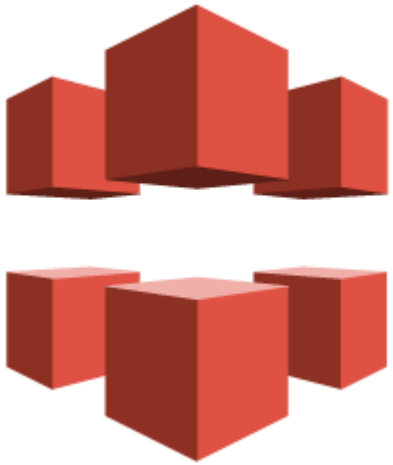


AWS CloudFront

Cloudfront

- Amazon Cloud Front is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js and image files to your users

- **Amazon** Cloud Front is a web service that gives business and web application developers an easy and cost effective way to distribute content with low latency and high data transfer speeds.

Cloudfront

- Content Delivery Network (CDN).
- Improves read performance, content is cached at the edge
- 216 Point of Presence globally(edge locations)
- DDos Protection, integration with Shield, AWS Web Application Firewall
- Can expose external HTTPS and can talk to internal HTTPS back ends

Need of AWS Cloudfront

Cloudfront

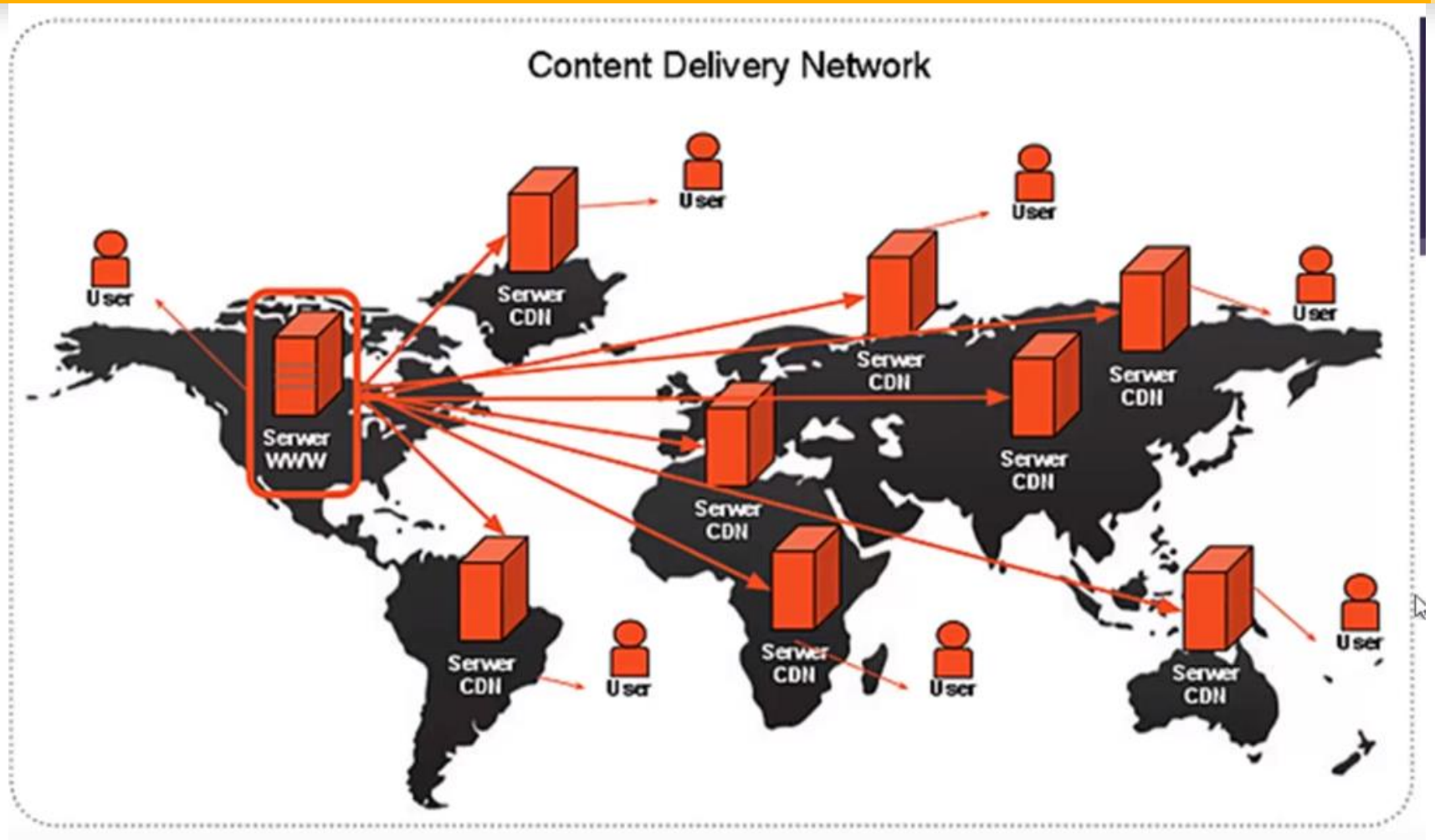
CloudFront Terminology

- **CDN:** Content Delivery Network is a network of distributed servers which deliver content to end users based on geographical locations of them, origin of the source page and a CDN server.
- **Edge Location**: Place where the content will be cached.
- **Origin**: Source of files/content that CDN will deliver / Distribute. Can be S3, EC2, ELB, Route53.
- **Distribution**: Collection of Edge location and your CDN network.
- **TTL**

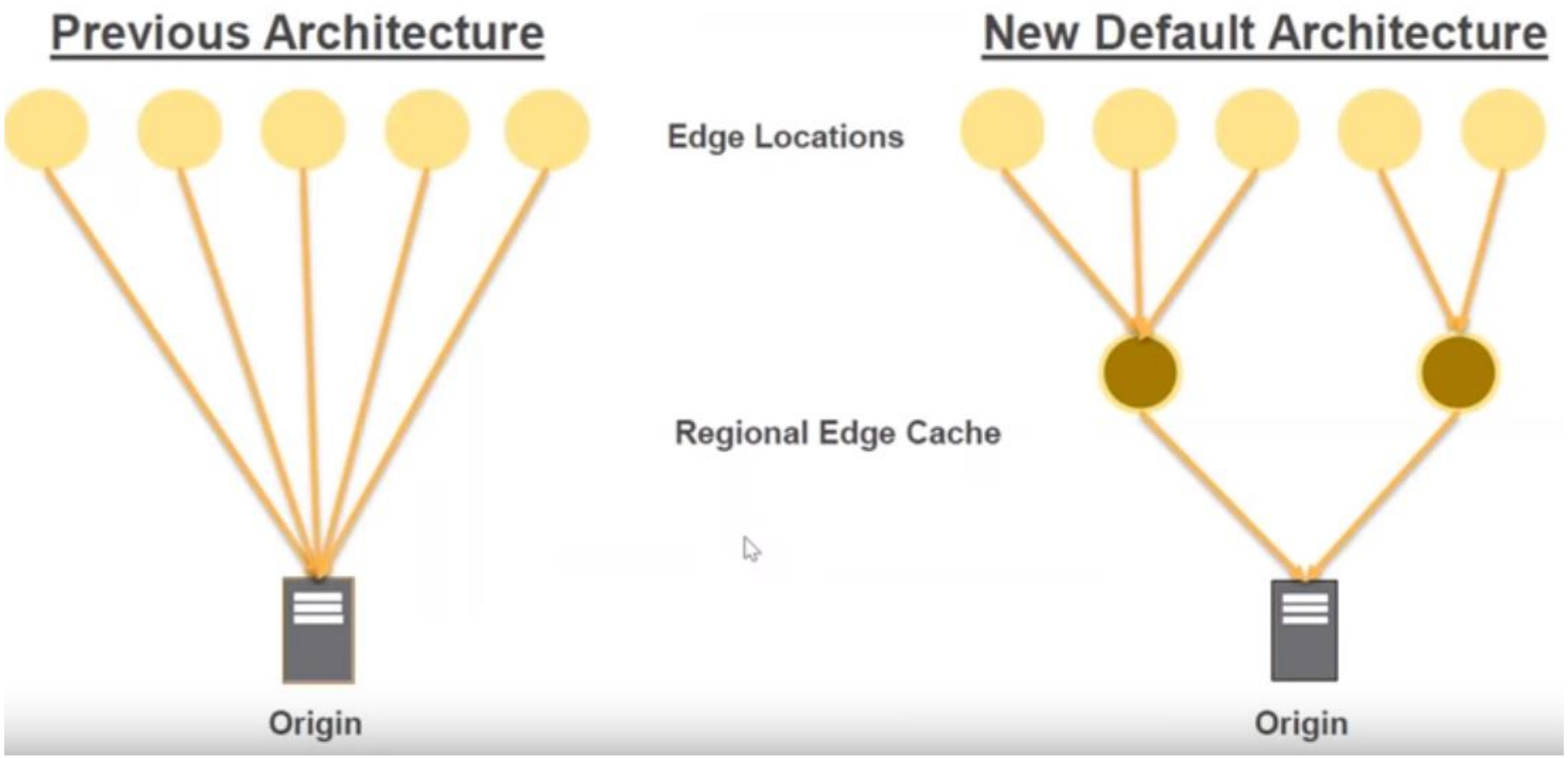
What is CDN?

- **A** content delivery network(CDN) uses a network of geographically dispersed servers(edge locations) to cache copies of content close to end users, lowering latency when they download or stream objects

Content Delivery Network



Cloudfront: Edge Locations



CloudFront: Components

- Distributions
- Origins
- Behaviors
- Restrictions, Error Pages, Tags
- AWS Web Application Firewall (WAF)
- Edge Locations

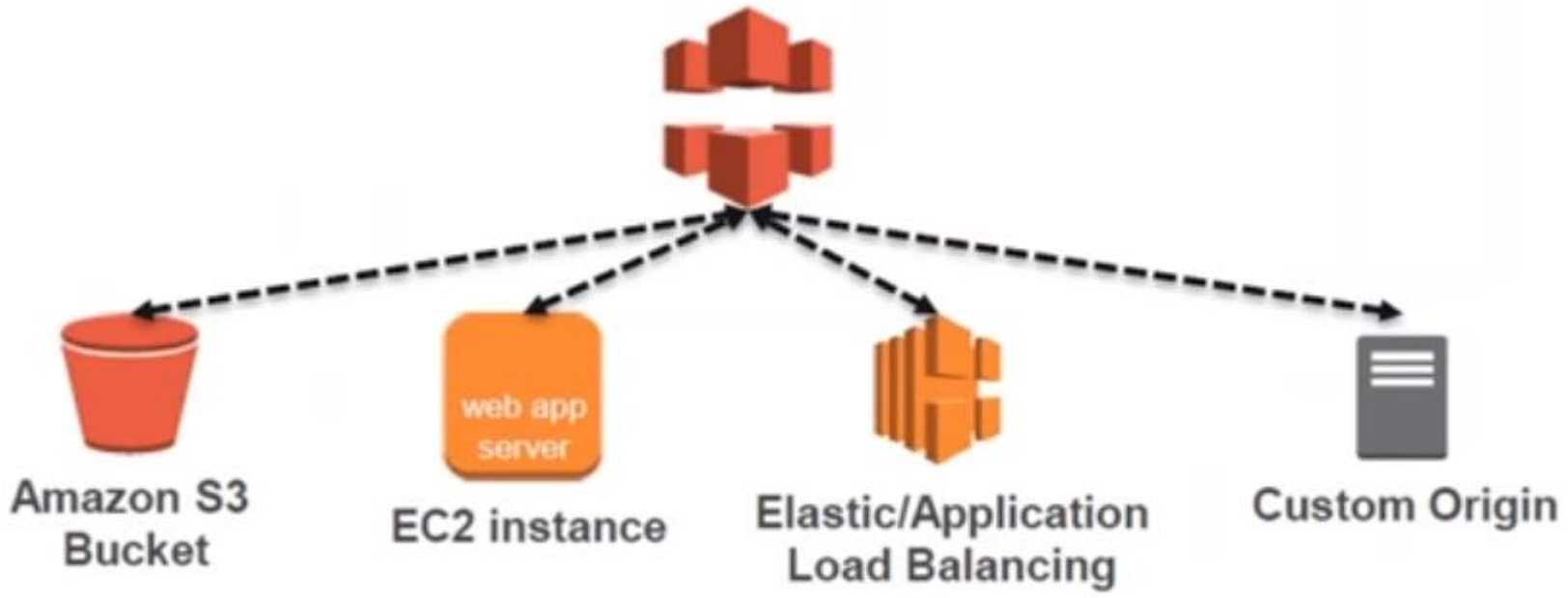
CloudFront: Distribution

Distribution: Collection of Edge location and your CDN network.

- Unique CloudFront.net Domain Name to Reference objects
  - Ex: d23xgvsk7zin70.cloudfront.net
- Specific Origins of Original Content Versions
  - Ex: origin.mysite.com
- Types provide for HTTP/HTTPS
  - https://origin.mysite.com
- Contain specific Configurations and Tags
  - Ex: origins, behaviors, error pages, restrictions

CloudFront: Origins

- Any publicly accessible amazon S3 bucket or S3 website or ELB or EC2 instance
- Source of files/content that CDN will deliver / Distribute. Can be S3, EC2, ELB, Route53.



CloudFront: Origins

- **Origin Access Identity**: If you use this, only CloudFront can access the S3 object. You cannot access directly S3 object URL. This is super secure for your S3 website.

- This is for Security Purpose.

CloudFront Signed URL / Signed Cookies

- You want to distribute paid shared content to premium users over the world
- We can use CloudFront Signed URL / Cookie. We attach a policy with:
  - Includes URL expiration
  - Includes IP ranges to access the data from
  - Trusted signers (which AWS accounts can create signed URL)
- How long should the URL be valid for ?
  - Shared content (movie, music): make it short (a few minutes)
  - Private content (private to user) : you can make it last for years
- **Signed URL** = access to individual files (one signed URL per file)
- **Signed Cookies** = access to multiple files (one signed cookie for many files)

CloudFront Signed URL Vs S3 Pre-signed URL

CloudFront Signed URL: Allow access to a path, no matter the origin

S3 Pre-Signed URL:

- Issue a request as the person who pre-signed the URL
- Only to S3 and limited lifetime.

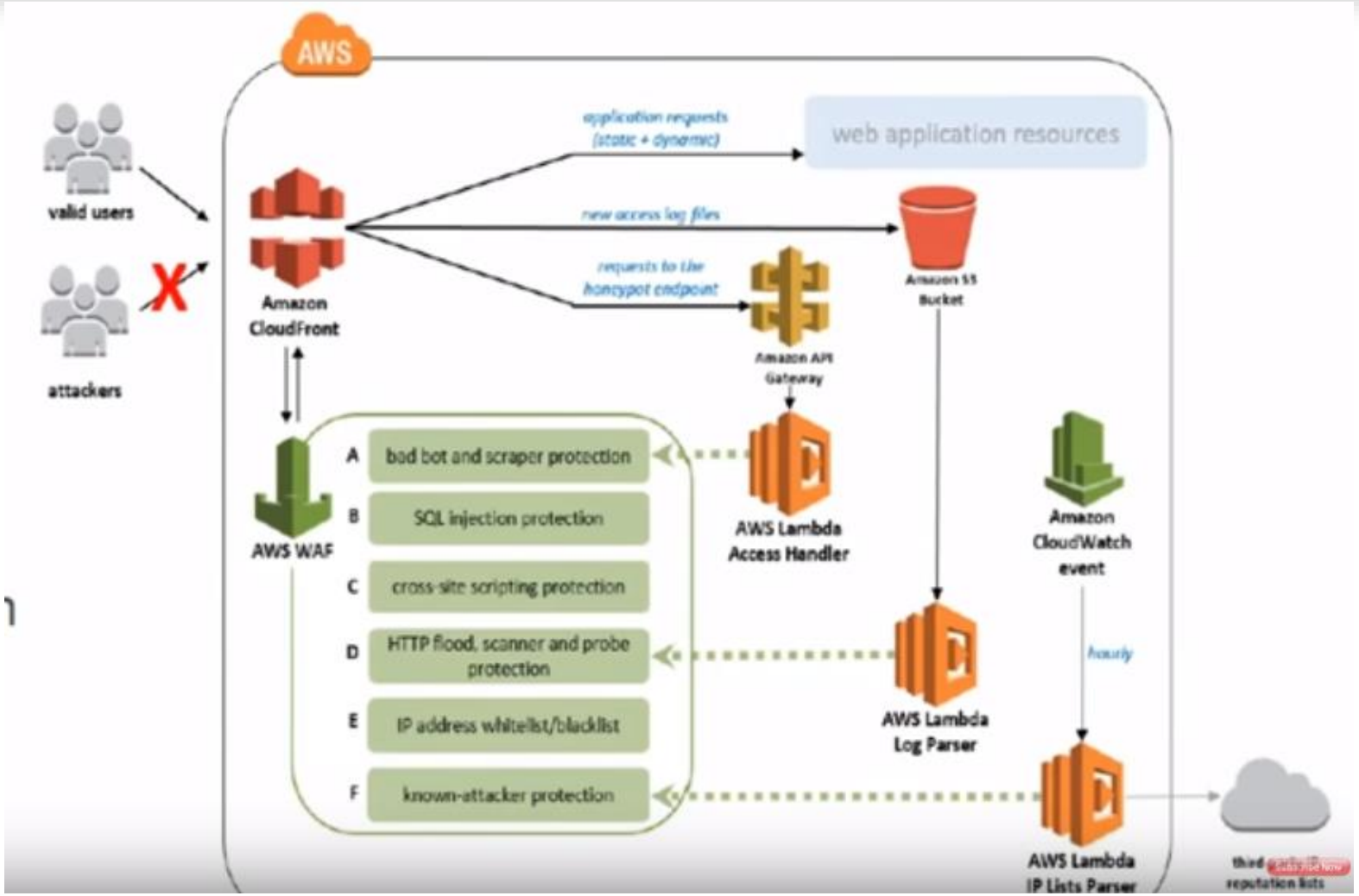
Cloudfront: Restrictions, Errors, Tags

- Geographical Restriction
  - White List or Black List
  - Country Level Granularity
- No Additional Charges

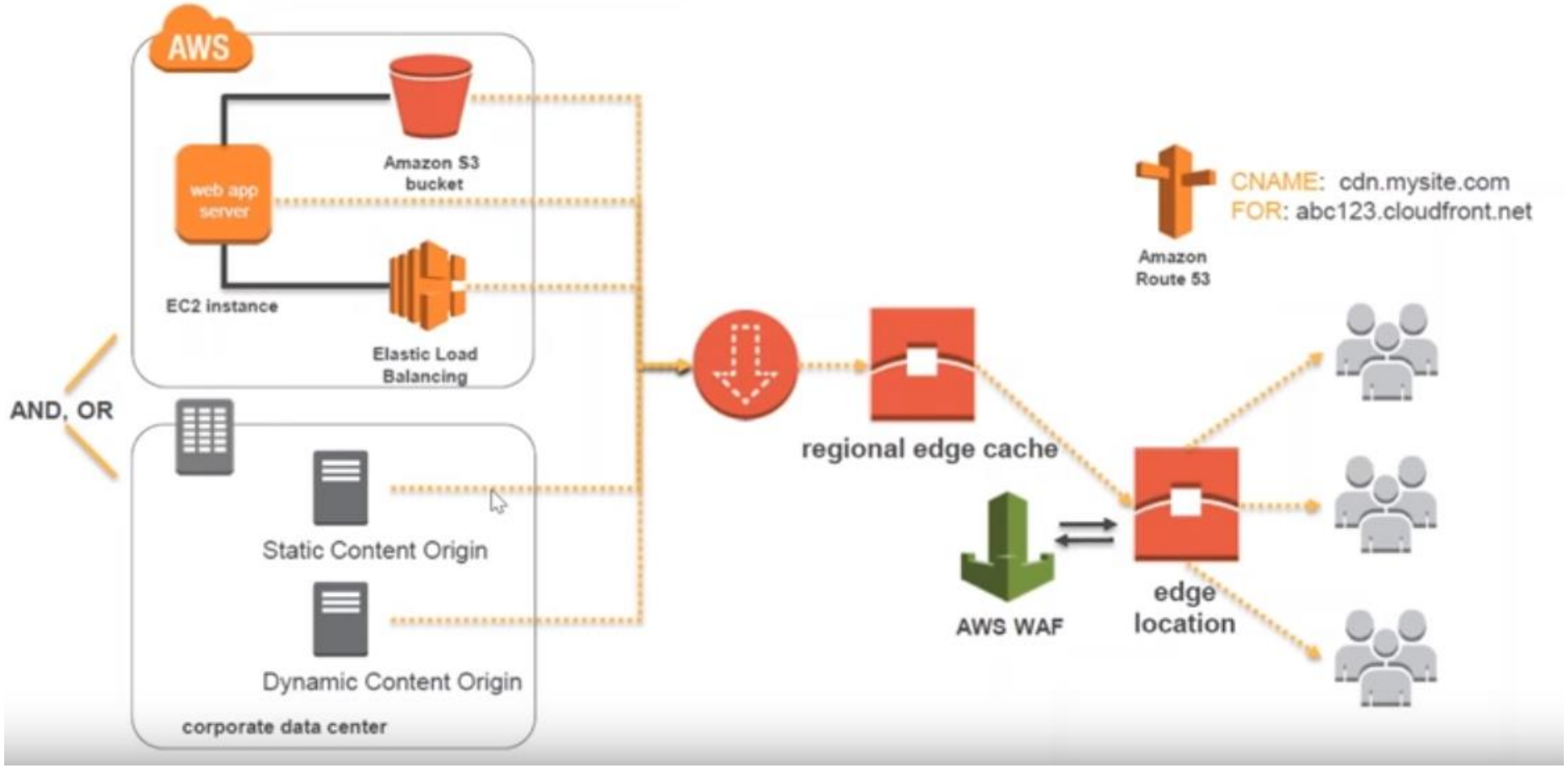
- Caching Error Pages
  - 4XX, 5XX Codes
  - Cache Default Page
  - Cache Custom Page

400: Bad Request
403: Forbidden
404: Not Found
405: Method Not Allowed
414: Request-URI Too Long
416: Requested Range Not Satisfiable
500: Internal Server Error
501: Not Implemented
502: Bad Gateway
503: Service Unavailable
504: Gateway Timeout

Cloudfront: WAF web ACLS



Cloudfront: Example Architecture

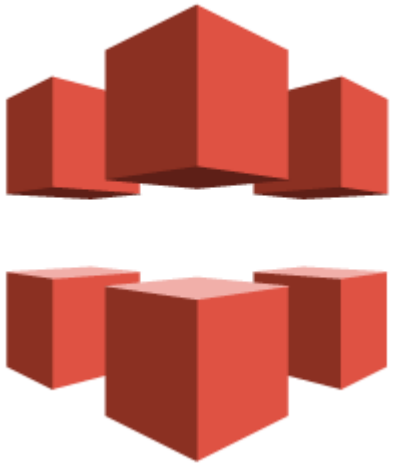


CloudFront Additional Info

- Edge locations can be used to read from and can write to them as well.
- Support for multiple origins
- Blacklist/whitelist geo-users/viewer access control is possible
- Your content will be cached for TTL and this can be defined.
- Cache can be cleared as well and will be charged for this operation.

CloudFront Exam Tips

- **Edge Location**: This is the location where content will be cached. This is separate to an AWS Region/AZ.
- **Origin: This i**s the origin of all the files that the CND will distribute. This can be either an S3 bucket, an EC2 instance, an ELB or Route53.
- **Distribution:** This is the name given to CDN which consist of collection of Edge locations.
- **Web Distribution:** Typically used for websites.
- **RTMP:** Used for Media Streaming
- Edge locations are not just READ only – you can write to them too(put an object to them)
- Objects are cached for the life of the TTL
- You can clear cached objects, but you will be charged.

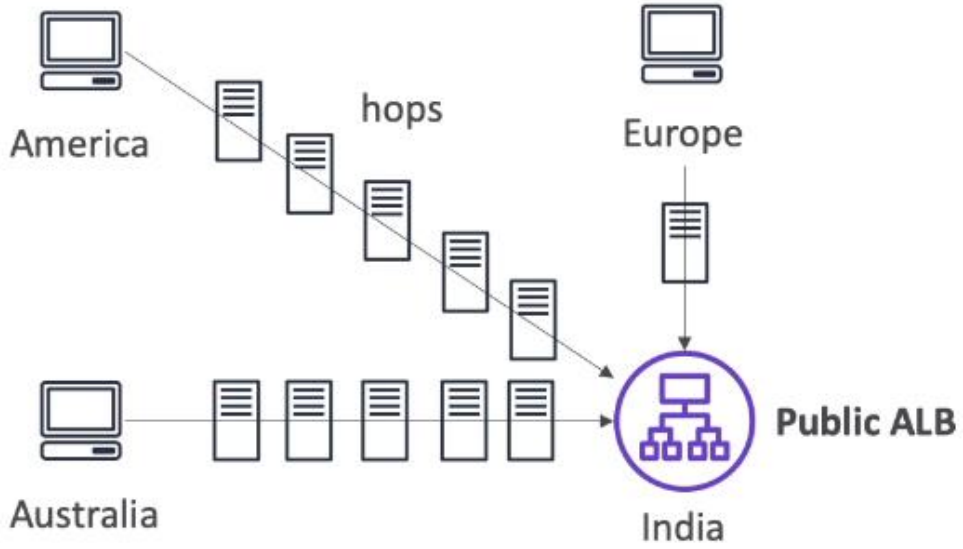


AWS Global Accelerator

Without Global Accelerator

Global Users for your application

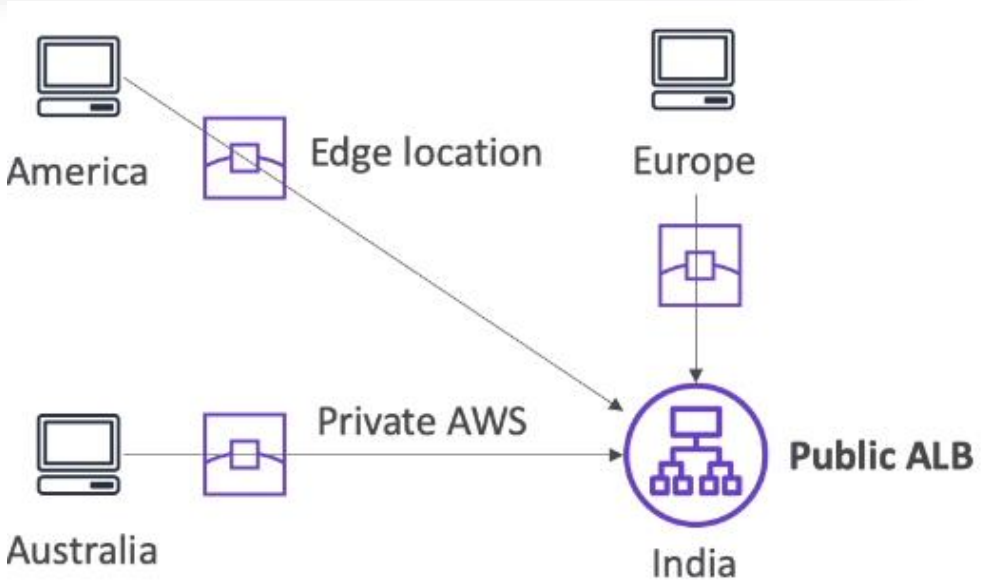
- You have deployed an application and have global users who want to access it directly
- They go over the public internet, which can add a lot of latency due to many hops
- We wish to go as fast as possible through AWS network to minimize latency



Client requests has to go to many hops and reach the application. If any hop fail, connection will lost

With Global Accelerator

- Leverage the AWS internal network to route to your application.
- 2 AnyCast IP are created for your application
- The Anycast IP send traffic directly to Edge Locations.
- The Edge locations send the traffic to your applications.



Note: Global Accelerator will use Edge location but not cache.

Request will reach edge location and from there it uses AWS internal network and reach directly to your application

Unicast IP: one server holds one IP address

Anycast IP: all servers hold the same IP address and the client is routed to the nearest one

Global Accelerator vs CloudFront

- They both use the AWS global network and its edge locations around the world
- Both services integrate with AWS Shield for DDoS protection

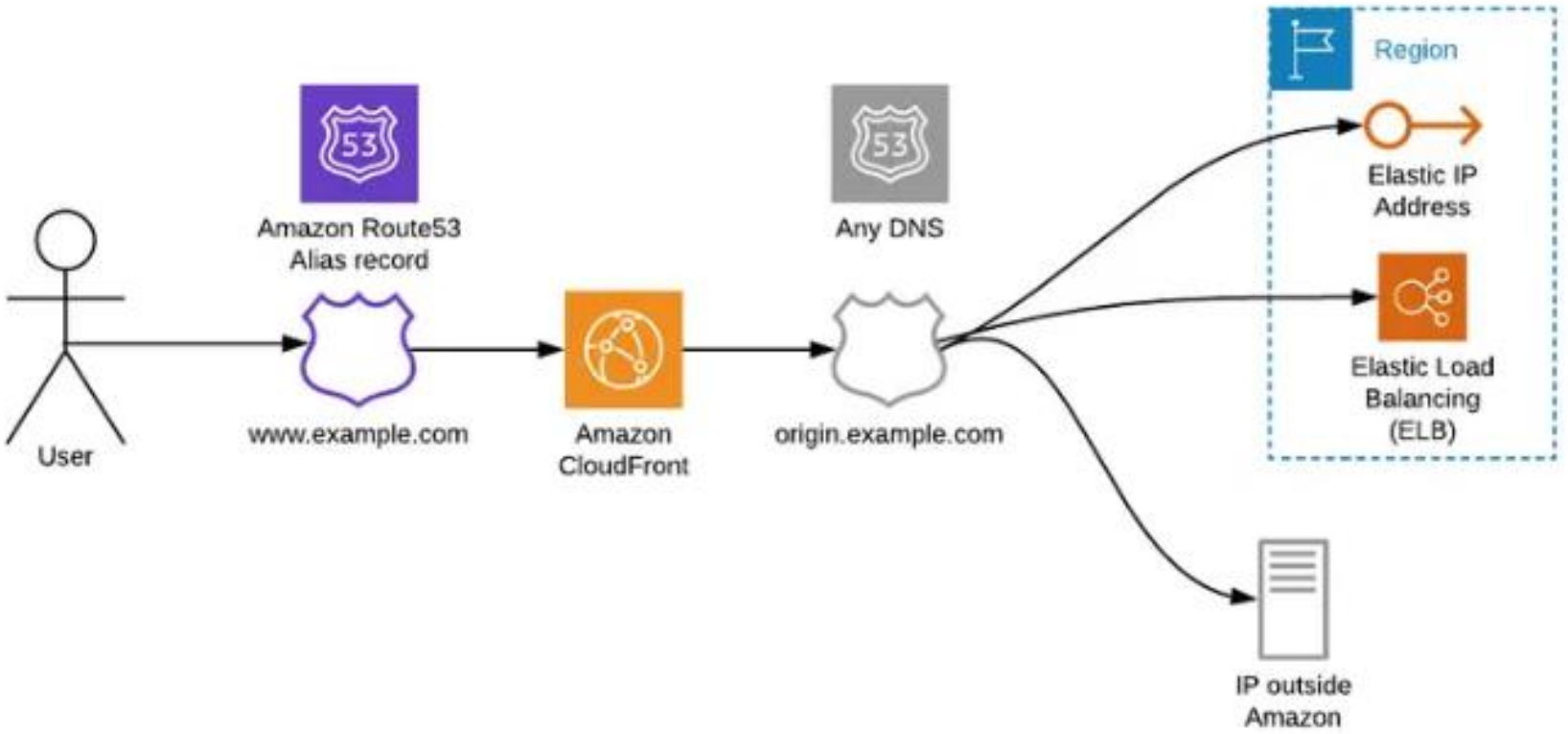
CloudFront

- Improves performance for both cacheable content (images and videos)
- Dynamic content (websites)
- Content is served at the edge

Global Accelerator

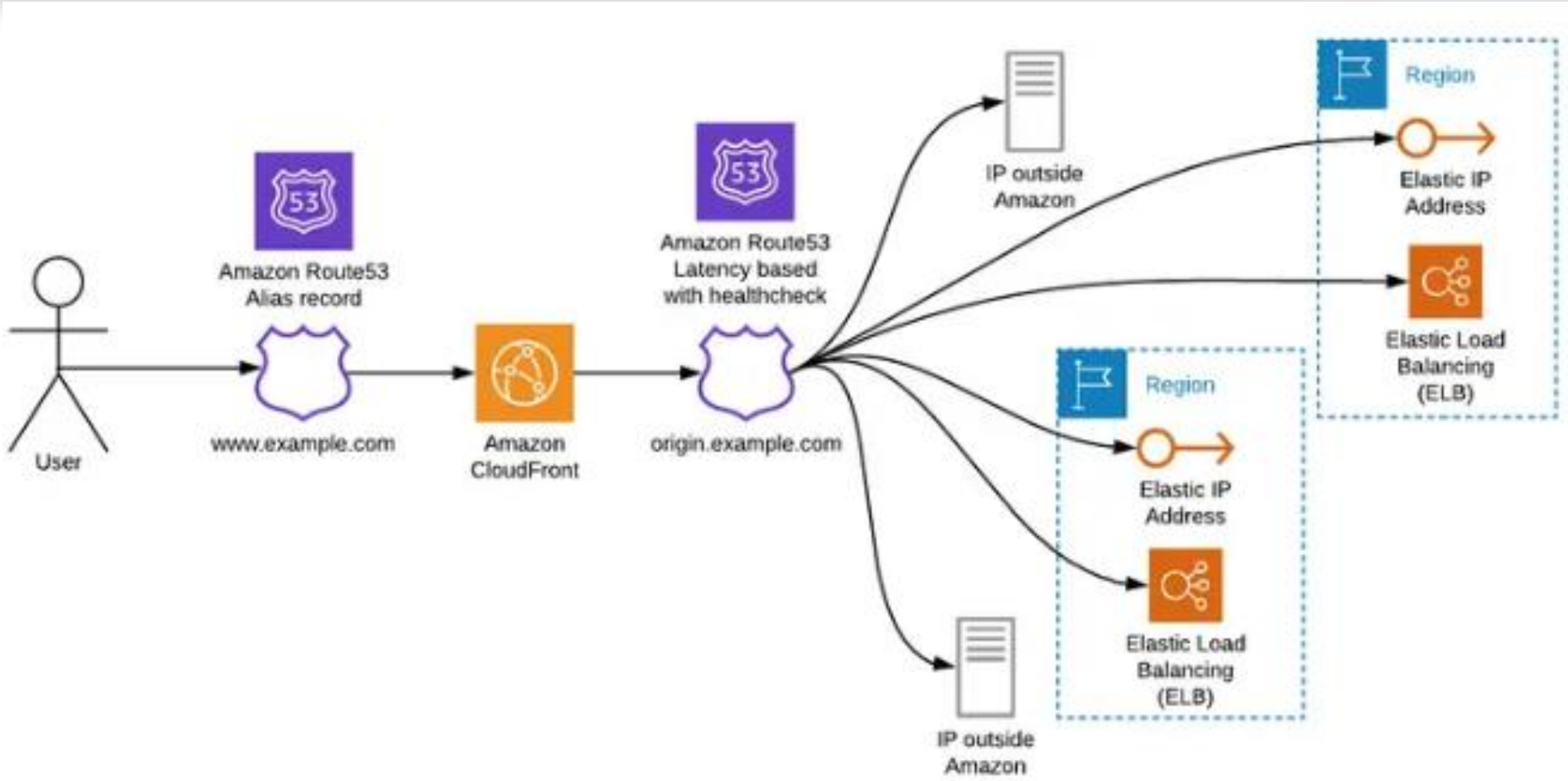
- Improves performance for a wide range of application over TCP or UDP
- Proxying packets at the edge to applications running in one or more AWS regions
- Can be used for failovers of applications in regions and static IP supported (cloudfront has many IPs)

The Old Good CloudFront



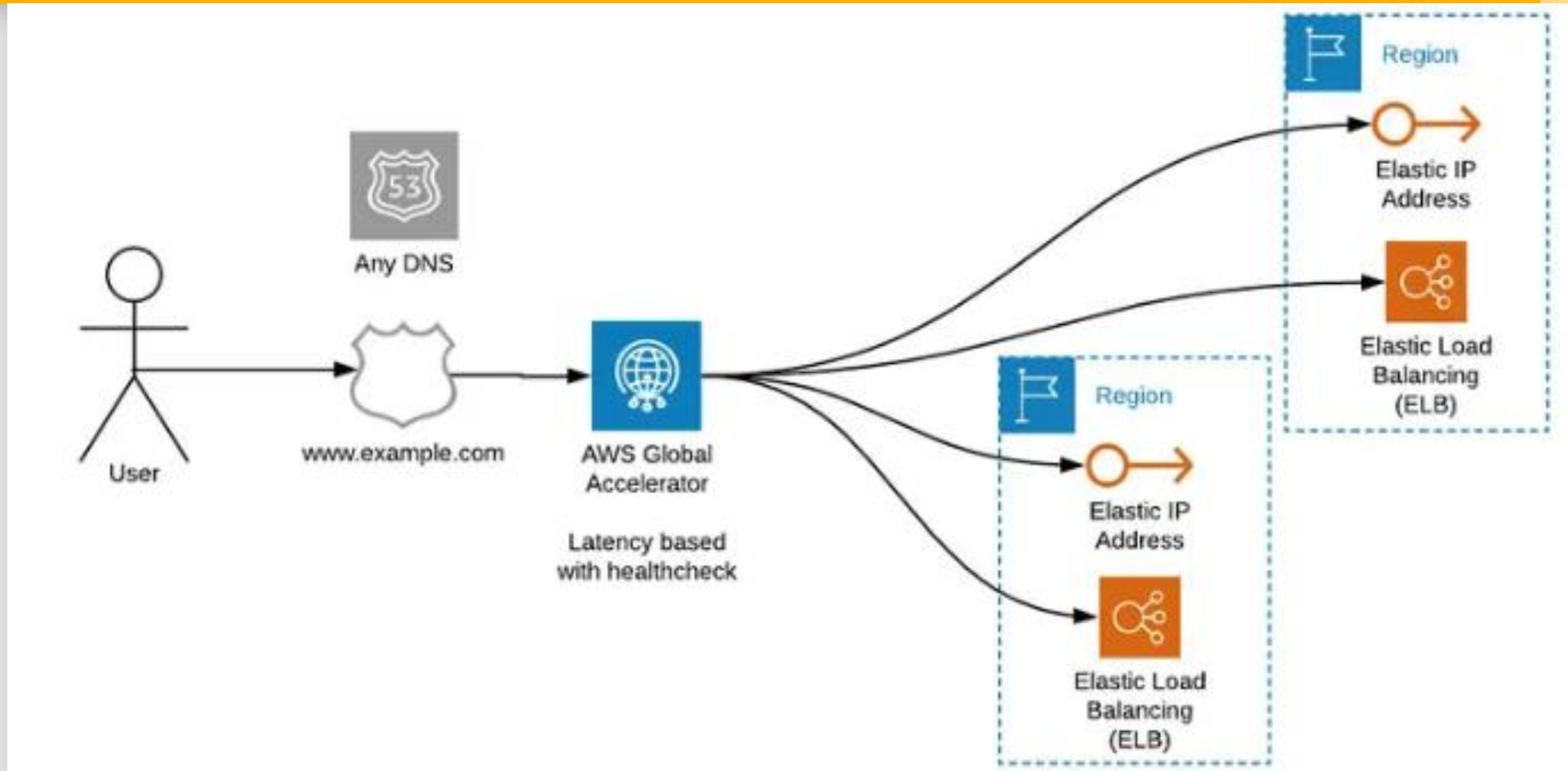
Schema 1. Website traffic goes via Cloudfront

Multi regional setup with CloudFront



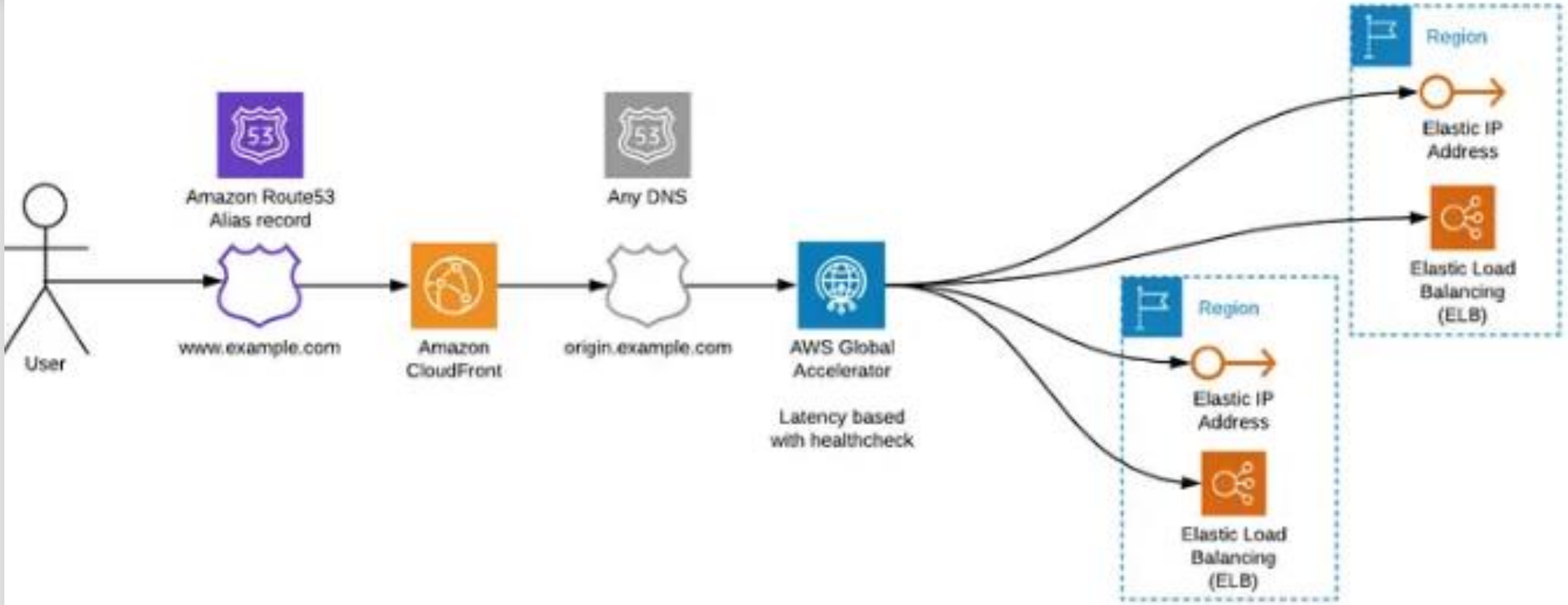
Schema 2. Multi regional setup with Cloudfront

AWS Global Accelerator without caching



Schema 3. Multi regional application using AWS Global Accelerator

Multi regional app with AWS Global Accelerator and CloudFront



Schema 4. Multi regional app using AWS Global Accelerator and Cloudfront

Demo

- Create a bucket and have a index.html page
- Create distribution and point to s3
- Access CDN.