, but you want to prevent resources on the internet from initiating communication with your instance, you **can use an egress-only internet gateway**.
- An egress-only internet **gateway is stateful**: it **forwards traffic from the instances in the subnet to the internet or other AWS services, and then sends the response back to the instances**.

NAT Instance : Home work

- NAT Instance uses Amazon Linux AMIs.
- NAT Instance limit depends on your instance type limit for the region.
- NAT Instance does not support IPv6 traffic.

NAT GW:

- NAT Gateway usage is charged to the customer on an hourly basis. (Billable)
- NAT Gateway does not support IPv6 traffic.

  AWS recommends the usage of NAT Gateway, since they provide better availability and bandwidth over NAT Instances.

What is a VPC Endpoint ?

- VPC Endpoint allows us to securely connect your VPC and supported AWS services powered by AWS PrivateLink**. AWS PrivateLink is a service that allows you to access AWS services by using private IP addresses**. In this case, traffic does not leave Amazon's network.
- **VPC endpoint does not require a NAT Gateway, NAT instance, Internet Gateway, or any VPN services to access AWS Services**.
- There are two types of VPC endpoints: Gateway and Interface.

What is an AWS VPC Endpoint service?

- VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by **AWS Private Link without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection**.
- Instances in your VPC do not require public IP addresses to communicate with resources in the service.
- Traffic between your VPC and the other service does not leave the Amazon network.

What is a Stateful Firewall ?

- Security groups are stateful**: This means any changes applied to an incoming rule will be automatically applied to the outgoing rule**.
- Incoming == out going (Stateful)
- If you allow an incoming port 22, the outgoing port 22 will be automatically opened.
- **Inspects packets in the context of their traffic flow, allows you to use more complex rules, and allows you to log network traffic and to log Network Firewall firewall alerts on traffic.**
- **Stateful rules consider traffic direction**.

What is a Stateless Firewall?

- Network ACLs are stateless: This means **any changes applied to an incoming rule will not be applied to the outgoing rule**.
- If you allow an incoming port 22, you would also need to apply the rule for outgoing traffic.
- Inspects each packet in isolation, without regard to factors such as the direction of traffic, or whether the packet is part of an existing, approved connection. This engine prioritizes the speed of evaluation. It takes rules with standard 5-tuple connection criteria.

A 5-tuple refers to a set of five different values that comprise a Transmission Control Protocol/Internet Protocol (TCP/IP) connection. It includes a source IP address/port number, destination IP address/port number and the protocol in use

What is AWS Site-to-Site VPN ?

- A VPN connection refers to the connection between your VPC and your own on-premises network. Site-to-Site VPN supports Internet Protocol security (IPsec) VPN connections.
- By default, instances that you launch into an Amazon VPC can't communicate with your own (remote/ on-premises) network.
- VPN connection: A secure connection between your on-premises equipment and your VPCs.
- VPN tunnel: An **encrypted link where data can pass** from the customer **network to or from** AWS.
- Customer gateway: An AWS resource which provides information to AWS about your customer gateway device.
- Customer gateway device: A physical device or software application on your(on prem) side of the Site-to-Site VPN connection.
- Virtual private gateway: The VPN concentrator on the Amazon side of the Site-to-Site VPN connection. You use a virtual private gateway or a transit gateway as the gateway for the Amazon side of the Site-to-Site VPN connection.

- Transit gateway: A transit hub that can be used to interconnect your VPCs and on-premises networks. You use a transit gateway or virtual private gateway as the gateway for the Amazon side of the Site-to-Site VPN connection.

What is inter region VPC peering?

VPC (Virtual Private Cloud) is an isolated network of resources created in the cloud, basically your isolated data center created in the cloud. **Inter-region VPC peering permits resources like, EC2 instances, databases, lambda functions running in VPCs within different AWS regions to communicate with each other using private addresses without requiring gateways or VPN connections**. Traffic using inter-region peering actually stays on the AWS global backbone network (internet) and never passes through the public internet where it **is exposed to threats** vectors like DDoS attacks, making it a more secure means of communication. It is a simple and cost effective way to share resources between different regions.

DNS hostnames

AWS provides your instance in a VPC with public and private DNS hostnames that correspond to the public IPv4 and private IPv4 addresses for the instance but do not provide DNS hostnames for IPv6 addresses.

What is a Transit gateway?

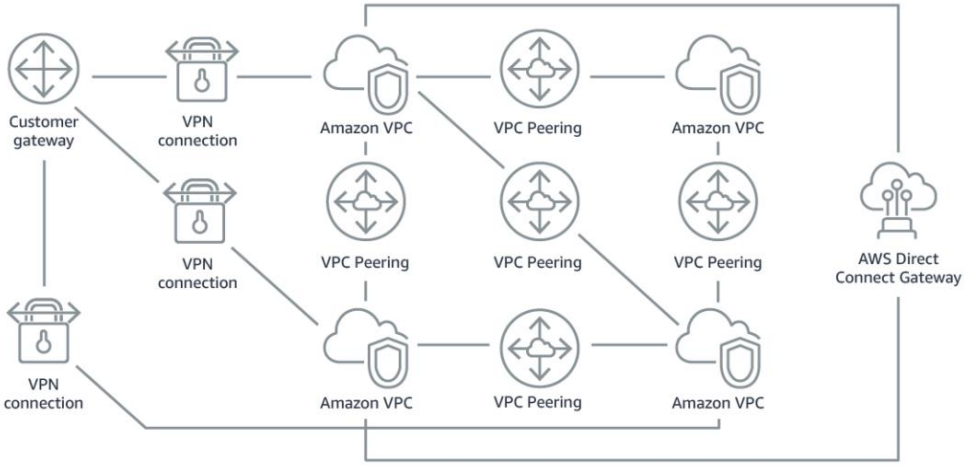
- The AWS Transit Gateway helps you connect multiple VPCs and on-premises networks through a central hub. It simplifies your network with VPCs and on-premises connections and solves the problem of complex peering relationships.
- With VPC peering using the Transit gateway, your data is always encrypted and no longer uses the public internet for communication.
- Benefits of using Transit gateway:
    - Easy to connect
    - Full control
    - Greater security
    - Multicast feature
- Reasons to use Transit gateway over VPC peering:
    - VPC peering does not support transitive peering meaning, you can only peer two VPC at a time.
    - To peer your VPC with an on-premise network, you can not use VPC peering. Transit gateway supports connecting on-premise networks.
- Transit gateway limits:
    - Per transit gateway, you can have 20 transit gateway route tables.
    - Per transit gateway, you can have 10,000 routes.
    - Per transit gateway, there can be 50 transit gateway attachments.
    - Per VPC you can have 5 unique transit gateway.

How Transit gateway can help you simplify your network?

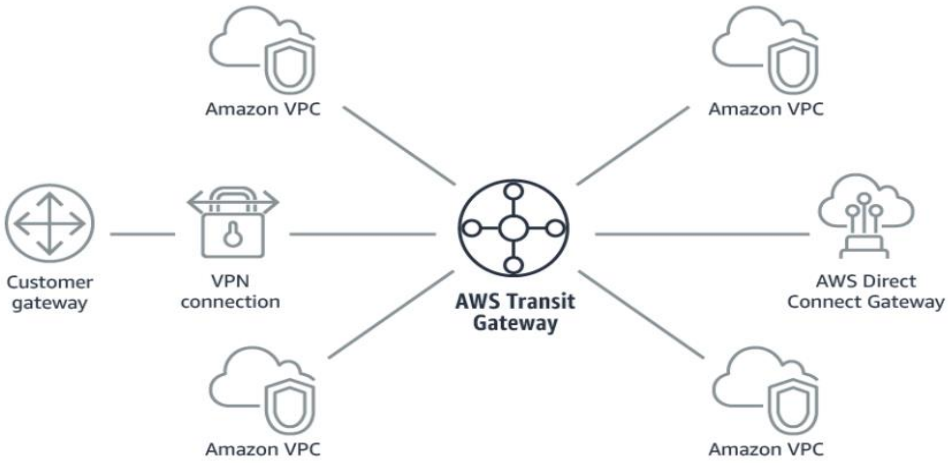
- Transit Gateway acts as a cloud router that supports connecting with the following resources:

- Amazon VPC
- VPN Connection having Customer Gateway
- AWS Direct Connect Gateway

- **Without Transit Gateway:**
  - VPC peering can have only one to one relationship between two VPCs. The complexity increases as you scale the number of connections.
  - Maintenance of the route table is another big challenge when you are scaling, you must keep the route table having routes to VPC and connection with the on-premise network using a separate network gateway for each new connection.



- **With Transit Gateway:**
  - To interconnect Amazon VPC with an on-premise network, we can use Transit Gateway.
  - The network is standardized and easily scalable. With Transit Gateway, you have one place to manage and monitor the number of active connections for each network.



- Since connecting to an on-premise network is not possible virtually, In this lab, you will learn how to create a Transit gateway and use it to peer VPC.

Transit gateway use cases

- Applications can be delivered around the world.
- Move your network design from Multi-AZ to Multi-region.
- Scale quickly and respond to spikes in traffic smoothly.

- Connect to all types of networks in one place.