Parul® University

AMAZON WEB SERVICES

Parul®
University

DIGITAL LEARNING CONTENT

CHAPTER-2

AWS Networking Services Overview

- **Networking Basics**
- **Virtual Private Cloud (VPC)**
- **Subnets**
- **Route Tables**
- **Security Groups**
- **VPC Security**
- **DNS: AWS Route 53**
- **CloudFront**
- **Build Your VPC in AWS and Launch a Web Server**

Introduction **Networking Basics**

- Networking is the foundation of communication between resources in cloud and on-premises environments. It enables data exchange between devices, servers, and services.

AWS Virtual Private Cloud

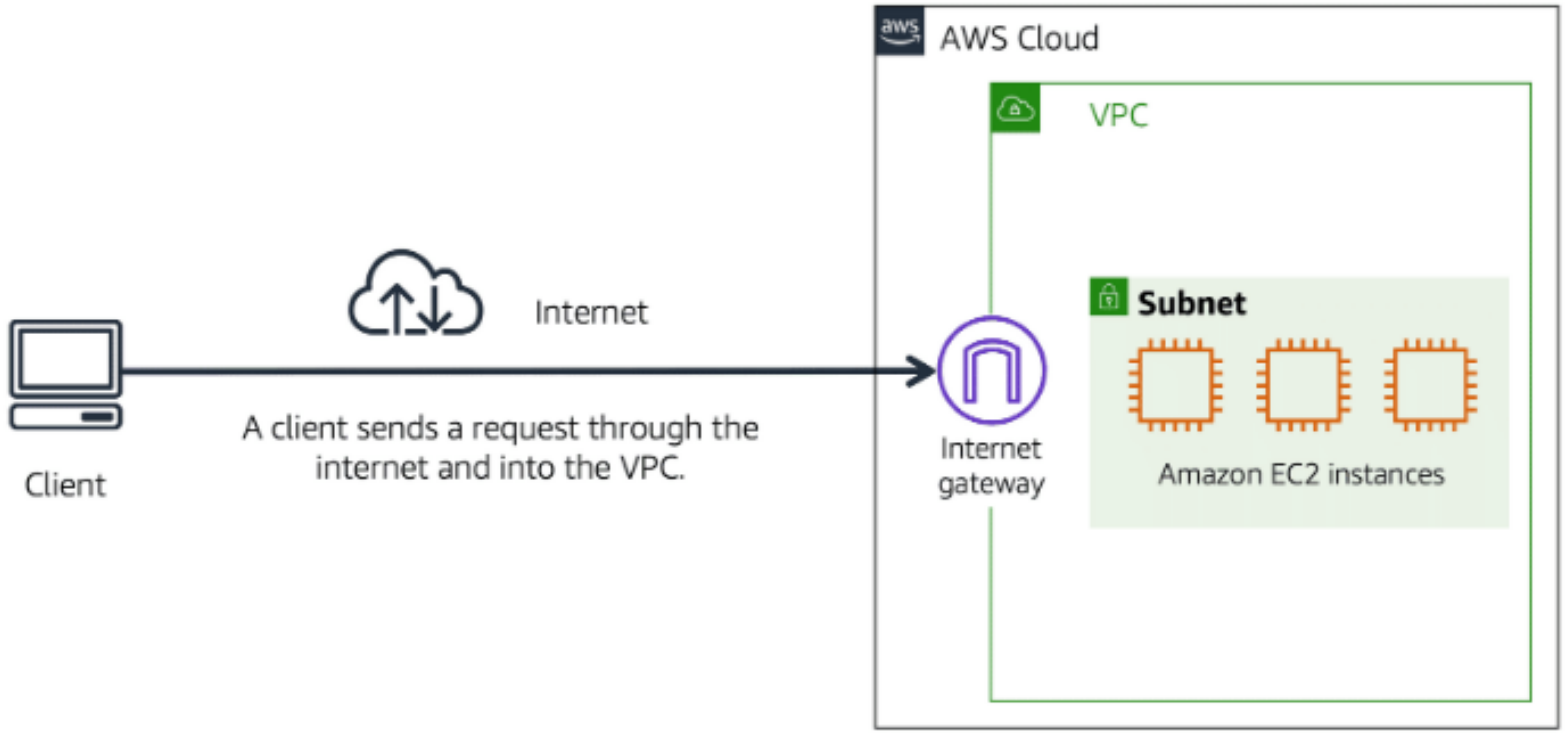
- AWS Virtual Private Cloud is also called AWS VPC.
- VPC is a service that lets you isolate your AWS resources in an isolated network.
- The boundaries created around the resources let AWS restrict the network traffic.
- In addition, it allows you to include the sections of the AWS Cloud that you want in the isolated network.
- Resources can be organized in subnets.
- A subnet is a section in the VPC that can contain specific resources.

Parul® University

DIGITAL LEARNING CONTENT

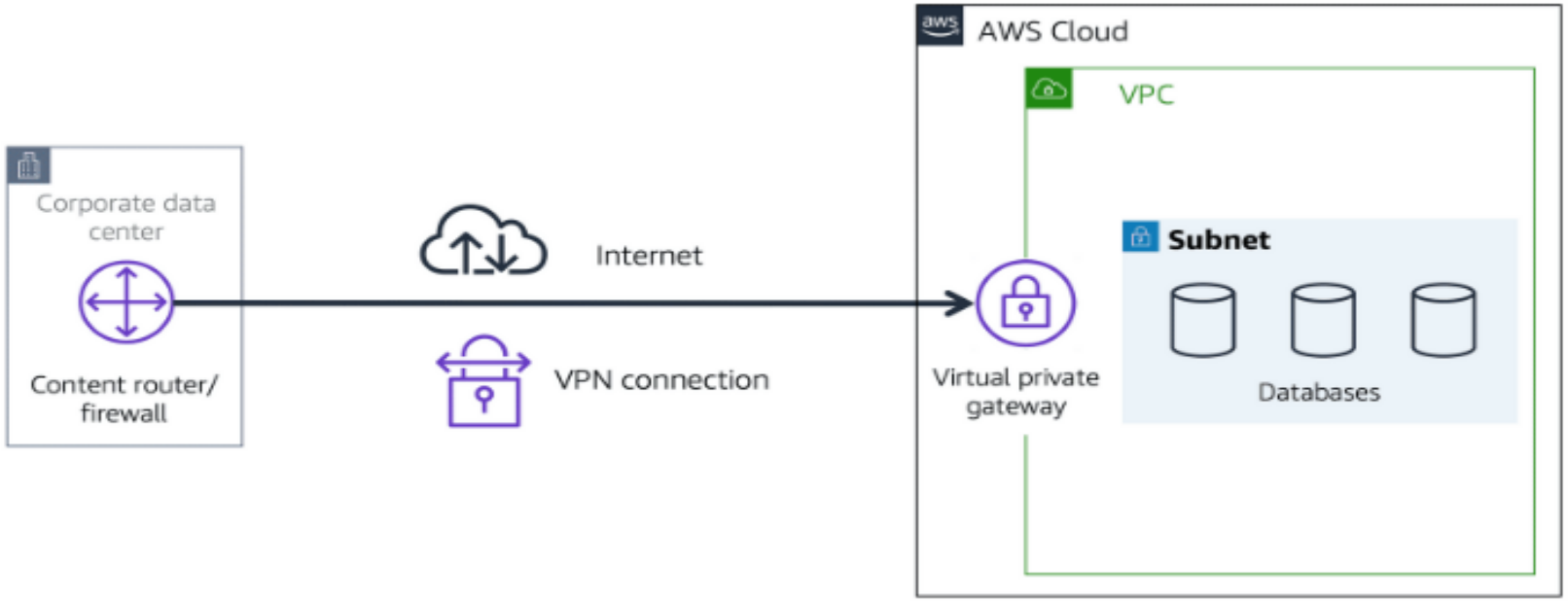
Internet Gateway?

- Public traffic can be allowed to your VPC.
- The traffic is allowed by an Internet Gateway.



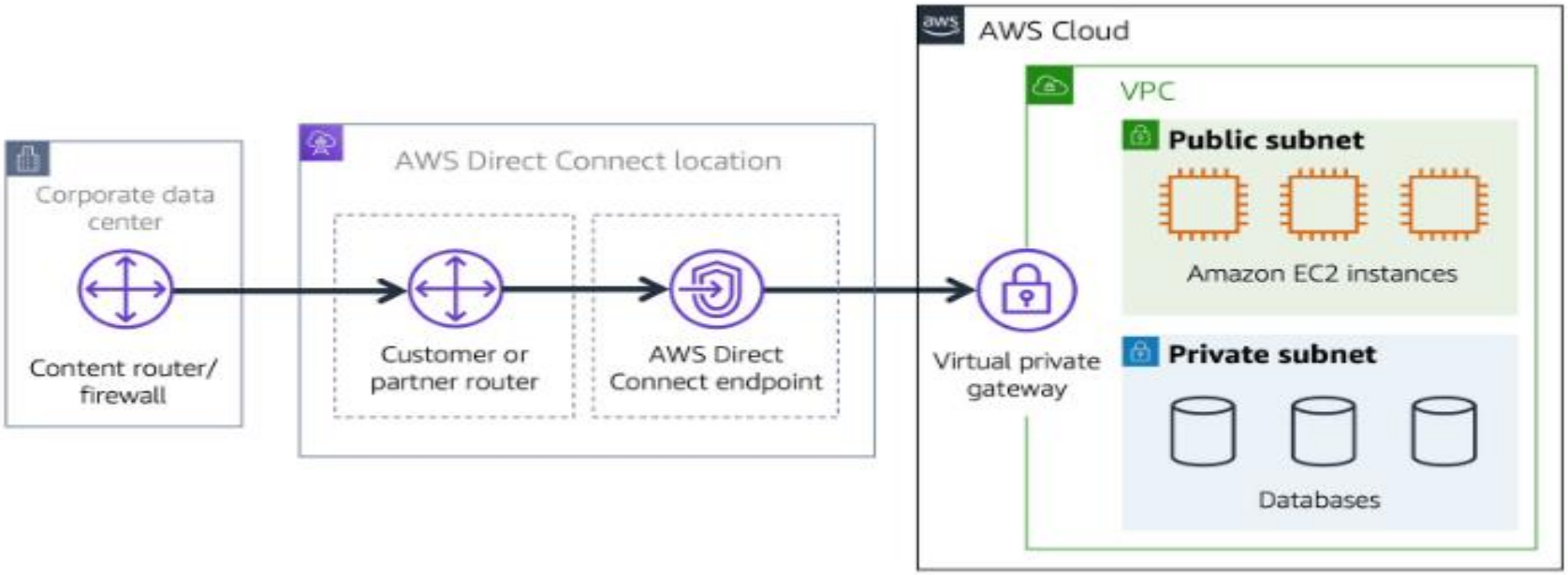
Virtual Private Gateway

- A Virtual Private Gateway is used to access private resources in the VPC.
- It has extra layers of protection.
- The Virtual Private Gateway encrypts the internet traffic, keeping it protected.
- It is a component that allows the encrypted traffic to enter the VPC.



AWS Direct Connect

- AWS Direct Connect lets you make a dedicated private connection between the Data Center and a VPC.
- A dedicated connection is to have the link for yourself.
- The link is not shared with others.
- Only you and your data can travel through the connection.



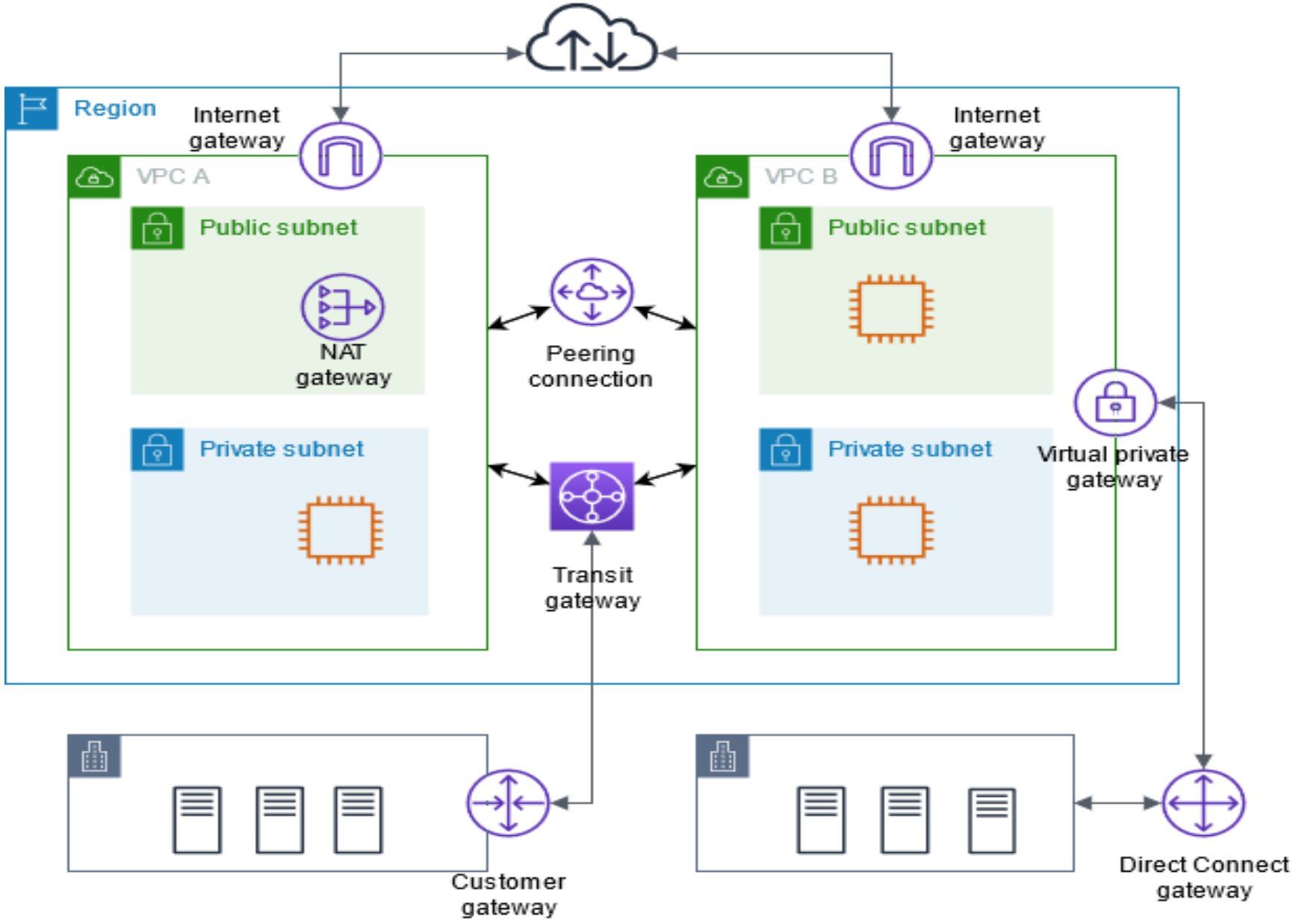
Parul®
University

DIGITAL LEARNING CONTENT

Virtual Private Cloud (VPC)

- A Virtual Private Cloud (VPC) is a logically isolated network within a public cloud like Amazon Web Services (AWS) or Google Cloud.
- It allows you to create a private network, providing security and control over your resources within the cloud environment. VPCs are like creating your own network in the cloud, allowing you to manage IP address ranges, subnets, and other networking aspects.

Virtual Private Cloud (VPC)



Virtual Private Cloud (VPC)

Key Concepts of VPC:

Isolation:
VPCs isolate resources from other users and workloads in the public cloud, enhancing security.

Control:
You have control over your virtual network, including configuring IP address ranges, subnets, route tables, and security groups.

Customization:
You can tailor your VPC to meet specific networking needs, including setting up subnets for different applications or services.

Scalability:
VPCs can be scaled up or down as needed, allowing you to adapt to changing business requirements.

Connectivity:
VPCs can connect to on-premises networks via VPN tunnels or Cloud Interconnect, enabling hybrid cloud deployments.

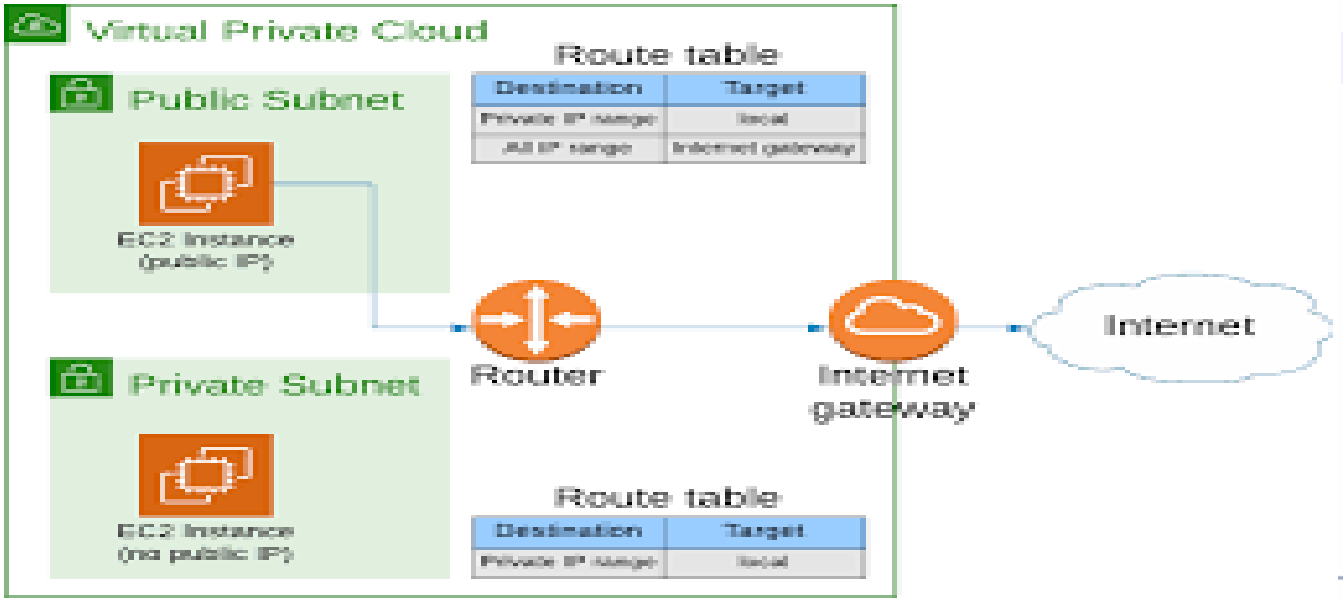
Virtual Private Cloud (VPC)

How VPCs Work (Example: AWS):

1. **VPC Creation:**
You create a VPC and specify its IP address range.
2. **Subnet Creation:**
Within the VPC, you create subnets, which are ranges of IP addresses within the VPC.
3. **Resource Launch:**
You launch resources like EC2 instances (virtual machines) into your subnets.
4. **Networking Configuration:**
You configure route tables, security groups, and other networking settings to control traffic flow within your VPC.
5. **Internet Gateway (Optional):**
If you want resources within your VPC to connect to the internet, you add an Internet Gateway.

AWS Subnets :

- In AWS, subnets are sections of a Virtual Private Cloud (VPC) that you can use to group resources based on security or operational needs.
- They are essentially IP address ranges within your VPC that you can assign to your AWS resources, like EC2 instances.



Key aspects of subnets in AWS:

IP Address Ranges:
Subnets are defined by a Classless Inter-Domain Routing (CIDR) block, which determines the range of IP addresses available within that subnet.

Public vs. Private:
Subnets can be public or private, depending on their ability to access the internet. Public subnets have direct routes to an internet gateway, while private subnets do not.

Route Tables:
Route tables are used to determine how network traffic flows into and out of subnets.

Security Groups:
Security groups act as virtual firewalls, controlling traffic flow in and out of subnets and individual resources.

Default Subnets:
When you create a VPC, AWS automatically creates a default subnet in each AZ.

Multiple Subnets:
You can create multiple subnets within a VPC, each with its own CIDR block.

Types of Subnets:

Public Subnets:
Allow resources to directly access the public internet through an internet gateway.

Private Subnets:
Do not have direct access to the internet and typically require a Network Address Translation (NAT) device or a VPN to communicate with the internet.

Isolated Subnets:
Have no external connectivity and can only be reached within the VPC.

VPN-only Subnets:
Have a route to a Site-to-Site VPN connection, but no direct access to the internet.

Why use Subnets?

Security:
Subnets allow you to isolate resources and control access based on security needs.

Organization:
Subnets help you organize your resources in a logical way, making it easier to manage your VPC.

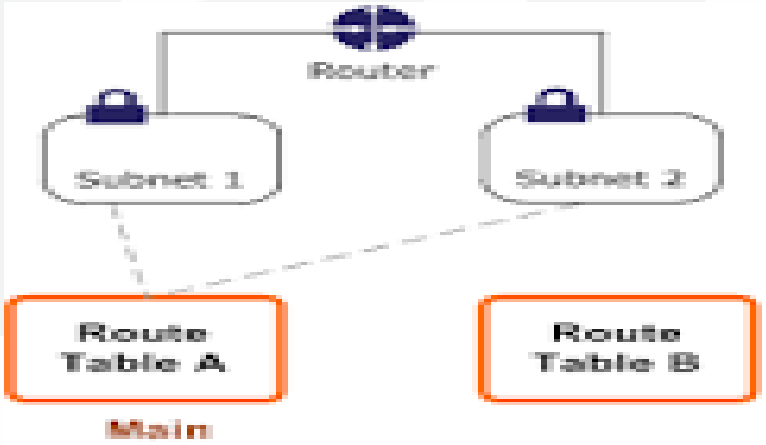
Scalability:
Subnets can be used to create more scalable networks by adding more subnets as needed.

High Availability:
By placing resources in different subnets across multiple AZs, you can achieve high availability and fault tolerance.

Network Control:
Subnets give you granular control over network traffic flow within your VPC.

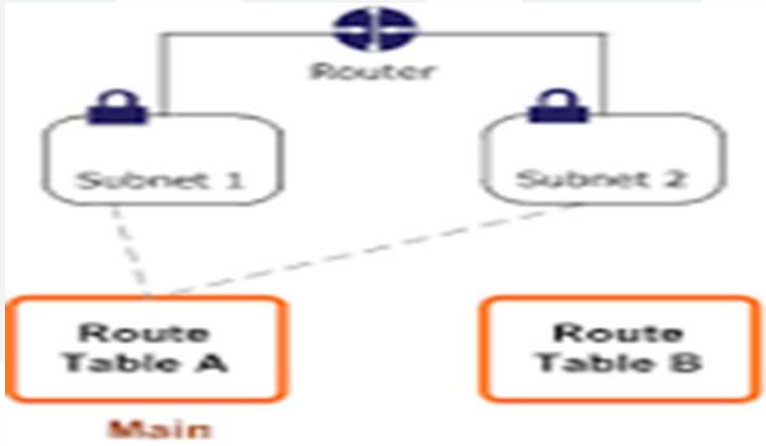
AWS Route Tables

- In AWS, route tables are essential for determining how network traffic flows within and outside your VPC.
- They act as a set of rules that direct traffic based on destination IP addresses (CIDR blocks). Each route table contains rules, called routes, that specify where traffic should go.



How Route Tables Work:

- A network packet arrives at a subnet within your VPC.
- The VPC router looks up the destination IP address of the packet in the route table associated with that subnet.
- The router finds the route that best matches the destination IP address.
- The router sends the packet to the target specified in the route.



Key Concepts:

Route Table: A table containing rules (routes) that dictate where network traffic is sent.
Routes: Individual rules within a route table that specify the destination and target for traffic.
Destination: The IP address range (CIDR block) where traffic is destined to go.
Target: The next hop for the traffic, such as a gateway, network interface, or connection.
VPC: A logically isolated network where resources can be launched.
Subnet: A range of IP addresses within a VPC.
Main Route Table: The default route table for a VPC, automatically created.
Custom Route Table: A route table created manually by the user.
Route Propagation: Automatically adding routes for virtual private gateways to subnet route tables.

Parul®
University

DIGITAL LEARNING CONTENT

AWS Security Groups

In AWS, a Security Group is a collection of rules that control inbound and outbound traffic for your instances. When you launch an instance, you can specify one or more Security Groups.

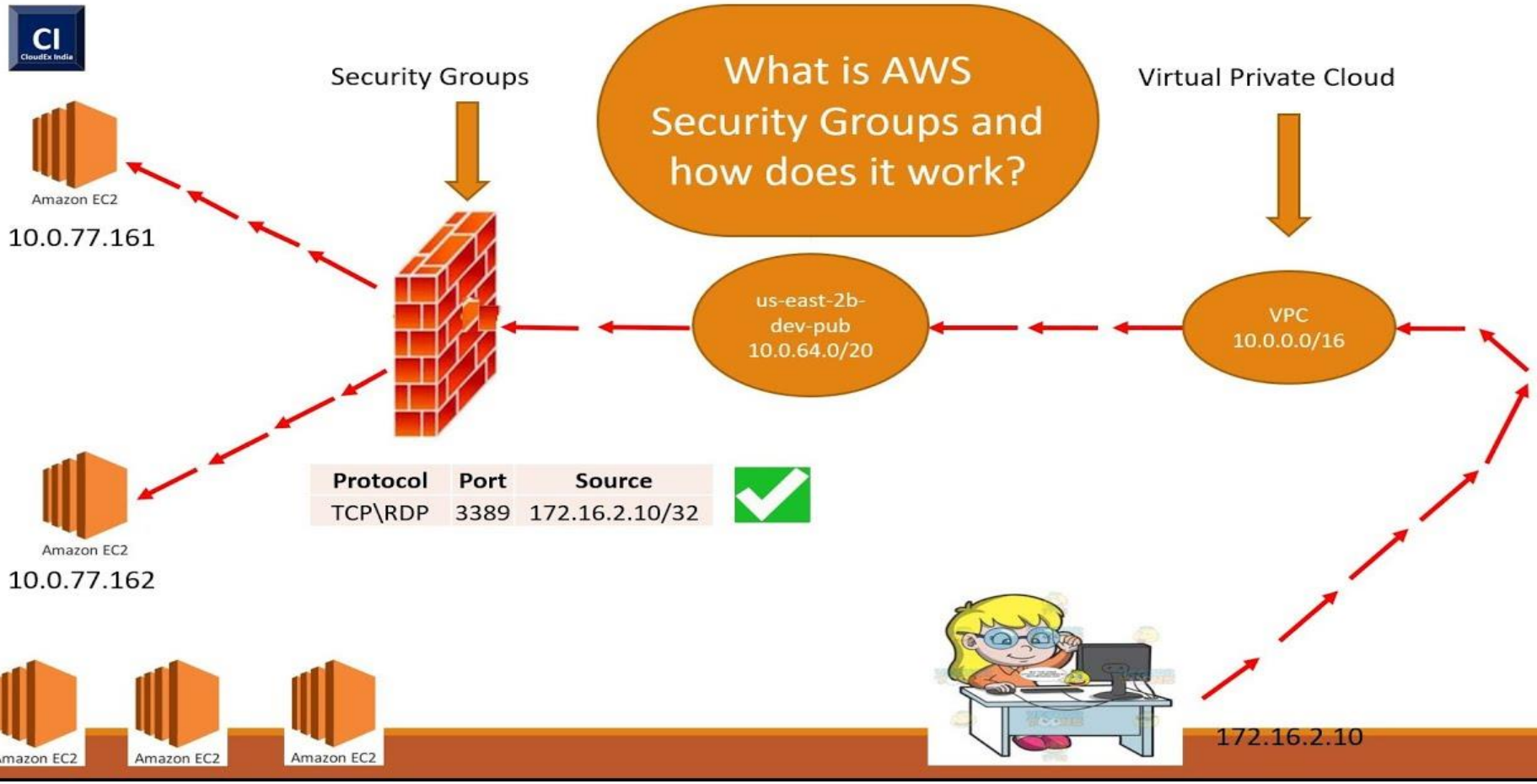
NOTE: We can't talk about Security Groups without mentioning Amazon Virtual Private Cloud (VPC). Amazon VPC is a virtual network that resembles a traditional network. Like a traditional network, your VPC has IP addresses, subnets, route tables, Internet gateways, and more. And of course, your VPC also needs some kind of firewall filtering which leads us to Security Groups.

If you don't specify a Security Group, Amazon EC2 uses the default Security Group. For example, after you associate a Security Group with an EC2 instance, inbound and outbound traffic for that instance will follow the rules of the Security Group. Security Groups apply to just instances, not the whole subnet.

Security Groups are stateful, ingress equals egress. Traffic that matches a rule for one direction will also be allowed automatically in the opposite direction.

Security Groups are found under the EC2 Service in the AWS Console:

AWS Security Groups



Which services need Security Groups?

Although most commonly used with EC2 compute instances, many AWS services rely on Security Groups.

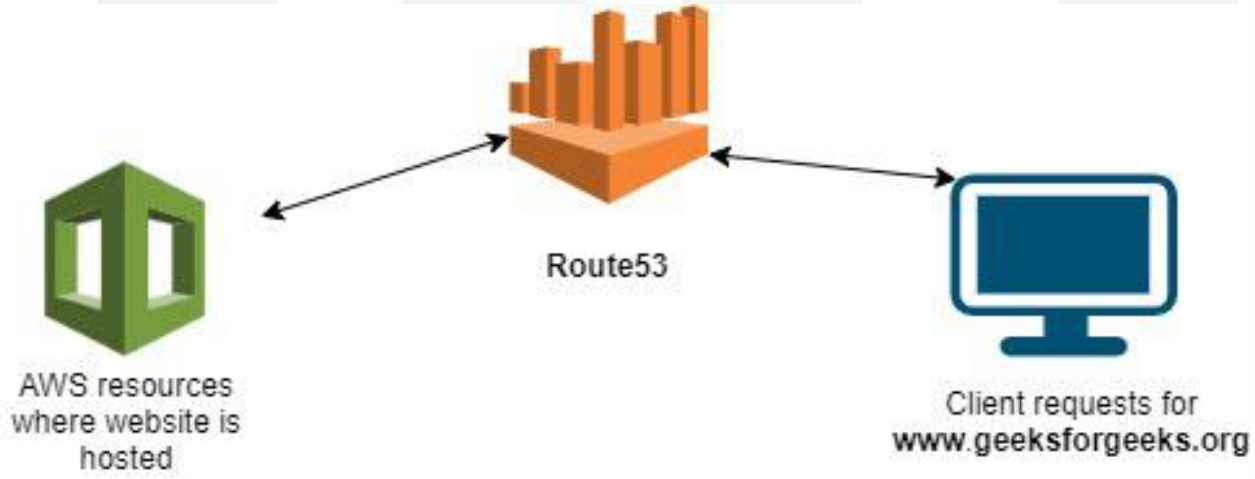
Of these services, Amazon EC2 is one of the most widely used. You should look further into this if you are wondering how to secure Amazon EC2 in general, especially if you want to fully understand securing SSH on Amazon EC2.

But more than just Amazon EC2, all the following AWS services rely on Security Groups in some way:

Amazon EC2 instances
AWS Lambda
AWS Elastic load balancing

AWS Route 53

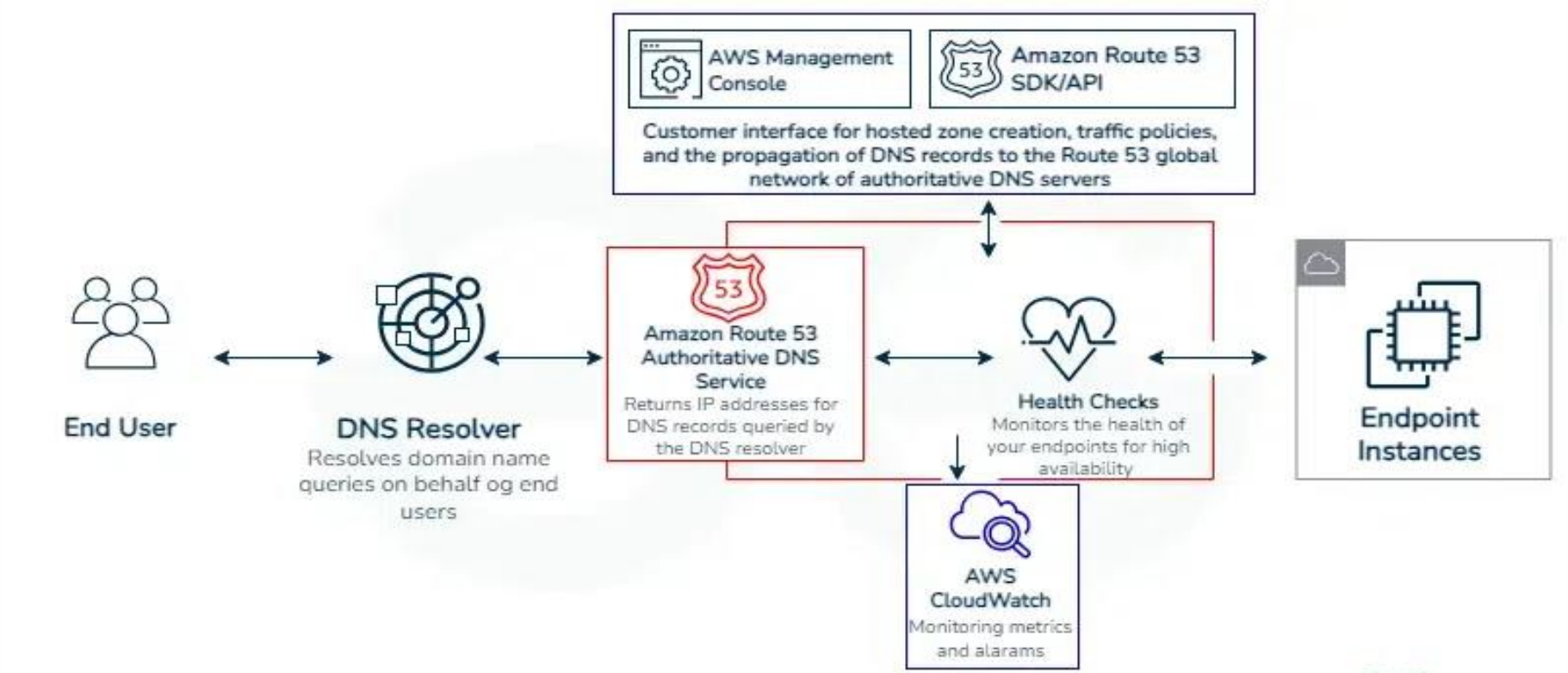
- Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed for developers and corporations to route the end users to Internet applications by translating human-readable names like www.geeksforgeeks.org into the numeric IP addresses like 192.0.1.1 that computers use to connect. You cannot use Amazon Route 53 to connect your on-premises network with AWS Cloud.



Functions Of Route53

- If a web application requires a domain name, Route53 service helps to register the name for the website (i.e domain name).
- Whenever a user enters the domain name, Route53 helps to connect the user to the website.
- If any failure is detected at any level, it automatically routes the user to a healthy resource.
- Amazon Route 53 is cost effective, secure and scalable.
- Amazon Route 53 is flexible, highly available and reliable.

Functions Of Route53



AWS CloudFront: CDN Cloud Service

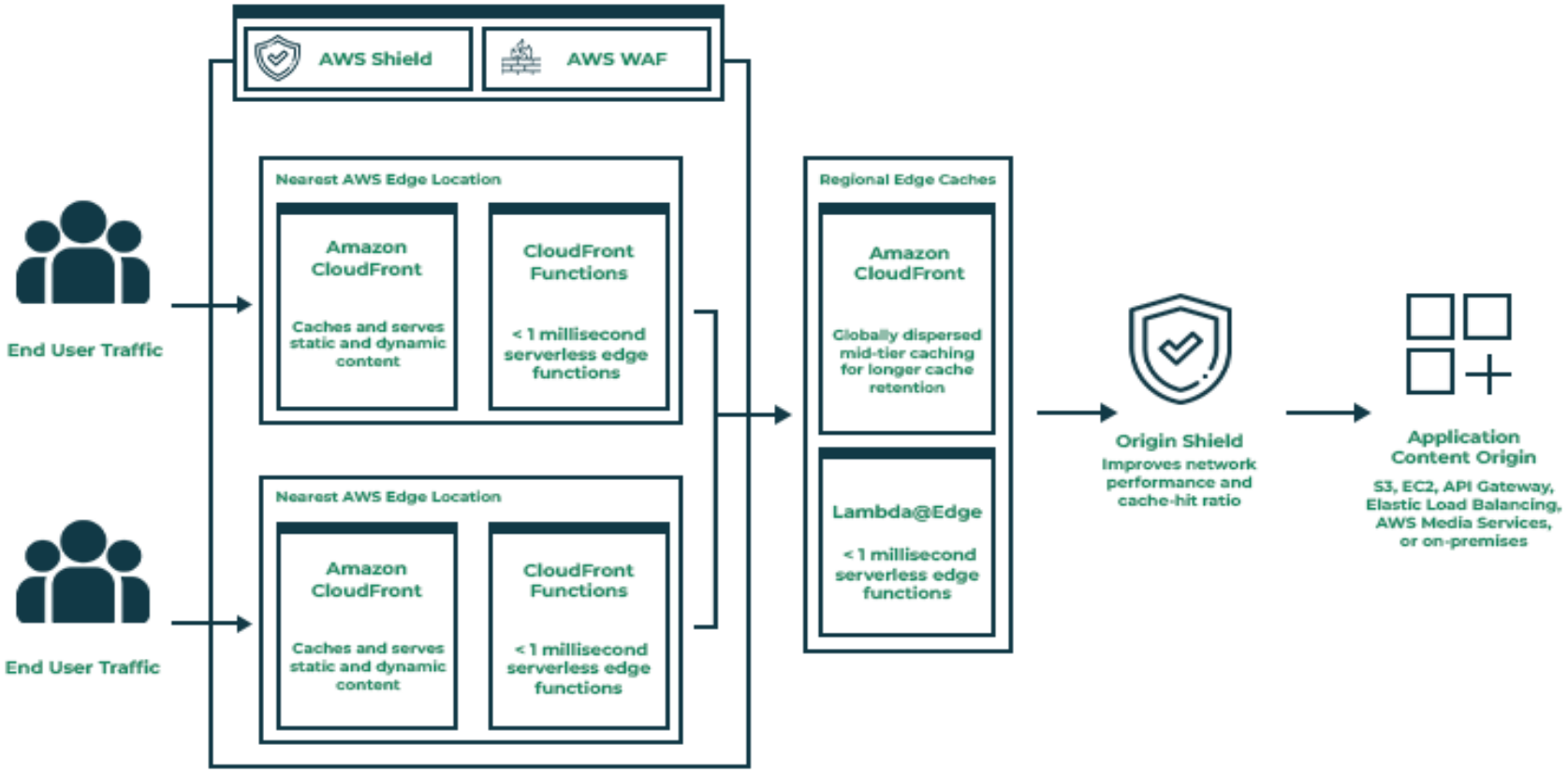
Amazon Web Services (AWS) offers a global content delivery network (CDN) service called AWS CloudFront. It makes it possible for companies to swiftly and effectively distribute content to users worldwide, including static or dynamic data, videos, images, and APIs.

CloudFront caches copies of your content in strategically located servers known as edge locations. When a user makes a request for your content, CloudFront delivers it from the nearest edge location, reducing latency and improving load times. This ensures low-latency delivery, high transfer speeds, and an optimized user experience.

Parul®
University

DIGITAL LEARNING CONTENT

AWS CloudFront: CDN Cloud Service



How does AWS CloudFront work

Step 1: User Requests Content
A user asks for something like an image, video, or webpage from a website or app.

Step 2: DNS Routes the Request
The DNS (Domain Name System) finds the closest CloudFront server and sends the request there for faster delivery.

Step 3: CloudFront Checks for Cached Content
CloudFront checks if the requested content is already stored in the nearest server:

If it’s stored: CloudFront gives the content right away.
If not stored: CloudFront sends the request to the main server to get the content.

How does AWS CloudFront work

Step 4: Content Comes from the Origin Server
The main server (like Amazon S3, EC2, or your own server) sends the requested content to the nearest CloudFront server.

Step 5: CloudFront Caches the Content
CloudFront saves the content in the server so that it can be used again in the future, making the system faster.

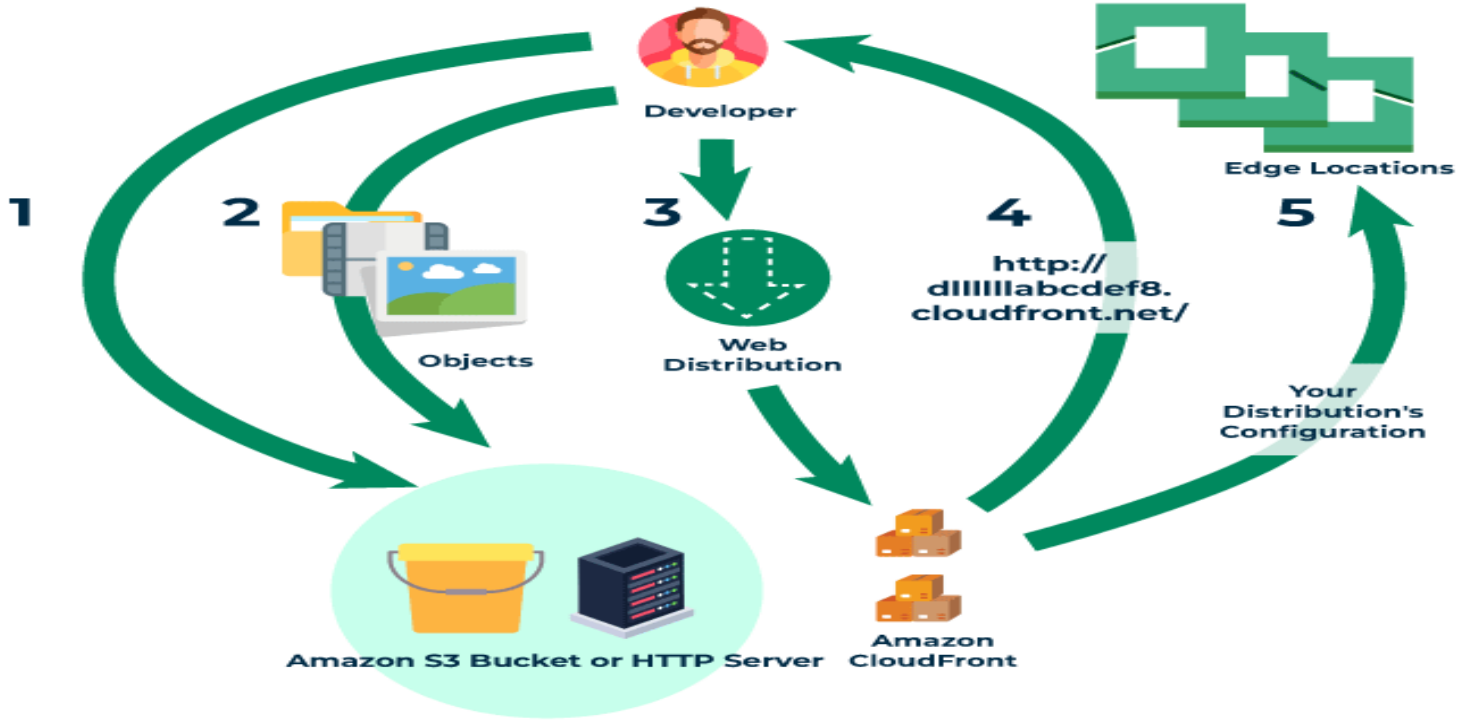
Step 6: CloudFront Delivers Content
CloudFront sends the content to the user from the nearest server, which makes it load faster because it’s closer to the user.

How does AWS CloudFront work

Step 7: Future Requests
For future requests, CloudFront gives the content directly from its cache, making the process even quicker.

Step 8: Cache Update (When Needed)
CloudFront checks with the main server regularly to see if the content has been updated. If it has, CloudFront fetches the new version and updates the cache for future use.

How does AWS CloudFront work



AWS CloudFront

Key Benefits of AWS CloudFront

- No up-front investment (Non-mandatory)
- Lowering operating cost
- Highly scalable, resilient
- Easy access
- Reducing business risks and maintenance expenses

Build Your VPC in AWS and Launch a Web Server

To build a VPC and launch a web server in AWS, you'll need to create a VPC, subnets, an Internet Gateway, and then launch an EC2 instance with a security group configured to allow HTTP traffic.

1. **Create a VPC:**

Navigate to the AWS VPC console.
Choose "Create VPC" and configure the VPC with a name, CIDR block, and other options like availability zones.

2. **Create Subnets:**

In the VPC console, navigate to "Subnets".
Create a public subnet associated with your VPC and select an availability zone.
Optionally, create a private subnet for your backend server if needed.

Build Your VPC in AWS and Launch a Web Server

3. Create an Internet Gateway:

In the VPC console, navigate to "Internet Gateways".

Create an Internet Gateway and associate it with your VPC.

4. Configure Route Tables:

In the VPC console, navigate to "Route Tables".

Create a route table and associate it with your public subnet.

Add a route to the internet gateway, allowing traffic to reach the internet.

5. Create a Security Group:

In the VPC console, navigate to "Security Groups".

Create a security group and allow HTTP (port 80) or HTTPS (port 443) traffic from your IP address.

Build Your VPC in AWS and Launch a Web Server

6. Launch an EC2 Instance:

In the EC2 console, launch an instance.

Choose the appropriate AMI (Amazon Machine Image), instance type, and security group.

Select the subnet you created earlier.

Start the instance and connect to it using SSH.

7. Configure the Web Server:

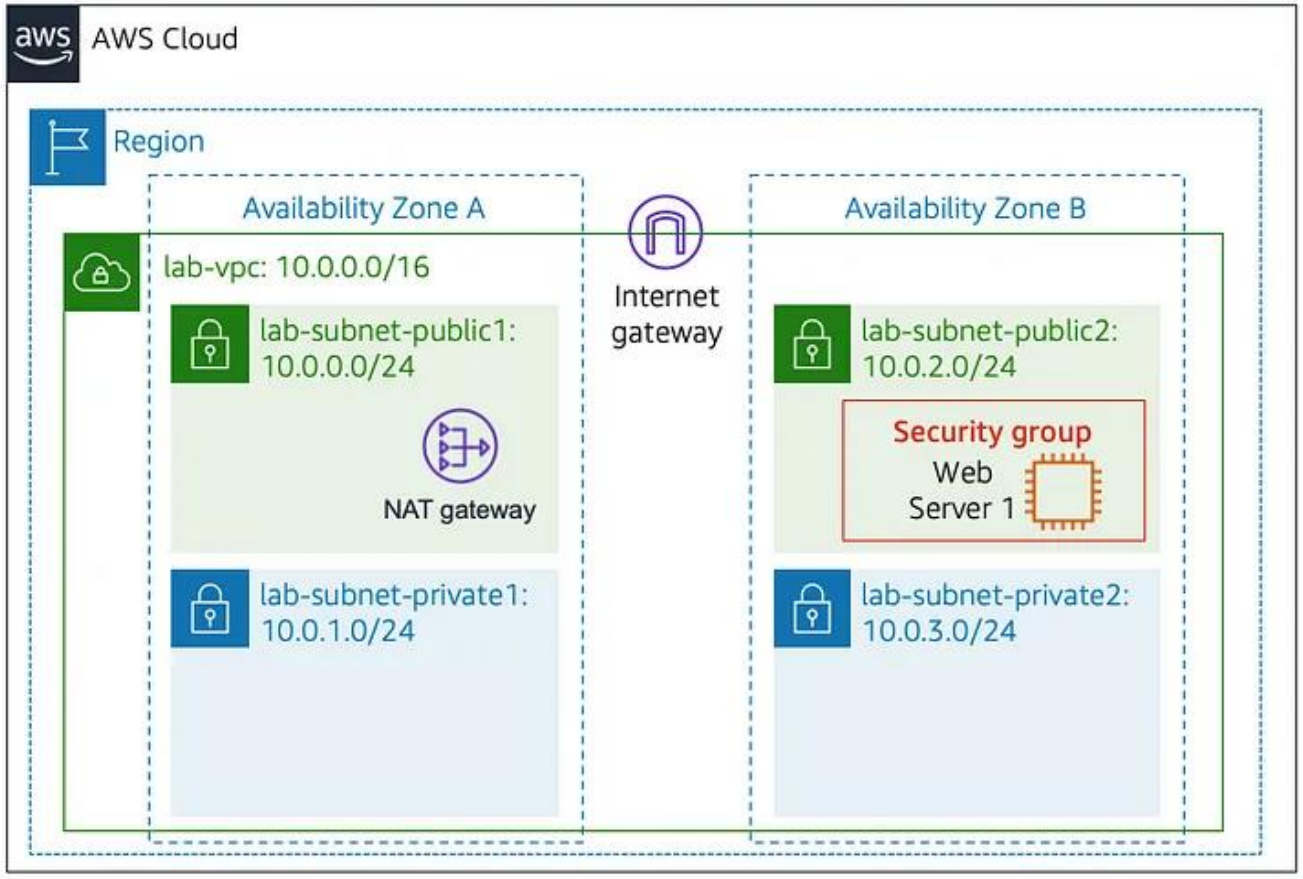
Install and configure a web server like Apache or Nginx on the EC2 instance.

Test that your web server is accessible by browsing to the instance's public IP address.

Parul®
University

DIGITAL LEARNING CONTENT

Build Your VPC in AWS and Launch a Web Server



Public Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	Internet gateway

Private Route Tables

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	NAT gateway

Parul®
University

DIGITAL LEARNING CONTENT

DIGITAL LEARNING CONTENT

Parul® University

www.paruluniversity.ac.in