API:

Lambda + API gateway: low cost

EBS:

Back up volumes to different region:

Create EBS snapshots then copy them to desired region

volume types:

General Purpose SSD(gp2)

Provisioned IOPS SSD(io1): consistent performance, long-time persistence,

Throughput Optimized HDD(st1): read-write intensive, large and sequential data, up to 50 MB/s, lowest cost

Cold HDD(sc1)

Disable DeleteOnTermination for EBS volume to retain EBS volume after EC2 instances are terminated

Static image/website contents:

AWS Couldfront + S3 as the origin

Cloudfront:

Lambda@Edge: a feature of Amazon CloudFront that lets you run code closer to users of your application, which improves performance and reduces latency.

For Static content that must be available everywhere (S3 bucket, cross region replication: for dynamic content that needs to be available at low-latency in few regions, S3 is good for hosting static websites)

Global Edge network

Origin access identity (OAI) to access S3 buckets (S3 policy to allow OAI read access)

S3 bucket:

Bucket policy: grant public access to bucket, force objects to be encrypted at update, grant access to another account

Search in S3: make you own DB system which stores metadata for search functionality

DynamoDB:

Consistent and single-digit millisecond latency, highly scalable and fully managed

Indexed data (key-value pair)

Virtually unlimited scalability

Serverless

No downtime

Backup:

On-demand backup allows you to create full backups of your Amazon DynamoDB table for data archiving, helping you meet your corporate and governmental regulatory requirements. You can back up tables from a few megabytes to hundreds of terabytes of data, with no impact on performance and availability to your production applications

Increment and decrement atomic operations:

Support both (add/delete items to list)

VPC flow log:

Capture information about IP traffic going into your interfaces:

VPC Flow Logs, Subnet Flow Logs, Elastic Network Interface Flow Logs

Diagnosing overly restrictive security group rules

Monitoring the traffic that is reaching your instance

Determining the direction of the traffic to and from the network interfaces

CloudTrail:

Get a history of events/API calls made within AWS Account

AWS Config:

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.

RDS:

RDS instance with encryption enabled, logs and backups are automatically encrypted

RDS retention: maximum 35 days, minimum 7 days

Amazon RDS Multi-AZ deployments complement Read Replicas for Amazon RDS for MySQL, MariaDB, and PostgreSQL

Import data from Oracle: Oracle SQL Developer to import a simple and small database, Oracle Data Pump to import complex databases or several hundred megabytes/terabytes.

IAM:

IAM policy is attached to IAM role (Users, groups, roles)

Create IAM role to AWS services

EC2:

Dedicated instance: visibility into the underlying sockets/physical cores of the hardware

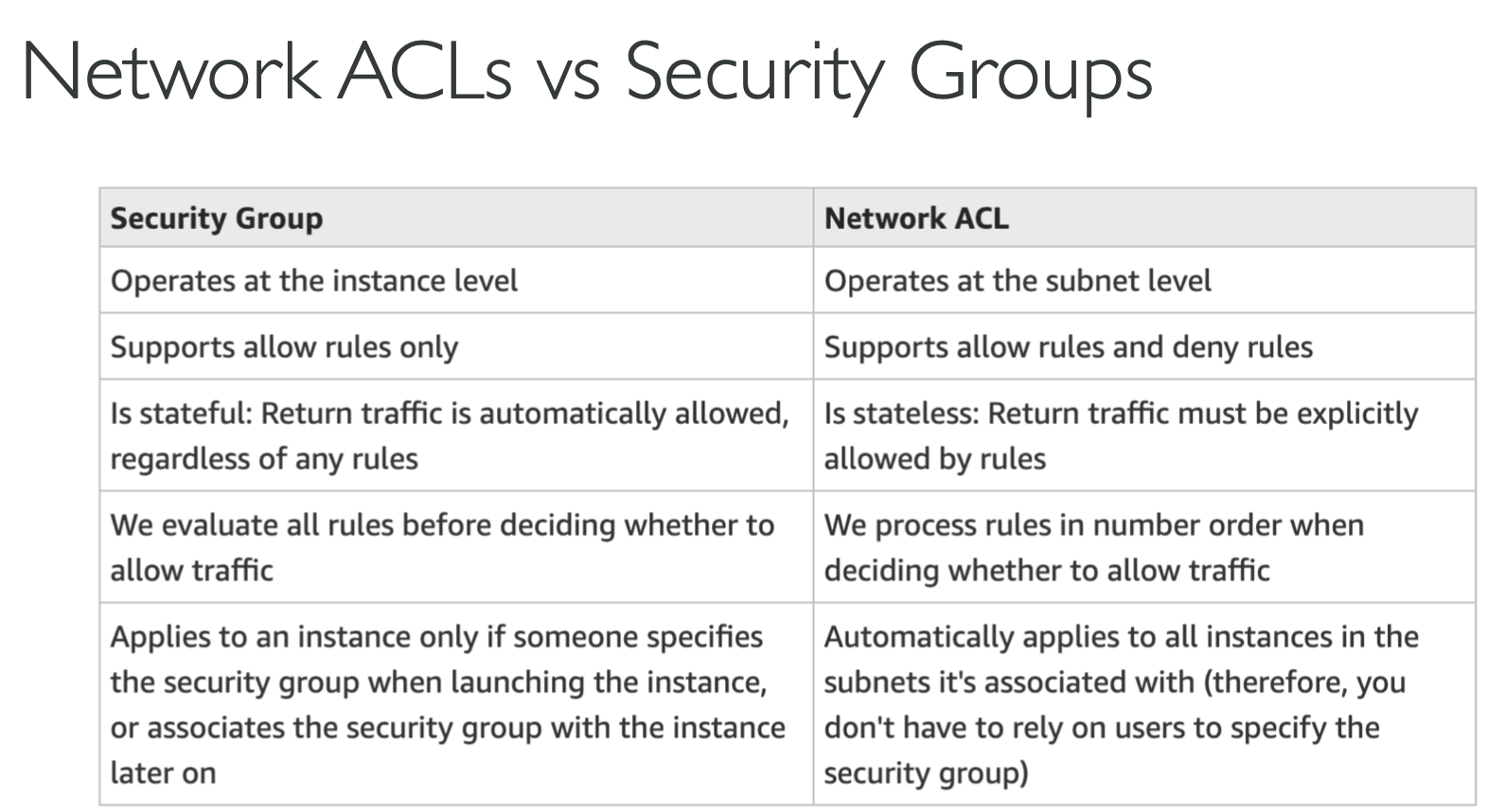
Query the local instance metadata to determine the whether it is using public IP or private IP

Soft limit 20 instances per region -> submit the limit increase form to increase the number

First launch EC2 -> do not select AZ, let AWS select the AZ. Additional EC2 instances -> user should specify AZ.

AWS Parameter Store:

Secure storage for configuration and secrets

Network ACLS vs Security Groupds

AWS WAF (web application firewall)

Block incoming attack from a specific IP address

Redis:

Redis Auth

Redshift:

You can enable encryption when you launch your cluster, or you can modify an unencrypted cluster to use AWS Key Management Service (AWS KMS) encryption. To do so, you can use either an AWS-managed key or a customer-managed key (CMK).

Columnar storage

Aurora: small downtime

RDS: small downtime

DynamoDB: NO downtime

Egress Only Internet Gateway:

Only for IPv6

Lambda:

Encrypted Lambda environment variables to store different passwords in different environments

AWS Organizations:

Restrict access to unapproved AWS services:

Configure AWS organisations, create an organisational unit (OU) and place all AWS accounts into the OU. Apply a service control policy (SCP) to the OU that denies the use of certain services.

Retrieving data:

AWS Glacier: cost-effective, no need for access, might take longer to retrieve, automatically encryption using AES-256

S3 Infrequent access: cost-effective, need for access, retrieved immediately, automatically encryption using AES-256

Discard/delete date after x days: S3

Application load balancer:

Secure load balancing: create SNI(Server Name indication) certificate

HTTP/HTTPS

support HTTP/HTTPS & Websockets protocols

Support routing based on hostname and path

Support redirects (from HTTP to HTTPS for example)

Support dynamic host port mapping with ECS

Application Load Balancer (Layer 7 of OSI):

NLB (Layer 4 of OSI) gets a static IP per AZ :

Public facing: must attach Elastic IP – can help whitelist by clients

Private facing: will get random private IP based on free ones at time of creation

Has cross zone balancing

Has SSL termination (Jan 2019)

ALB & NLB:

Data encryption in transition:

Use ALB with HTTPS listener, then install SSL certifications on the ALB and EC2 instances

Use NLB with TCP listener, then terminate SSL on EC2 instances

Active-Active Failover:

Use this failover configuration when you want all of your resources to be available the majority of the time.

Active-Passive Failover:

Use an active-passive failover configuration when you want a primary resource or group of resources to be available the majority of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable

PrivateLink:

simplifies the security of data shared with cloud-based applications by eliminating the exposure of data to the public Internet. AWS PrivateLink provides private connectivity between VPCs, AWS services, and on-premises applications, securely on the Amazon network.

Amazon Inspector:

is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices

Auto scaling cool down period:

Cool down period for each instance starts after the instance is launched. The group remains locked until the last instance that was launched has completed its cool down period.

Time of the Last instance launched + cool down period = Auto Scaling accept another scaling activity request.

SES (Simple Email Service):

to send emails in a serverless way

AWS VPN CloudHub:

The AWS VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. Use this design if you have multiple branch offices and existing internet connections and would like to implement a convenient, potentially low cost hub-and-spoke model for primary or backup connectivity between these remote offices.

Key pairs:

Consist of public key and private key, use the private key to create a digital signature, AWS uses the corresponding public key to validate the signature.

Only used for AWS EC2 and CloudFront

SQS:

Supports unlimited number of queues and unlimited number of messages per queue for each user. Automatically delete messages in queue for more than 4 days.

EMR Elastic MapReduce:

helps creating Hadoop clusters (Big Data) to analyze and process vast amount of data

1 IOPS (input/output operations per second) = 256 kb I/O

Region > VPC > AZ > subnet