VPC & Networking

Sunday, February 11, 2024 6:39 PM

IP Addresses in AWS:

* IPv4 - Internet Protocol version 4
* Public IPv4 - Every time you stop the EC2 & start again, you get a new address.
* Private: A fixed address used within our network.
* Elastic IP: allows you to attach a fixed public IPV4 address to EC2.
* IPv6: Every IP address is public.

VPC & Subnets Primer:

* VPC - Virtual Private Cloud: Private network to deploy your resources
* Subnets allow you to partition your network inside your VPC.
* Public Subnet - Accessible from internet
* Private Subnet - Vice versa.
* Route Tables are used to define access to the internet and between subnets

Internet Gateways:

* Helps our VPC instances / subnets connect with the internet.
* Public subnets have a route to Internet Gateway.

NAT Gateway:

* It allows your private subnets' instances to connect with the internet.
* It creates a route & intermediate between private subnet & Internet Gateway.

Network ACL & Security Groups:

* NACL is a firewall that controls in/out at subnet level
* Can have allow & Deny Rules
* Security Groups control at EC2 instance level
* Can only have allow rules.

VPC Flow Logs:

* Capture information about IP traffic going into your interfaces.
  - VPC Flow Logs
  - Subnet Flow Logs
  - Elastic Network Interface Flow Logs
* Helps to monitor & troubleshoot connectivity issues

VPC Peering:

* Connect two VPC, privately using AWS network
* Make them behave as if they were in the same network

VPC Endpoint:

* Endpoints allows you to connect your AWS service using a private network instead of public network.
* Enhanced security
* VPC Endpoint Gateway: S3 & DynamoDB
* VPC Endpoint Interface: Rest.

AWS Private Link:

* Most secure & scalable way to expose a service to 1000's of VPCs.
* Does not require VPC peering, internet gateway, NAT and route tables.
* Requires a network load balancer & ENI (customer VPC).

Site to Site VPN & Direct connect:

* Connect an on-premises VPN to AWS
* Connection is encrypted & goes over public network - Customer Gateway
* Direct Connect (DX) is a physical connection between on-premises & AWS
* Goes over a private network and fast.

AWS Client VPN:

* Connect from your computer using Open VPN to your private network.

Transit Gateway:

* Hub & spoke connection to 1000s of VPC's to avoid a mess of many connections