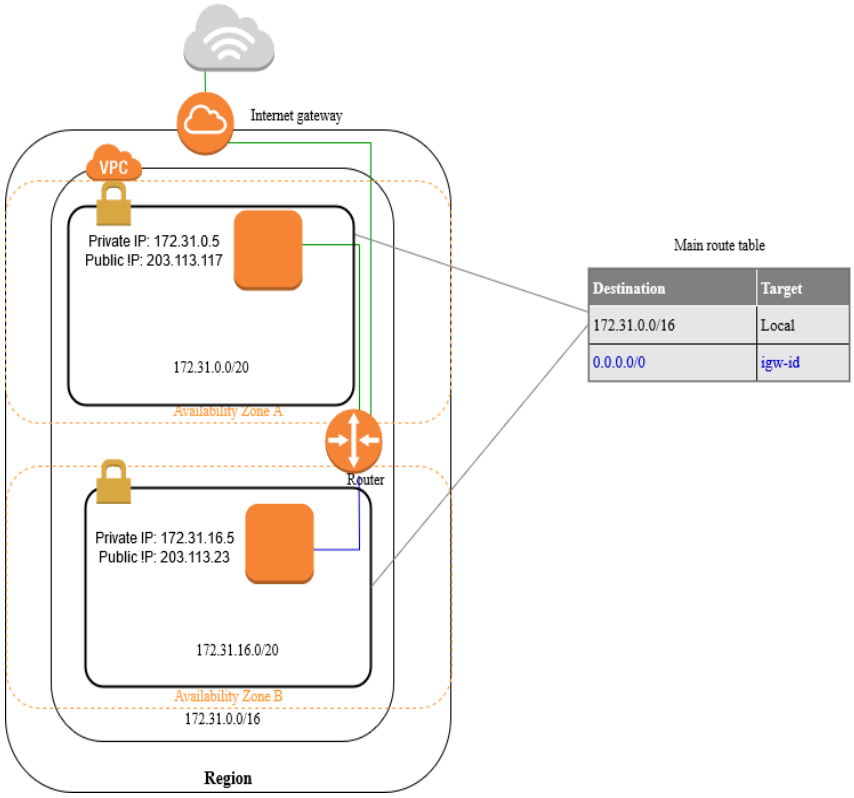

amazon
VPC

❖ AMAZON VPC (VIRTUAL PRIVATE CLOUD):

- Amazon VPC enables you to launch AWS resources into a virtual network that you've defined.
- It is a virtual network dedicated to your AWS account. It is a logically isolated from other virtual networks in the AWS Cloud.
- This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

➢ DEFAULT VPC:

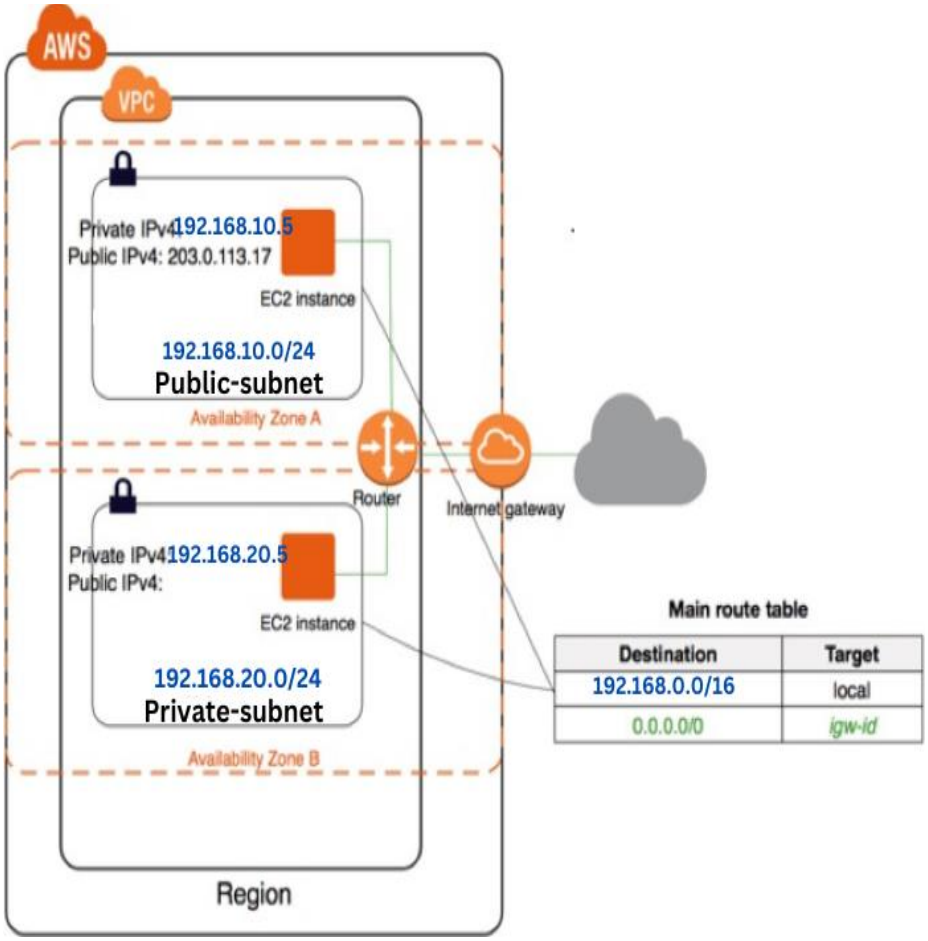
- The default VPC comes with preconfigured setup in your AWS account.
- It is a different setup than a non-default VPC.
- In the default VPC, all subnets have a Route to the internet via route table and an attached to IGW
- Each instance in the default VPC has a Private and Public Ip address.
- A default VPC is ready for you to use so that you don't have to create and configure your own VPC.
- The default vpc architecture:



➢ NON-DEFAULT VPC:

- A non-default vpc or custom vpc is not automatically created when EC2 resources are provisioned.
- Customer needs to create own VPC.
- No internet gateway, No route Tables by default.
- If you understand VPC reasonably well, then you should always create your own VPC. This is because you have full control over the structure.

NOTE: By default, number of VPC's per region 5.



➢ VPC COMPONENTS:

- Amazon VPC is the networking layer for Amazon EC2.
- The following are the key concepts for VPCs:

CIDR:

- Classless Inter-Domain Routing (CIDR).
- CIDR is a set of Internet protocol (IP) standards that is used to create unique identifiers for networks and individual devices.
- An internet protocol address allocation and route aggregation methodology.

E.g.: 192.168.0.0/16 10.0.0.0/8

SUBNETS:

- A subnet is a range of IP addresses in your VPC, typically a LAN.
- A Subnet lives within a single Availability Zone in VPC.

E.g.: 192.168.10.0/24 192.168.15.0/24

ROUTER:

- Routers interconnect subnets and direct traffic between Internet gateways, virtual private gateways, NAT gateways, and subnets.

ROUTE TABLES:

- A Route table contain a set of rules, called routes that are used to determine where network traffic is directed.
- Route tables direct network traffic between instances inside a subnet.
- A route table rules are comprised of two main components.
  DESTINATION: CIDR block range of the target (Where the data is routed to)
  TARGET: A name identifier of where the data is being routed to.

INTERNET GATEWAY (IGW):

- An Internet gateway is a network "node" that connects two different networks that allows communication between instances in your VPC and the Internet.

EGRESS -ONLY INTERNET GATEWAY:

- A stateful gateway to provide egress only access for IPv6 traffic from the VPC to the Internet.

CARRIER GATEWAYS:

- A carrier gateway provides connectivity to the carrier network for resources in a Wavelength VPC.

DHCP OPTIONS SETS:

- The Dynamic Host Configuration Protocol (DHCP) provides a standard for passing configuration information to hosts on a TCP/IP network.
- The options field of a DHCP message contains the configuration parameters. Some of those parameters are the domain name, domain name server, and the NetBIOS-node-type.

PRIVATE IP-ADDRESS:

- The Private IP address is used for internal communication between instances within the VPC.

PUBLIC IP-ADDRESS:

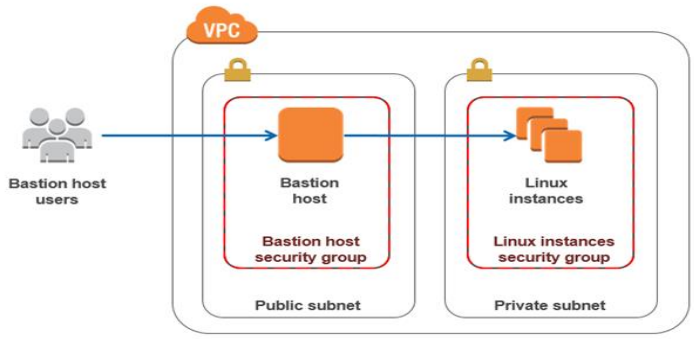
- A Public IP address is required if you want the Ec2 instance to have direct communication with resources across the open internet.

ELASTIC IP-ADDRESS:

- Static IP-Address for Dynamic Cloud Computing.
- An EIP is a static Ipv4 address designed for Dynamic cloud computing.
- Attaching an EIP to an instance will replace its default public IP address for as long as it is attached.

BASTION HOST:

- Bastion hosts are instances that sit within your public subnet and are typically accessed using SSH or RDP.
- Once remote connectivity has been established with the bastion host, it then acts as a 'jump' server within your VPC.
- It essentially acts as a bridge to your private instances via the internet.



VPC FLOW LOGS:

- It Capture information about the IP traffic going to and from network interfaces in your VPC.
- Flow log data can be published to AWS CloudWatch Logs and AWS S3.
- Flow log data is collected outside of the path of your network traffic, and therefore does not affect network throughput or latency.
- The maximum aggregation interval is 10 minutes.

NAT GATEWAY:

- A highly available, managed Network Address Translation (NAT) service for your resources in a private subnet to access the Internet.

NAT INSTANCE:

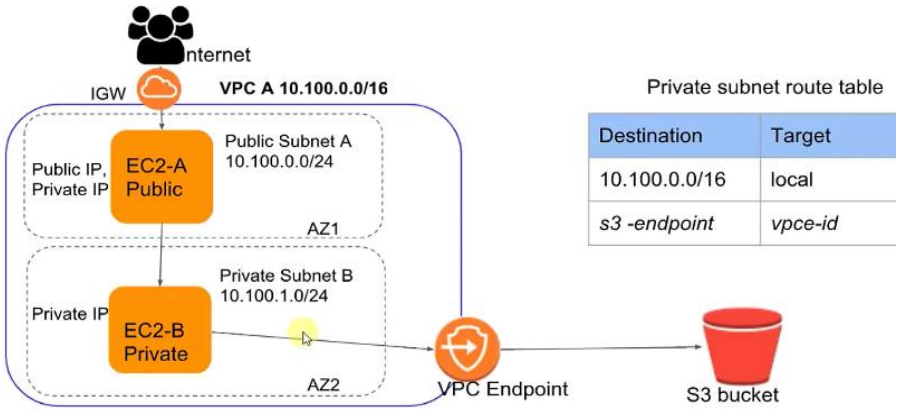
- A NAT instance is, like a bastion host, an EC2 instance that lives in your public subnet.
- A NAT instance, however, allows your private instances outgoing connectivity to the internet while at the same time blocking inbound traffic from the internet.

ENDPOINTS:

- Endpoints are virtual devices. They allow Traffic between your VPC and the other service does not leave the Amazon network.
- Allows private access to S3 and DynamoDB.
- There are two types of VPC endpoints:

  INTERFACE ENDPOINT: It is an elastic network interface with a private IP address from the IP address range of your subnet that serves as an entry point for traffic destined to a supported service.

  GATEWAY ENDPOINT: It is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service.

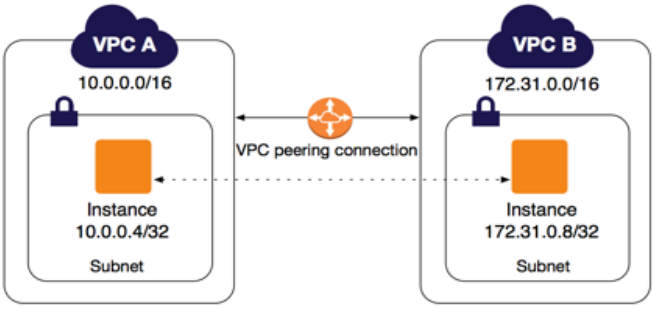


ENDPOINT SERVICES:

- To connect programmatically to an AWS service, you use an endpoint. An endpoint is the URL of the entry point for an AWS web service.
- The AWS SDKs and the AWS Command Line Interface (AWS CLI) automatically use the default endpoint for each service in an AWS Region.

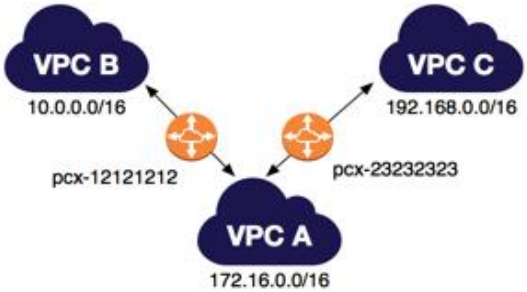
PEERING CONNECTION:

- It is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses.
- A VPC peering connection helps you to facilitate the transfer of data.
- For example, if you have more than one AWS account, you can peer the VPCs across those accounts to create a file sharing network.
- The VPCs can be in different regions (also known as an inter-region VPC peering connection).



MULTIPLE VPC PEERING CONNECTIONS:

- A VPC peering connection is a one-to-one relationship between two VPCs.



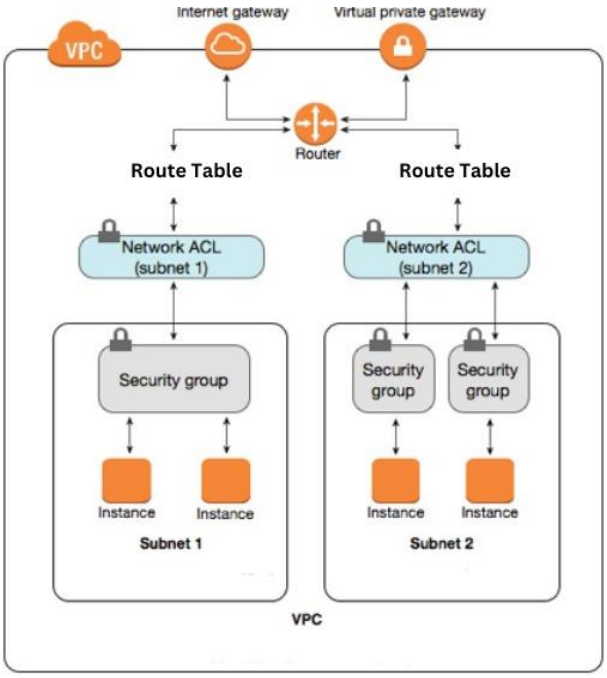
➢ VPC SECURITY:

SECURITY GROUPS:

- Security Groups are act as firewalls for controlling traffic at the instance level.
- Security Groups support only allow rules. That means stateful.

NETWORK ACCESS CONTROL LIST (NACLs):

- It is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.
- ACLs operate at the network/subnet level.
- All IN and OUT traffic deny by default. That means stateless.



➢ DNS FIREWALL:

- The DNS Firewall configuration for your VPC determines whether Route 53 Resolver allows queries through or blocks them during failures
- You can configure a VPC to fail open or fail closed.
  - By default, the failure mode is closed, which means that Resolver blocks any queries for which it doesn't receive a reply from DNS Firewall. This approach favors security over availability.
  - If you enable fail open, Resolver allows queries through if it doesn't receive a reply from DNS Firewall.

➢ NEWORK FIREWALL:

- AWS Network Firewall is a managed service that makes it easy to deploy essential network protections for all of your Amazon Virtual Private Clouds.
- AWS Network Firewall also offers web filtering that can stop traffic to known bad URLs and monitor fully qualified domain names.

➢ VPN CONNECTION:

VIRTUAL PRIVATE NETWORK:

- By default, instances that you launch into an Amazon VPC can't communicate with your own (remote) network.
- You can connect your VPC to remote networks by using a VPN connection.

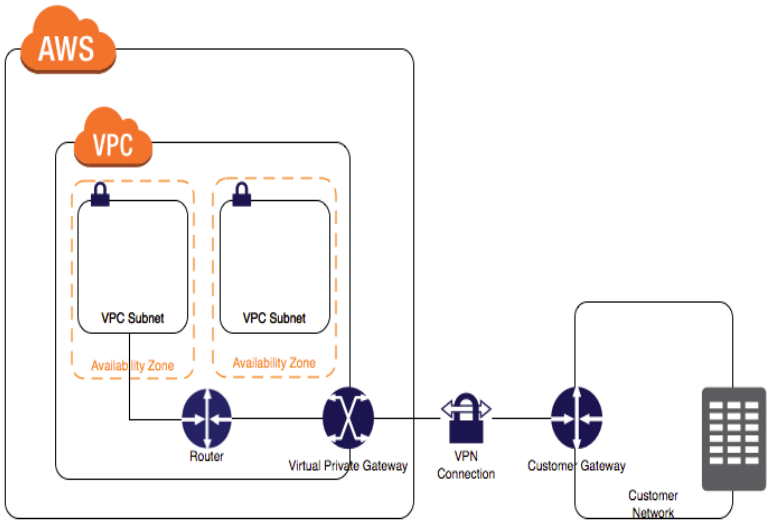
CUSTOMER GATEWAY:

- It is a physical device or software application on your side of the VPN connection.

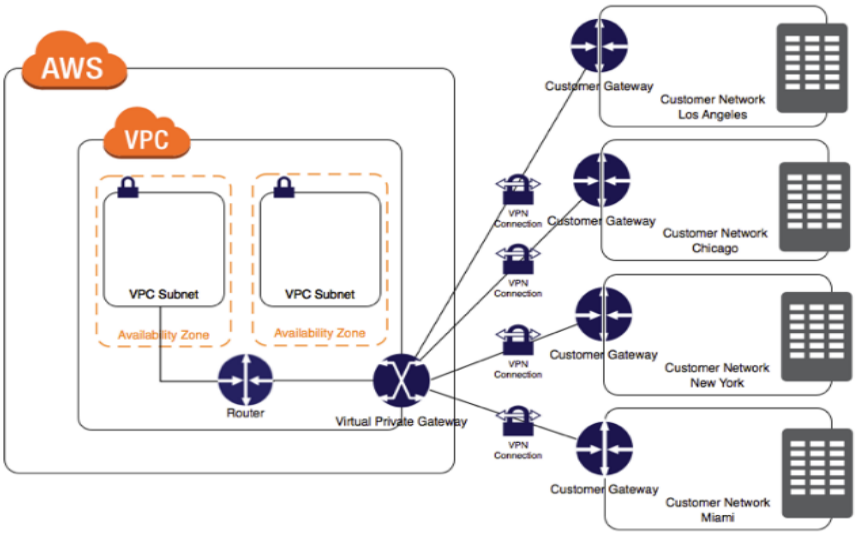
VIRTUAL PRIVATE GATEWAY:

- It is the VPN concentrator on the Amazon side of the site-to-site VPN connection.

A SINGLE VPN CONNECTION:

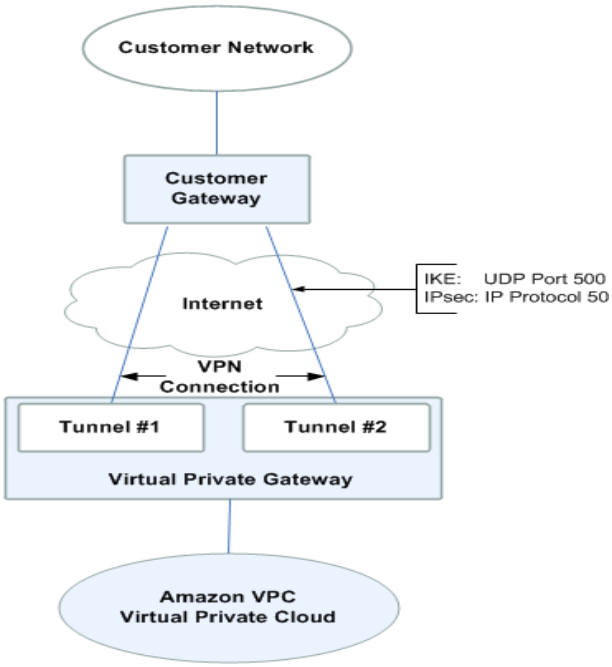


MULTIPLE VPN CONNECTIONS:



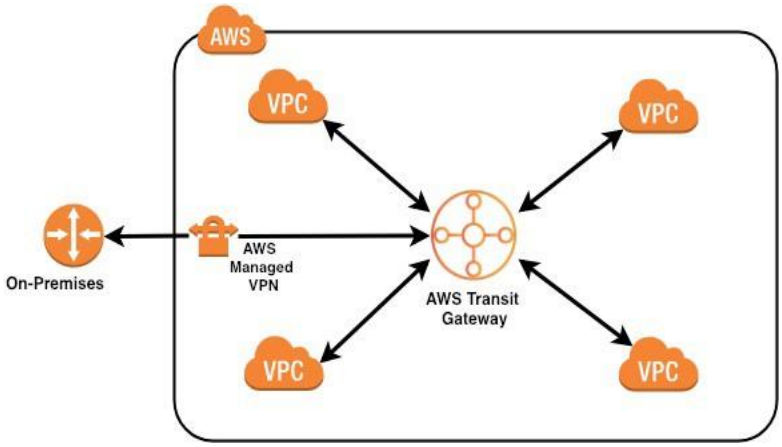
VPN TUNNEL:

- VPN connection consists of two **tunnels** to provide increased availability for the VPC service.
- If there's a device failure within AWS, your VPN connection automatically fails over to the second tunnel so that your access isn't interrupted.



➢ TRANSIT GATEWAY:

- A transit gateway is a transit hub that you can use to interconnect your virtual private clouds (VPC) and on-premises networks to a single gateway.
- Transit Gateway acts as a hub that controls how traffic is routed among all the connected networks which act like spokes.



➢ TRAFFIC MIRRORING:

- It can replicate the network traffic from an EC2 instance within their Amazon VPC and forward that traffic to security and monitoring appliances for content inspection, threat monitoring, and troubleshooting.
- Traffic Mirroring supports filters and packet truncation
- Traffic Mirroring key concepts:
  - **TARGET** : The destination for mirrored traffic.
  - **FILTER** : A set of rules that defines the traffic that is copied in a traffic Mirror session.
  - **SESSION** : An entity that describes Traffic Mirroring from a source to a target using filters

BENEFITS:

- Simplified operation
- Enhanced security
- Increased monitoring options

➢ VPC LIMITS:

- VPCs per region 5
- Subnets per region 200
- 5 Elastic IP addresses.
- 5 Internet Gateways.
- 5 NAT gateways per Availability Zone
- 1 Carrier gateways per VPC
- Route tables per VPC 200
- Network ACLs per VPC 200
- Rules per network ACL 20
- VPC security groups per region 2,500
- Inbound or outbound rules per security group 60
- Security groups per network interface 5
- Active VPC peering connections per VPC 50
- 50 VPN connections per region.
- 50 Customer Gateways per Region.
- Transit gateways per VPC 5

NOTE: It can be increased upon request.