VPC

What is VPC?

- 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 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.

What is VPC?

- You can easily customize the network configuration for your Amazon VPC. For example, you can create a public-facing subnet for your web servers that has access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access.
- You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

VPC Connectivity Options

- Connect directly to the Internet (public subnets)– You can launch instances into a publicly accessible subnet where they can send and receive traffic from the Internet.
- Connect to the Internet using Network Address Translation (private subnets) – Private subnets can be used for instances that you do not want to be directly addressable from the Internet. Instances in a private subnet can access the Internet without exposing their private IP address by routing their traffic through a Network Address Translation (NAT) gateway in a public subnet.

VPC Connectivity Options

- Connect securely to your corporate datacenter– All traffic to and from instances in your VPC can be routed to your corporate datacenter over an industry standard, encrypted IPsec hardware VPN connection.
- Connect privately to other VPCs- Peer VPCs together to share resources across multiple virtual networks owned by your or other AWS accounts.
- Privately connect to AWS Services without using an Internet gateway, NAT or firewall proxy through a VPC Endpoint.
- Privately connect to SaaS solutions supported by AWS PrivateLink.

NACL vs Security Groups

- Security group is the firewall of EC2 Instances whereas Network ACL Is the firewall of the Subnet.
- Security groups are stateful: This means any changes applied to an incoming rule will be automatically applied to the outgoing rule. e.g. If you allow an incoming port 80, the outgoing port 80 will be automatically opened.
- Network ACLs are stateless: This means any changes applied to an incoming rule will not be applied to the outgoing rule. e.g. If you allow an incoming port 80, you would also need to apply the rule for outgoing traffic.
- Security groups evaluate all the rules in them before allowing a traffic whereas NACLs do it in the number order, from top to bottom.

Subnet

- The practice of dividing a network into two or more networks is called subnetting. AWS provides two types of subnetting one is Public which allow the internet to access the machine and another is private which is hidden from the internet.

Route Table

- A *route table* contains a set of rules, called *routes*, that are used to determine where network traffic from your subnet is directed.

The following are the key concepts for route tables.

- **Main route table**—The route table that automatically comes with your VPC. It controls the routing for all subnets that are not explicitly associated with any other route table.
- **Custom route table**—A route table that you create for your VPC.
- **Route table association**—The association between a route table and subnet. The route table that's associated with a subnet controls the routing for that subnet.
- **Destination**—The destination CIDR where you want traffic from your subnet to go. For example, an external corporate network with a 172.16.0.0/12 CIDR.
- **Target**—The target through which to send the destination traffic; for example, an internet gateway.
- **Local route**—A default route for communication within the VPC.

Elastic IP

- An Elastic IP address is a static IPv4 address designed for dynamic cloud computing. An Elastic IP address is associated with your AWS account. With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account.
- An Elastic IP address is a public IPv4 address, which is reachable from the internet. If your instance does not have a public IPv4 address, you can associate an Elastic IP address with your instance to enable communication with the internet; for example, to connect to your instance from your local computer.

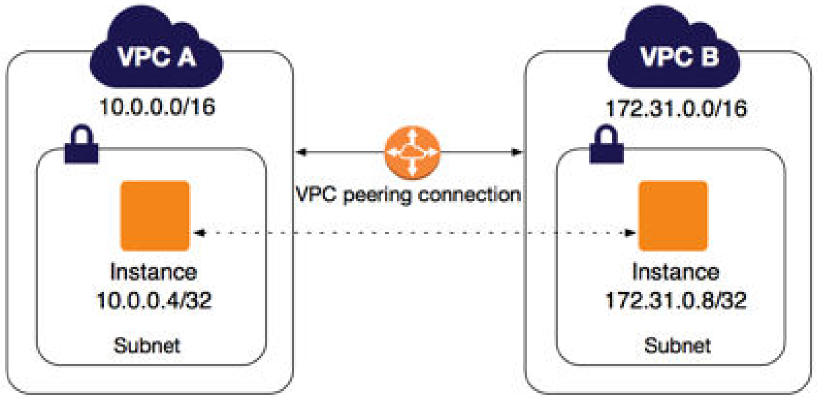
Internet Gateway

- Internet Gateways. An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic.
- An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

NAT Gateway

- You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.
- You are charged for creating and using a NAT gateway in your account. NAT gateway hourly usage and data processing rates apply.

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. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).

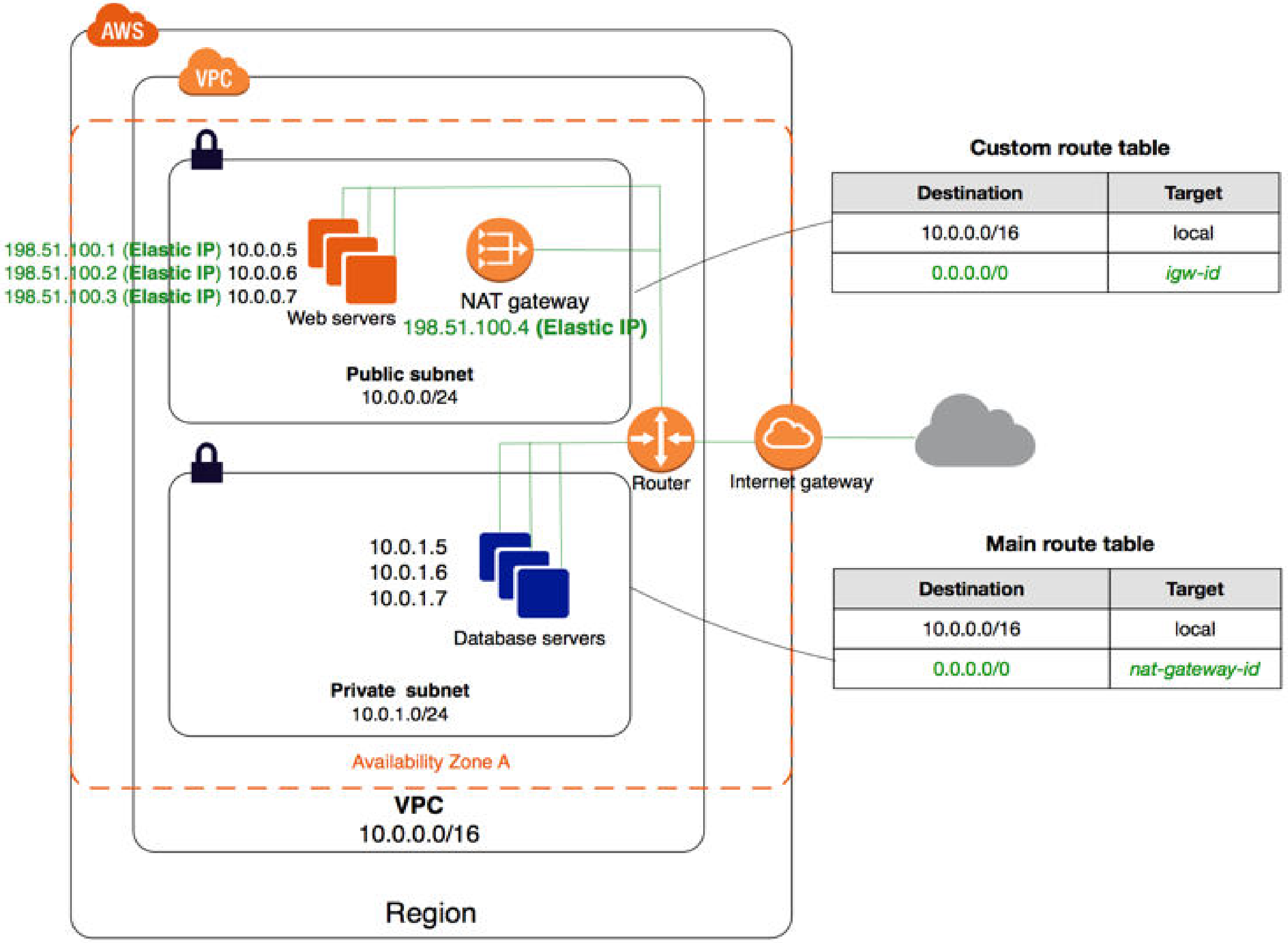
VPC Peering

- 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. You can also use a VPC peering connection to allow other VPCs to access resources you have in one of your VPCs.
- You can establish peering relationships between VPCs across different AWS Regions (also called Inter-Region VPC Peering). This allows VPC resources including EC2 instances, Amazon RDS databases and Lambda functions that run in different AWS Regions to communicate with each other using private IP addresses, without requiring gateways, VPN connections, or separate network appliances
- Traffic always stays on the global AWS backbone, and never traverses the public internet, which reduces threats, such as common exploits, and DDoS attacks.

VPC Peering

- Let us consider an example where we have three VPC’s, VPC A, VPC B and VPC C.
- A peering connection between VPC A and VPC B and another peering connection between VPC B and VPC C. This does not imply traffic can go from VPC A to VPC C through VPC B.
- That peering connection from VPC A to VPC C has to be established separately.

VPC Architecture – Private and Public Subnet



Custom route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Main route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*nat-gateway-id*