AWS Certification – Networking Services – Cheat Sheet

VPC

- helps define a logically isolated dedicated virtual network within the AWS
- provides control of IP addressing using CIDR block from a minimum of /28 to maximum of /16 block size
- Components
  - Internet gateway (IGW) provides access to the Internet
  - Virtual gateway (VGW) provides access to on-premises data center through VPN and Direct Connect connections
  - VPC can have only one IGW and VGW
  - Route tables determine where network traffic from subnet is directed
  - Ability to create subnet with VPC CIDR block
  - A Network Address Translation (NAT) server provides outbound Internet access for EC2 instances in private subnets
  - Elastic IP addresses are static, persistent public IP addresses
  - Instances launched in the VPC will have a Private IP address and can have a Public or a Elastic IP address associated with it
  - Security Groups and NACLs help define security

    - Flow logs – Capture information about the IP traffic going to and from network interfaces in your VPC
- allows Tenancy option for instances
    - shared, by default, allows instances to be launched on shared tenancy
    - dedicated allows instances to be launched on a dedicated hardware
- NAT
    - allows internet access to instances in private subnet
    - performs the function of both address translation and port address translation (PAT)
    - needs source/destination check flag to be disabled as it is not actual destination of the traffic
    - NAT gateway is a AWS managed NAT service that provides better availability, higher bandwidth, and requires less administrative effort
- Route Tables
    - defines rules, termed as routes, which determine where network traffic from the subnet would be routed
    - Each VPC has a Main Route table, and can have multiple custom route tables created
    - Every route table contains a local route that enables communication within a VPC which cannot be modified or deleted
    - Route priority is decided by matching the most specific route in the route table that matches the traffic
- Subnets
    - map to AZs and do not span across AZs

        - have a CIDR range that is a portion of the whole VPC.
        - CIDR ranges cannot overlap between subnets within the VPC.
        - AWS reserves 5 IP addresses in each subnet – first 4 and last one
        - Each subnet is associated with a route table which define its behavior
            - Public subnets – inbound/outbound Internet connectivity via IGW
            - Private subnets – outbound Internet connectivity via an NAT or VGW
            - Protected subnets – no outbound connectivity and used for regulated workloads
- Elastic Network Interface (ENI)
        - a default ENI, eth0, is attached to an instance which cannot be detached with one or more secondary detachable ENIs (eth1-ethn)
        - has primary private, one or more secondary private, public, Elastic IP address, security groups, MAC address and source/destination check flag attributes associated
        - AN ENI in one subnet can be attached to an instance in the same or another subnet, in the same AZ and the same VPC
        - Security group membership of an ENI can be changed
        - with pre allocated Mac Address can be used for applications with special licensing requirements
- Security Groups vs Network Access Control Lists

    - Stateful vs Stateless
    - At instance level vs At subnet level
    - Only allows Allow rule vs Allows both Allow and Deny rules
    - Evaluated as a Whole vs Evaluated in defined Order
- Elastic IP
    - is a static IP address designed for dynamic cloud computing.
    - is associated with AWS account, and not a particular instance
    - can be remapped from one instance to an other instance
    - is charged for non usage, if not linked for any instance or instance associated is in stopped state
- VPC Peering
    - allows routing of traffic between the peer VPCs using private IP addresses and no IGW or VGW required
    - No single point of failure and bandwidth bottlenecks
    - cannot span across regions
    - IP space or CIDR blocks cannot overlap
    - cannot be transitive, one-to-one relationship between two VPC
    - Only one between any two VPCs and have to be explicitly peered
    - Private DNS values cannot be resolved
    - Security groups from peered VPC cannot be referred for ingress and egress rules in security group, use CIDR block instead

- VPC Endpoints
    - enables creation of a private connection between VPC and another AWS service (currently only S3) using its private IP address
    - does not require a public IP address, access over the Internet, NAT device, a VPN connection or AWS Direct Connect
    - traffic between VPC & AWS service does not leave the Amazon network
    - do not support cross-region requests
    - cannot be extended out of a VPC i.e. resources across the VPN, VPC peering, AWS Direct Connect connection cannot use the endpoint

Direct Connect & VPN

- VPN
    - provide secure IPSec connections from on-premise computers or services to AWS over the Internet
    - is quick to setup, is cheap however it depends on the Internet speed
- Direct Connect
    - is a network service that provides an alternative to using Internet to utilize AWS services by using private dedicated network connection
    - provides Virtual Interfaces
        - Private VIF to access instances within an VPC via VGW
        - Public VIF to access non VPC services
    - requires time to setup probably months, and should

    - not be considered as an option if turnaround time is less
    - does not provide redundancy, use either second direct connection or IPSec VPN connection
    - Virtual Private Gateway is on the AWS side and Customer Gateway is on the Customer side
    - route propagation is enabled on VGW and not on CGW
- Direct Connect vs VPN IPSec
    - Expensive to Setup and Takes time vs Cheap & Immediate
    - Dedicated private connections vs Internet
    - Reduced data transfer rate vs Internet data transfer cost
    - Consistent performance vs Internet inherent variability
    - Do not provide Redundancy vs Provides Redundancy

Route 53

- Highly available and scalable DNS & Domain Registration Service
- Reliable and cost-effective way to route end users to Internet applications
- Supports multi-region and backup architectures for High availability. ELB , limited to region, does not support multi region HA architecture
- supports private Intranet facing DNS service
- internal resource record sets only work for requests originating from within the VPC and currently cannot extend to on-premise

- Global propagation of any changes made to the DN records within ~ 1min
- Route 53 to create an alias resource record set that points to ELB, S3, CloudFront. An alias resource record set is an Route 53 extension to DNS. It’s similar to a CNAME resource record set, but supports both for root domain – zone apex *e.g. example.com*, and for subdomains for e.g. *www.example.com*.
- CNAME resource record sets can be created only for subdomains and cannot be mapped to the zone apex record
- Routing policy
  - Simple routing – simple round robin policy
  - Weighted round robin – assign weights to resource records sets to specify the proportion *for e.g. 80%: 20%*
  - Latency based routing – helps improve global applications as request are sent to server from the location with minimal latency, is based on the latency and cannot guarantee users from the same geographic will be served from the same location for any compliance reasons
  - Geolocation routing – Specify geographic locations by continent, country, state limited to US, is based on IP accuracy
  - Failover routing – failover to a backup site if the primary site fails and becomes unreachable
- Weighted, Latency and Geolocation can be used for Active-Active while Failover routing can be used for

Active-Passive multi region architecture