# I Về lý thuyết

## Giao thức cổng đường biên là gì? What is Border Gateway Protocol

<https://aws.amazon.com/what-is/border-gateway-protocol/#:~:text=Border%20Gateway%20Protocol%20(BGP)%20is,%2C%20devices%2C%20and%20communication%20technologies>.

Giao thức cổng đường biên (BGP) là một tập hợp các quy tắc xác định những tuyến mạng tốt nhất để truyền dữ liệu trên Internet. Internet bao gồm hàng nghìn mạng riêng, công cộng, của công ty và của chính phủ được liên kết với nhau thông qua các giao thức, thiết bị và công nghệ giao tiếp được chuẩn hóa. Khi bạn duyệt Internet, dữ liệu sẽ di chuyển qua nhiều mạng trước khi đến đích. Trách nhiệm của BGP là xem xét tất cả các đường dẫn sẵn sàng truyền dữ liệu và chọn tuyến tốt nhất. Ví dụ: Khi một người dùng ở Hoa Kỳ tải một ứng dụng có máy chủ gốc ở châu Âu, BGP sẽ giúp hoạt động giao tiếp đó diễn ra nhanh chóng và hiệu quả.

## What is jiter

<https://www.gearupbooster.com/vi/blog/what-is-jitter-in-networking.html>

Các gói dữ liệu thường được ngăn cách đều đặn trong một khoảng thời gian định trước. Khi có sự dao động hoặc "thay đổi độ trễ của gói" khi truyền một trong các gói dữ liệu này qua kết nối mạng của bạn, điều này dẫn đến hiện tượng giật hình mà bạn có thể nhận thấy trong cuộc gọi VoIP hoặc cuộc họp video dưới dạng âm thanh hoặc video chậm hoặc các biến dạng khó chịu khác.

Để đưa nó vào một định nghĩa, Jitter là độ lệch của tính chu kỳ của tín hiệu hoặc sự kiện định kỳ so với mục tiêu hoặc tần số thực của nó. Jitter cũng được sử dụng trong viễn thông để mô tả sự dao động về độ trễ của các gói cung cấp dữ liệu âm thanh hoặc video thông qua kết nối truyền thông.

Jitter thường bị nhầm lẫn với độ trễ, vì vậy hãy cùng nêu ra sự khác biệt. Jitter là sự thay đổi về lượng thời gian cần thiết để một gói dữ liệu di chuyển qua mạng. Các gói dữ liệu bị dừng trên đường đến người nhận do tắc nghẽn mạng. Chúng sẽ xuất hiện trong các khoảng thời gian ngẫu nhiên, giống như âm thanh bị rè trong cuộc gọi hoặc hiển thị dưới dạng video pixel trong cuộc gọi điện video. Mặt khác, độ trễ là thời gian cần thiết để một gói dữ liệu di chuyển qua mạng. Với độ trễ, toàn bộ quá trình truyền hoàn chỉnh, các bit và các mảnh, sẽ đến muộn hơn dự kiến.

## 3 what is IpSec ( Vpc support protocol security ‘ipSec’)

Link: <https://aws.amazon.com/vi/what-is/ipsec/#:~:text=IPSec%20l%C3%A0%20h%E1%BB%87%20th%E1%BB%91ng%20c%C3%A1c,c%C6%B0%E1%BB%9Dng%20b%E1%BA%A3o%20m%E1%BA%ADt%20giao%20th%E1%BB%A9c>.

-Amazon supports Internet Protocol Security (IPSec) VPN connections. Data transferred between your VPC and datacenter routes over an encrypted VPN connection to help maintain the confidentiality and integrity of data in transit. An internet gateway is not required to establish an AWS Site-to-Site VPN connection.

IPSec là hệ thống các quy tắc hoặc giao thức truyền thông dùng để thiết lập kết nối an toàn qua một mạng. Giao thức Internet (IP) là tiêu chuẩn phổ biến giúp xác định cách dữ liệu truyền qua Internet. IPSec bổ sung khả năng mã hóa và xác thực để tăng cường bảo mật giao thức. Ví dụ: IPSec xáo trộn dữ liệu tại nguồn và khôi phục dữ liệu bị xáo trộn tại đích của giao thức này. IPSec cũng xác thực nguồn dữ liệu.

## 4 what is dual home instance (VPC)

A Host or Virtual machine with more than one network interfaces is called dual-homed Instance. A dual-homed instance is a system fitted with two network interfaces (NICs) that sits between an untrusted network (like the Internet) and trusted network (such as a corporate network) to provide secure access.

## 5. What is proxy protocol ( Loadbanlacer)

<https://www.google.com/search?q=wwhat+is+proxy+protocol&oq=wwhat+is+proxy+protocol&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTILCAEQABgNGBMYgAQyCwgCEAAYDRgTGIAEMgoIAxAAGBMYFhgeMgoIBBAAGBMYFhgeMgoIBRAAGIAEGKIEMgoIBhAAGIAEGKIEMgcIBxAAGO8FMgcICBAAGO8F0gEIODkwNWowajeoAgCwAgA&sourceid=chrome&ie=UTF-8>

Proxy protocol is an internet protocol used to carry connection information from the source requesting the connection to the destination for which the connection was requested. Elastic Load Balancing uses proxy protocol version 1, which uses a human-readable header format.

## 6. Limit params of AWS

<https://docs.bitnami.com/aws/faq/get-started/understand-limits/#:~:text=static%20IP%20addresses.-,EC2%20Instances,up%20on%20your%20AWS%20account>.

Link detail:

<https://docs.aws.amazon.com/organizations/latest/userguide/orgs_reference_limits.html#:~:text=Limit%20increases%20can%20be%20granted,the%20default%20of%2010%20accounts>.

### Max have 20 EC2 in all account with in a region. Request more need create new request

### By default, AWS sets a limit of 5 static IP addresses per region. This includes IP addresses unassigned and currently assigned to a server.To increase IP addresses limit, [request a higher limit](http://aws.amazon.com/contact-us/eip_limit_request/) by providing information about the new limit and regions where it should be applied.

### The AWS default limit for all snapshots is 10000 snapshots per region.To increase the number of snapshots allowed, [contact AWS Support](https://aws.amazon.com/contact-us/) and request a higher limit.

* Max 10 account for org

## 7. What is Subject Alternative Name san?

The Subject Alternative Name (SAN) is an extension to the X. 509 specification that allows users to specify additional host names for a single SSL certificate. The use of the SAN extension is standard practice for SSL certificates, and it's on its way to replacing the use of the common name.

## 8. What is Server Name Indication (SNI) ?

Server Name Indication (SNI) is an extension to the TLS protocol that is supported by browsers and clients released after 2010. If you configure CloudFront to serve HTTPS requests using SNI, CloudFront associates your alternate domain name with an IP address for each edge location.

* Server Name Indication, often abbreviated SNI, is an extension to TLS that allows multiple hostnames to be served over HTTPS from the same IP address.

## 9. Database Clustering là gì?

Link: <https://topdev.vn/blog/database-clustering-la-gi-khi-nao-nen-su-dung/>

## 10 what is s3 transfer acceleration

<https://aws.amazon.com/vi/s3/transfer-acceleration/#:~:text=S3TA%20shortens%20the%20distance%20between,Edge%20Locations%20to%20your%20application>.

S3TA shortens the distance between client applications and AWS servers that acknowledge PUTS and GETS to Amazon S3 using our global network of hundreds of CloudFront Edge Locations. We automatically route your uploads and downloads through the closest Edge Locations to your application.

## 11 What is Amazon Elastic File System (EFS)

<https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html#:~:text=Amazon%20Elastic%20File%20System%20(Amazon,managing%20storage%20capacity%20and%20performance>.

Amazon Elastic File System (Amazon EFS) provides serverless, fully elastic file storage so that you can share file data without provisioning or managing storage capacity and performance.

**What is Amazon Elastic File System (EFS) and how is it different from Amazon Elastic Block Store (EBS)?**

 a.

EFS is a fully managed, scalable file storage for AWS Cloud services and on-premises resources, while EBS provides persistent block-level storage volumes for use with Amazon EC2 instances.

## 12 type of Storage

<https://www.futurelearn.com/info/courses/aws-cloud-technical-essentials/0/steps/287929#:~:text=AWS%20storage%20services%20are%20grouped,file%20storage%2C%20and%20object%20storage.&text=You%20may%20be%20familiar%20with,Explorer%20or%20Finder%20on%20MacOS>.

## 13 what is AWS Data Pipeline

<https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/what-is-datapipeline.html>

AWS Data Pipeline is a web service that you can use to automate the movement and transformation of data. With AWS Data Pipeline, you can define data-driven workflows, so that tasks can be dependent on the successful completion of previous tasks.

## 14 what is Amazon Kinesis Data Firehose

<https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html>

Within this overall flow, Kinesis Data Firehose covers stream ingestion, storage, processing, and destination delivery. It provides near real-time streaming extract, transform, and load (ETL) processing for any data, at any scale, and at low cost

## 15. What is the difference between a public IP address and an Elastic IP address in Amazon VPC?

A public IP address is assigned to an instance when it's launched and cannot be associated with a different instance. An Elastic IP address is a static IP address that can be associated with and disassociated from instances.

## 16. What is the difference between strongly consistent and eventually consistent read?

Strong consistency guarantees that all reads reflect the latest write, while eventual consistency may sometimes return stale data but offers cost savings by using half the capacity units

## 17. Batch Operations (dynamoDB)

Amazon DynamoDB also provides several operations designed for working with large batches of items, including BatchGetItem and BatchWriteItem. Using the BatchWriteItem action, you can perform up to 25 item creates or updates with a single operation. This allows you to minimize the overhead of each individual call when processing large numbers of items.

## 18. Amazon DynamoDB table can scale horizontally through the use of partitions

to meet the storage and performance requirements of your application. Each individual partition represents a unit of compute and storage capacity

* One single partition can hold about 10GB of data and supports a maximum of 3,000 read capacity units or 1,000 write capacity units.

1B,2D,3C,4A,5B,6A,7B,8B(A),9D,10A,11A(B),12B,13ACD,14CD,15ABC,16ABC,17A(C),18A,19BD,20CD(BC)

## 19. SQS (note)

- Each message can have up to 10 attributes.

- The maximum length of a message ID is 100 characters. (name | id is identify in message-queue)

- The maximum length of a receipt handle is 1,024 characters.

- long poll :max 20

- delay queue max : 15 min (900s)

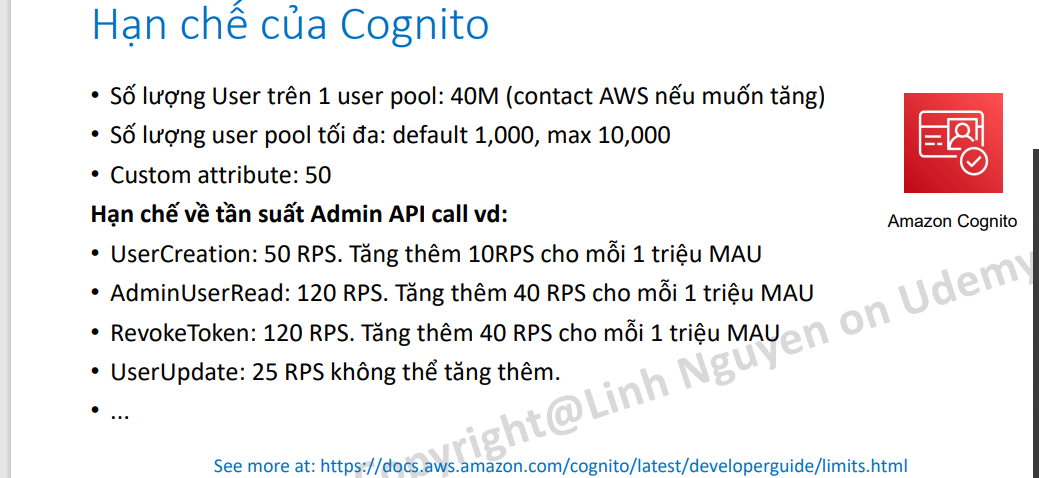
- visibility queue min-max: 30s-12 hours

-dead letter queue retain message in: default= 4day, max=14 days

## 20 SNS (note)

* Số lượng topic/account 100000, FIFO: 1000
* Subcription: 12500000/topic, Fifo: 100/topic
* Delivery rate for email: 10message/s (extendable)
* Message size : 256 KB
* You can use the following protocols with Amazon SNS: HTTP, HTTPS, SMS, email, email-JSON, Amazon SQS, and AWS Lambda
* When you create a new Amazon SNS topic, an Amazon ARN is created automatically.
* Topic names should typically be available for reuse approximately 30–60 seconds after the previous topic with the same name has been deleted

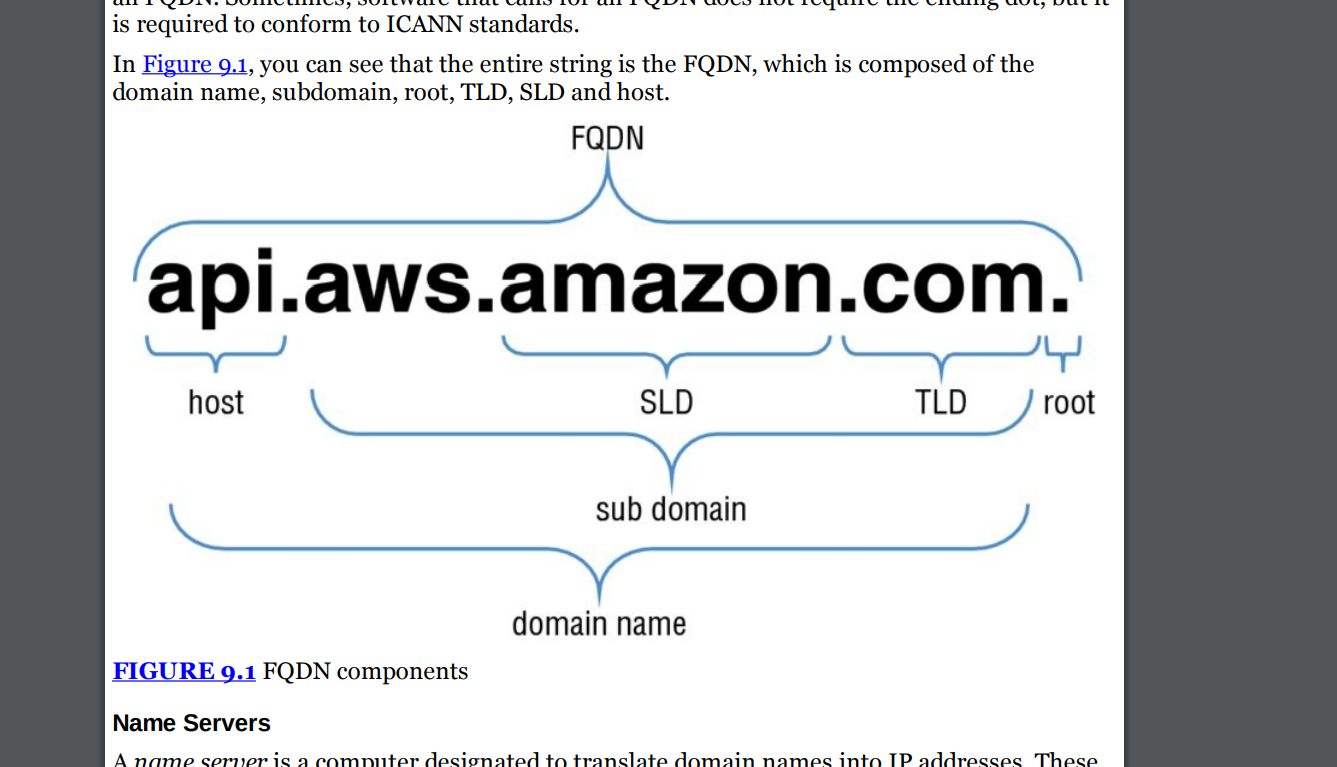
## 21 cognito (limit)



22 SWF (note)

* Actors can be workflow starters, deciders, or activity workers.
* Amazon SWF provides activity workers and deciders with work assignments, given as one of three types of tasks: activity tasks, AWS Lambda tasks, and decision tasks.
* It is possible to have more than one workflow in a domain; however, workflows in different domains cannot interact with one another.
* The decider schedules the activity tasks and provides input data to the activity workers. The decider also processes events that arrive while the workflow is in progress and closes the workflow when the objective has been completed

## 23. Khái niệm về thành phần của 1 domain (full)



* .com = TLD (top level domain)
* .amazon = SLD ( second level domain)
* .amazon.com is domain
* .Aws = sub domain
* Api = host
* Diff hostname ( chir trong1 amsy tinhs)
* Domain name (khái niệm trên internet

## 24. Cần nhớ các nhiệm vụ của record in file zone

• SOA (SOA) Record A Start of Authority (SOA) record is mandatory in all zone files, and it identifies the base DNS information about the domain. Each zone contains a single SOA record.

• A Record (Address Record): Xác định một địa chỉ IPv4 cho tên miền. Nó ánh xạ một tên miền vào một địa chỉ IP v4

• AAAA Record (IPv6 Address Record): Tương tự như A Record, nhưng sử dụng để xác định một địa chỉ IPv6 cho tên miền.

• CNAME Record (Canonical Name Record): Nó được sử dụng để tạo đường dẫn từ một tên miền thứ cấp (subdomain) đến một tên miền ở bất cứ đâu trên internet.

• MX Record (Mail Exchanger Record): Xác định các máy chủ chịu trách nhiệm nhận và xử lý thư điện tử cho một tên miền. Nó được sử dụng để định vị máy chủ email. AWS Cloud for beginner Các loại DNS Record Copyright Linh Nguyen – All right reserved 10

• TXT Record (Text Record): Cho phép bạn lưu trữ các dữ liệu văn bản tùy ý cho tên miền. Nó thường được sử dụng để xác thực tên miền và cung cấp thông tin khác nhau cho các dịch vụ khác.

• SRV Record (Service Record): Xác định vị trí và cấu hình dịch vụ cụ thể trên mạng. Nó được sử dụng chủ yếu trong việc xác định các máy chủ chịu trách nhiệm cho các dịch vụ như VoIP (Voice over IP) và IM (Instant Messaging).

• NS Record (Name Server Record): Xác định máy chủ tên miền (name server) chịu trách nhiệm quản lý các bản ghi DNS cho tên miền cụ thể. Nó cho phép bạn chỉ định máy chủ DNS mà bạn muốn sử dụng cho tên miền của mình.

• PTR Record (Pointer Record): Sử dụng để thực hiện ánh xạ địa chỉ IP thành tên miền. Nó được sử dụng chủ yếu trong việc xác định tên miền từ một địa chỉ IP cụ thể

## 25. Amazon Route 53 allows you to have several different routing policies, including the following:

* Simple—Most commonly used when you have a single resource that performs a given function for your domain
* Weighted—Used when you want to route a percentage of your traffic to one particular resource or resources
* Latency-Based—Used to route your traffic based on the lowest latency so that your users get the fastest response times
* Failover—Used for DR and to route your traffic from your resources in a primary location to a standby location
* Geolocation—Used to route your traffic based on your end user’s location

## 26 . DNS note

* uses port 53.
* DNS primarily uses UDP to serve requests.
* A. The TCP protocol is used by DNS server when the response data size exceeds 512 bytes or for tasks such as zone transfers.

## 27 what is OpsWork

<https://docs.aws.amazon.com/opsworks-cm/latest/APIReference/Welcome.html#:~:text=AWS%20OpsWorks%20CM%20is%20a,for%20the%20servers%20to%20manage>.

AWS OpsWorks CM is a service that runs and manages configuration management servers. You can use AWS OpsWorks CM to create and manage AWS OpsWorks for Chef Automate and OpsWorks for Puppet Enterprise servers, and add or remove nodes for the servers to manage.

## Một số note trong sách

### S3

- create bucket is private deafult

- . Bucket names can contain up to 63 lowercase letters, numbers, hyphens, and periods

- Objects can range in size from 0 bytes up to 5TB, and a single bucket can store an unlimited number of objects

- Each object consists of data (the file itself) and metadata (data about the file). The data portion of an Amazon S3 object is opaque to Amazon S3. This means that an object’s data is treated as simply a stream of bytes—Amazon S3 doesn’t know or care what type of data you are storing, and the service doesn’t act differently for text data versus binary data. The metadata associated with an Amazon S3 object is a set of name/value pairs that describe the object.

- Amazon S3 scales automatically, but for request rates over 100 GETS per second, it helps to make sure there is some randomness in the key space. Replication and logging will not affect performance or scalability. Using sequential key names could have a negative effect on performance or scalability.

- Amazon Glacier Is frequently erased within 90 days. Data is stored in encrypted archives that can be as large as 40TB. Archives typically contain TAR or ZIP files (a archives = 40TB), need 3-5 hours to restore

- Amazon Glacier can be used as a standalone service and as an Amazon S3 storage class.

### EC2

Max size of a volumn EBS is 16TB

#### Addressing an Instance:

- Public Domain Name System (DNS) Name—When you launch an instance, AWS creates a DNS name that can be used to access the instance. This DNS name is generated automatically and cannot be specified by the customer

- Public IP—A launched instance may also have a public IP address assigned. This IP address is assigned from the addresses reserved by AWS and cannot be specified

- Elastic IP—An elastic IP address is an address unique on the Internet that you reserve independently and associate with an Amazon EC2 instance

- Can modify type of instand :

Instance Type The ability to change the instance type of an instance contributes greatly to the agility of running workloads in the cloud

#### Security Groups:

If an instance is running in an Amazon VPC (discussed in Chapter 4), you can change which security groups are associated with an instance while the instance is running. For instances outside of an Amazon VPC (called EC2-Classic), the association of the security groups cannot be changed after launch.

* While termination instance but cli still can access instance. Turn on termination protection will disable termination in cli

. In order to prevent termination via the AWS Management Console, CLI, or API, termination protection can be enabled for an instance. While enabled, calls to terminate the instance will fail until termination protection is disabled. This helps to prevent accidental termination through human error.

#### Pricing Options

- On-Demand Instances

- Reserved Instances

+ All Upfront—Pay for the entire reservation up front. There is no monthly charge for the customer during the term.

+ Partial Upfront—Pay a portion of the reservation charge up front and the rest in monthly installments for the duration of the term.

+ No Upfront—Pay the entire reservation charge in monthly installments for the duration of the term.

- Spot Instances

#### Tenancy Options

- Shared Tenancy Shared tenancy is the default tenancy model for all Amazon EC2 instances, regardless of instance type, pricing model, and so forth

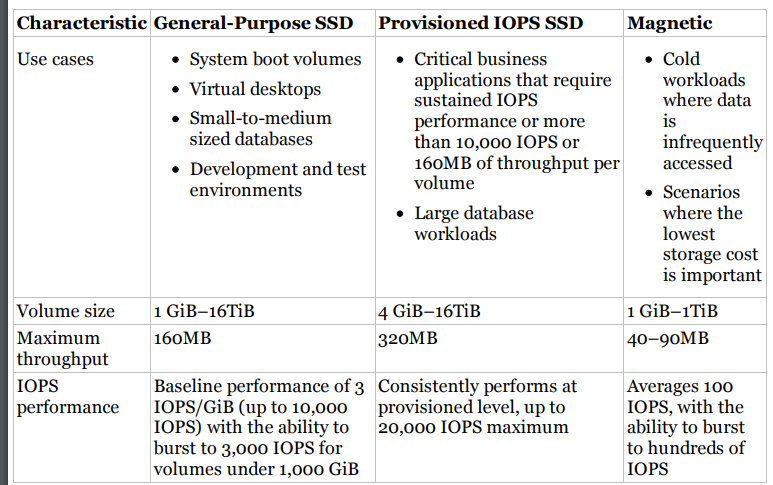
- Dedicated Instances Dedicated Instances run on hardware that’s dedicated to a single customer

- Dedicated Host An Amazon EC2 Dedicated Host is a physical server with Amazon EC2 instance capacity fully dedicated to a single customer’s use.

#### Amazon Elastic Block Store (Amazon EBS)

- Magnetic Volumes

A magnetic Amazon EBS volume can range in size from 1 GB to 1 TB and will average 100 IOPS, but has the ability to burst to hundreds of IOPS. They are best suited for: Workloads where data is accessed infrequently Sequential reads Situations where low-cost storage is a requirement

* General-Purpose SSD 1GB- 16TB max 10000 IOPS, 1TB =3000IOPS ⬄ 3TB=10000IOPS
* Provisioned IOPS SSD Provisioned IOPS SSD volumes are designed to meet the needs of I/O-intensive workloads
* 

# II.Questions

## 2.1. Elastic Load Balancing supports which of the following types of load balancers? (Choose 3 answers)

* Internet-facing
* Internal
* Hypertext Transfer Protocol Secure (HTTPS) using Secure Sockets Layer (SSL)

##### **What is a network ACL in Amazon VPC?**

##### A network ACL is a firewall that controls traffic to and from subnets in a VPC. network ACL is a firewall that controls traffic to and from subnets in a VPC.