Learn

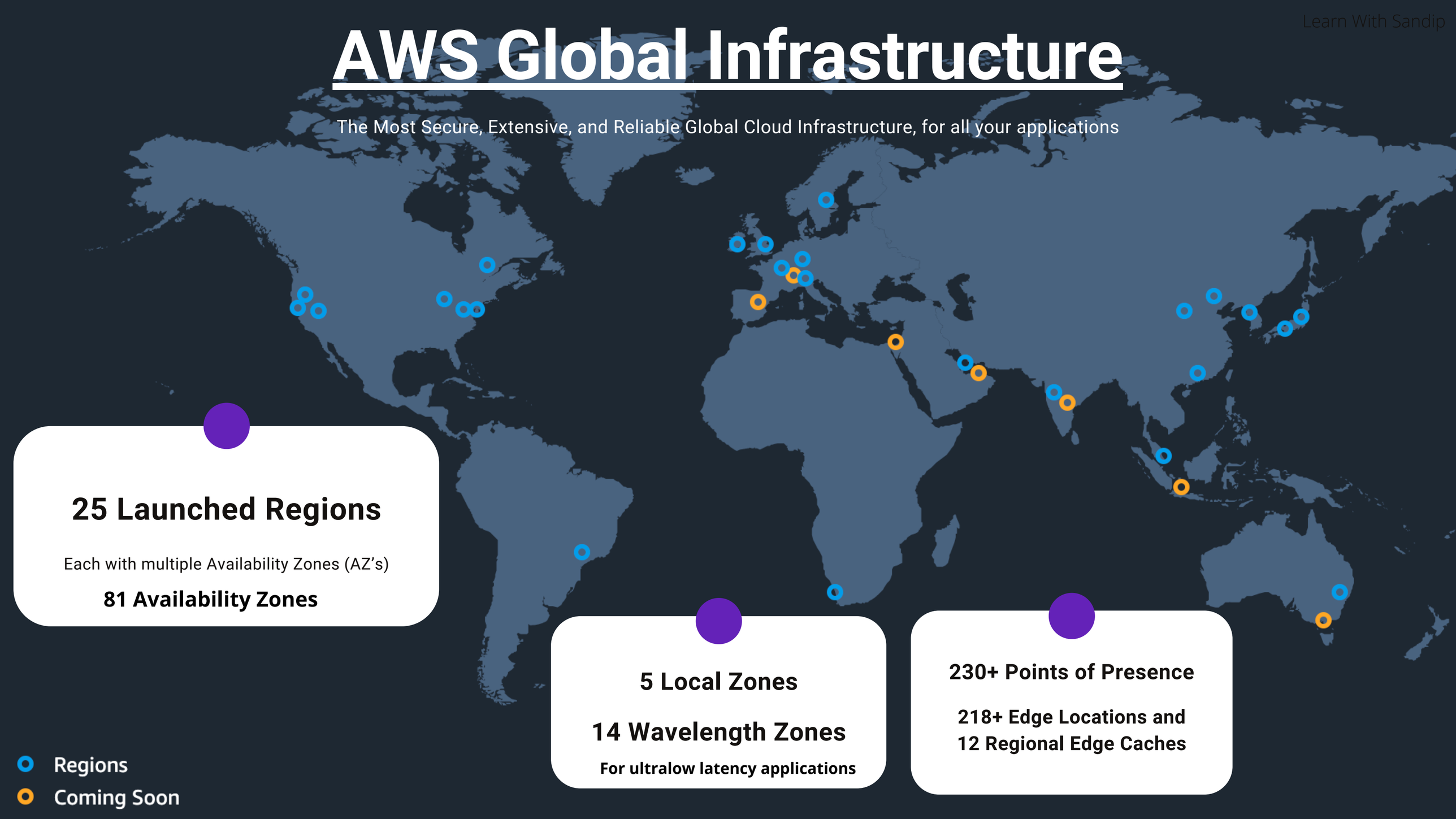
In & Out Of AWS Networking

What is AWS Networking?

AWS networking helps the user to isolate the cloud infrastructure. It also helps to scale the request handling capacity and connect the physical and private virtual network

AWS Global Infrastructure

The Most Secure, Extensive, and Reliable Global Cloud Infrastructure, for all your applications



25 Launched Regions

Each with multiple Availability Zones (AZ's)

81 Availability Zones

5 Local Zones

14 Wavelength Zones

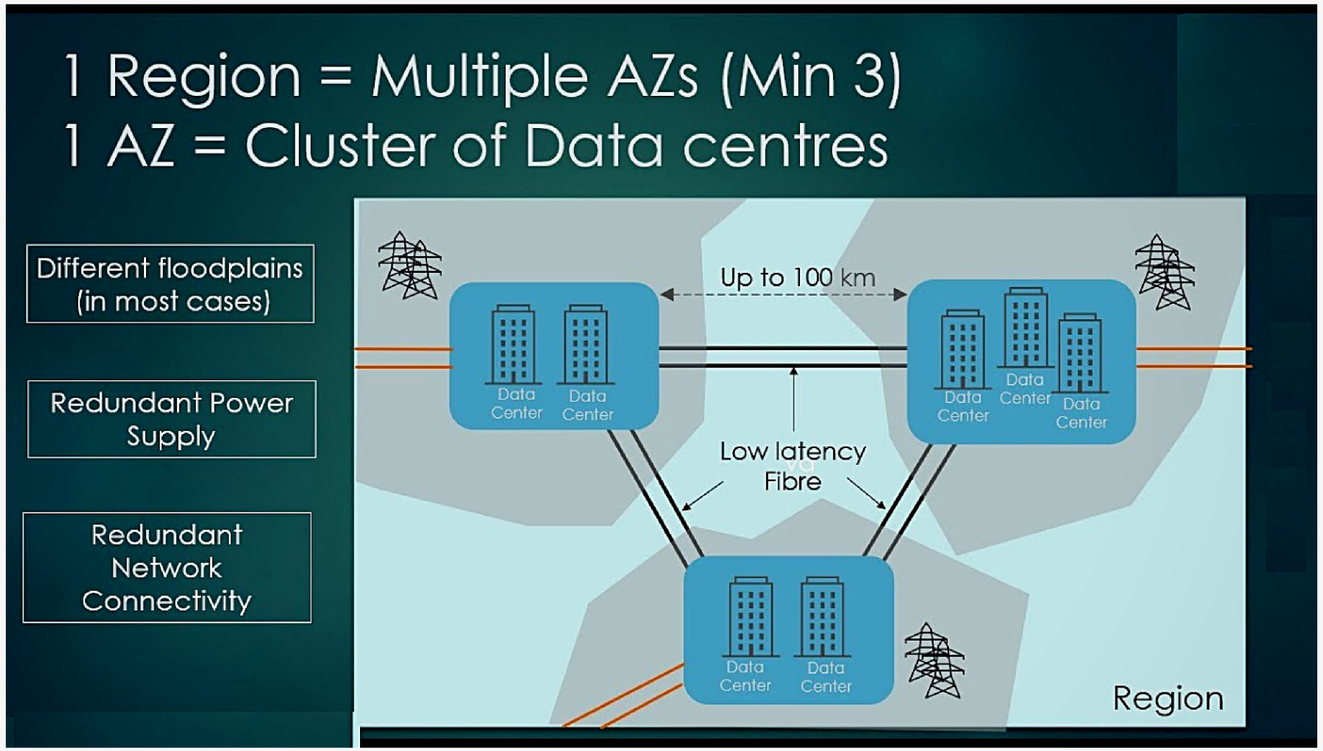
For ultralow latency applications

230+ Points of Presence

218+ Edge Locations and
12 Regional Edge Caches

Regions

Coming Soon



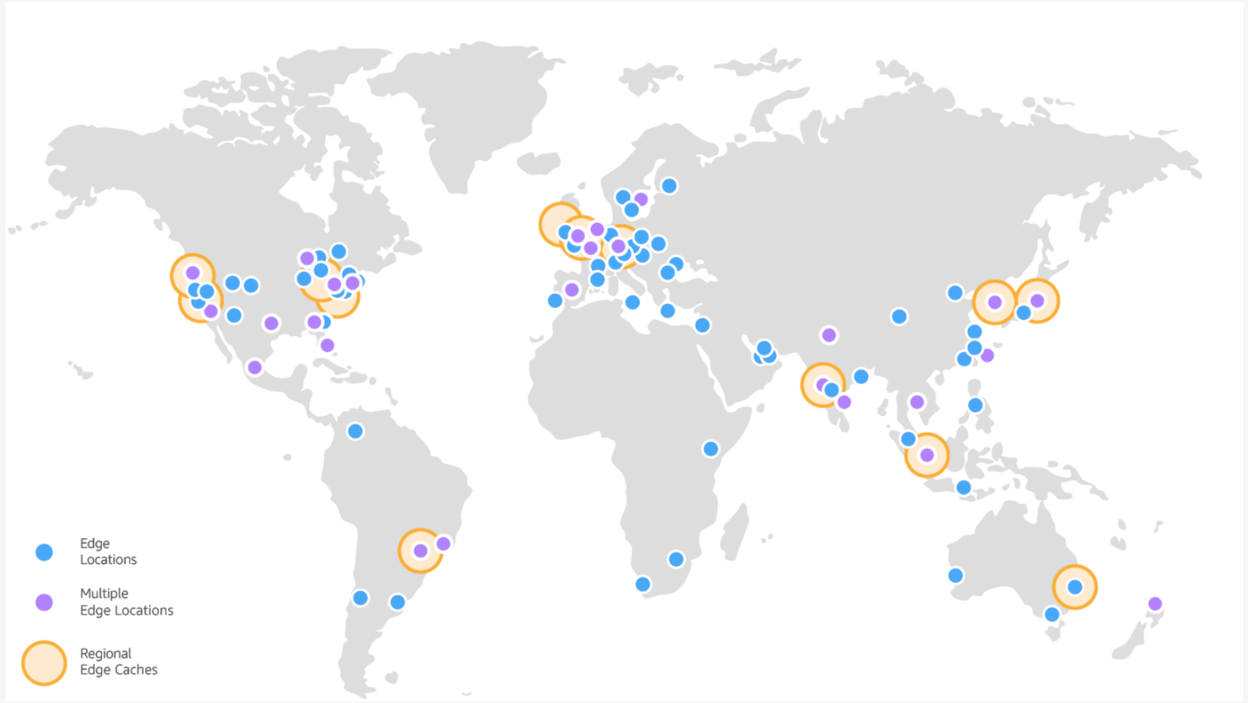
What is Region & Avilability Zones?

AWS has the concept of a **Region**, which is a physical location around the world where they cluster data centers.

They call each group of logical data centers an **Availability Zone**.

Each AWS Region consists of multiple, isolated, and physically separate AZs within a geographic area

To know more click here



What is Edge Locations?

An edge location is where end-users access services located at AWS, the cloud computing division of US-headquartered Amazon. They are located in most of the major cities around the world and are specifically used by CloudFront (CDN) to distribute content to end-users to reduce latency.

To learn more Click Here

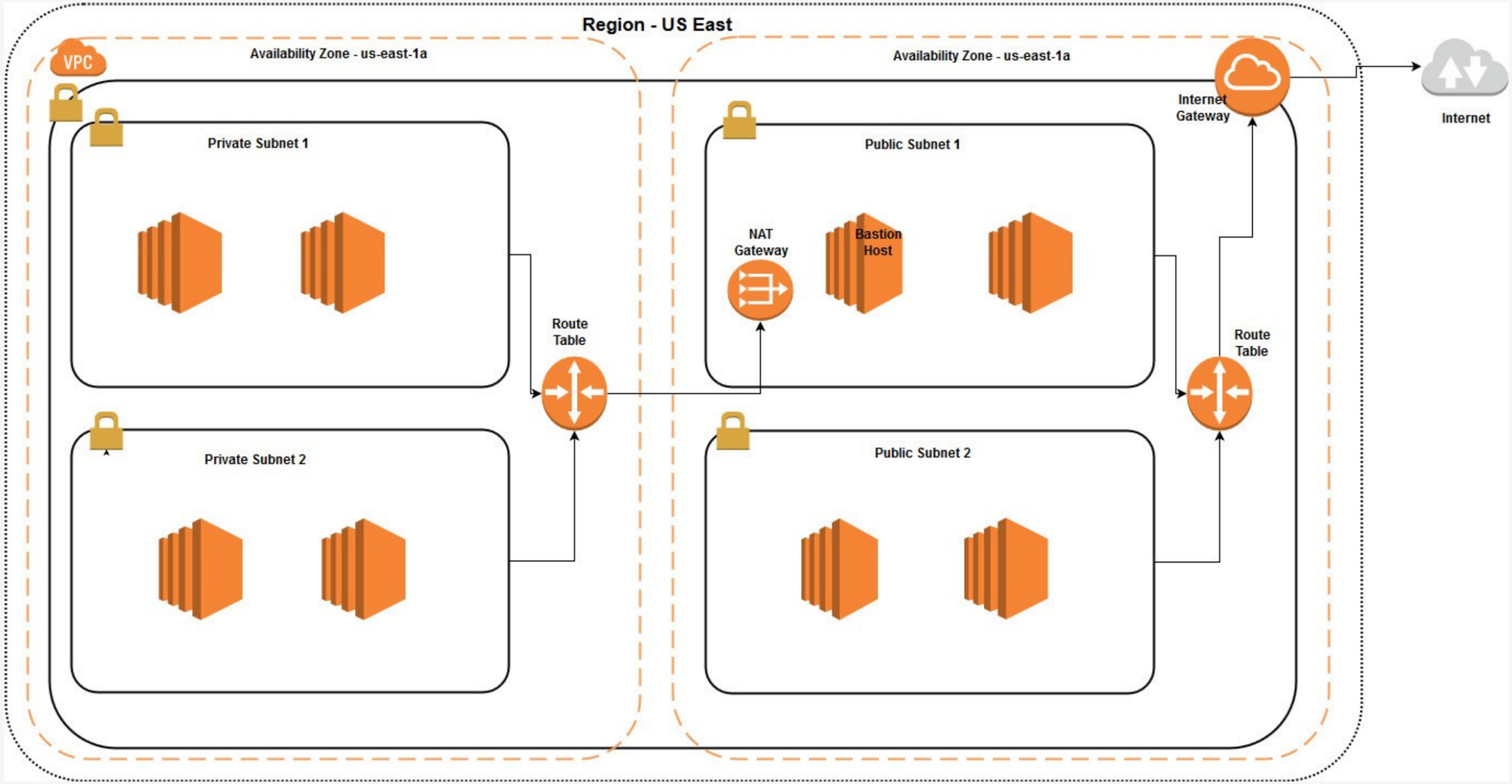
Tip

Edge location > Availability Zones > Regions

Amazon Virtual Private Cloud (VPC)

Build on a logically isolated virtual network in the AWS cloud

Amazon Virtual Private Cloud (Amazon 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 virtual private cloud, helping to ensure secure and easy access to resources and applications.



AWS VPC Benifits

Reachability Analyzer: Reachability Analyzer is a static configuration analysis tool that enables you to analyze and debug network reachability between two resources in your VPC. After you specify the source and destination resources in your VPC, Reachability Analyzer produces hop-by-hop details of the virtual path between them when they are reachable, and identifies the blocking component when they are unreachable. You can learn about how to get started with this feature here.

VPC Flow Logs: You can monitor your VPC flow logs delivered to Amazon S3 or Amazon CloudWatch to gain operational visibility into your network dependencies and traffic patterns, detect anomalies and prevent data leakage, or troubleshoot network connectivity and configuration issues. The enriched metadata in flow logs helps you gain additional insights into who initiated your TCP connections and the actual packet-level source and destination for traffic flowing through intermediate layers such as the NAT Gateway. You can also archive your flow logs to assisst in meeting certain compliance requirements. You can learn about how to get started with this feature here.

VPC Traffic Mirroring: VPC traffic mirroring allows you to copy network traffic from an elastic network interface of Amazon EC2 instances and then send the traffic to out-of-band security and monitoring appliances for deep packet inspection. With VPC traffic mirroring, you can detect network and security anomalies, gain operational insights, implement compliance and security controls, and troubleshoot issues. VPC Traffic Mirroring as a feature that gives you direct access to the network packets flowing through your VPC. You can learn about how to get started with this feature here.

Ingress Routing: This allows you to route all incoming and outgoing traffic flowing to/from an Internet Gateway (IGW) or Virtual Private Gateway (VGW) to a specific EC2 instance’s Elastic Network Interface. With this feature, you can configure your virtual private cloud to send all traffic to an IGW, VGW or EC2 instance before the traffic reaches your business workloads. Learn more about this feature here.

Security Groups: Security groups act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level. When you launch an instance, you can associate it with one or more security groups that you've created. Each instance in your VPC could belong to a different set of security groups. If you don't specify a security group when you launch an instance, the instance is automatically associated with the default security group for the VPC. For more information, see security groups for your VPC.

Network Access Control List: A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC. Click here to read about the specific differences between security groups and network ACLs.

AWS VPC Components

Virtual private cloud (VPC) — A virtual network dedicated to your AWS account.

Subnet — A range of IP addresses in your VPC It is a portion of the network that shares a common address component.
All devices whose addresses have the same prefix are in the same subnet. For example, all those devices whose IP address would start with 172.31.1 would be part of the same subnet. There are two types of subnets. Private Subnet where resources are not exposed to the outside world and Public Subnet where resources are exposed to the internet through Internet Gateway..

Route table — A set of rules, called routes, that are used to determine where network traffic is directed., Route table specifies the destination (IP address) and target (where do want to send the traffic of that destination). The target can be Internet gateway, NAT gateway, Virtual private gateway, VPC peering connection, etc

Internet gateway — A gateway that you attach to your VPC to enable communication between resources in your VPC and the internet.

VPC endpoint — Enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network. For more information, see AWSPrivateLink and VPC endpoints.

CIDR block —Classless Inter-Domain Routing. An internet protocol address allocation and route aggregation methodology. For more information, see Classless Inter-Domain Routing in Wikipedia.

NAT Gateway: Network Address Translation (NAT) Gateway is used when higher bandwidth, availability with lesser administrative effort is required. NAT gateway always resides inside the public subnet of an Availability Zone. It updates the route table of the private subnet such that it sends the traffic to the NAT gateway. Elastic IP must be attached to the NAT gateway while creating. It supports only TCP, UDP, and ICMP protocols.

Elastic IP: It is a static IP address that never changes and is a reserved public IP address that can be assigned to any Instance in a particular region. An elastic IP is reserved for your AWS account and is yours until you release it.

Ref: AWS Documentation

AWS VPC Components

Security Groups: Security groups are a set of firewall rules that controls the traffic for your instance. In Amazon Firewall the only action that can be carried out is allowed. You cannot create a rule to deny. The destination is always the instance on which the service security group is running. You can have a single security group associated with multiple instances.

VPC Peering: A VPC peering connection allows you to route traffic between two Virtual Private Cloud's using IPv4 or IPv6 private addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. A VPC peering connection helps you to facilitate the transfer of data

Network Access Control Lists (NACL): an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC. The default network ACL is configured to allow all traffic to flow in and out of the subnets to which it is associated.

Virtual Private Gateway: A virtual private gateway is the VPN concentrator on the Amazon side of the VPN connection. You create a virtual private gateway and attach it to the VPC from which you want to create the VPN connection.

Customer Gateway: An Amazon VPC VPN connection links your data center (or network) to your Amazon VPC (virtual private cloud). A customer gateway is an anchor on your side of that connection. It can be a physical or software appliance.

Network Interface: Network Interface is a point of connection between a public and a private network. Every instance has a default network interface, called the primary network interface. Network traffic is automatically shifted to the new instance if you move it from one instance to the other.

Ref: AWS Documentation

AWS VPC Cost

AWS Site-to-Site VPN and Accelerated Site-to-Site VPN Connection Pricing:
$0.05 per Site-to-Site VPN connection per hour
Amazon VPC Reachability Analyzer Pricing:
Price per analysis processed by VPC Reachability Analyzer: $0.10
AWS PrivateLink Pricing
Pricing per VPC endpoint per AZ ($/hour) $0.01

Below pricing tiers apply on the total data processed by all Interface Endpoints in an AWS Region:

Data Processed per month in an AWS Region	Pricing per GB of Data Processed ($)
First 1 PB	$0.01
Next 4 PB	$0.006
Anything over 5 PB	$0.004

Gateway Load Balancer Endpoint pricing
Pricing per VPC endpoint per AZ ($/hour): $0.01
Pricing per GB of Data Processed ($): $0.0035

Amazon VPC Traffic Mirroring Pricing: Hourly Price per ENI: $0.015

Ref: AWS Pricing Page

Amazon VPC Ingress Routing
Amazon VPC ingress routing is available in all AWS commercial and AWS GovCloud (US) Regions at no additional cost.
NAT Gateway Pricing:
Price per NAT gateway ($/hour): $0.045
Price per GB data processed ($) : $0.045

Looking forward to meet you all on next session!

Also, thank you for watching this session