VPC

ow

Agenda

- What is VPC?
- Subnets, Route Tables, and Gateways
- Elastic Load Balancing
- Subnets, Route Tables, and Gateways

Overview VPC

- With Amazon VPC, we can launch AWS resources in a logically isolated virtual networks you defined.
- For example :

Imagine Amazon VPC as a virtual private space within Amazon Web Services (AWS), kind of like a private office or room in a big building. In this virtual space, you can create your own network environment just like you would set up your own office with different rooms and areas.

- VPC is a logical data center in AWS. It has subnets, route tables, internet gateway, network access control lists, and security groups.

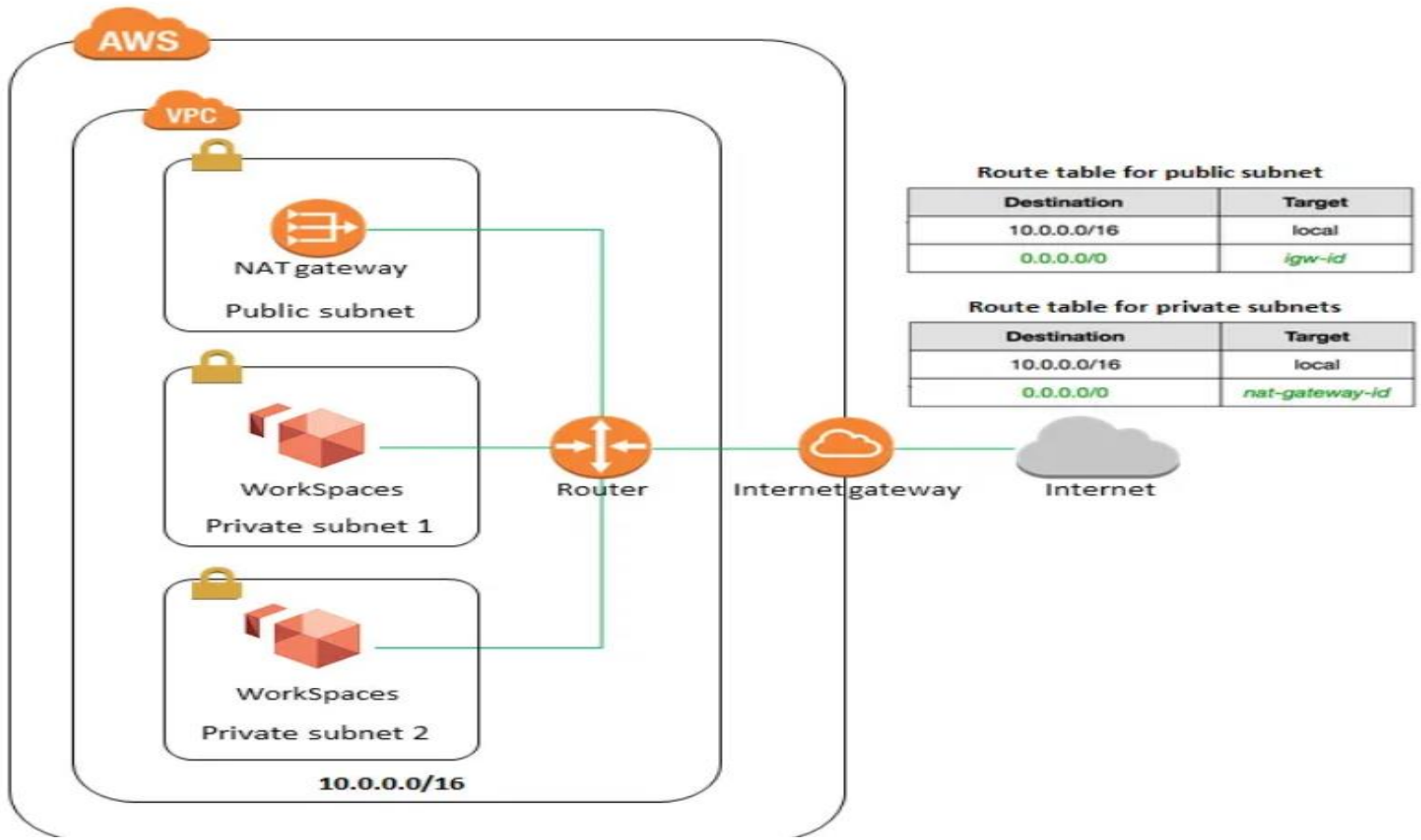
What we get?

- Isolation: Just like how your office is separate from other offices in the building, Amazon VPC keeps your network isolated from others using AWS.
- Customization: With Amazon VPC, you can design your network layout, choose IP addresses, create sub-networks, and control how different parts of your network communicate.
- Security: Amazon VPC lets you set up security measures such as firewalls, access controls, and encryption to protect your data from unauthorized access or cyber threats.

IP Address for VPC

- Specify an IPv4 CIDR block (or IP address range) for your VPC.
- If there is an Amazon VPC IP Address Manager (IPAM) IPv4 address pool available in this Region, you can get a CIDR from an IPAM pool. If you select an IPAM pool, the size of the CIDR is limited by the allocation rules on the IPAM pool (allowed minimum, allowed maximum, and default).
- If there is no IPv4 IPAM pool in this Region, you can manually input an IPv4 CIDR. The CIDR block size must have a size between /16 and /28.

..


AWS
VPC
NAT gateway
Public subnet
WorkSpaces
Private subnet 1
WorkSpaces
Private subnet 2
10.0.0.0/16
Router
Internet gateway
Internet
Route table for public subnet
Destination
Target
10.0.0.0/16
local
0.0.0.0/0
igw-id
Route table for private subnets
Destination
Target
10.0.0.0/16
local
0.0.0.0/0
nat-gateway-id

Need of VPC

- Whenever you are opening up service within a public cloud, there are high chances of attacks from the internet because your service is opening up to the world.
- So you lock the services within a VPC which lock your instances and ultimately secure the service from external attacks. The VPC then restricts the types of IP addresses, users, and traffic that can access your instances.
- These restrictions prevent unwanted guests that access your resources and secure you. VPC can be used to lock the services safely in a private network.

VPC Components

- Following are VPC components
- Subnet
- Route Table
- Internet Gateway

Subnet

- A subnet is a range of IP addresses in your VPC. After creating a VPC, you can add one or more subnets in each Availability Zone.
- A subnet is defined as the practice of subdividing a network into multiple sub-networks. The subnet mask and arrangement of IP addresses help in launching the subnet.
- Since maintenance of the small network is easier when compared to maintaining the large network subnets are used where large networks are divided into sub-networks.

Use Cases

- Consider an example: In any organization, there are different teams such as Finance, Marketing, HR, Technology, Support, Operations, and Sales.
- So when the data that has to be accessed to one team it cannot be given to the other team.
- Hence, the need for sub-networks arises and they are created so that it is easy to access and maintain the network
- It consists of a Virtual private cloud that includes the availability zones. Inside each availability zone, a subnet is created. Without the subnets in the VPC, it is not possible to launch an instance.

..

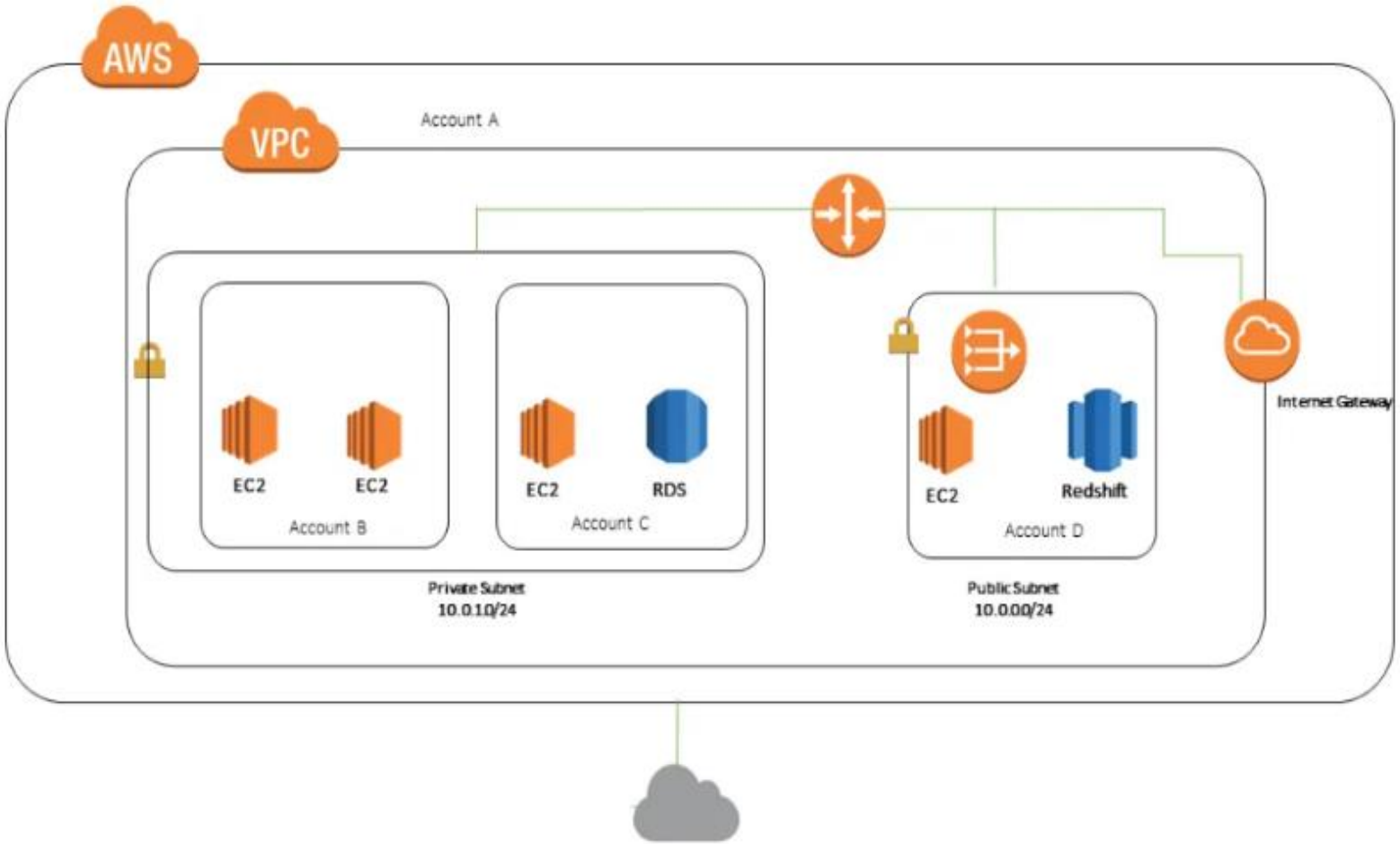


Image Source: AWS

Type of Subnet

- The subnets are of two types:
- Public Subnet: When the resources are connected to the internet it is called Public Subnet. The Subnet is made public because the subnets traffic receives from the main route table that is destined for the internet to the internet gateway. For example- Web Server.

- Private subnets: When the resources do not need an internet connection, or when you want to protect from the internet it is called a private subnet. For example- Database Instance.

Route table

- A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.
- A table containing the rules for directing the traffic within and outside a subnet is known as Route Table. The Internet Gateway is added to the subnet by using the route table. A VPC can hold multiple route tables.
- As a subnet can be linked to one route table only, hence each subnet is linked to a route table. Whereas multiple subnets can be associated with one route table. Usually, VPCs have their own default route table.
- The VPC usually leaves the original state and a new route table is created so that the network traffic routes are customized to associate with the VPC.

..

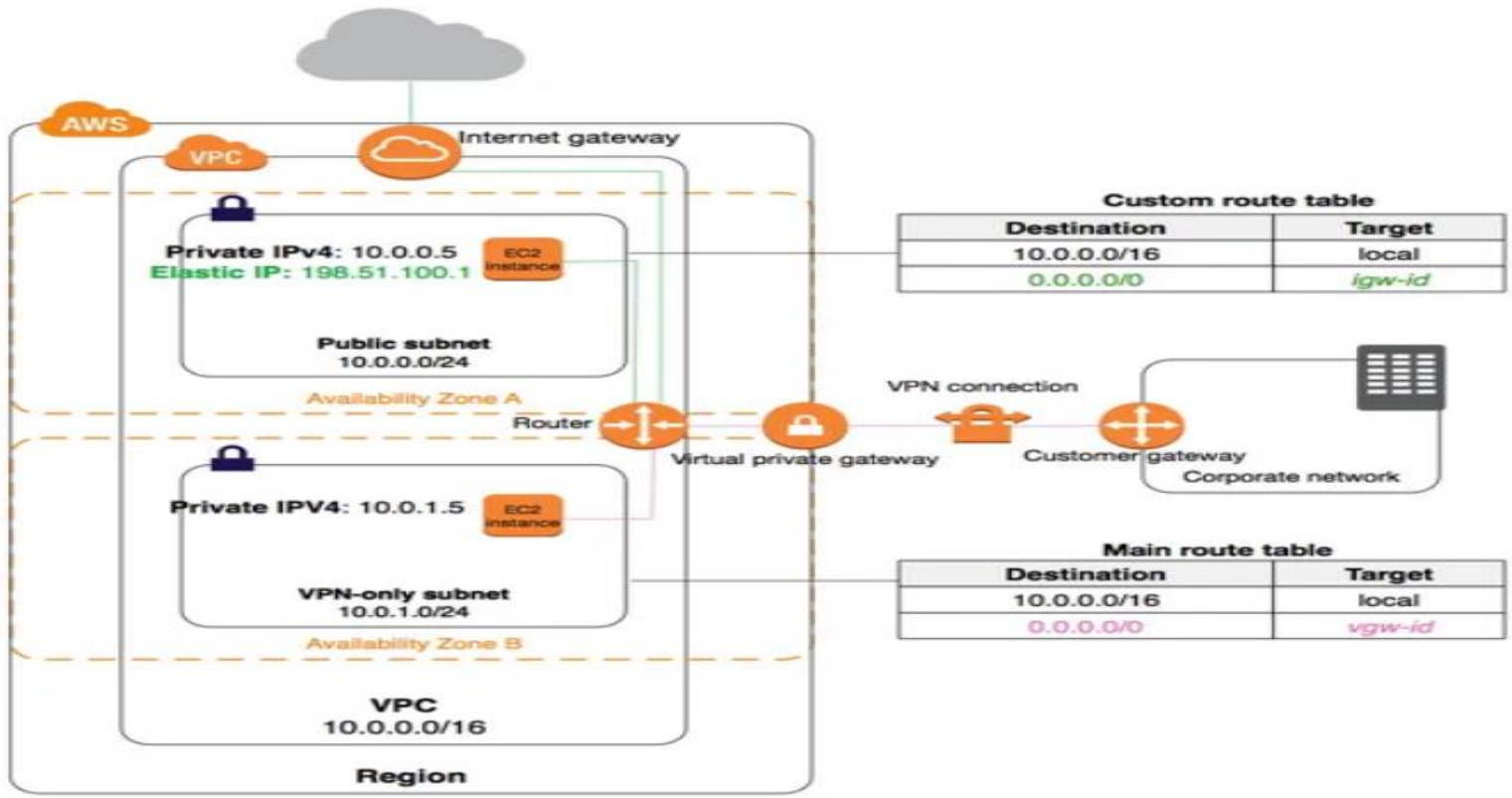


Image Source: AWS

..

- The given block diagram shows two route tables i.e. the main route table and the custom route table.
- The internet gateway is informed by the custom route table for directing internet traffic to the public subnet.
- The main route table does not allow internet traffic. Thus, the default route table still associates with the private subnet. The traffic inside the private subnet remains local

What is Internet Gateway?

- Internet Gateway is one of the components that enable you to communicate between your instance and the internet.
- An internet gateway is a highly available VPC component that is redundant and horizontally scalable
- For the internet route table traffic, a target is provided in the VPC route tables.
- For the instances with public IPv4 addresses, Network Address Translation (NAT) is performing.

..

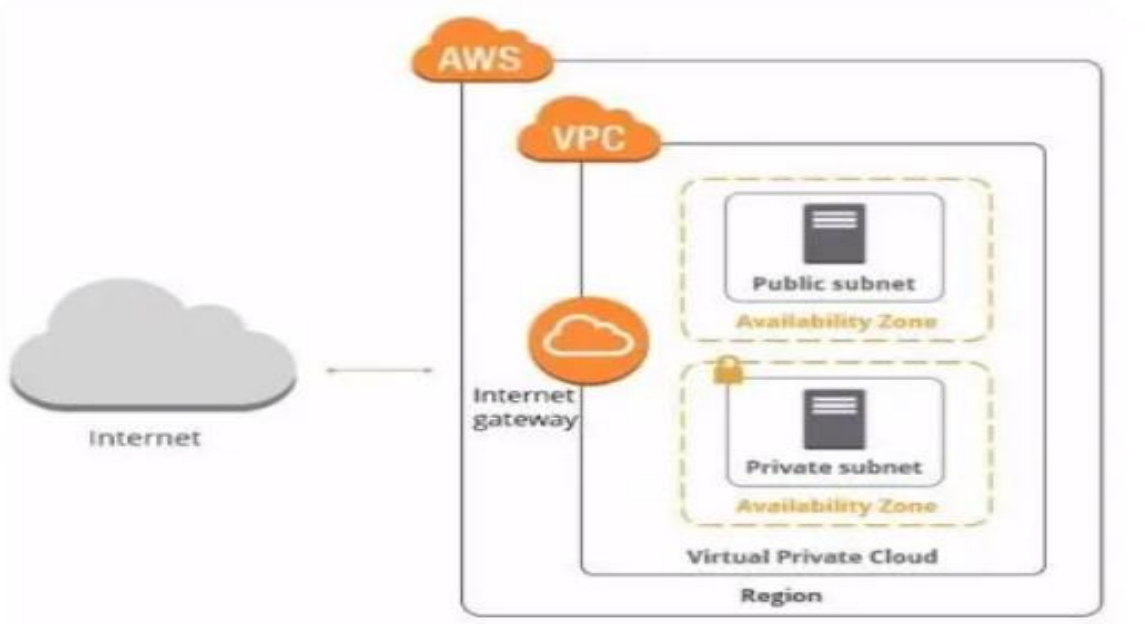


Image Source: AWS

..

- The diagram shows the internet gateway providing a connection. It shows the connections to the internet to your VPC. There are certain rules to follow so that the EC2 instance is internet-connected:
- VPC is to be attached to an Internet Gateway.Make sure whether your instance is having either a public IP address or a private IP address.
- Lead the route table of a subnet to the internet gateway.
- Take note whether the network access control and security group are allowing relevant traffic to flow in and out of instance.