# AWS Certified Cloud Practitioner

# Networking with AWS
# Virtual Private Cloud (VPC) & CloudFront

Instructor: Tim Platt, Cloud Solution Architect

# Virtual Private Cloud (VPC)

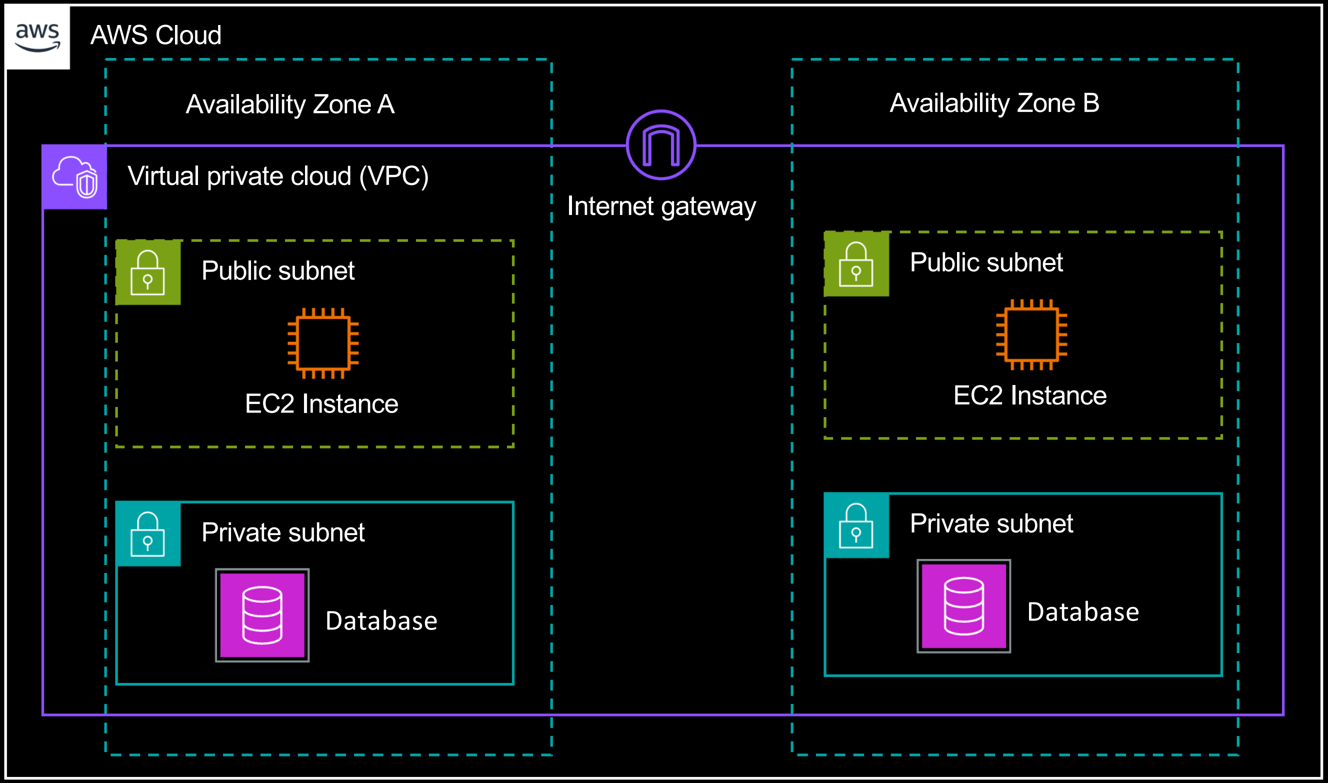
## Network

A virtual network for your virtual servers in the cloud

## Key Points

- A logically isolated section of the cloud where you can launch AWS resources
- Proper network design dictates having a layered or tiered network with “Defense in Depth” applying network level access controls
- Key sub-components:
  - Subnets (Public & Private)
  - Internet Gateway (IGW)
  - Route Table entries for the virtual router
  - Firewall rules – Network Access Control Lists (ACLs) and Security Groups
  - NAT Gateway (Network Address Translation)
- SUPERPOWER: Virtual equivalents of all the components needed to build a computer network: subnets, route tables, firewall rules, Domain Name System (DNS) name resolution, and more

# A Best Practices based VPC

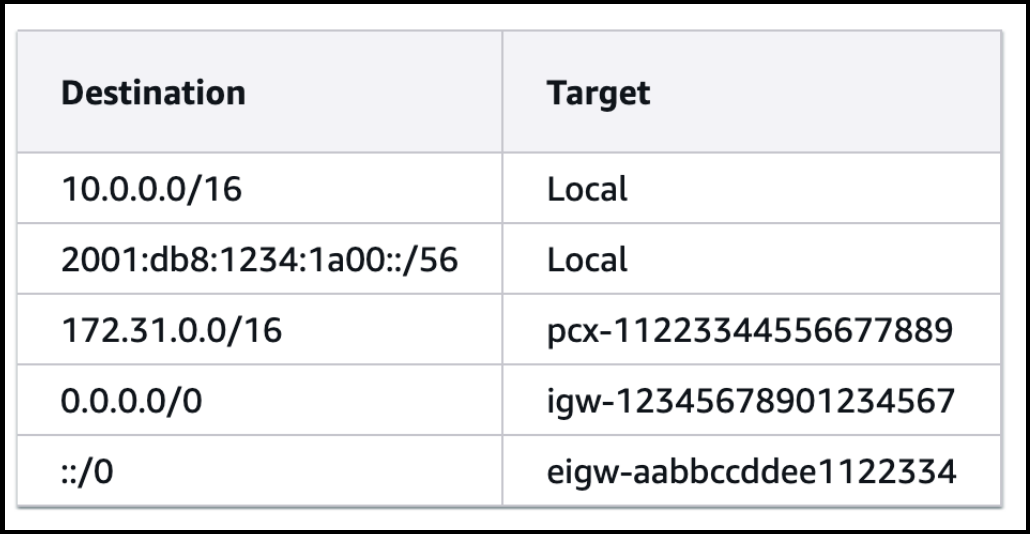


## Key Points

- Public Subnets for Internet facing resources
- Internet Gateway facilitates Internet access (inbound and outbound)
- Private Subnets for things that should NEVER be accessible from the Internet
- More than one AZ (Notice the redundancy in the web servers and database nodes.

We are minimizing Single Points of Failure

# Route Tables



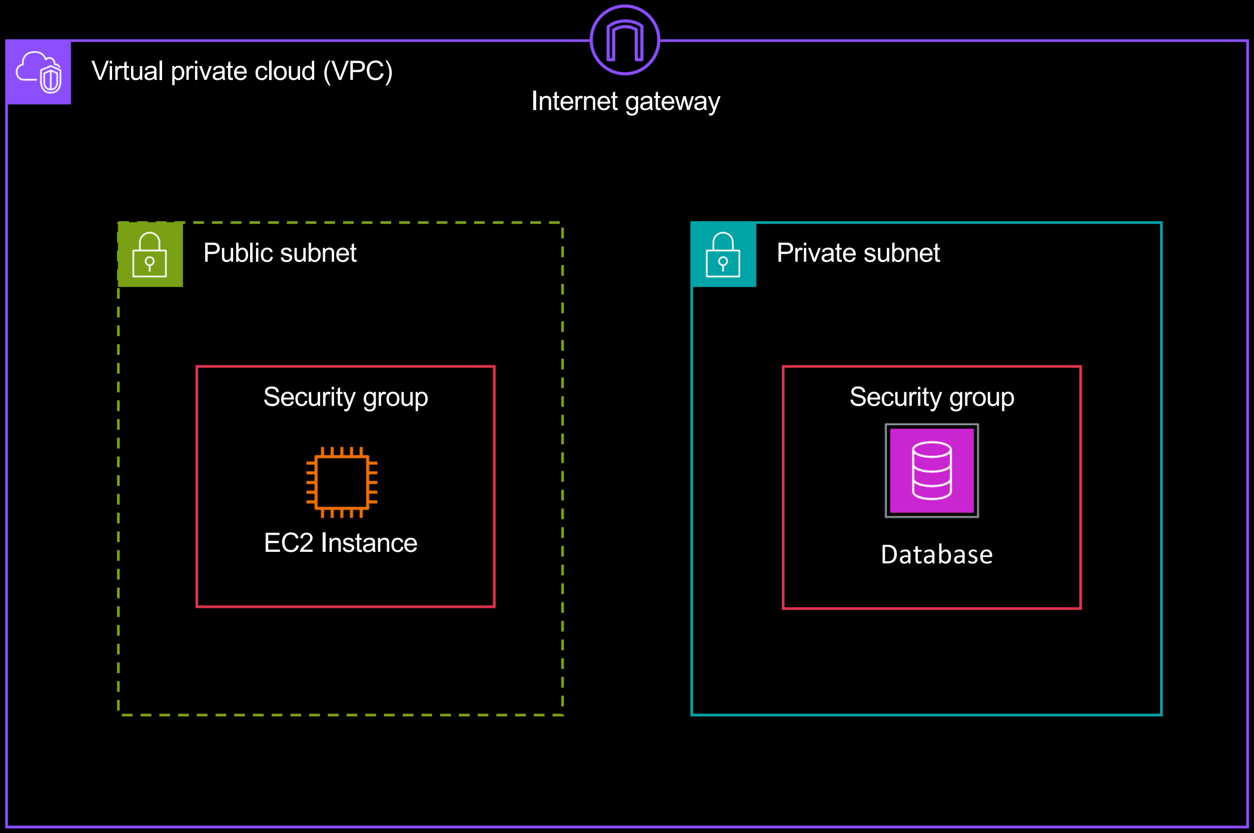
| Destination | Target |
|---|---|
| 10.0.0.0/16 | Local |
| 2001:db8:1234:1a00::/56 | Local |
| 172.31.0.0/16 | pcx-11223344556677889 |
| 0.0.0.0/0 | igw-12345678901234567 |
| ::/0 | eigw-aabbccddee1122334 |

Your Virtual Network (VPC) has a Virtual Router – you can't see it or access it, but you control the traffic routing rules.

A *route table* serves as the traffic controller for your virtual private cloud (VPC).

Each route table contains a set of rules, called *routes*, that determine where network traffic from your subnet or gateway is directed.

# What about Network Security? We have FIREWALLS

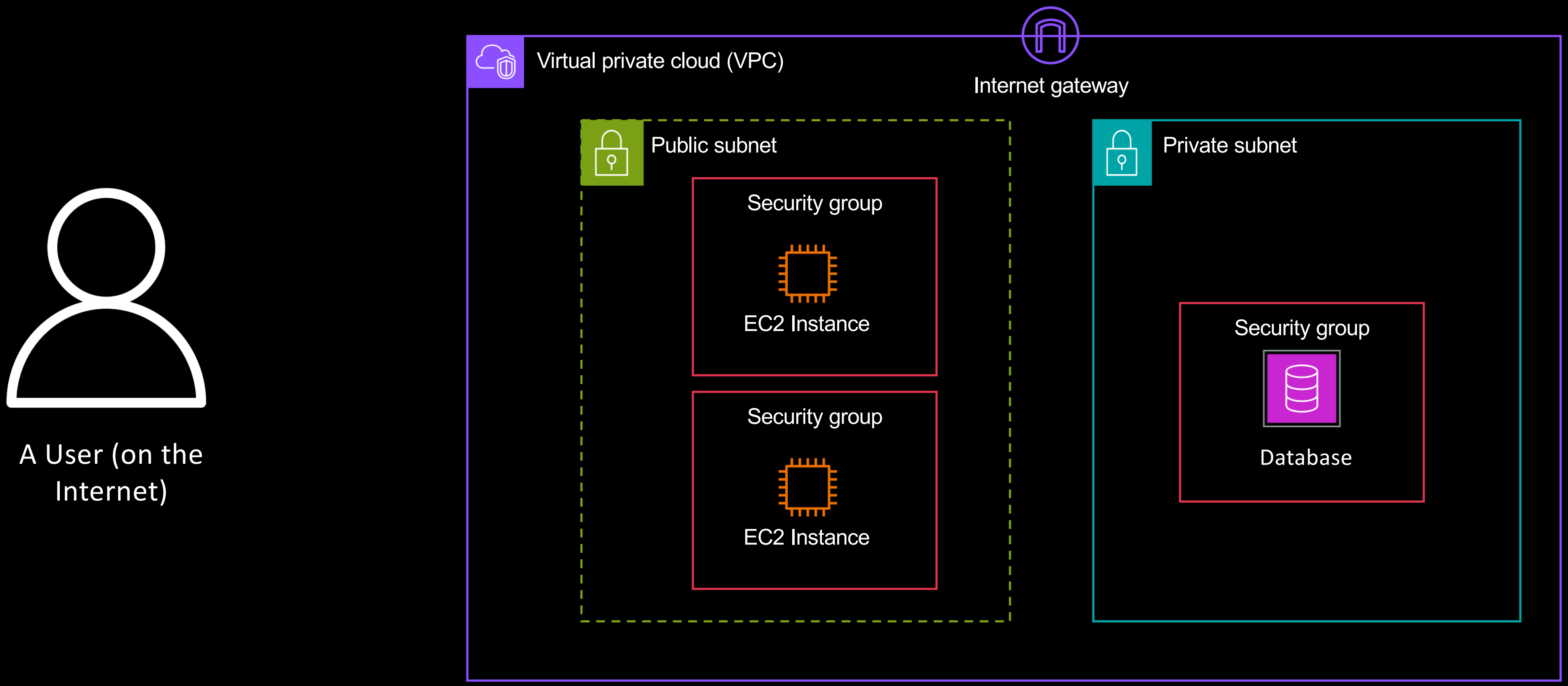


- Subnets have **Network Access Control Lists (ACLs)** that protect the entire subnet

- Within the subnet you have **Security Groups** that let you protect each instance with very specific rules

## Why?

- We need to be able to precisely control inbound and outbound traffic
- Not just to the Internet, also within our own VPC
- That’s “Defense in Depth”



A User (on the Internet)

Virtual private cloud (VPC)

Internet gateway

Public subnet

Security group

EC2 Instance

Security group

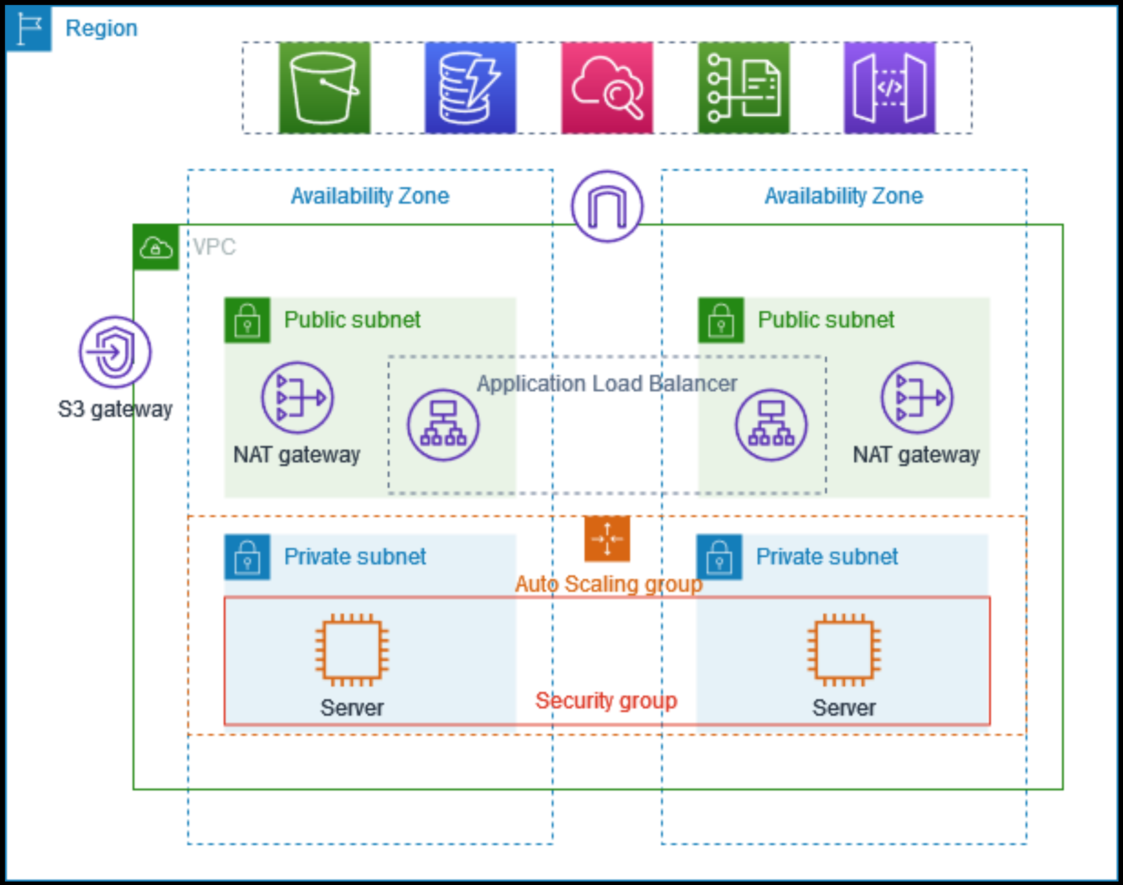
EC2 Instance

Private subnet

Security group

Database

# Another example - with access to AWS services from Private



The servers in Private Subnet can securely access Web Services over the Internet by sending traffic outbound via the **NAT Gateway**

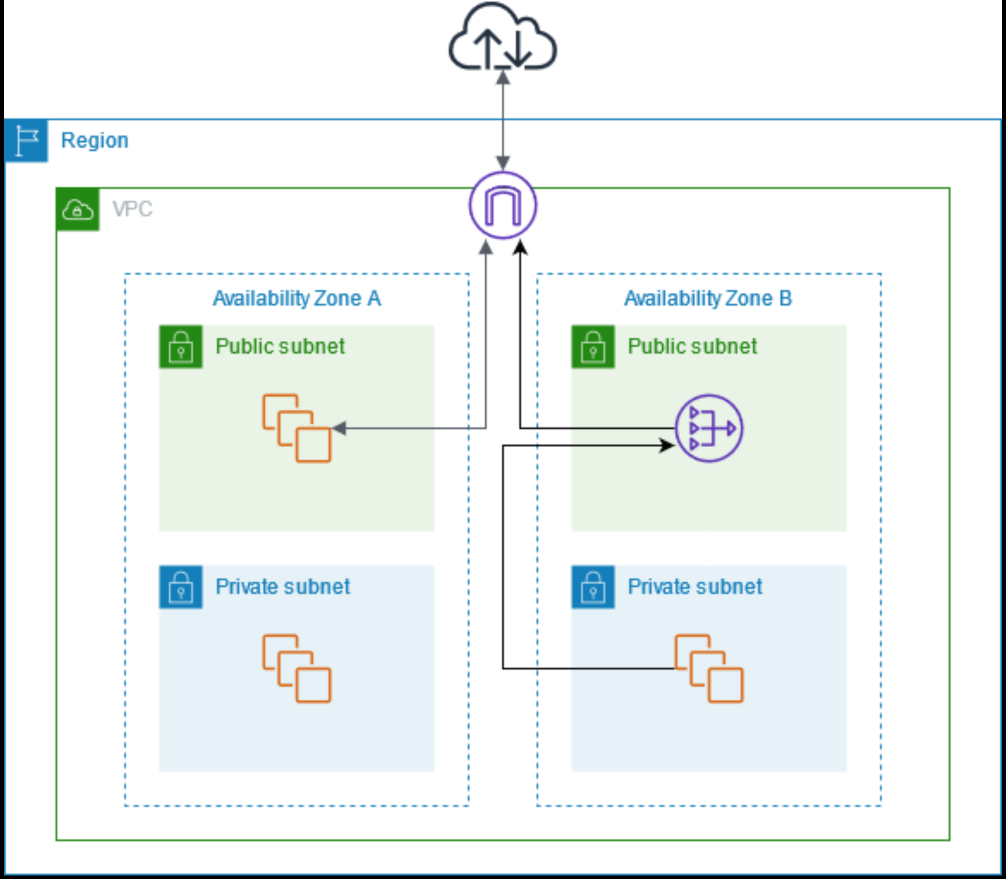
S3, DynamoDB, CloudWatch, etc. are WEB SERVICES.

They are accessed over the INTERNET – that's why they are called WEB Services.

Notice that S3, DynamoDB live in the REGION – NOT in your VPC.

Tutorial to set this up

# 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 can't initiate a connection with those instances.

In this scenario, the servers in the private subnet can initiate outbound connections to the Internet (to communicate with other clouds, or to download software, or to access web services)

NOTE: The arrows represent connections being opened. Understand NAT Gateway will NOT allow the Internet to initiate an inbound connection.

# Route 53 – DNS (Domain Name System)

## DNS

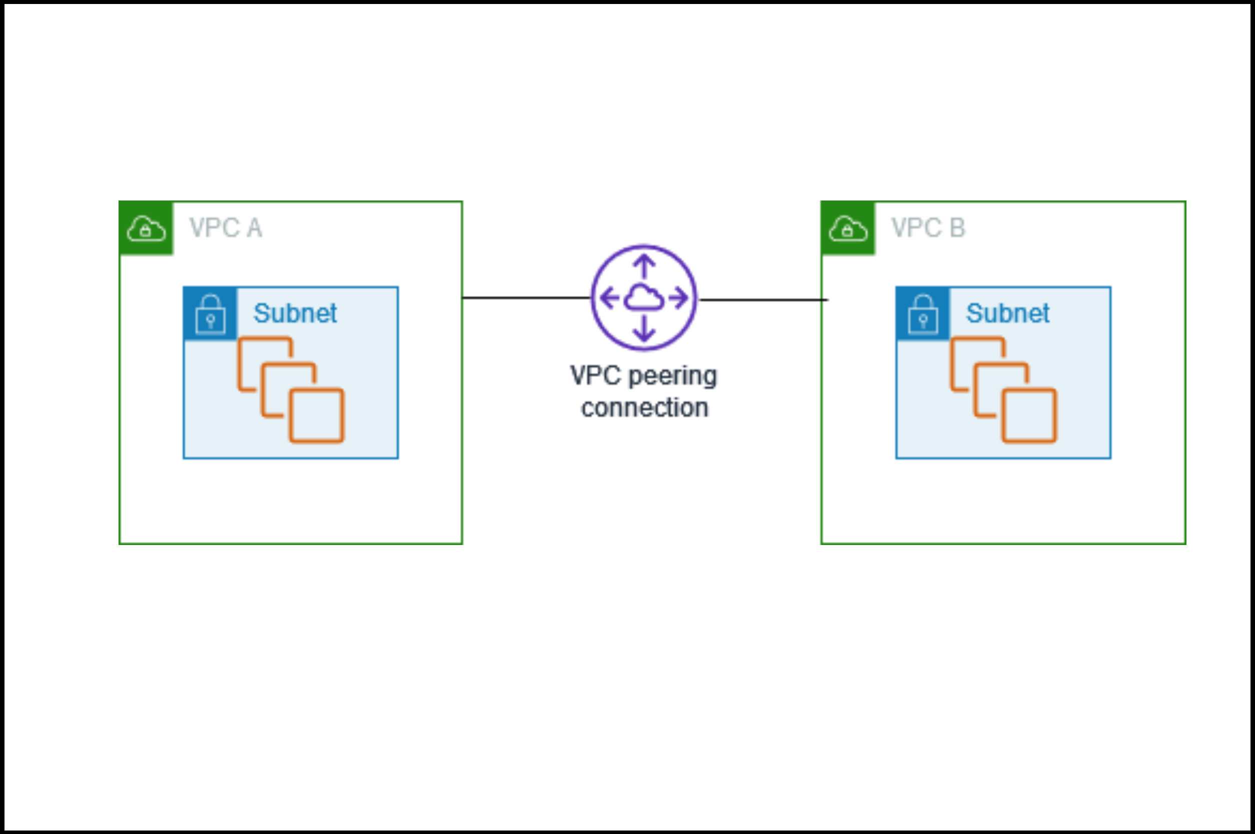
Manage custom DNS Names with powerful features

## Key Points

- The DNS (Domain Name System) is what resolves friendly domain names (like www.amazon.com or www.awstrainer.com ) to IP addresses
- Route 53 can be used to Register Domains but also to define the sets of Name records
- Hosted Zone - a container that holds information about how you want Amazon Route 53 to respond to DNS queries for a domain and its subdomains.
  - Public Hosted Zone – Names are resolvable over the Internet
  - Private Hosted Zone – Names are resolvable only in your VPCs
- SUPERPOWER: Route 53 has lots of high performance features that simpler DNS services don't provide – like health checks, failover routing, and much more

**TIP: Route "53" gets its name from the network port used for DNS traffic – which is port 53.**

# VPC Peering – Simple connectivity between VPCs

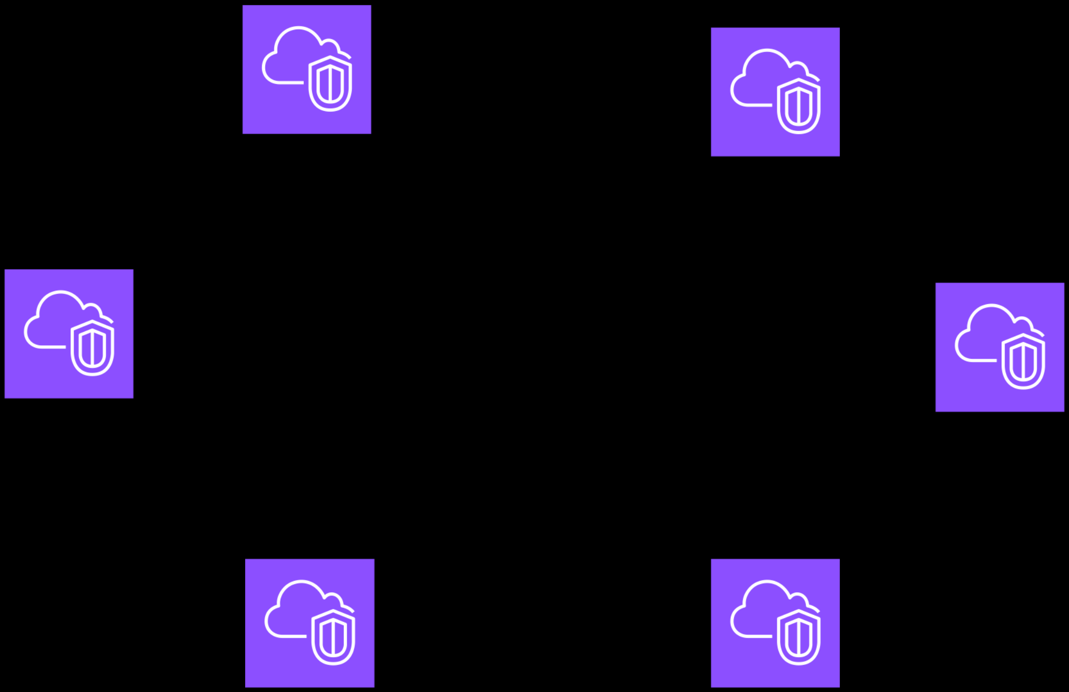


A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IP addresses.

The VPCs can be in same region, different regions, same account, or difference accounts.

NOTE: VPC Peering is a non-transitive 1:1 connection between only two VPCs.

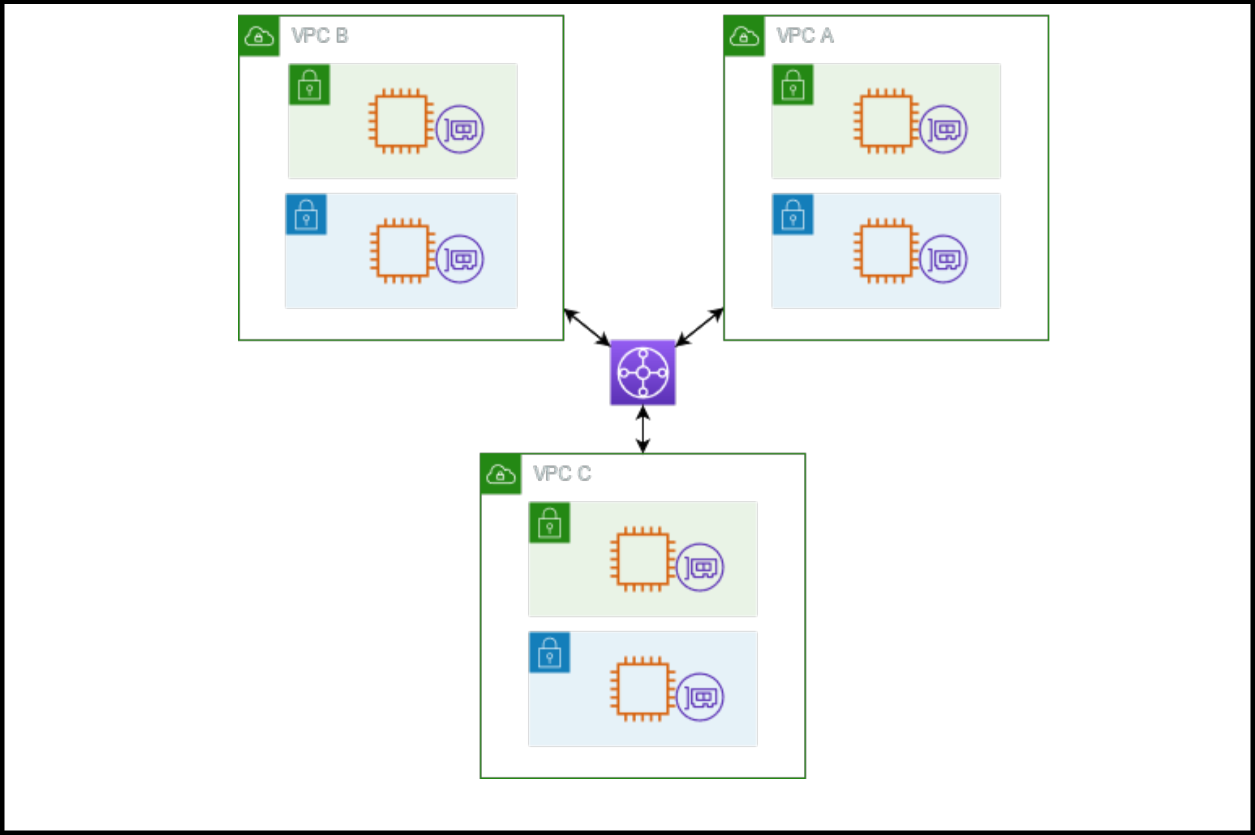
# VPC Peering – How many connections for 6 VPCs?



How many VPC Peering connections would we need to FULLY CONNECT 6 VPCs?

ANSWER: TOO MANY

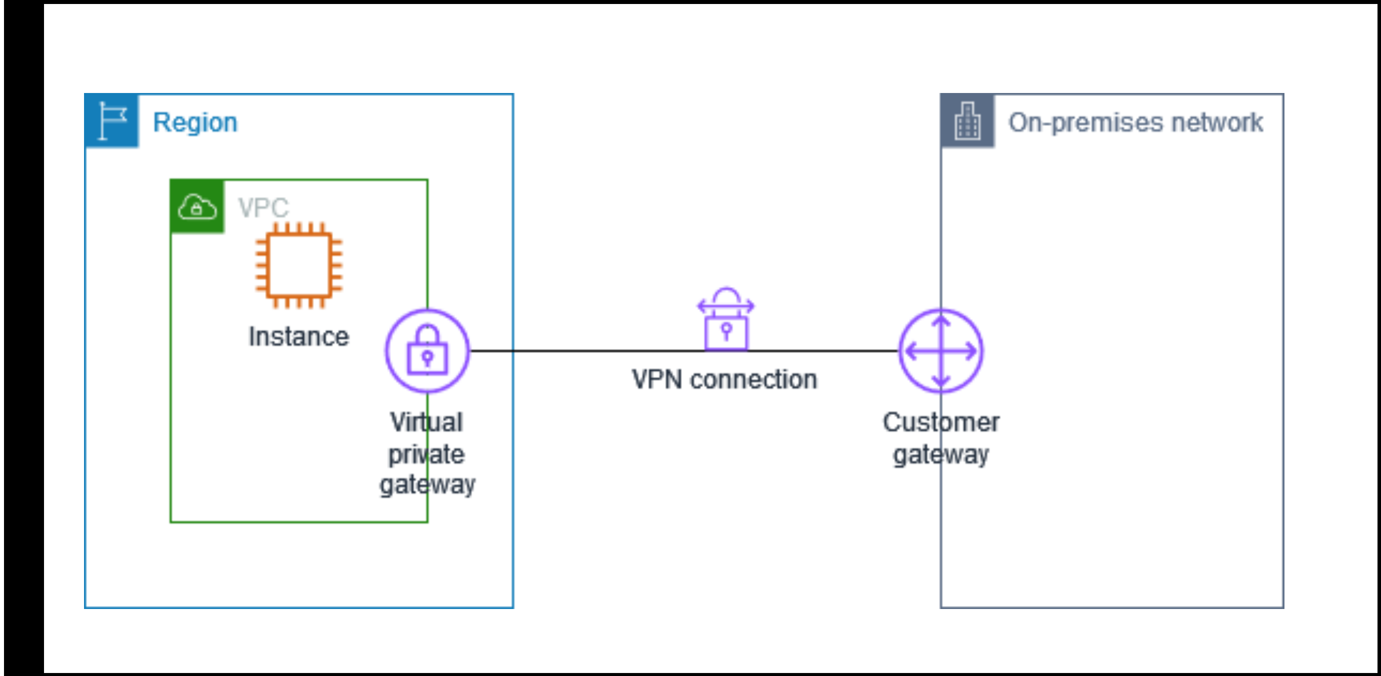
# Transit Gateway – For large scale inter-connectivity



AWS Transit Gateway is a network transit hub used to interconnect multiple virtual private clouds (VPCs) and on-premises networks.

NOTE: Use this to overcome the complexity of VPC Peering's transitive nature (VPC Peering is 1:1 only)

# Hybrid connectivity - Site-to-Site Virtual Private Network (VPN)



NOTE: Virtual Private Gateway supports IPSec protocol only!

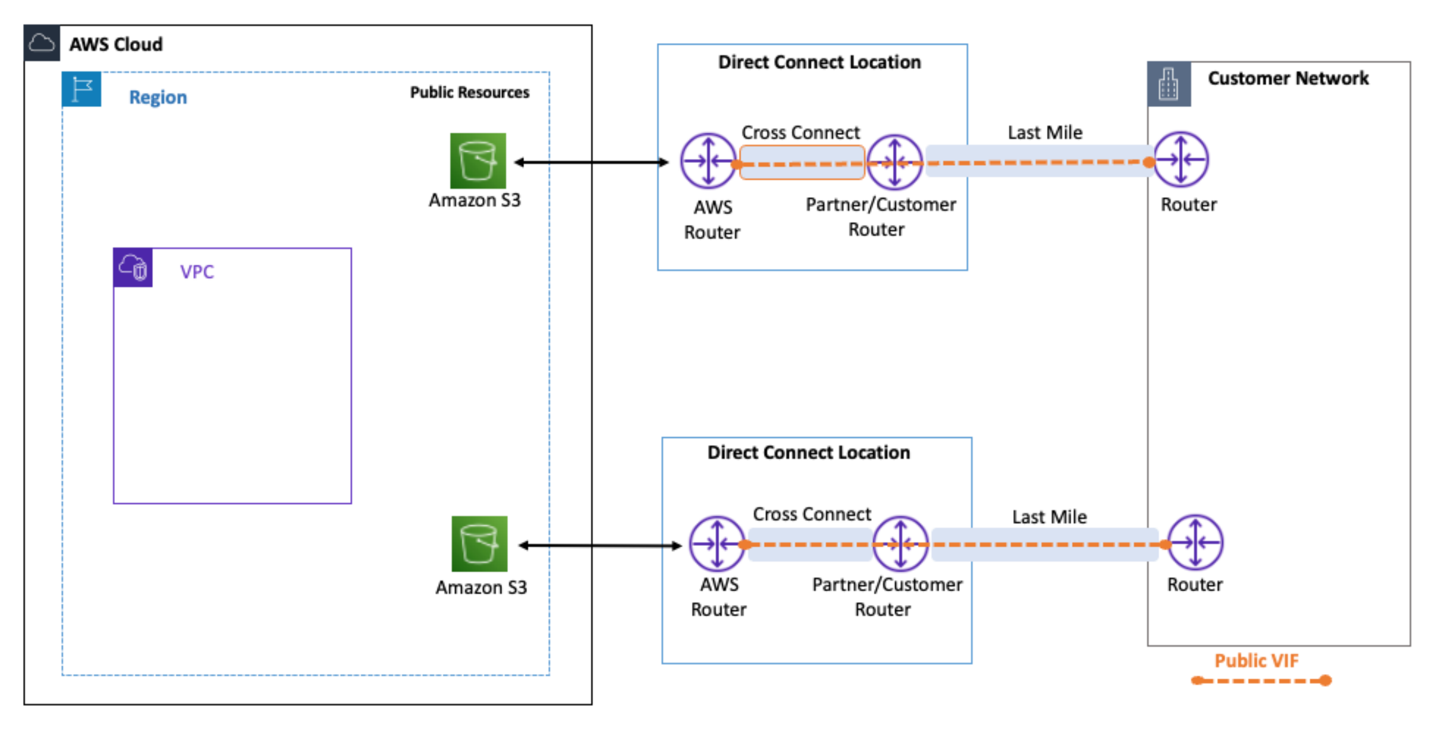
A Site-to-Site VPN is a way to connect two different locations securely over the Internet.

There are two devices (routers or equivalent) that maintain an encrypted tunnel so that traffic is secure.

The router or firewall on the customer side is known as a Customer Gateway

The virtual device on the AWS side is a Virtual Private Gateway (VGW)

# Need more speed? Consider AWS Direct Connect instead

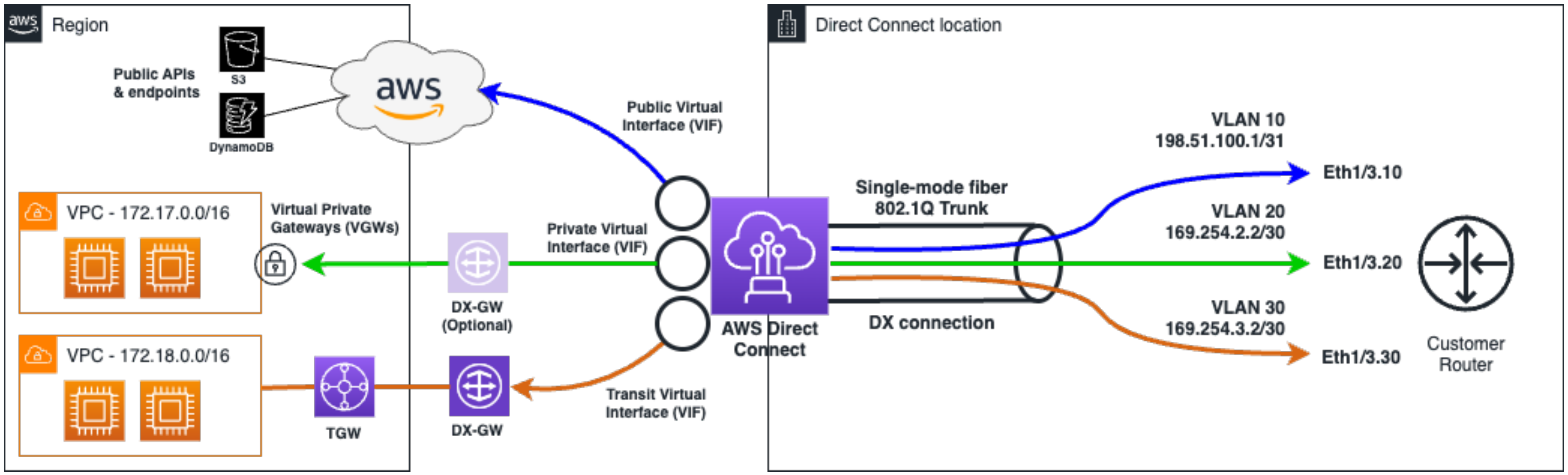


Direct Connect is a private fiber-optic connection that does NOT go over the Internet.

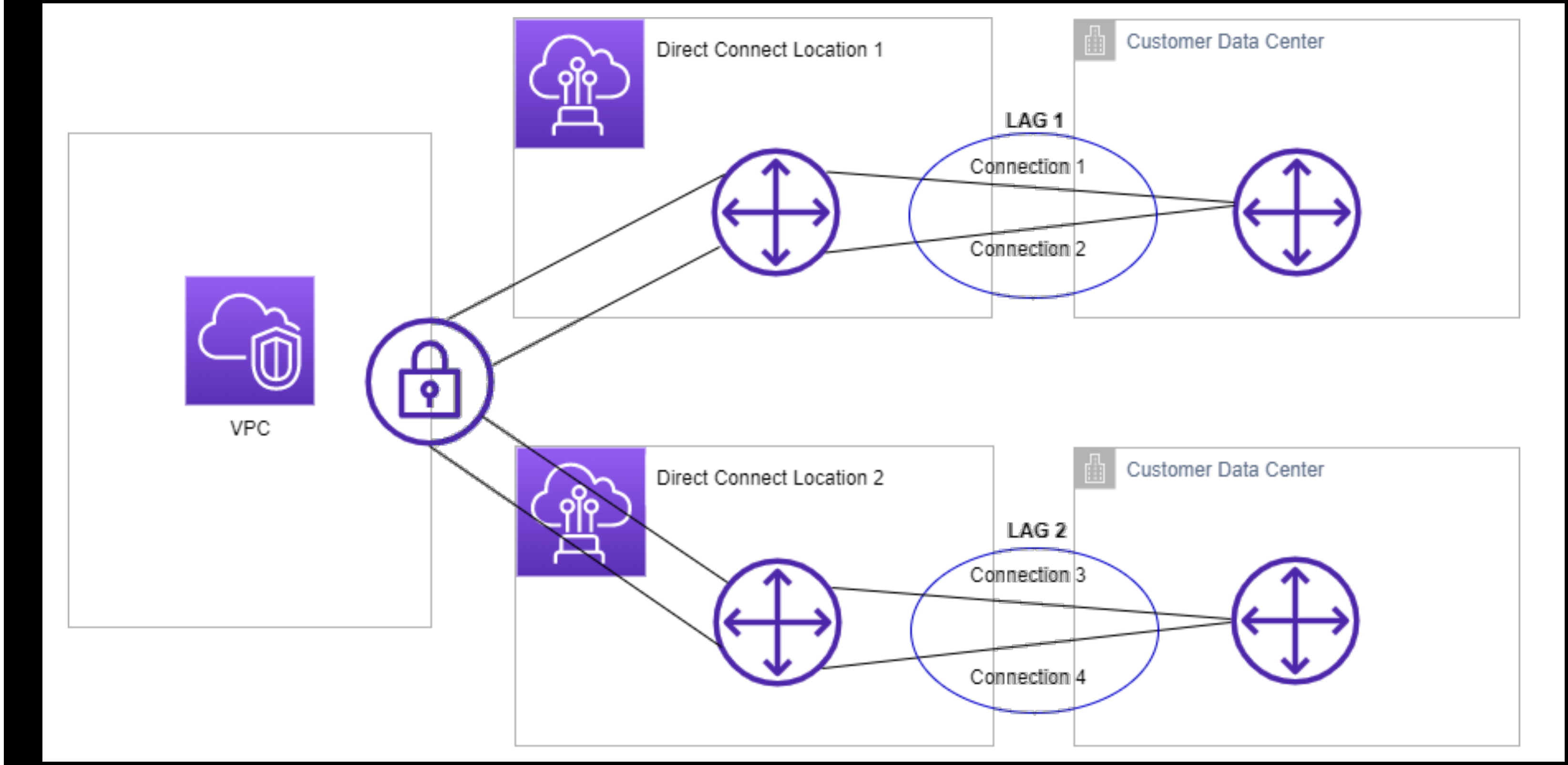
Up to 400 Gbps

(Compare to only 1.25 Gbps with site-to-site VPN)

# Direct Connect: Virtual Interfaces (VIFs) provide different connectivity options



# Link Aggregation Groups (LAGs) to "team up" multiple connections



In Direct Connect, you can use combine the bandwidth of multiple (same-sized) connections into a single logical connection

Here, the aggregate bandwidth of LAG 1 and 2 would be 2x a single connection

# Amazon CloudFront

## Content Delivery Network (CDN)

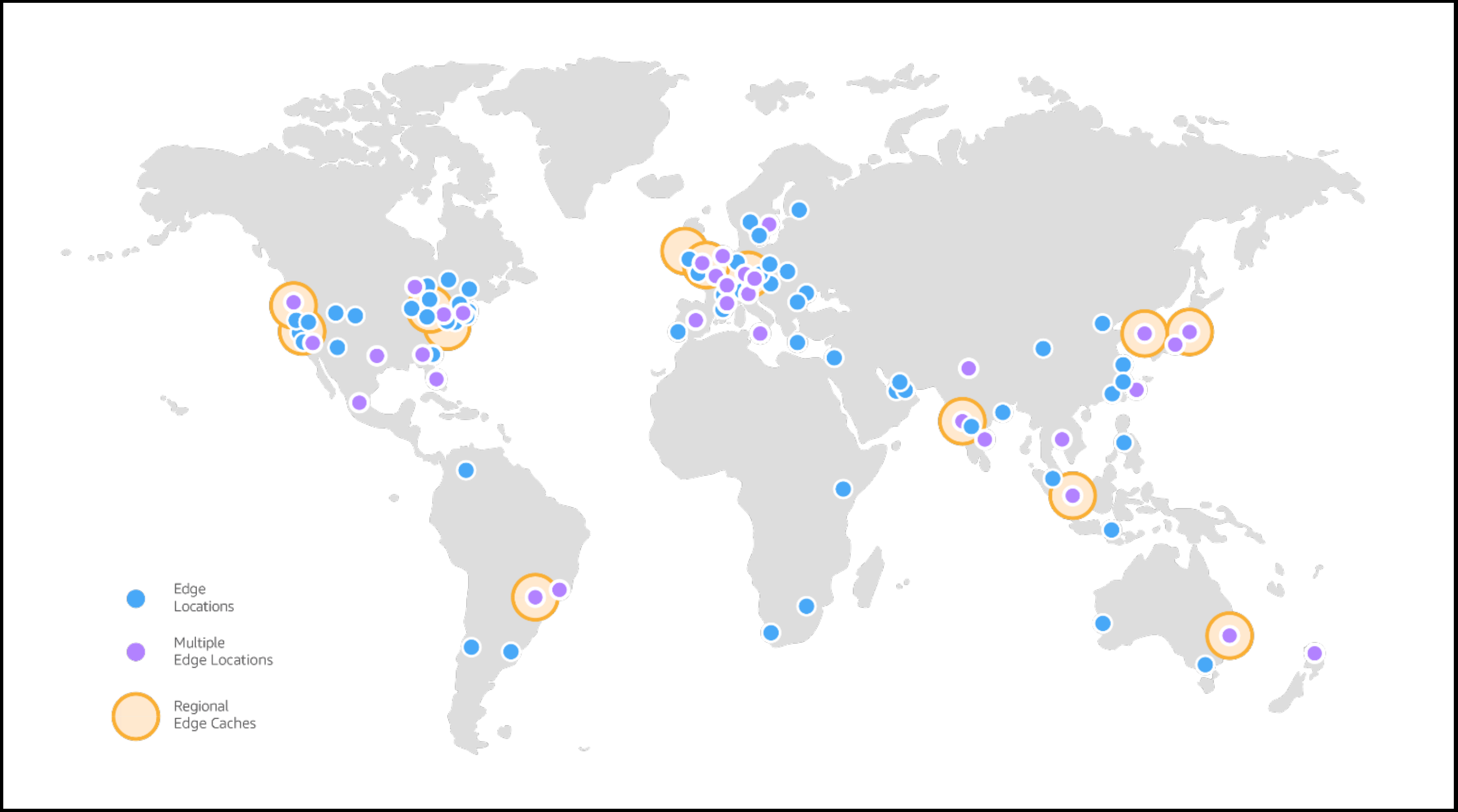
Speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users.

## Key Points

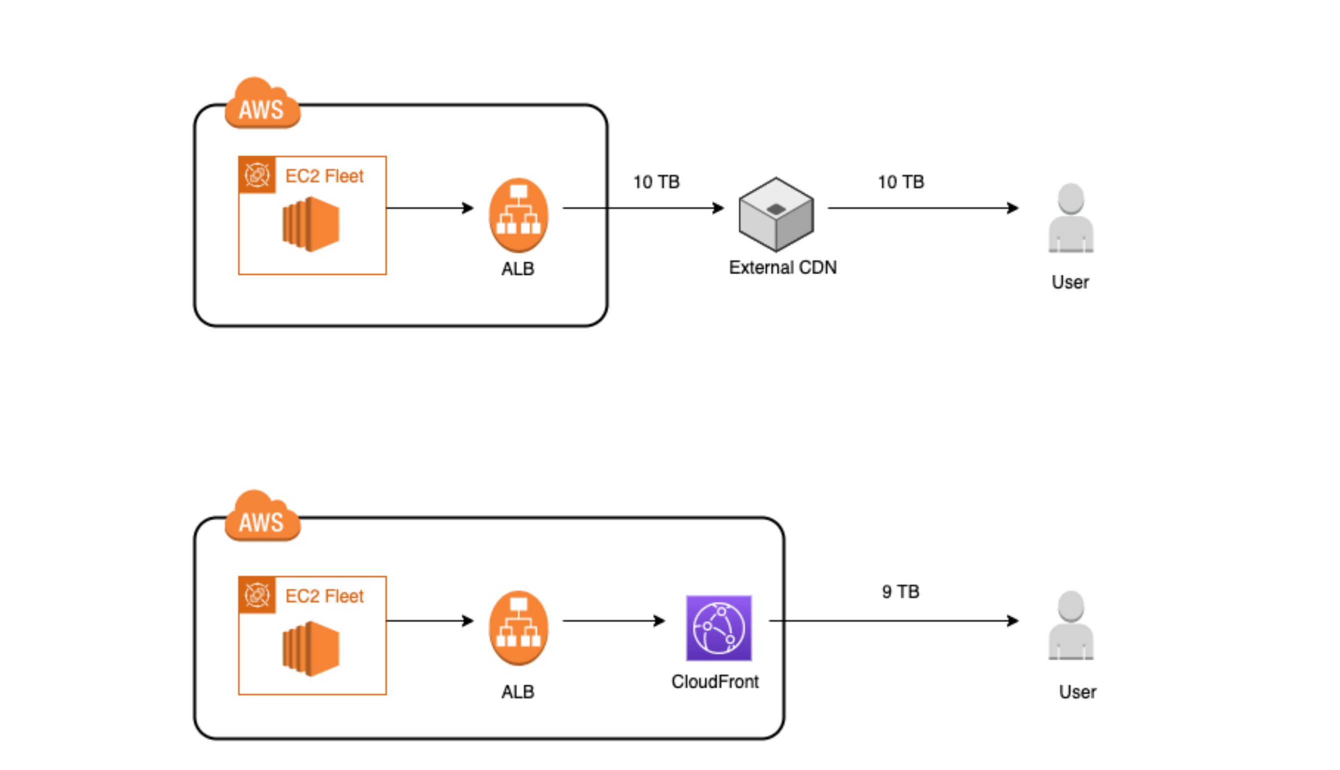
- CloudFront delivers your content through a worldwide network of data centers called edge locations.
- These hundreds of **EDGE LOCATIONS** are used for **caching** the content.
- You define a **DISTRIBUTION** which dynamically retrieves and caches files and pages from your **ORIGIN** (the source of content)
- This process is transparent to the end user of your web site
- SUPERPOWER: Edge locations all over the globe to ensure coverage
- SUPERPOWER: Edge locations are connected to the AWS Regions through the AWS network backbone, a fully redundant, multiple 100GbE parallel fiber that circles the globe and links with tens of thousands of networks

NOTE: Edge Locations are sometimes referred to as CloudFront POPs – Points of Presence

# CloudFront Edge Locations



# CloudFront Architecture vs External CDN

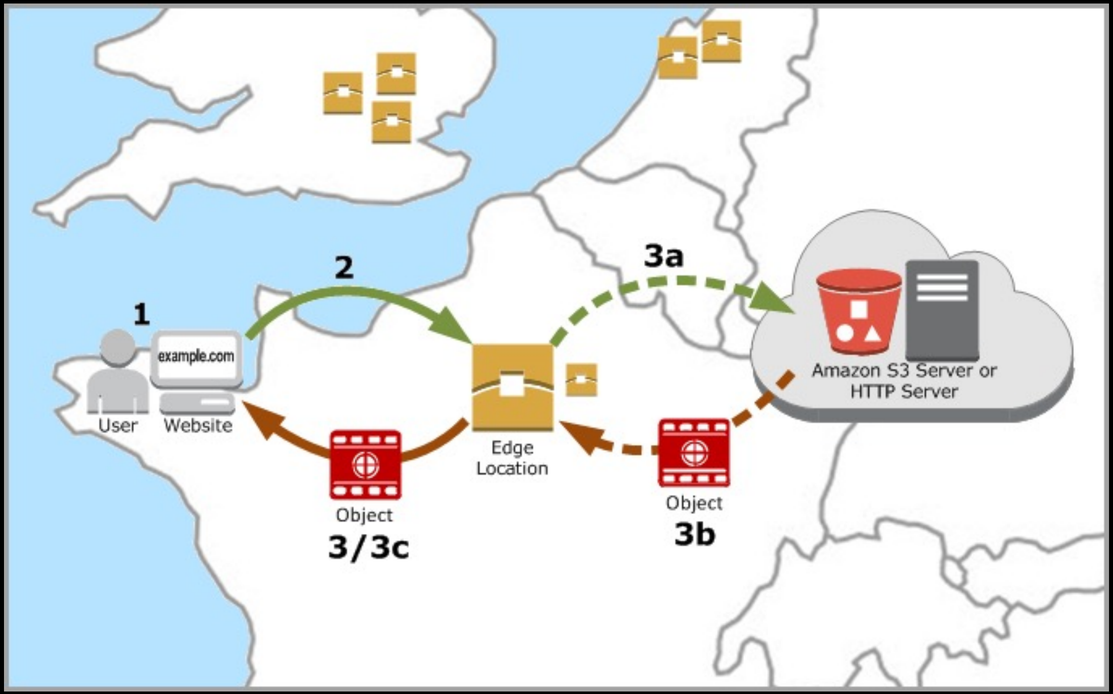


The CDN sits “in front” of the source of your content.

You can use an external CDN with your web application, but there will be considerable data transfer out fees (to the Internet)

By using CloudFront you avoid Data Transfer to the Internet and will pay the more cost-effective rate for CloudFront Data Transfersa

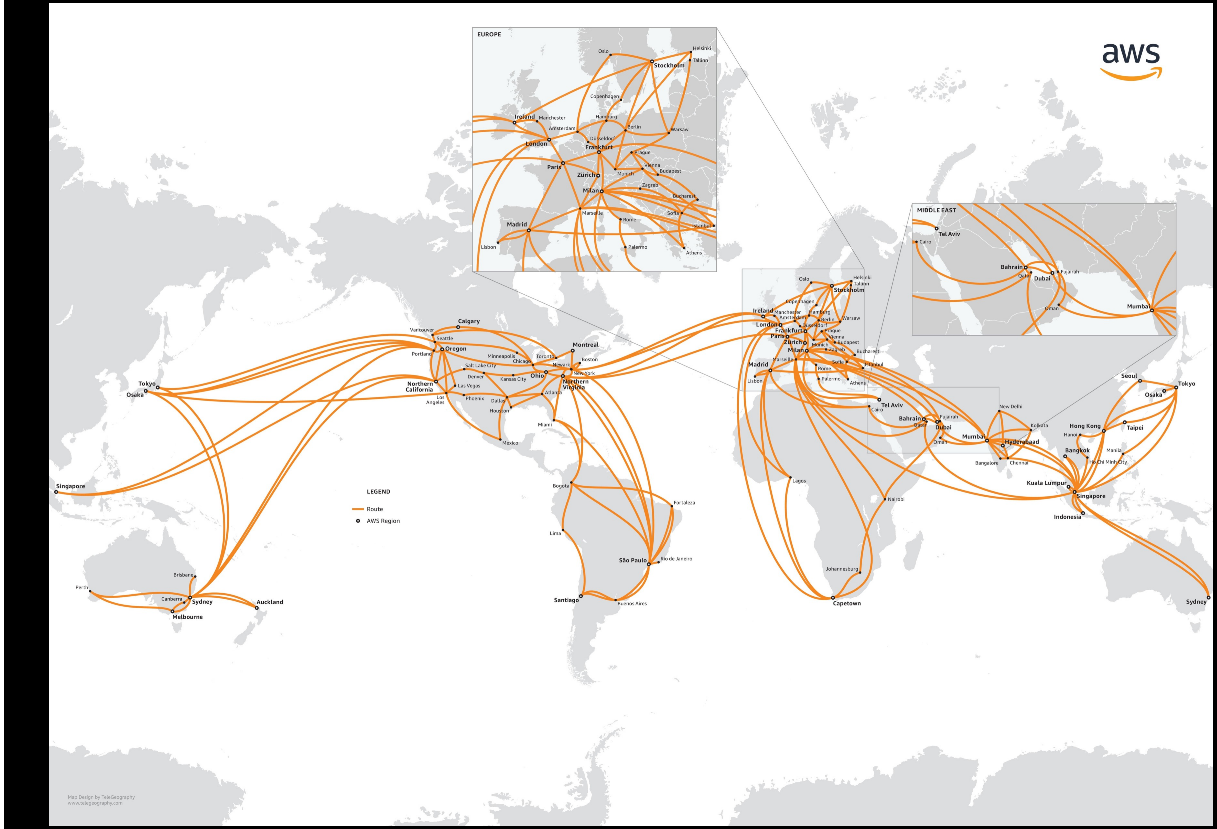
# CloudFront – Get the data CLOSER to the end user



The big idea is to cache the data closer to the end-user, so it downloads quicker and provides a better user experience.

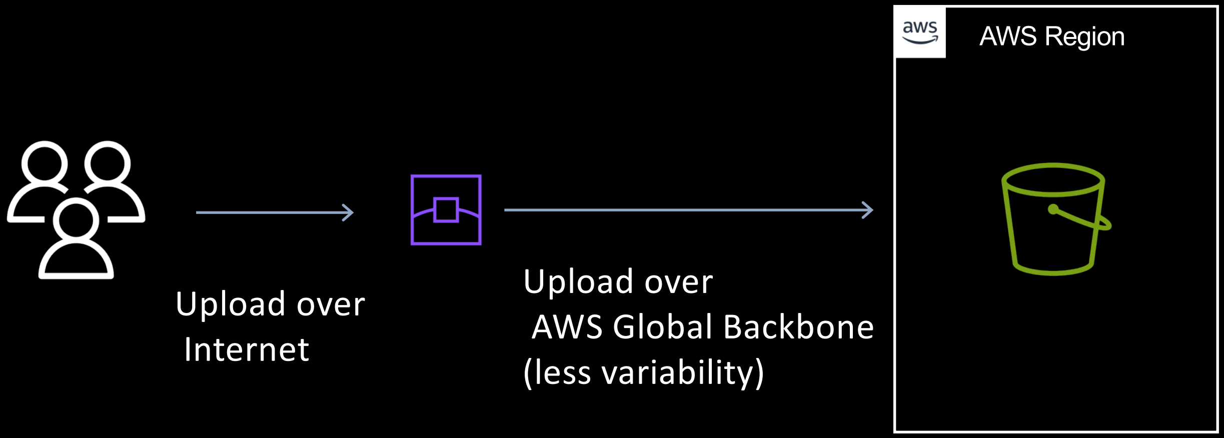
This diagram shows S3 content being cached at the Edge Location which is physically closer to the user by hundreds of miles.

# AWS Global Network



- EVERYTHING is inter-connected through a global fiber backbone network.  6 million kilometers of fiber.
- This includes regions, local zones, edge locations.
- This is NOT the Internet. This is private, exclusive network connectivity monitor, maintained, and managed by AWS
- This is the foundation upon which CloudFront, Transfer Acceleration, and other services are provided

# S3 Transfer Acceleration



Upload data faster and more reliably from remote locations by hopping on the AWS Global Backbone

# Links (1 of 3)

- CIDR.XYZ: https://cidr.xyz/
- VPC Tutorial (Step by Step): https://docs.aws.amazon.com/vpc/latest/userguide/create-a-vpc-with-private-subnets-and-nat-gateways-using-aws-cli.html
- What is a VPC? https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
- Security Groups: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html
- Network Access Control Lists: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html
- Configure Route Tables: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html

# Links (2 of 3)

- AWS Direct Connect: https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html
- AWS Direct Connect link aggregation groups (LAGs): https://docs.aws.amazon.com/directconnect/latest/UserGuide/lags.html

# Links (3 of 3)

- Amazon CloudFront Points of Presence: https://docs.aws.amazon.com/whitepapers/latest/aws-fault-isolation-boundaries/points-of-presence.html
- Amazon S3 Transfer Acceleration Speed Comparison: https://s3-accelerate-speedtest.s3-accelerate.amazonaws.com/en/accelerate-speed-comparsion.html
- AWS Global Network: https://aws.amazon.com/about-aws/global-infrastructure/global-network/
- AWS Global Network – Network Map: https://d1.awsstatic.com/onedam/marketing-channels/website/aws/en_US/global-infrastructure/approved/images/aws-global-network.30fed1dc131cf602a6593048159956cfae07c340.jpg