AWS Networking Terms from A-Z : ANS Certification.

Document made by BobbySheki /HS

Hi All, I have compiled Networking terms in AWS covering majority of them here. Hope this is useful for those who struggle with remembering services.

A

Access Control List (ACL):

- ACLs are **stateless** security filters applied at the **subnet level** inside a VPC.
- You define explicit **allow or deny rules** for inbound and outbound traffic, which means if you allow inbound on port 80, you must explicitly allow outbound return traffic.
- Useful for broad subnet-level filtering. ACLs are evaluated **before** Security Groups.

Amazon Route 53:

- AWS's highly available and scalable **Domain Name System (DNS)** web service.
- Supports complex routing policies including **latency-based routing** (route users to the region with lowest latency), **geolocation routing**, **failover routing**, and **weighted routing** to split traffic for blue/green deployments.

AWS Direct Connect (DX):

- Dedicated network connection from your data center or office to AWS.
- Offers consistent **low latency** and high throughput (1 Gbps to 100 Gbps links).

- Bypasses the public internet, improving security and performance.
- Supports **Link Aggregation Groups (LAGs)** to combine multiple links for higher bandwidth and failover.

AWS Global Accelerator:

- Provides a fixed set of **Anycast IPs** that route user traffic through AWS's global network to the optimal regional endpoint, reducing latency and improving availability.
- Monitors application health and reroutes traffic around unhealthy endpoints automatically.

AWS Global Infrastructure:

The physical network of AWS Regions and Availability Zones, designed for redundancy and global reach.

Amazon VPC (Virtual Private Cloud):

- **Definition:** A logically isolated section of AWS where you can launch resources in a virtual network.
- **Example:** Creating a VPC with CIDR `10.0.0.0/16` and subnets in two AZs.

AWS Transit Gateway (TGW):

- **Definition:** A hub-and-spoke model for connecting multiple VPCs, VPNs, and Direct Connect.
- **Example:** Attaching 5 VPCs to a TGW for centralized routing.

Active/Active Failover:

A routing configuration where all resources are active simultaneously and share the traffic. If one resource becomes unhealthy, traffic is distributed among the remaining healthy resources.

Example: Using Route 53 with weighted routing or multi-value answer routing to distribute traffic across multiple EC2 instances in different Availability Zones,

where all instances are actively serving requests.

Active/Passive Failover:

A routing configuration where one resource is active (primary) and handles all traffic, while another resource (secondary) is on standby. If the primary becomes unhealthy, traffic is automatically routed to the secondary.

Example: Using Route 53 failover routing policy to direct traffic to a primary ALB in one region and a secondary ALB in a disaster recovery region.

Anycast IP Address:

A network addressing and routing method where data is routed to the "nearest" or "best" destination among multiple possible destinations identified by the same IP address.

Example: AWS Global Accelerator uses Anycast IP addresses as static entry points for your applications, leveraging the AWS global network to route users to the nearest healthy endpoint.

API Gateway:

A fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. While not strictly a networking service, it's often integrated with other networking components for microservices architectures.

Example: An API Gateway endpoint could integrate with a private VPC using a VPC Link to access backend services securely.

***App Mesh*:**

Service mesh that controls service-to-service communication.

Application Load Balancer (ALB):

A Layer 7 (application layer) load balancer that routes traffic based on content of the request (e.g., URL path, host header). It's ideal for HTTP/HTTPS traffic.

Example: Routing `/images` requests to a target group of EC2 instances serving images, and `/api` requests to a different target group of API servers.

Appliance Mode (Transit Gateway):

A Transit Gateway attachment setting that ensures all traffic for a specific connection (e.g., to a centralized inspection VPC with a firewall) goes through a single network interface, preventing asymmetric routing.

Example: Configuring a Transit Gateway attachment to an inspection VPC in appliance mode to force all traffic between spoke VPCs to pass through a Network Firewall in the inspection VPC.

Auto Scaling:

A service that automatically adjusts the number of EC2 instances in your application based on demand, helping maintain application availability and performance. Integrates heavily with load balancers.

Example: An Auto Scaling group launching new EC2 instances in response to increased CPU utilization, and these new instances are automatically registered with an ALB's target group.

Availability Zone (AZ):

A distinct location within an AWS Region that is isolated from failures in other Availability Zones. Multiple AZs provide high availability and fault tolerance.

Example: Deploying your web servers across three Availability Zones within a VPC to ensure that if one AZ experiences an outage, your application remains available.

B

BGP (Border Gateway Protocol):

- Dynamic routing protocol used for exchanging routing information between networks (e.g., between AWS Direct Connect or VPN Gateway and your on-premises router).

- AWS supports **BGP with dynamic route advertisement** for VGW and Direct Connect, enabling automatic route failover.
- Key attributes include **AS Path**, **Local Preference**, and **MED** that influence path selection.

Bandwidth:

- Maximum data transfer rate of a network connection.
- For example, Direct Connect offers 1 Gbps, 10 Gbps, or higher links for predictable throughput.

***Bastion Host*:**

Public instance used to access private resources securely.

Blackhole Route:

- **Definition:** A route where traffic is dropped because the target is invalid.
- **Example:** A route pointing to a deleted NAT Gateway.

Burst Capacity:

- Some AWS services or network interfaces allow temporary **bursts** of traffic above their baseline throughput to accommodate spikes.
- Important to understand for workloads with variable traffic patterns.

C

CIDR (Classless Inter-Domain Routing):

- IP address allocation method defining network ranges with prefixes (e.g., 10.0.0.0/16 means the first 16 bits are network bits, 65,536 addresses).
- CIDR allows flexible subnetting and aggregation of IP blocks.

- AWS VPCs require a CIDR block for IP allocation, and subnet CIDRs must be subsets of the VPC CIDR.

CloudFormation:

An Infrastructure as Code (IaC) service that allows you to define and provision AWS infrastructure deployments using templates.

- **Example:** Using a CloudFormation template to deploy an entire VPC, including subnets, route tables, Internet Gateways, and Security Groups, in a repeatable manner.

CloudFront:

- AWS Content Delivery Network (CDN) that caches content globally at edge locations, reducing latency for end-users.
- Integrates tightly with AWS WAF for application-layer security and supports HTTPS, custom SSL certs.

CloudTrail (AWS CloudTrail):

A service that records API calls and related events made by users, roles, or AWS services. Crucial for auditing and security, including network changes.

- **Example:** Monitoring CloudTrail logs to identify who made changes to your VPC route tables or security group rules.

Cloud WAN:

Centralized global network for multiple AWS regions.

Client VPN:

- Fully managed, elastic VPN service that allows users to connect securely to AWS and on-premises resources.
- Uses TLS (SSL) protocol with certificate-based authentication or Active Directory integration.

Cross-Region Peering:

- Connects VPCs across different AWS Regions privately without using the internet.
- Enables low-latency, high-throughput communication between resources in separate geographic locations.
- Has some limitations (e.g., no transitive routing).

Customer Gateway (CGW): A virtual representation of your on-premises VPN device or router, configured in AWS to establish a Site-to-Site VPN connection.

- **Example:** When setting up a Site-to-Site VPN, you provide AWS with the public IP address of your on-premises router as the Customer Gateway.

D

Default Route:

- Typically represented as `0.0.0.0/0`, meaning **all traffic** not matched by more specific routes.
- Commonly routes traffic to the Internet Gateway for public subnet or NAT Gateway/Instance for private subnets.

Direct Connect (AWS Direct Connect):

A cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Bypasses the public internet, offering higher bandwidth and a more consistent network experience.

Example: Connecting your corporate data center to AWS using a 1 Gbps Direct Connect circuit to handle large data transfers to S3 and low-latency database access in RDS.

Direct Connect Gateway:

- Allows sharing a single Direct Connect connection across multiple VPCs and Regions.

- Simplifies hybrid connectivity architecture, especially in multi-region setups.

DNS (Domain Name System):

- The system for translating human-readable domain names (e.g., www.example.com) into IP addresses computers use.
- Route 53 is AWS's managed DNS service.

DNS Resolver:

A component that performs the lookup process for DNS queries. AWS provides Route 53 Resolver for internal and hybrid DNS resolution.

Example: Configuring Route 53 Resolver inbound endpoints to allow your on-premises DNS servers to resolve private hosted zone records in your VPC.

***DHCP Options Set* :**

Set domain name, DNS servers in a VPC. These are collections of DHCP configuration options that you can create and associate with your VPCs.

DDoS (Distributed Denial of Service):

- Attack where multiple sources flood a network or service to exhaust resources.
- AWS Shield Standard protects all customers at the network and transport layers, with Shield Advanced offering additional detection, mitigation, and cost protection.

E

Edge Location:

A location used by AWS for content delivery and caching, separate from Availability Zones and Regions.

Egress-Only Internet Gateway (Egress-Only IGW):

A gateway that allows outbound-only communication over IPv6 from instances in your VPC to the internet.

Example: Allowing an EC2 instance in a private subnet with an IPv6 address to initiate connections to the internet (e.g., for software updates) but preventing unsolicited inbound connections.

Elastic IP Address (EIP):

A static, public IPv4 address that you can allocate to your AWS account and associate with an EC2 instance or network interface.

Example: Assigning an EIP to a NAT Gateway in a public subnet to provide a consistent public IP address for outbound traffic from private subnets.

Elastic Network Interface (ENI)

- **Definition:** Virtual network card for EC2 instances.
- **Example:** Attaching a secondary ENI for failover.

Enhanced Networking (ENA/SR-IOV)

- **Definition:** High-performance networking for EC2 (up to 100 Gbps).
- **Example:** Using `c5n.18xlarge` with ENA for low latency

Elastic Load Balancer (ELB):

- Distributes incoming application traffic across multiple targets (EC2 instances, containers, IP addresses).
- Types:
  - **ALB (Application Load Balancer):** Operates at Layer 7, supports HTTP/S, WebSockets, path-based routing.

- **NLB (Network Load Balancer):** Operates at Layer 4, handles millions of requests per second with ultra-low latency and static IPs.
- **CLB (Classic Load Balancer):** Legacy, less feature-rich.

Endpoint (VPC Endpoint):

- Enables private connections from your VPC to AWS services without using internet gateways or NAT.
- Types: **Interface endpoints** (powered by PrivateLink, use ENIs) and **Gateway endpoints** (for S3 and DynamoDB).

Encapsulation:

The process of wrapping data with headers and footers to facilitate network transmission. Important for VPNs (IPsec) and Transit Gateway Connect (GRE).

Example: IPsec VPN tunnels encapsulate IP packets within another IP header for secure transmission over the public internet.

ECMP (Equal-Cost Multi-Path):

- Allows traffic to be load-balanced across multiple paths with the same routing cost, improving redundancy and throughput.
- Supported by AWS Transit Gateway and BGP.

F

Failover Routing Policy (Route 53): Routes traffic to a healthy primary resource, or to a secondary resource if the primary becomes unhealthy.

Example: Routing users to your main application deployment in `us-east-1`, but automatically switching to a disaster recovery site in `us-west-2` if `us-east-1` experiences an outage.

Fargate:

Networking managed via task-level ENIs.

Fully Qualified Domain Name (FQDN):

The complete domain name for a specific host or computer on the internet, including the hostname and the domain name.

Example: `www.example.com` is an FQDN, where `www` is the hostname and `example.com` is the domain name.

Firewall:

- Security device or service controlling inbound/outbound traffic based on rules.
- AWS firewall layers include:
  - Security Groups (stateful)
  - Network ACLs (stateless)
  - AWS Network Firewall (managed, Suricata-based)
  - WAF (Web Application Firewall) for HTTP/S traffic.

Firewall Manager

- **Definition:** Central security policy management for AWS.
- **Example:** Enforcing WAF rules across multiple accounts.

Flow Logs:

- Capture metadata about IP traffic flowing to/from network interfaces, stored in CloudWatch Logs or S3.
- Critical for troubleshooting, compliance, and security analysis.

G

Gateway:

- Network device that routes traffic between different networks.
- Examples in AWS:
  - **Internet Gateway (IGW):** For VPC-to-Internet traffic.
  - **Virtual Private Gateway (VGW):** For VPN or Direct Connect attachments.

Global Network:

- AWS's global backbone connecting Regions, Availability Zones, and edge locations with fiber-optic cables and redundant paths.

Global Accelerator

- **Definition:** Improves performance using AWS edge locations.
- **Example:** Routing traffic to the nearest ALB endpoint.

Gateway Load Balancer (GWLB)

- **Definition:** Distributes traffic to third-party security appliances.
- **Example:** Inspecting traffic via a Palo Alto VM.

GENEVE (Generic Network Virtualization Encapsulation):

A tunneling protocol used by GWLB to encapsulate traffic between the load balancer and virtual appliances.

Example: GWLB uses GENEVE to send traffic to your firewall appliance and receive it back after inspection, maintaining the original packet information.

Geolocation Routing Policy (Route 53):

Routes traffic to resources based on the geographic location of your users.

Example: Directing users from Europe to a server located in the `eu-west-1` region, and users from North America to `us-east-1`.

Geo Proximity Routing Policy (Route 53):

Routes traffic to your resources based on the geographic location of your users and your resources, with the ability to bias traffic towards a specific region or away from it.

Example: Routing users to the closest data center but, during a maintenance window, shifting a percentage of traffic from one region to another.

GRE (Generic Routing Encapsulation):

A tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork. Used by Transit Gateway Connect.

Example: Transit Gateway Connect attachments use GRE tunnels to connect to SD-WAN appliances, simplifying routing and increasing bandwidth compared to multiple IPsec tunnels.

H

Hybrid Network:

- Architecture that connects on-premises networks with AWS via VPN or Direct Connect, allowing resources in both environments to communicate securely.

Hosted Connection:

- Direct Connect connections provisioned through AWS partners that resell dedicated connectivity, typically with lower bandwidth options.

Health Checks (Route 53, ELB):

Mechanisms to monitor the health and availability of your resources.

Example: An ALB continuously performs health checks on its registered EC2 instances, and if an instance fails a check, the ALB stops sending traffic to it.

Hosted Connection (Direct Connect):

A type of Direct Connect connection provided by an AWS Direct Connect Partner. You work with the partner to provision a connection on their existing Direct Connect infrastructure.

Example: You have a smaller bandwidth requirement (e.g., 50 Mbps) and your colocation facility is a Direct Connect partner; you can request a hosted connection through them.

Hosted Zone (Route 53):

A container for records that defines how you want to route traffic for a domain and its subdomains. Can be public or private.

Example: Creating a public hosted zone for `example.com` to manage DNS records for your public website, and a private hosted zone for `internal.example.com` to manage internal application DNS.

Hybrid Cloud:

An IT infrastructure environment that combines and integrates on-premises data centers with cloud resources (e.g., AWS).

Example: Extending your corporate network to AWS using Direct Connect and Site-to-Site VPN, allowing applications in your VPC to access databases on-premises.

I

Internet Gateway (IGW):

- Allows communication between instances in a VPC and the internet.
- Enables public IPv4 traffic and serves as a target for default routes.

Instance Profile:

A container for an IAM role that you can attach to an EC2 instance, allowing applications running on the instance to securely make API calls to AWS services.

Example: An EC2 instance needing to write VPC Flow Logs to an S3 bucket would have an instance profile attached with an IAM role granting S3 write permissions.

IPSec:

- A protocol suite for securing IP communications by authenticating and encrypting each IP packet in a data stream.
- Used in AWS VPNs for encrypting traffic between on-premises and AWS.

Ingress:

- Traffic **entering** a network interface, subnet, or instance.

IPAM (IP Address Manager):

An AWS service that makes it easier for you to plan, track, and monitor IP addresses for your AWS workloads.

Example: Using IPAM to centrally manage IP address allocations across multiple VPCs in different accounts, preventing CIDR overlaps and streamlining IP planning.

J

Jumbo Frames

- **Definition:** Ethernet frames > 1500 MTU (AWS supports 9001 MTU).
- **Example:** Enabling jumbo frames for high-throughput workloads.

K

Key Pair

- **Definition:** SSH key for EC2 instance access.
- **Example:** Using `my-key.pem` to log into a Linux instance.

L

Latency:

- The time delay for a packet to travel from source to destination, critical for user experience and application responsiveness.

Latency-Based Routing Policy (Route 53):

Routes traffic to the region that provides the lowest latency for the user.

Example: For a global application, Route 53 directs a user in London to your server in `eu-west-2` (closest and lowest latency) rather than a server in `us-east-1`.

Link Aggregation Group (LAG):

- Combines multiple physical Direct Connect links into one logical link, increasing bandwidth and providing redundancy.

Local Preference (BGP):

A BGP attribute used to influence outbound routing decisions. A higher local preference value means a route is preferred.

Example: In a dual Direct Connect setup, setting a higher local preference on one DX connection to prefer it for outbound traffic.

M

MAC Address:

ENIs have AWS-assigned MACs.

Managed Prefix List:

A collection of one or more CIDR blocks that you can use to simplify the configuration of your security groups and route tables.

Example: Creating a managed prefix list containing the IP ranges of your corporate offices and then referencing this list in multiple security groups instead of individual CIDRs.

Multicast:

- Network transmission method sending a packet to multiple receivers simultaneously.
- AWS Transit Gateway supports multicast for applications requiring this communication style.

Multi-Value Answer Routing Policy (Route 53):

Returns up to eight healthy records to DNS queries, allowing clients to randomly select an IP address. Does not inherently provide health checks unless used with Route 53 health checks.

Example: Returning multiple healthy IP addresses for a web server, allowing the client's resolver to choose one randomly for simple load distribution.

Multi-AZ Deployment

- **Definition:** High-availability across Availability Zones.
- **Example:** RDS with standby replica in another AZ.

MTU (Maximum Transmission Unit):

The largest size of a network layer packet that can be transmitted in a single frame across a network link. Jumbo frames (MTU > 1500) are important for performance.

Example: EC2 instances typically have an MTU of 9001 (jumbo frames) within a VPC to allow for larger packet sizes and reduce overhead.

Monitoring:

- Observability services like CloudWatch, VPC Flow Logs, and Traffic Mirroring enable performance tracking and troubleshooting.

N

NAT Gateway:

- Managed AWS service providing **Network Address Translation** to enable instances in private subnets to access the internet without exposing inbound traffic.

NACL (Network Access Control List):

- Stateless subnet-level firewall with explicit allow/deny rules for inbound and outbound traffic.

Network Firewall (AWS Network Firewall):

A fully managed firewall service for your VPCs, offering stateful and stateless inspection, intrusion prevention, and web filtering.

Example: Deploying AWS Network Firewall in an inspection VPC to centrally enforce security policies, block malicious traffic, and filter URLs for all traffic flowing between VPCs via Transit Gateway.

Network Load Balancer (NLB):

A Layer 4 (transport layer) load balancer that handles millions of requests per second with extremely low latency. Supports TCP, UDP, and TLS traffic.

Example: Distributing high-throughput, low-latency traffic for gaming servers or real-time applications where static IP addresses are required.

Network Manager (AWS Network Manager):

A service that provides a central operational dashboard for your global network across AWS and on-premises environments, offering visibility and monitoring of Transit Gateways and their connections.

Example: Using Network Manager to visualize your global network topology, monitor performance of Direct Connect and VPN connections, and quickly identify routing issues.

O

- ***Outposts*: AWS infrastructure on-prem.**
- ***Outbound Rules*: SGs/NACLs define allowed egress traffic.**
- ***Overlay Networks*: Often built using VPN/IPSec tunnels.**

Overlapping CIDR

- **Definition:** Two networks with the same IP range.
- **Example:** VPC peering fails due to `10.0.0.0/16` overlap.

Overlay Network:

- Virtual network built on top of physical networks to provide isolation and segmentation, e.g., VPC Peering or Transit Gateway connectivity.

On-Premises:

- Refers to local infrastructure or datacenter equipment outside of AWS.

P

Peering (VPC Peering):

- Private networking connection between two VPCs enabling direct routing without using gateways, VPNs, or the internet.

PrivateLink:

- AWS technology enabling private connectivity between VPCs, AWS services, and customer-owned applications without traversing the public internet.

Private Hosted Zone (Route 53):

A container for records that defines how you want to route traffic for a domain and its subdomains within your VPCs.

Example: Creating a private hosted zone for `mycorp.internal` to resolve internal service names (e.g., `database.mycorp.internal`) within your VPCs without exposing them to the public internet.

Private Subnet:

A subnet whose routing table does not have a route to an Internet Gateway, meaning instances in it cannot directly access the internet.

Example: Placing your database servers in a private subnet to ensure they are not directly accessible from the internet.

Proxy Protocol: A protocol that provides connection information (like client IP address and port) from a load balancer to the backend instance.

Example: An NLB using Proxy Protocol to pass the client's original IP address to the backend EC2 instance, which is useful for logging and security.

Public Hosted Zone (Route 53): A container for records that defines how you want to route traffic for a domain and its subdomains on the public internet.

Example: Managing the DNS records for your public website, `www.example.com`, so that users can reach it from anywhere on the internet.

Public Subnet: A subnet whose routing table has a route to an Internet Gateway, allowing instances in it to send and receive traffic from the internet.

Example: Placing your public-facing web servers or load balancers in a public subnet.

Prefix List

- **Definition:** Group of CIDRs for security group rules.
- **Example:** Allowing only corporate IPs via a prefix list.

Q

- ***QoS*:** Not natively implemented but possible via traffic shaping.
- ***Quick Connect*:** Service connector via Connect contact center.

Query Logging (Route 53)

- **Definition:** Logs DNS queries for analysis / Auditing DNS requests in CloudWatch Logs.

R

Reachability Analyzer:

A network diagnostics tool that enables you to determine reachability between resources in your VPCs. It analyzes your network configurations to help identify network connectivity issues.

Example: Using Reachability Analyzer to confirm that an EC2 instance can reach a database in a different subnet, identifying any blocking security groups or route table entries.

Region (AWS Region):

A geographical area where AWS clusters its data centers. Each region consists of multiple Availability Zones.

Example: Deploying your application in the `us-east-1` (N. Virginia) region.

Resource Access Manager (RAM) (AWS RAM):

A service that enables you to easily and securely share your AWS resources with any AWS account or within your AWS Organization.

Example: Sharing a Transit Gateway, Private Hosted Zone, or a subnet with other accounts in your AWS Organization.

Route 53 (Amazon Route 53): A highly available and scalable cloud Domain Name System (DNS) web service.

Example: Configuring DNS records for your public and private domains, setting up health checks, and implementing various routing policies.

Route Table:

- A set of rules, called routes, that determine where network traffic is directed.

Route Propagation:

- The automatic addition of routes learned from a VPN or Direct Connect gateway into a route table.

Redundancy:

- Duplication of critical network components or paths to ensure availability in case of failure.

Relational Database Service (RDS):

A managed service for setting up, operating, and scaling a relational database in the cloud.

S

Service Endpoint: Same as **VPC Endpoint**.

Shared Responsibility Model:

A framework that defines the security responsibilities between AWS and the customer. AWS is responsible for "security of the cloud," and the customer is responsible for "security in the cloud."

Example: AWS is responsible for the physical security of data centers, while you are responsible for configuring your Security Groups and NACLs correctly.

Shared VPC (VPC Sharing):

A feature that allows multiple AWS accounts to create their application resources (e.g., EC2 instances, RDS databases) in shared, centrally managed VPCs.

Example: A central networking account owns the VPCs, and application teams in other accounts can deploy their resources into those shared VPCs, simplifying network management.

Shield (AWS Shield):

A managed Distributed Denial of Service (DDoS) protection service. Standard is free and automatically protects against common layer 3/4 attacks. Advanced provides more sophisticated protection.

Example: AWS Shield Advanced protecting your public-facing application (behind an ALB or CloudFront) from large-scale DDoS attacks.

Site-to-Site VPN (AWS Site-to-Site VPN):

A service that creates an encrypted IPsec VPN connection between your on-premises network and your VPCs or Transit Gateways over the public internet.

Example: Connecting your small branch office to your VPC using a Site-to-Site VPN for secure access to cloud resources.

Subnet:

A logical subdivision of an IP network. In AWS, subnets are associated with a single Availability Zone.

Example: Creating a public subnet for web servers and a private subnet for databases within your VPC.

Security Group:

- Stateful firewall associated with EC2 instances or ENIs, controlling inbound and outbound traffic.

Single AZ :

A deployment strategy that provides high availability within a single Availability Zone.

Site-to-Site VPN:

- Encrypted VPN connection over the internet between on-premises network and AWS VPC.

T

Target Group (ELB):

A logical grouping of targets (e.g., EC2 instances, IP addresses, Lambda functions) that an Elastic Load Balancer routes traffic to.

Example: An ALB target group configured to send HTTP traffic to a set of healthy web server instances.

***TGW Route Table*:**

Controls routing between attachments.

***TTL*: Time to Live**

DNS record expiration time.

Traffic Mirroring (VPC Traffic Mirroring):

A feature that allows you to capture and inspect network traffic from an Elastic Network Interface (ENI) of an EC2 instance.

Example: Mirroring traffic from a specific web server instance to a security appliance for deep packet inspection and threat analysis.

Traffic Policy (Route 53):

A complex routing configuration in Route 53 that allows you to combine various routing policies and health checks into a single, comprehensive routing solution.

Example: Creating a traffic policy that routes users based on geolocation, but then applies weighted routing within each geographic region, and also includes failover to a disaster recovery site.

Transit Gateway (TGW):

AWS-managed router connecting multiple VPCs, VPNs, and Direct Connect gateways, enabling scalable network architectures.

Transit Gateway Connect:

A feature of AWS Transit Gateway that allows native integration of Software-Defined Wide Area Network (SD-WAN) appliances into AWS using GRE tunnels and BGP.

Example: Integrating your Cisco SD-WAN solution with AWS via Transit Gateway Connect to extend your SD-WAN fabric into the cloud with simplified routing.

Transit Virtual Interface (VIF) (Direct Connect):

A type of virtual interface used with Direct Connect to connect to a Direct Connect Gateway, which then allows connectivity to Transit Gateways across multiple VPCs and regions.

Example: Establishing a Transit VIF over your Direct Connect connection to link your on-premises network to your Transit Gateway.

Tunnel (VPN):

An encrypted communication path over a public network. Site-to-Site VPN connections consist of two redundant tunnels.

Example: Your Site-to-Site VPN connection has two IPsec tunnels for high availability.

TLS (Transport Layer Security):

Cryptographic protocol that provides end-to-end security for internet communications (e.g., HTTPS, Client VPN).

TCP Keepalive -

it basically involves **sending empty packages over the otherwise idle connections and check that there will be ACK -packages coming in return - and the connection will be shut down after a failover**

Traceroute

- **Definition:** Diagnoses network path issues.
- **Example:** `traceroute 8.8.8.8` to check connectivity.

Traffic Mirroring:

Duplicates network traffic from EC2 ENIs to monitoring and analysis tools for troubleshooting or security.

U

UDP (User Datagram Protocol):

- Connectionless transport layer protocol, often used by VPNs and real-time applications.

Uplink:

- Physical or logical connection between a local network and a broader network or service provider.

Underlay : Physical AWS infrastructure.

V

VPC (Virtual Private Cloud):

- Isolated virtual network in AWS with configurable IP addressing, routing, and security.

Virtual Private Gateway (VGW):

- AWS-managed VPN concentrator on the AWS side of a VPN connection.

VPC Endpoint:

- Enables private connectivity to AWS services without traversing the public internet.

VPC Peering:

- Direct network routing between two VPCs in the same or different AWS accounts/regions.

VPC Lattice: Manage communication between services.

W

WAF (Web Application Firewall):

- Protects web applications from common attacks like SQL injection, XSS by filtering HTTP/S traffic.

Wildcard:

- Symbol used in routing/security rules to match multiple IPs or domains (e.g., `.example.com`).

Weighted Routing Policy (Route 53):

Routes traffic to multiple resources in proportions that you specify.

Example: Sending 90% of traffic to your production environment and 10% to a new version of your application for A/B testing.

X

- ***X.509*: Certificates used in VPN and SSL.**
- ***XML*: Legacy policy format in some contexts.**

X-Forwarded-For Header

- **Definition:** Identifies client IP in ALB logs.
- **Example:** Logging user IPs for analytics.

Y

- ***YAML*: Used in IaC like CloudFormation, CDK.**
- ***YubiKeys*: Used for MFA in IAM login.**

Z

- ***Zone Awareness*: Distribute resources across AZs.**
- ***Zonal Subnet*: Subnet resides in one AZ.**
- ***ZTP*: Not native, but can be scripted for network appliances.**