Networking
Amazon VPC

Amazon Virtual Private Cloud (VPC)

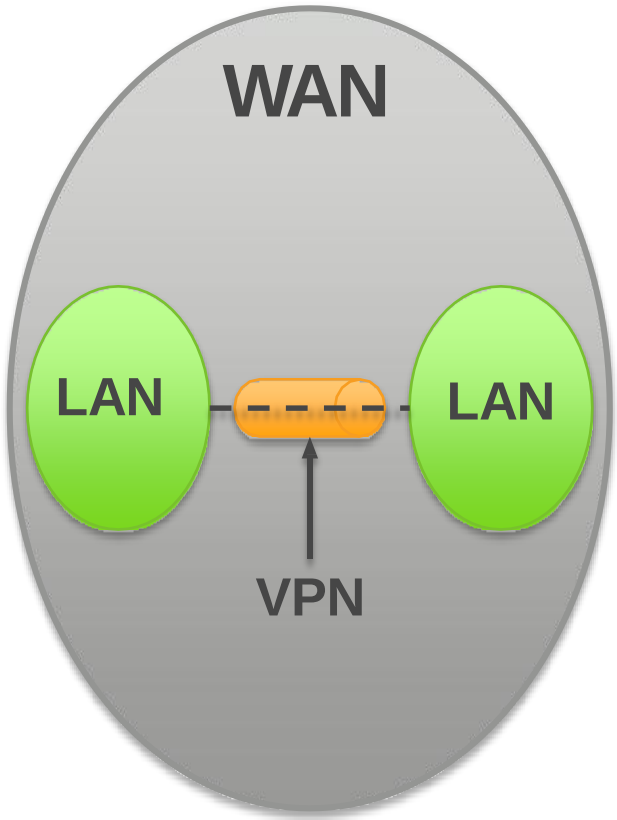
Amazon VPC

- Provision a **private, isolated virtual network** on the AWS cloud.
- Have complete control over your virtual networking environment.

Networking Concepts

What is a Network?

A network is two or more computers linked to share resources, exchange files, or allow electronic communications.



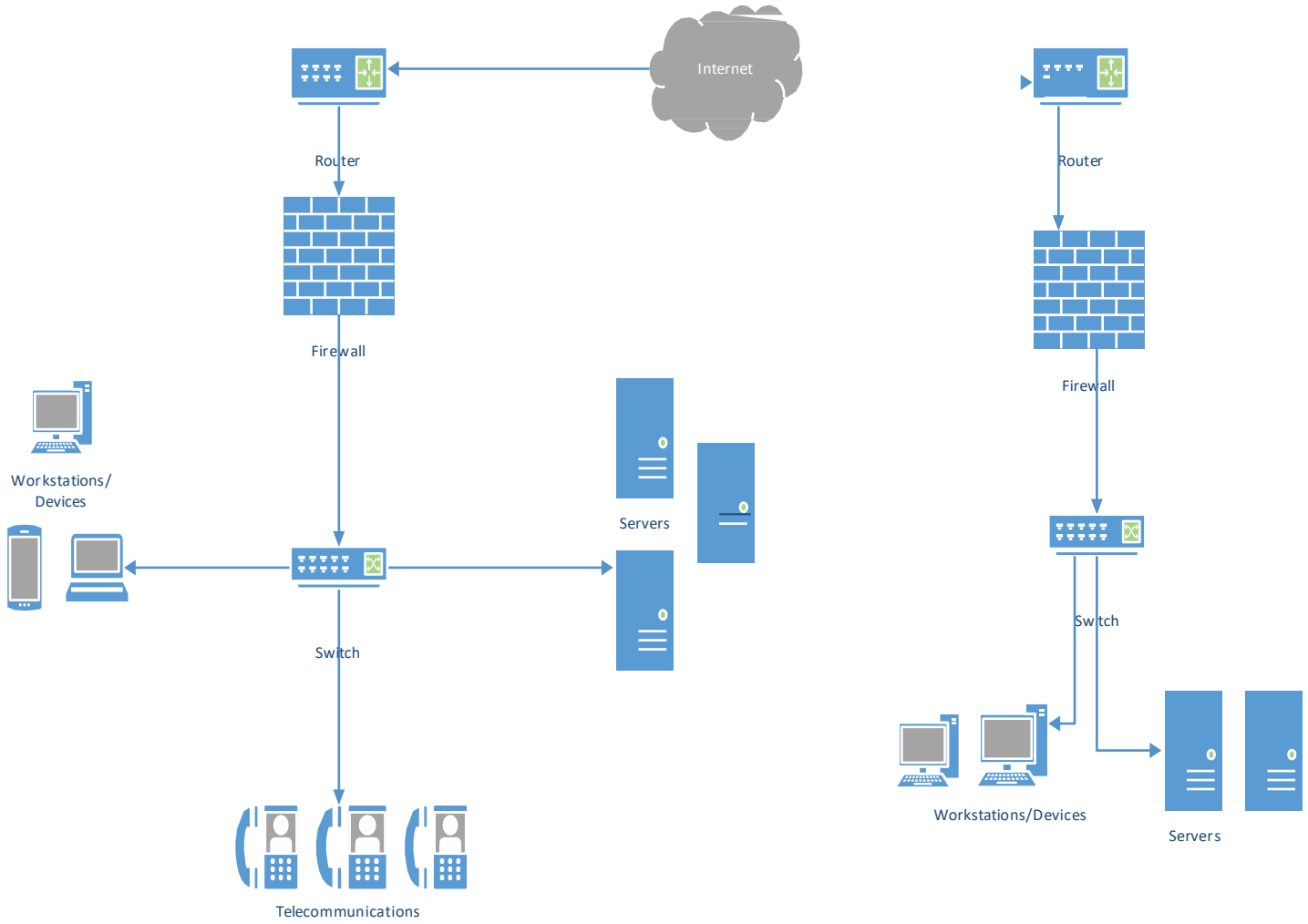
Network Types:

- Local Area Network (LAN)
- Wide Area Network (WAN)
- Virtual Private Network (VPN)

Physical vs. Logical Topology

- A physical topology defines how the systems are physically connected.
- A logical topology defines how the systems communicate across the physical topologies.

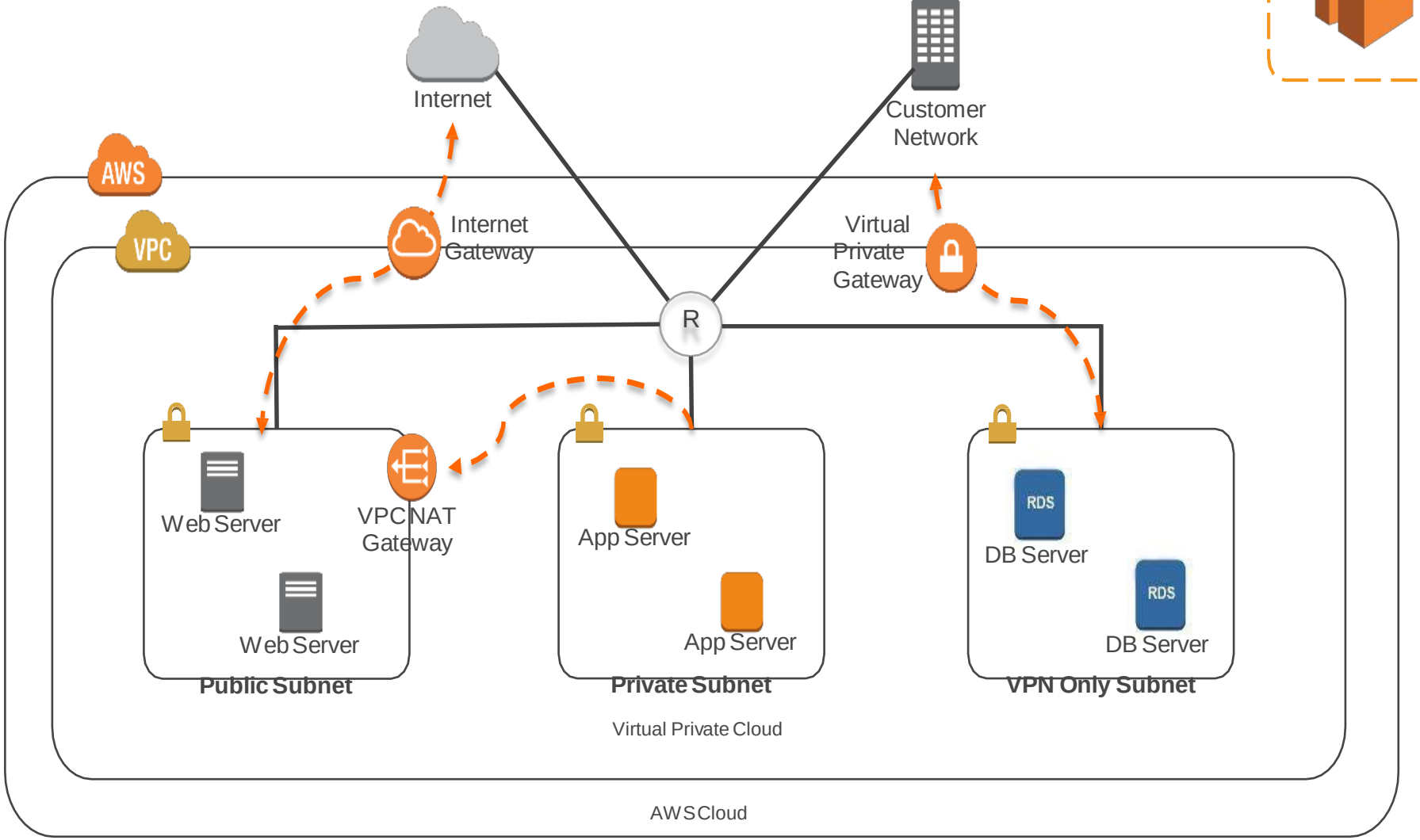
Physical Network Hardware/Devices



VPCs and Subnets

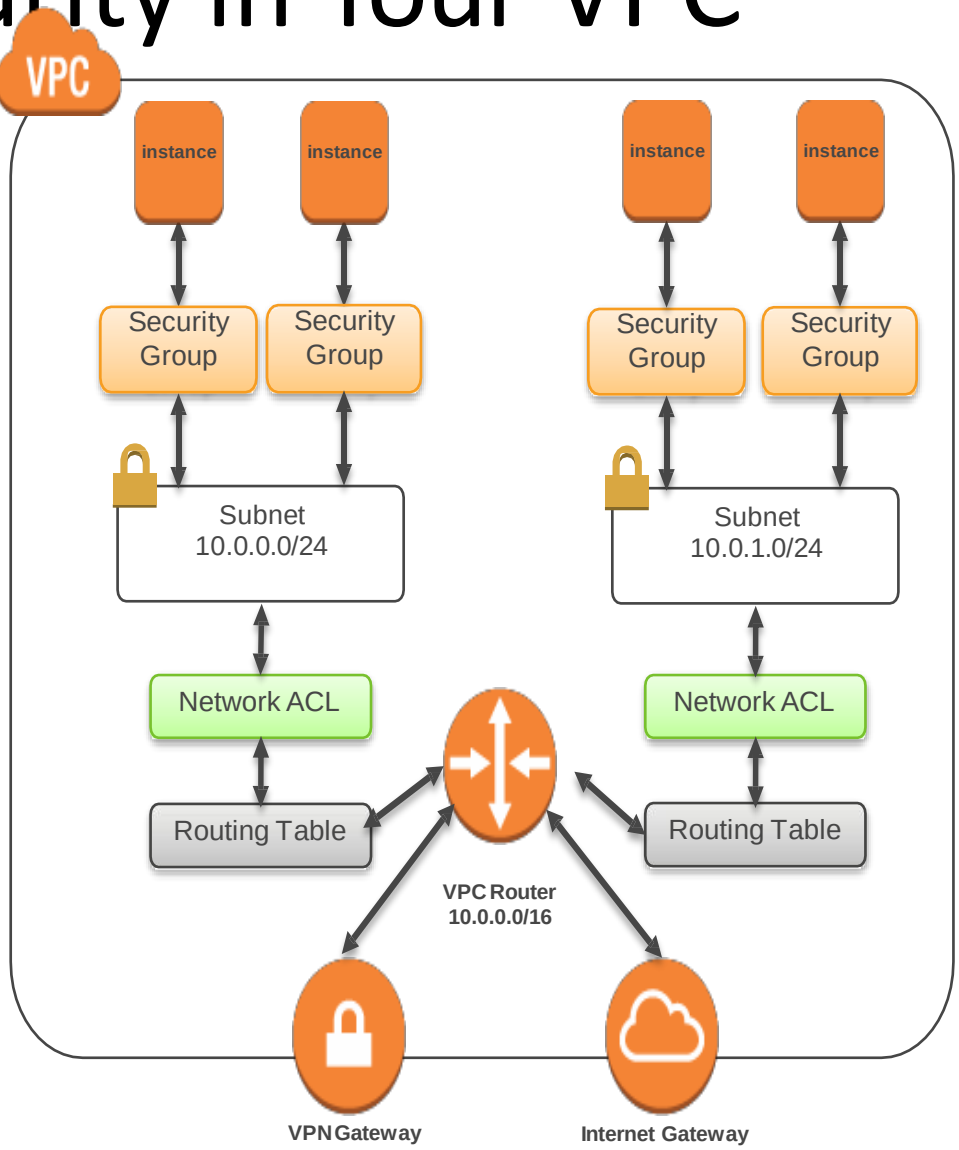
- A **subnet** defines a range of IP addresses in your VPC.
- You can launch AWS resources into a subnet that you select.
- A **private subnet** should be used for resources that won't be accessible over the Internet.
- A **public subnet** should be used for resources that will be accessed over the Internet.
- Each subnet must reside entirely within one Availability Zone and cannot span zones.

Amazon VPC Example



Security in Your VPC

- Security groups
- Network access control lists (ACLs)
- Key Pairs



VPN Connections

VPN Connectivity option	Description
AWS Hardware VPN	You can create an **IPsec** hardware VPN connection between your VPC and your remote network.
AWS Direct Connect	AWS Direct Connect provides a **dedicated private** connection from a remote network to your VPC.
AWS VPN CloudHub	You can create multiple **AWS hardware VPN** connections via your VPC to enable communications between various remote networks.
Software VPN	You can create a VPN connection to your remote network by using an Amazon EC2 instance in your VPC that's running a

amazon web services Virtual Private Cloud (VPC)

- 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.
- VPC allows you to select its IP address range, create subnets, and configure route tables, network gateways, and security settings.
- When you create a VPC, you specify the set of IP addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block. For e.g, 10.0.0.0/16, which allows 2^16 (65536) IP address available within the VPC
- It's possible to specify a range of publicly routable IP addresses; direct access to the Internet is not currently supported from publicly routable CIDR blocks in a VPC

amazon web services Virtual Private Cloud (VPC)

Difference Between Region & Availability Zone

- Amazon EC2 is hosted in multiple locations world-wide.
- These locations are composed of regions and Availability Zones.
- Each *region* is a separate geographic area.
- Each region has multiple, isolated locations known as *Availability Zones*.
- Amazon EC2 provides you the ability to place resources, such as instances, and data in multiple locations. Resources aren't replicated across regions unless you do so specifically.

amazon web services Virtual Private Cloud (VPC)

- CIDR block from private (non-publicly routable) IP address can be assigned to an VPC

10.0.0.0 – 10.255.255.255 (10/8 prefix)

172.16.0.0 – 172.31.255.255 (172.16/12 prefix)

192.168.0.0 – 192.168.255.255 (192.168/16 prefix)

amazon web services Virtual Private Cloud (VPC)

- It’s possible to specify a range of publicly routable IP addresses; direct access to the Internet is not currently supported from publicly routable CIDR blocks in a VPC
- CIDR block once assigned to the VPC cannot be modified
- Each VPC is separate from any other VPC created with the same CIDR block even if it resides within the same AWS account
- VPC allows VPC Peering connections with other VPC within the same or different VPC accounts

amazon web services Virtual Private Cloud (VPC)

VPC Deletion:

- Deletion of the VPC, possible only after terminating all instances within the VPC, deletes all the components with the VPC for e.g. subnets, security groups, network ACLs, route tables, Internet gateways, VPC peering connections, and DHCP options

amazon web services Virtual Private Cloud (VPC)

Private IP Addresses

- Private IP addresses are not reachable over the Internet, and can be used for communication between the instances in your VPC

- All instances are assigned a private IP address, within the IP address range of the subnet, to the default network interface

- Primary IP address is associated with the network interface for its lifetime, even when the instance is stopped and restarted and is released only when the instance is terminated
- Additional Private IP addresses, known as secondary private IP address, can be assigned to the instances and these can be reassigned from one network interface to another

amazon web services Virtual Private Cloud (VPC)

Public IP address (Associated IP Address)

- Public IP addresses are reachable over the Internet, and can be used for communication between your instances and the Internet, or with other AWS services that have public endpoints
- Public IP address assignment to the Instance depends if the Public IP Addressing is enabled for the Subnet.
- Public IP address can also be assigned to the Instance by enabling the Public IP addressing during the creation of the instance, which overrides the subnet's public IP addressing attribute
- Public IP address is assigned from AWS pool of IP addresses and it not associated with the AWS account and hence released when the instance is stopped and restarted

amazon web services Virtual Private Cloud (VPC)

Elastic IP address

- Elastic IP addresses are static, persistent public IP addresses which can be associated and disassociated with the instance, as required

- Elastic IP address is allocated at an VPC and owned by the account unless released
- A Network Interface can be assigned either a Public IP or an Elastic IP. If you assign an instance with Public IP an Elastic IP, the public IP is released
- Elastic IP addresses can be moved from one instance to another and the instance can be within the same VPC or different VPC within the same account
- Elastic IP are charged for non usage i.e. if it is not associated or associated with a stopped instance or an unattached Network Interface

amazon web services Virtual Private Cloud (VPC)

- Elastic Network Interface (ENI)
  - Each Instance is attached with default elastic network interface (Primary Network Interface eth0) and cannot be detached from the instance
  - ENI has the following attributes
    - Primary private IP address
    - One or more secondary private IP addresses
    - One Elastic IP address per private IP address
    - One public IP address, which can be auto-assigned to the netw for eth0 when you launch an instance, but only when you creat interface for eth0 instead of using an existing network interface
    - One or more security groups, A MAC address
    - A source/destination check flag

amazon web services Virtual Private Cloud (VPC)

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,
  - To perform network address translation (NAT) for instances that have been assigned public IP addresses.

amazon web services Virtual Private Cloud (VPC)

Enable Internet Access through Internet GW

- Attaching Internet gateway to the VPC
- Subnet should have Route tables associated with the Route pointing to the Internet gateway
- Instances should have a Public IP or Elastic IP address assigned
- Security groups and NACLs associated with the Instance should allow relevant traffic

amazon web services Virtual Private Cloud (VPC)

VPC Security

Security within a VPC is provided through

- Security groups – Act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level
- Network access control lists (ACLs) – Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level
- Flow logs – Capture information about the IP traffic going to and from network interfaces in your VPC

amazon web services Virtual Private Cloud (VPC)

- Subnets
  - Subnet spans a Single Availability Zone, distinct locations that are engineered to be isolated from failures in other Availability Zones, and cannot span across AZs
  - Subnet can be Public or Private and it depends on where it has the Internet connectivity i.e. is able to route traffic to the Internet through the Internet gateway
  - Instances within the Public Subnet should be assigned a Public IP or Elastic IP address to be able to communicate with the Internet
  - For Subnets not connected to the Internet, but has traffic routed through Virtual Private Gateway only is termed as VPN-only subnet

amazon web services Virtual Private Cloud (VPC)

NAT Overview

- Network Address Translation (NAT) devices, launched in the public subnet, enables instances in a private subnet to connect to the Internet, but prevent the Internet from initiating connections with the instances.
- Instances in private subnets would need internet connection for performing software updates or trying to access external services
- NAT device prevents instances to be directly exposed to the Internet and having to be launched in Public subnet and assignment of the Elastic IP address to all.
- NAT device performs the function of both address translation and port address translation (PAT)

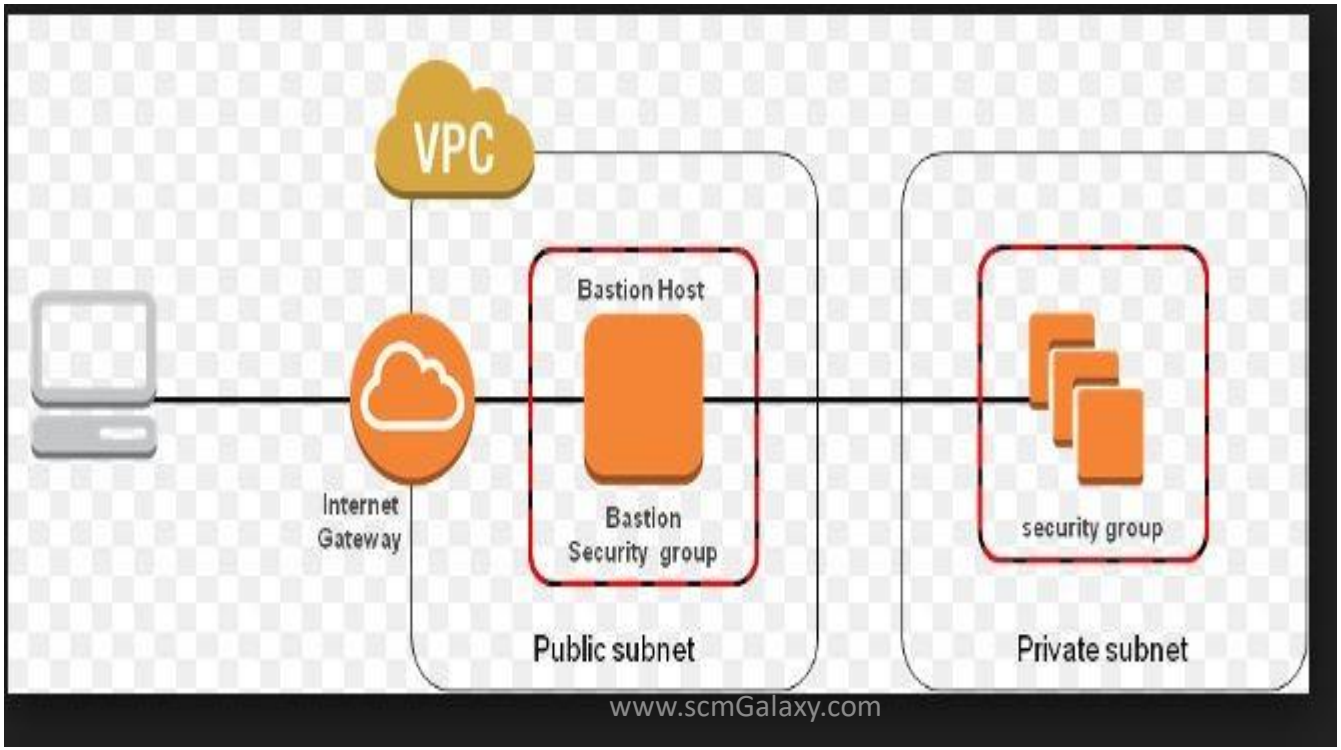
Virtual Private Cloud

Bastion Host Overview

- Bastion means a structure for Fortification to protect things behind it
- In AWS, a Bastion host (also referred to as a Jump server) can be used to securely access instances in the private subnets.
- Bastion host launched in the Public subnets would act as a primary access point from the Internet and acts as a proxy to other instances.

amazon web services Virtual Private Cloud (VPC)

Bastion Host



amazon web services Virtual Private Cloud (VPC)

VPC Peering Overview

- A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IP addresses.
- Instances in either VPC can communicate with each other as if they are within the same network
- VPC peering connection can be established between your own VPCs, or with a VPC in another AWS account within a single region.
- AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

amazon web services Virtual Private Cloud (VPC)

VPC Peering Rules & Limitations

- VPC peering connection cannot be created between VPCs that have matching or overlapping CIDR blocks.
- VPC peering connection cannot be created between VPCs in different regions.
- VPC peering connection are limited on the number active and pending VPC peering connections that you can have per VPC.
- VPC peering does not support transitive peering relationships
- VPC peering does not support Edge to Edge Routing Through a Gateway or Private Connection

Virtual Private Cloud

Hands-On Lab:

- Create VPC with Public Subnet
- Create Internet Gateway
- Attached IGW
- Create Route on Route table
- Create Subnet
- Add IGW Route on route Table
- Test Internet Connectivity *(By creating EC2 Instance)*