ADVANCED VPC Networking

VPC Flow Logs

VPC Flow logs is a feature allowing the monitoring of traffic flow to and from interfaces within a VPC

- VPC Flow logs can be added at a VPC, Subnet or Interface level.
- Flow Logs DON'T monitor packet contents (that requires a packet sniffer) only packet meta data
- Flow Logs can be stored on S3 or CloudWatch Logs EXAM: VPC flow logs ONLY CAPTURE METADATA, NOT CONTENTS

Flow Logs can monitor at 3 levels:

1. VPC (monitors VPC + Subnets in VPC + ENI's in subnets)
2. Subnet (monitors Subnet + ENI's in subnet)
3. ENIs directly (Elastic Network Interface) --> These logs capture meta data from capture point and down (so if VPC flow log, it also captures Subnet and ENIs metadata) EXAM: - Flow Logs is NOT real time data !! --> real time data requires

- Log Destinations: S3 or CloudWatch Logs
  - S3 distination: use when 3rd party software for log analysis or with Athena (SQL like query to access data and be billed only on data being read)
  - CloudWatch logs destination: use when integration with other AWS services: eg stream data and access programatically or through console
- Flow Logs can capture ACCEPTED, REJECTED, or ALL METADATA

VPC flow log records

VPC flow logs captures the meta data of packets in the form of VPC flow log records. Which is a collection of rows and each row has the following fields (`most important fields`): version, account-id, interface-id, `source-address`, `destination-address`, `destination-port`, `protocol`, packets, bytes, start, end, `action`, log-status 2 ACC-ID eni-ID, `119.18.34.78`, `10.16.48.20` `0` `0` `1` 4 336 1432917027 1432917142 `ACCEPT` OK protocol number: ICMP = 1, TCP=6, UDP=17 (might feature on exam as elimnation but good to know for daily usage) action: ACCEPTED, REJECTED: means if packet is accepted or rejected (blocked) by Security Group or NACL (Network Acces Control List)

Egress-Only Internet gateway

Egress-Only internet gateways allow OUTBOUND (and response) only access to the public AWS services and Public Internet for IPv6 enabled instances or other VPC based services

- TL;DR Egress-Only is OUTBOUND-ONLY for IPv6

VPC Endpoints - Gateway

- Gateway endpoints are a type of VPC endpoint which allow private access to public services S3 and DynamoDB WITHOUT using PUBLIC addressing. (normally S3 and DynamoDB are public)

- Gateway endpoints add 'prefix lists' to route table, allowing the VPC router to direct traffic flow to the public services via the gateway endpoint.
    - Gateway Endpoint => 1 per service, per region
    - REGION RESILIENT: Highly Available across all AZs in a region by default
- Endpoint Policy can control what it can access (like certain S3 buckets)
- CANNOT access cross-region services

VPC Endpoints Gateway use cases

- Private VPC that needs private (secured) access to S3/DynamoDB
- Preventing Leaky Buckets: S3 buckets can be set to private only by allowing access ONLY from a gateway endpoint -> bucket can not be accessed from the public internet but only through Enpoint Gateway

VPC Endpoints - Interface

Interface endpoints are used to allow private IP addressing to access public AWS services (S3, SQS, SNS, Kinesis etc.)

- DynamoDB is handled by gateway endpoints - other supported services are handled by interface endpoints. S3 now supported by interface endpoints
- Added to specific subnets, an ENI. Not Highly Available
    - For HA, you need an endpoint in each subnet in each AZ used in VPC
- EXAM - TCP and IPv4 ONLY
- uses PrivateLink: allows AWS or 3rd party svc's to be injected into your vpc and be given network interfaces
- Apps can access Interface Endpoints via Regional DNS, Zonal DNS, or Private DNS (that overrives default DNS)
    - Private DNS associates a private R53 hosted zone to the VPC changing the default svc DNS to resolve to the interface endpoint IP

DEMO - VPC Endpoints - Interface - PART1 / PART2 / PART3 - Skipping for now

VPC Peering

VPC peering is a software defined and logical networking connection between two AND ONLY TWO VPC's

- VPCs in the same or different accounts and the same or different regions.
- EXAM - TWO VPCs connected only
- If VPCs in same region, SGs can reference peer SGs. If not in same region you have to refrence IP adresses or ranges.
- EXAM - VPC Peering does NOT support transitive peering (AKA A -> B peering, then B -> C peering... C is not auto peered to A. If you want A peered to C as well you need to create another VPC peer between A and C.)
- With peering, you're basically setting up gateways in each VPC which requires Routing Configuration on EACH side. SGs/NACLs must be set up to allow traffic through
- EXAM - 4 VPCs... how many peering connection to connect all? 6
- EXAM - IP ranges of VPC Peers CANNOT OVERLAP

DEMO - VPC Peering - Skipping for now