Name	Mohammad Faraz M khan
Enrolment Number	A70405219039
Experiment Number	8
Batch	1

AIM OF THE EXPERIMENT: Prepare Case Study report on Cloud Security.

Cloud Security Introduction

Cloud security is a collection of procedures and technology designed to address external and internal threats to business security. Organizations need cloud security as they move toward their digital transformation strategy and incorporate cloud-based tools and services as part of their infrastructure.

Cloud Security, or Cloud Computing Security, is a sub-domain of computer /network/ information security and represents a wide set of technologies, policies, apps, and controls used to protect data, virtualized IP, apps, services, and the associated cloud computing infrastructure.

Automated Security
Centralization of Security
Cost Optimization
Cloud Security
Reliability
Ease of Management
Ease of Access

The advent of cloud computing and its growing popularity has enabled and given rise to cloud computing security and turned it into a stand-alone category of the modern cloud landscape. This trend also gave birth to cloud security platforms and providers in a separate branch known as Security-as-a-Service or SaaS.

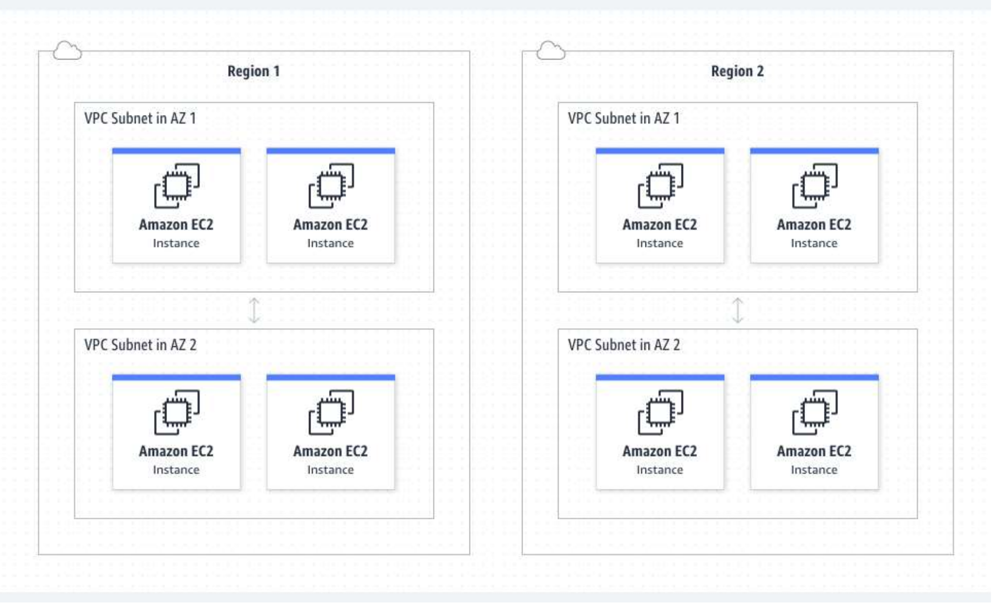
Much like it is the case with the Software-as-a-Service (or SaaS) providers, the SaaS typically works as a monthly subscription model capable of reducing the overall cost of both a company’s workflow and costs.

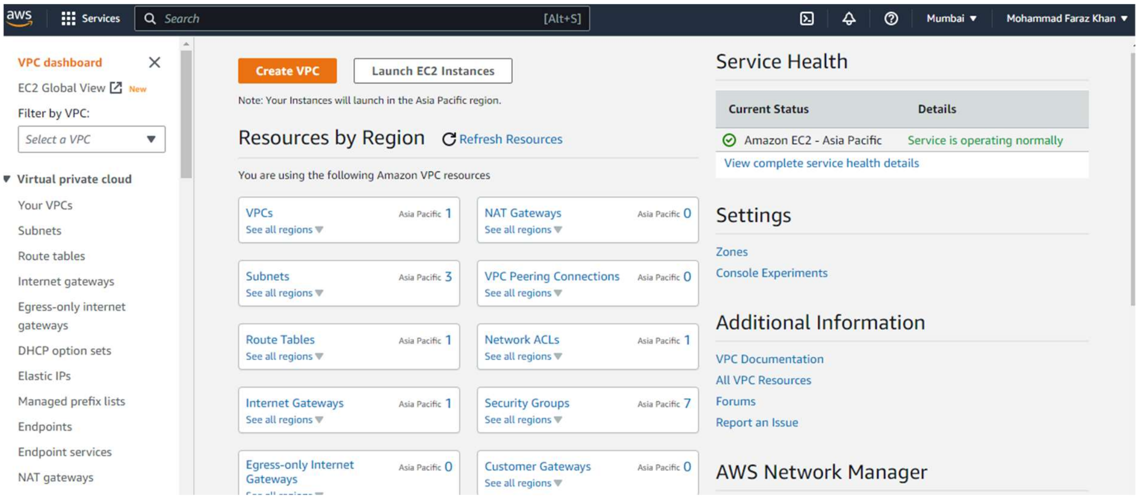
Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) gives you full control over your virtual networking environment, including resource placement, connectivity, and security. Get started by setting up your VPC in the AWS service console.

Amazon Virtual Private Cloud (VPC) is a service that lets you launch AWS resources in a logically isolated 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 for most resources in your VPC, helping to ensure secure and easy access to resources and applications.

As one of AWS's foundational services, Amazon VPC makes it easy to customize your VPC's network configuration. You can create a public-facing subnet for your web servers that have access to the internet. It also lets you place your backend systems, such as databases or application servers, in a private-facing subnet with no internet access. Amazon VPC lets you to use multiple layers of security, including security groups and network access control lists, to help control access to Amazon Elastic Compute Cloud (Amazon EC2) instances in each subnet.





Note: Your Instances will launch in the Asia Pacific region.

Resources by Region

You are using the following Amazon VPC resources

Resource	Region	Count
VPCs	Asia Pacific	1
NAT Gateways	Asia Pacific	0
Subnets	Asia Pacific	3
VPC Peering Connections	Asia Pacific	0
Route Tables	Asia Pacific	1
Network ACLs	Asia Pacific	1
Internet Gateways	Asia Pacific	1
Security Groups	Asia Pacific	7
Egress-only Internet Gateways	Asia Pacific	0
Customer Gateways	Asia Pacific	0

Service Health

Current Status	Details
✓ Amazon EC2 - Asia Pacific	Service is operating normally

View complete service health details

Settings

Additional Information

AWS Network Manager

Subnet

A subnet, or subnetwork, is a segmented piece of a larger network. More specifically, subnets are a logical partition of an IP network into multiple, smaller network segments. The Internet Protocol (IP) is the method for sending data from one computer to another over the internet. Each computer, or host, on the internet has at least one IP address as a unique identifier.

Organizations will use a subnet to subdivide large networks into smaller, more efficient subnetworks. One goal of a subnet is to split a large network into a grouping of smaller, interconnected networks to help minimize traffic. This way, traffic doesn't have to flow through unnecessary routs, increasing network speeds.

Subnetting, the segmentation of a network address space, improves address allocation efficiency. It is described in the formal document, Request for Comments 950, and is tightly linked to IP addresses, subnet masks and Classless Inter-Domain Routing (CIDR) notation.

Subnets are classified as public, private, or VPN-only depending on how VPC is set up:

- Public subnet: Through an internet gateway or an egress-only internet gateway, traffic from the subnet is forwarded to the public internet. See Connect to the internet using an internet gateway for further details.

- Private subnet: Traffic from the subnet cannot pass through an internet gateway or an egress-only internet gateway to access the public internet. A NAT device is necessary for internet access to other users.

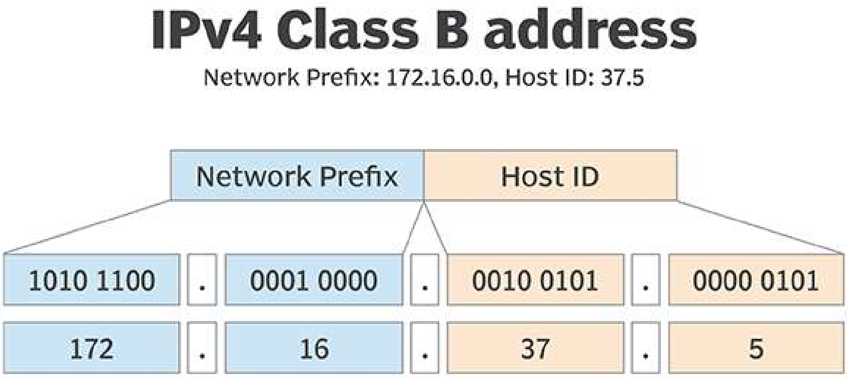
- VPN-only subnet: Via a virtual private gateway, the subnet traffic is forwarded to a Site-to-Site VPN connection. Through an internet gateway, subnet traffic cannot access the general internet. Consult the AWS Site-to-Site VPN User Guide for further details.

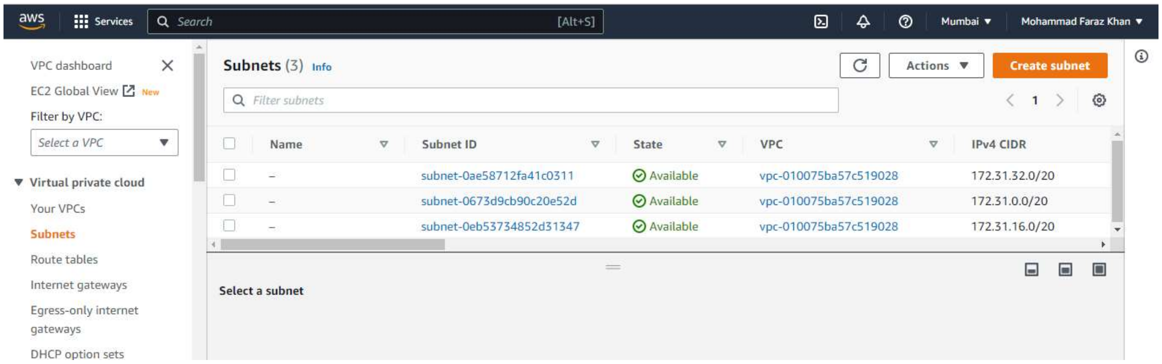
Each subnet allows its connected devices to communicate with each other, while routers are used to communicate between subnets. The size of a subnet depends on the connectivity requirements and the network technology employed. A point-to-point subnet allows two devices to connect, while a data center subnet might be designed to connect many more devices.

Each organization is responsible for determining the number and size of the subnets it creates, within the limits of the address space available for its use.

Additionally, the details of subnet segmentation within an organization remain local to that organization.

An IP address is divided into two fields: a Network Prefix (also called the Network ID) and a Host ID. What separates the Network Prefix and the Host ID depends on whether the address is a Class A, B or C address. Figure 1 shows an IPv4 Class B address, 172.16.37.5. Its Network Prefix is 172.16.0.0, and the Host ID is 37.5.





Subnets (3)

□	Name	Subnet ID	State	VPC	IPv4 CIDR
□	–	subnet-0ae58712fa41c0311	✓ Available	vpc-010075ba57c519028	172.31.32.0/20
□	–	subnet-0673d9cb90c20e52d	✓ Available	vpc-010075ba57c519028	172.31.0.0/20
□	–	subnet-0eb53734852d31347	✓ Available	vpc-010075ba57c519028	172.31.16.0/20

Select a subnet

Route Table

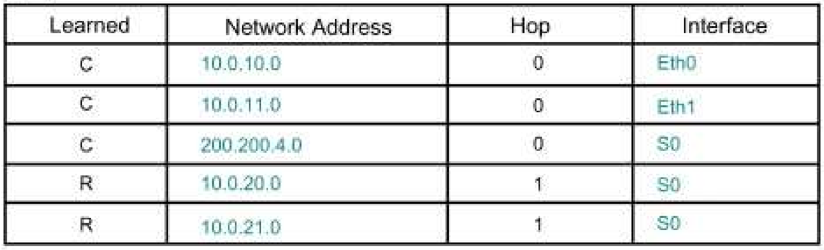
In computer networking, a routing table, or routing information base (RIB), is a data table stored in a router or a network host that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. The routing table contains information about the topology of the network immediately around it.

A routing table is a set of rules, often viewed in table format, that's used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. This table is usually stored inside the Random Access Memory of forwarding devices, such as routers and network switches.

In computer networking, each routing table is unique and acts as an address map for networks. It stores the source and destination IP addresses of the routing devices in the form of prefixes along with the default gateway addresses and corresponding routing information.

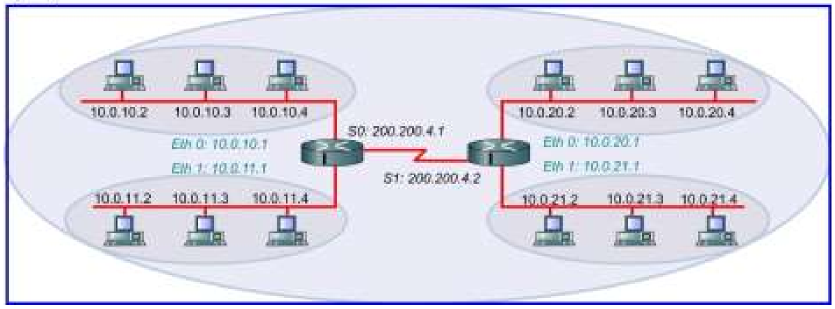
Routing tables are typically updated dynamically through network routing protocols. But sometimes network administrators might add static entries manually.

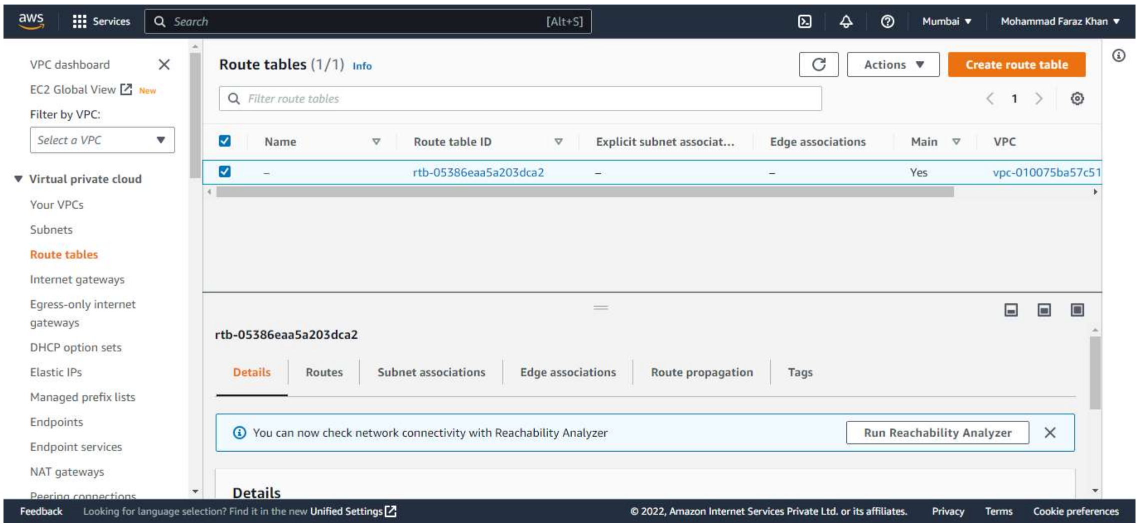
(A)



Learned	Network Address	Hop	Interface
C	10.0.10.0	0	Eth0
C	10.0.11.0	0	Eth1
C	200.200.4.0	0	S0
R	10.0.20.0	1	S0
R	10.0.21.0	1	S0

(B)





Route tables (1/1) Info

☑	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
☑	–	rtb-05386eaa5a203dca2	–	–	Yes	vpc-010075ba57c51

rtb-05386eaa5a203dca2

You can now check network connectivity with Reachability Analyzer

Details

IGP

An interior gateway protocol (IGP) or Interior routing protocol is a type of routing protocol used for exchanging routing table information between gateways (commonly routers) within an autonomous system (for example, a system of corporate local area networks). This routing information can then be used to route network-layer protocols like IP.

Interior gateway protocols can be divided into two categories: distance-vector routing protocols and link-state routing protocols. Specific examples of IGPs include Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Intermediate System to Intermediate System (IS-IS) and Enhanced Interior Gateway Routing Protocol (EIGRP).

By contrast, exterior gateway protocols are used to exchange routing information between autonomous systems and rely on IGPs to resolve routes within an autonomous system.

An interior gateway protocol (IGP) is a dynamic route update protocol used between routers that run on TCP/IP hosts within a single autonomous system. The routers use this protocol to exchange information about IP routes.

NAT Gateway

A NAT gateway is a Network Address Translation (NAT) service. You can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances.

Connectivity types:

- Public – (Default) Instances in private subnets can connect to the internet through a public NAT gateway, but cannot receive unsolicited inbound connections from the internet. You create a public NAT gateway in a public subnet and must associate an elastic IP address with the NAT gateway at creation. You route traffic from the NAT gateway to the internet gateway for the VPC. Alternatively, you can use a public NAT gateway to connect to other VPCs or your on-premises network. In this case, you route traffic from the NAT gateway through a transit gateway or a virtual private gateway.
- Private – Instances in private subnets can connect to other VPCs or your on-premises network through a private NAT gateway. You can route traffic from the NAT gateway through a transit gateway or a virtual private gateway. You cannot associate an elastic IP address with a private NAT gateway. You can attach an internet gateway to a VPC with a private NAT gateway, but if you route traffic from the private NAT gateway to the internet gateway, the internet gateway drops the traffic.

Security Groups

A security group controls the traffic that is allowed to reach and leave the resources that it is associated with. For example, after you associate a security group with an EC2 instance, it controls the inbound and outbound traffic for the instance.

When you create a VPC, it comes with a default security group. You can create additional security groups for each VPC. You can associate a security group only with resources in the VPC for which it is created.

For each security group, you add rules that control the traffic based on protocols and port numbers. There are separate sets of rules for inbound traffic and outbound traffic.

Characteristics of security groups are as follows:

When you create a security group, you must provide it with a name and a description. The following rules apply:

A security group name must be unique within the VPC.

Names and descriptions can be up to 255 characters in length.

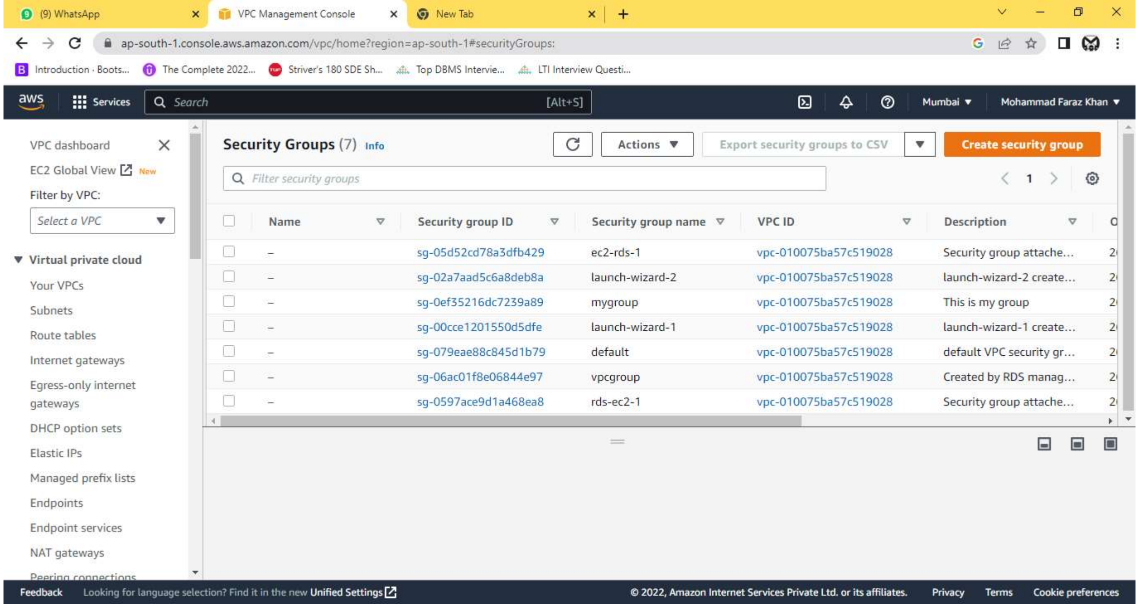
Names and descriptions are limited to the following characters: a-z, A-Z, 0-9, spaces, and._-:/()#,@[]+=&;{}!$*.

When the name contains trailing spaces, we trim the space at the end of the name. For example, if you enter "Test Security Group " for the name, we store it as "Test Security Group".

A security group name cannot start with sg-.

Security groups are stateful. For example, if you send a request from an instance, the response traffic for that request is allowed to reach the instance regardless of the inbound security group rules. Responses to allowed inbound traffic are allowed to leave the instance, regardless of the outbound rules.

There are quotas on the number of security groups that you can create per VPC, the number of rules that you can add to each security group, and the number of security groups that you can associate with a network interface. For more information, see Amazon VPC quotas.



Security Groups (7) Info

□	Name	Security group ID	Security group name	VPC ID	Description	O
□	–	sg-05d52cd78a3dfb429	ec2-rds-1	vpc-010075ba57c519028	Security group attache...	2
□	–	sg-02a7aad5c6a8deb8a	launch-wizard-2	vpc-010075ba57c519028	launch-wizard-2 create...	2
□	–	sg-0ef35216dc7239a89	mygroup	vpc-010075ba57c519028	This is my group	2
□	–	sg-00cce1201550d5dfe	launch-wizard-1	vpc-010075ba57c519028	launch-wizard-1 create...	2
□	–	sg-079eae88c845d1b79	default	vpc-010075ba57c519028	default VPC security gr...	2
□	–	sg-06ac01f8e06844e97	vpcgroup	vpc-010075ba57c519028	Created by RDS manag...	2
□	–	sg-0597ace9d1a468ea8	rds-ec2-1	vpc-010075ba57c519028	Security group attache...	2