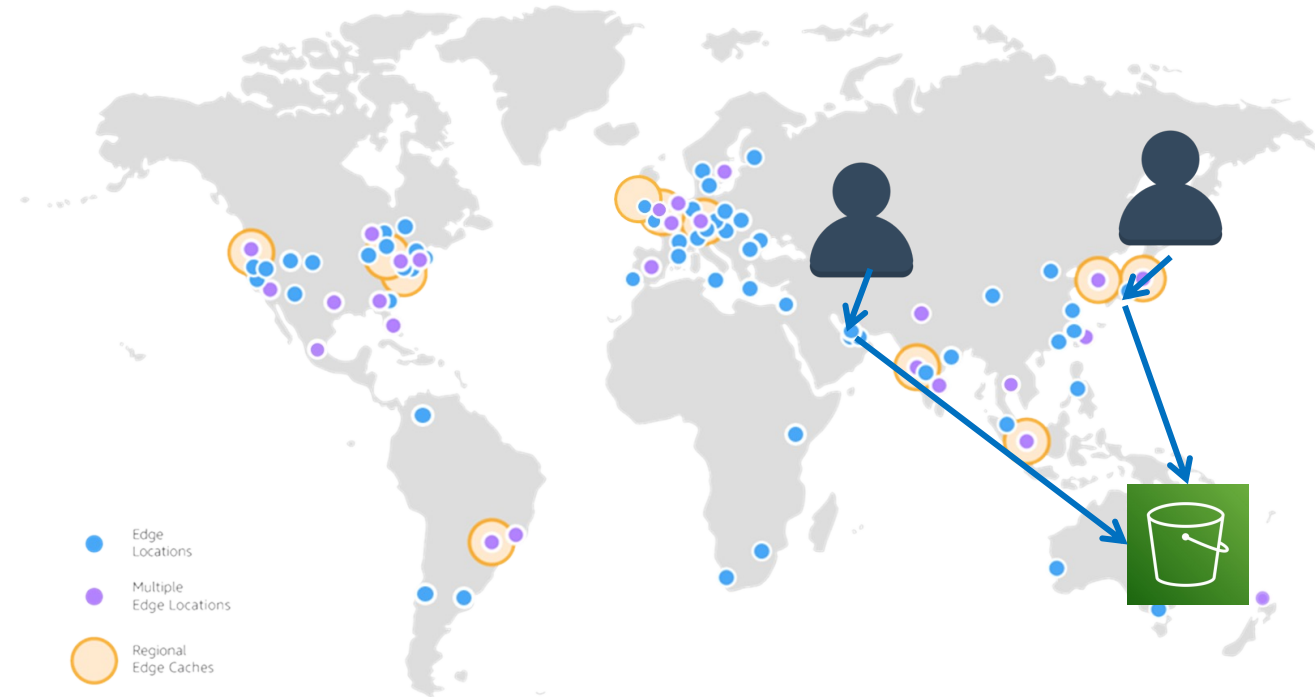


# CloudFront

# CloudFront

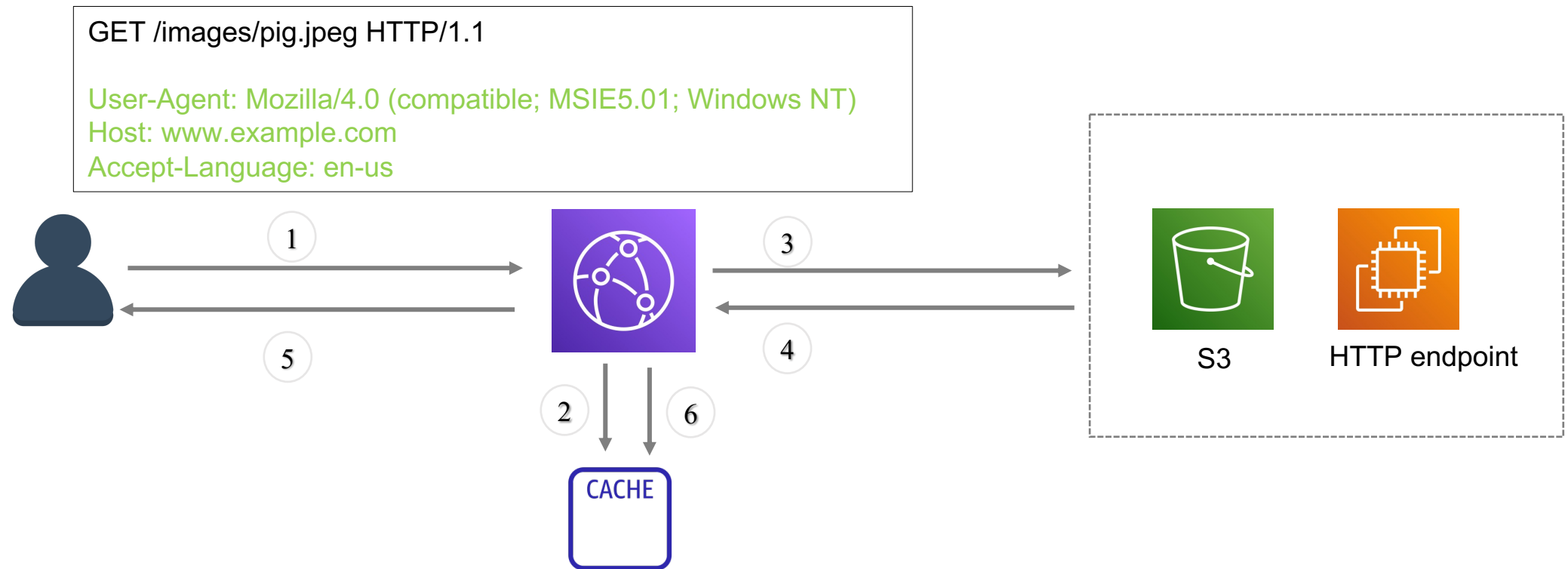
- Content Delivery Networking (CDN)
- Sử dụng để Caching content,
- Giúp tăng hiệu năng ứng dụng
- Content được lưu trữ tại **Edge Location**
- Giảm nhẹ tấn công DDoS
  - AWS Shield
  - AWS Web Application Firewall



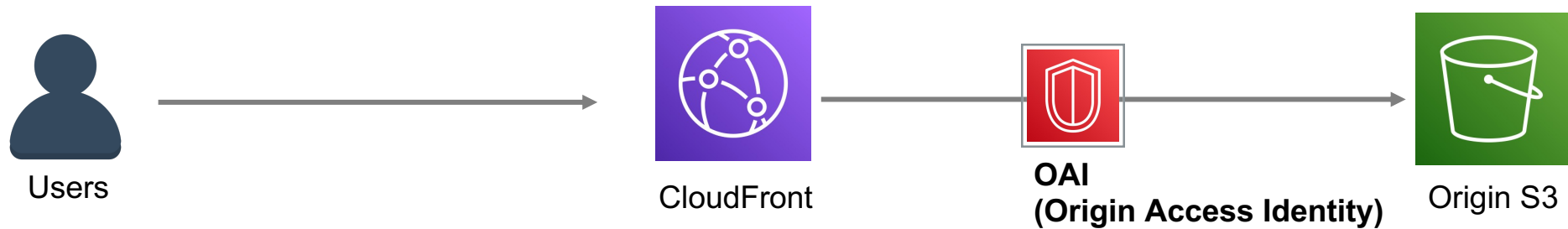
# CloudFront Origin

- **S3**
  - Cho phép cache S3 objects tại **Edge Location**
  - Sử dụng **OAI (Origin Access Identity)** kết hợp với **Bucket Policy** để kiểm soát chặt chẽ truy cập vào S3 Objects
- **Custom HTTP Endpoint**
  - Application Load Balancer (ALB)
  - EC2
  - S3 static website or any HTTP endpoint

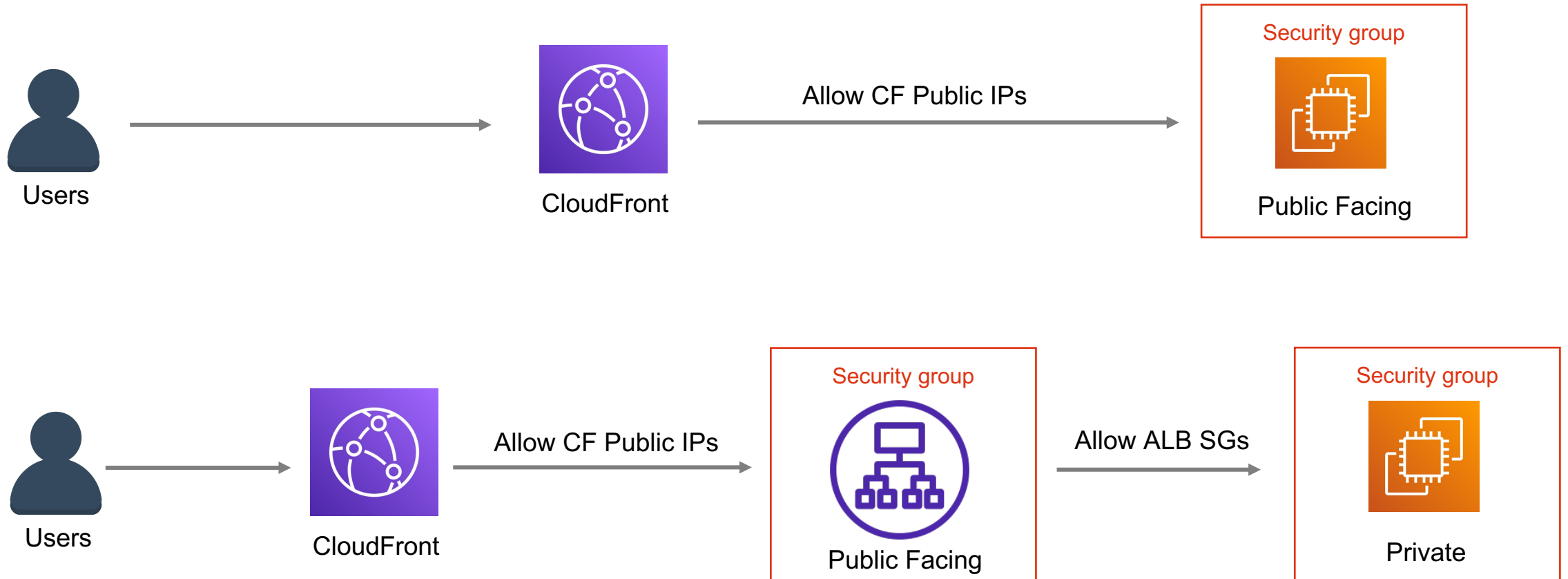
# Cách CloudFront cache contents?



# CloudFront vs S3 origin



# CloudFront vs EC2 and ALB



# Knowledge Check

**Question:** You have a static website hosted on an S3 bucket. You have created a CloudFront Distribution that points to your S3 bucket to better serve your requests and improve performance. After a while, you noticed that users can still access your website directly from the S3 bucket. You want to enforce users to access the website only through CloudFront. How would you achieve that?

- A. Configure your CloudFront Distribution and create an Origin Access Identity, then update your S3 Bucket Policy to only accept requests from your CloudFront Distribution OAI user
- B. Send an email to your clients and tell them to not use the S3 endpoint
- C. Use S3 Access Points to redirect clients to CloudFront

# CloudFront

## Signed URL and Cookies

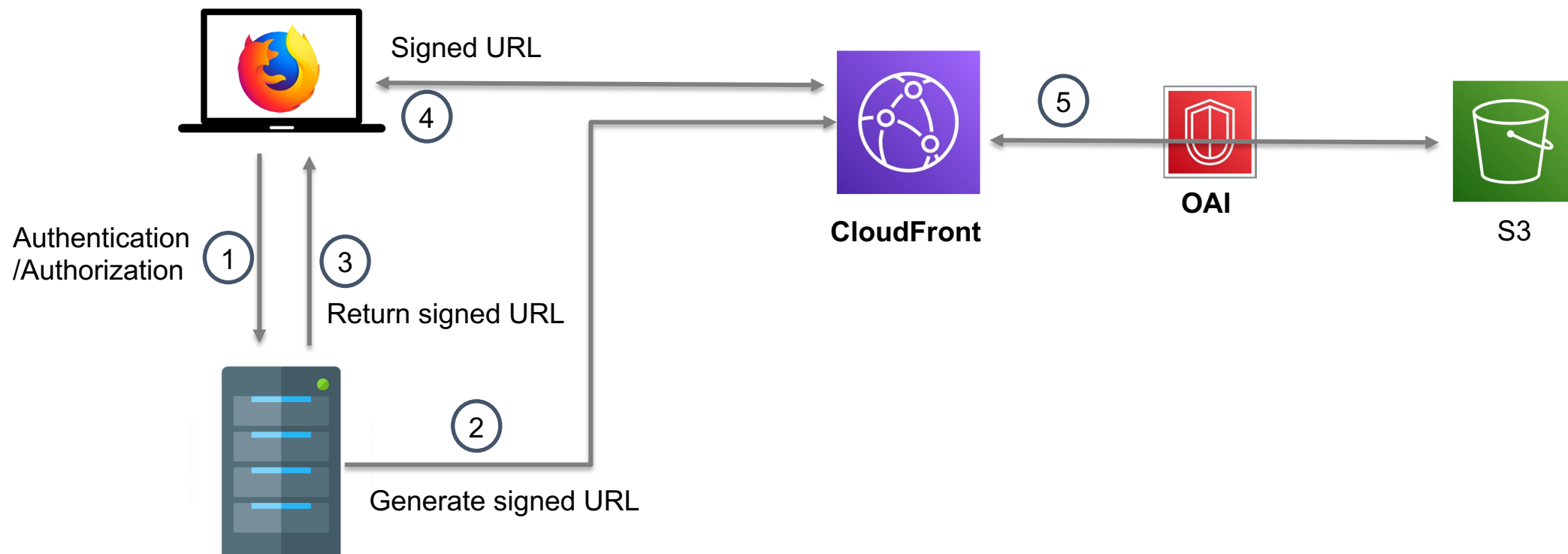


# CloudFront signed URL and Signed Cookies?

---

- A **Signed URL** dành cho một Object
- A **Signed Cookie** dành cho nhiều Objects (multiple Objects)
- Sử dụng Signed URL hoặc Signed Cookie có thể thiết lập:
  - URL expiration (Thời gian mà URL còn hữu dụng)
  - IP ranges (Dải đại chỉ IP có thể truy cập các Objects)
  - Trusted Signers (Chỉ định thực thể có thể ký)

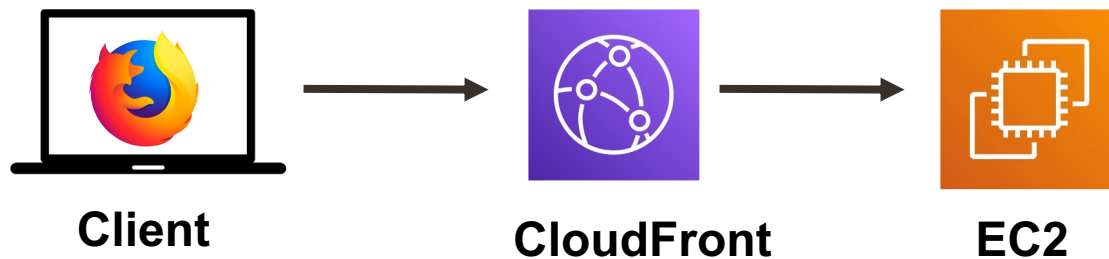
# Cách Signed URL hoạt động



# CloudFront signed và S3 pre-signed URL

## CloudFront signed URL

- Làm việc với các Origin khác nhau (S3, HTTP endpoints)
- Quản lý Key Group
- Giới hạn truy cập theo IP, path, date expiration
- Có thể tận dụng tính năng Cache của CloudFront



## S3 pre-signed URL

- Chỉ làm việc được với origin là S3
- Thời gian valid hữu hạn
- Request có quyền tương tự như người tạo ra URL này



# Exam tips

---

- Sử dụng Signed URL hay Signed Cookies khi muốn bảo mật nội dung (Chỉ cho phép người dung được cấp quyền mới được truy cập)
- Signed URL dành cho 1 Object. **1 URL = 1 object (file)**
- Signed dành cho nhiều Objects (multiple Objects). **1 cookie = multiple object (files)**
- CloudFront signed URL có thể làm việc với nhiều loại Origin khác nhau (S3, ALB, EC2....)
- S3 pre-signed URL chỉ làm việc được với S3 origin

# Knowledge Check



**Question:** A website is hosted on a set of EC2 instances fronted by an Application Load Balancer. You have created a CloudFront Distribution and set up its origin to point to your ALB. What should you use to provide access to hundreds of private files served by your CloudFront distribution?

- A. CloudFront Signed URLs
- B. CloudFront Origin Access Identity
- C. CloudFront HTTPS Encryption
- D. CloudFront Signed Cookies

# Exam tips

---

- **Edge Location** là nơi cache content
- **Origin** là nơi cung cấp content, files (S3, ALB, EC2, HTTP endpoint)
- **Geo Restriction** được sử dụng để kiểm soát truy cập dựa vào vị trí địa lý
- **Object** được cache trong một khoảng thời gian gọi là **TTL** (Time To Live)