Network

Đà Nẵng, năm COVID thứ 2

Virtual Private Cloud (VPC)

- A virtual network for your account inside the AWS Cloud.

CIDR block:

- Can have a mask from /16 to /28.

Subnets:

- A subnet resides in only one Availability Zone.
- AWS reserves 5 IP addresses per Subnet (first 4 and last 1).
- Automatic routing between subnets inside a VPC.

Sharing VPC/Subnets:

- VPC sharing allows multiple AWS accounts to create their resources into shared, centrally-managed VPCs.
- In this model, the account that owns the VPC (owner) shares one or more subnets with other accounts (participants) that belong to the same organization from AWS Organizations.
- After a subnet is shared:
  - Participants can view, create, modify, and delete their application resources in the subnets shared with them.
  - Participants cannot view, modify, or delete resources that belong to other participants or the VPC owner.
- You must enable resource sharing from the management account for your organization.
- You cannot share:
  - default subnets,
  - any subnets in the default VPC.

VPC Security Groups:

- Ingress & egress, stateful firewall.
- By default, a security group includes an outbound rule that allows all outbound traffic. Network Access Control List (NACL):
- Source/dest and protocol filtering, Stateless.
- Applied at the subnet level,
- Rules can be allow or deny.
- Rules are numbered (have an order).
- Default Network ACL:
  - Your VPC automatically comes with a modifiable default network ACL.
  - By default, it allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic.

Route table:

- A VPC has a default route table (Main route table) but you can add other route tables (Custom tables).
- The most specific route wins.

Internet Gateway (IGW):

- A resource to enable a VPC to connect to internet.

Egress-only Internet Gateway (EIGW):

- Stateful egress-only IPv6-only gateway.
- Allows outbound communication over IPv6 from instances in your VPC to the internet, and prevents the internet from initiating an IPv6 connection with your instances.

NAT Gateway:

- A service managed by Amazon,

NAT Instance:

- You create and manage the instance and NAT software.
- You need to disable Source/Destination check on the network interface.

VPC Endpoint (VPCE):

- Enables you to access an AWS service (like S3) or a VPC Endpoint Service directly from your VPC without going out through the Internet and an Internet Gateway. AWS PrivateLink:
- A technology that enables you to privately access services by using private IP addresses.
- A "VPC Endpoint Service" is a service hosted by another AWS customer or Partner in their own VPC. VPC Endpoint Types:
- Interface endpoint:
  - an elastic network interface.
- Gateway endpoint:
  - Only two supported AWS services: Amazon S3 and DynamoDB.
  - Route tables control the routing of traffic between your VPC and the target service.

VPC Peering:

- Enables direct VPC to VPC communications without going out to Internet.
- Not transitive.

AWS Site-to-Site VPN:

- The AWS side of a VPN connection can be either a Virtual Private Gateway (only one VPC) or a Transit Gateway.
- A virtual private gateway is one of the VPN concentrator types on the Amazon side of the Site-to-Site VPN connection.

Virtual Private Gateway (VGW):

- A virtual private gateway is one of the VPN concentrator types on the Amazon side of the Site-to-Site VPN connection.
- You create a virtual private gateway and attach it to the VPC from which you want to create the Site-to-Site VPN connection.

Transit Gateway (TGW):

- Acts as a Regional virtual router for traffic flowing between your VPCs and on-premises networks.

Direct Connect (DX):

- links your internal network to an AWS Direct Connect location over a standard Ethernet fiber-optic cable (LX, LR or LR4).
- One end of the cable is connected to your router or the APN partner router in DX location, the other end of the cable is connected to an AWS Direct Connect router.

VPC Flow Logs:

- A feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC.
- Flow log data can be published to Amazon CloudWatch Logs or Amazon S3.