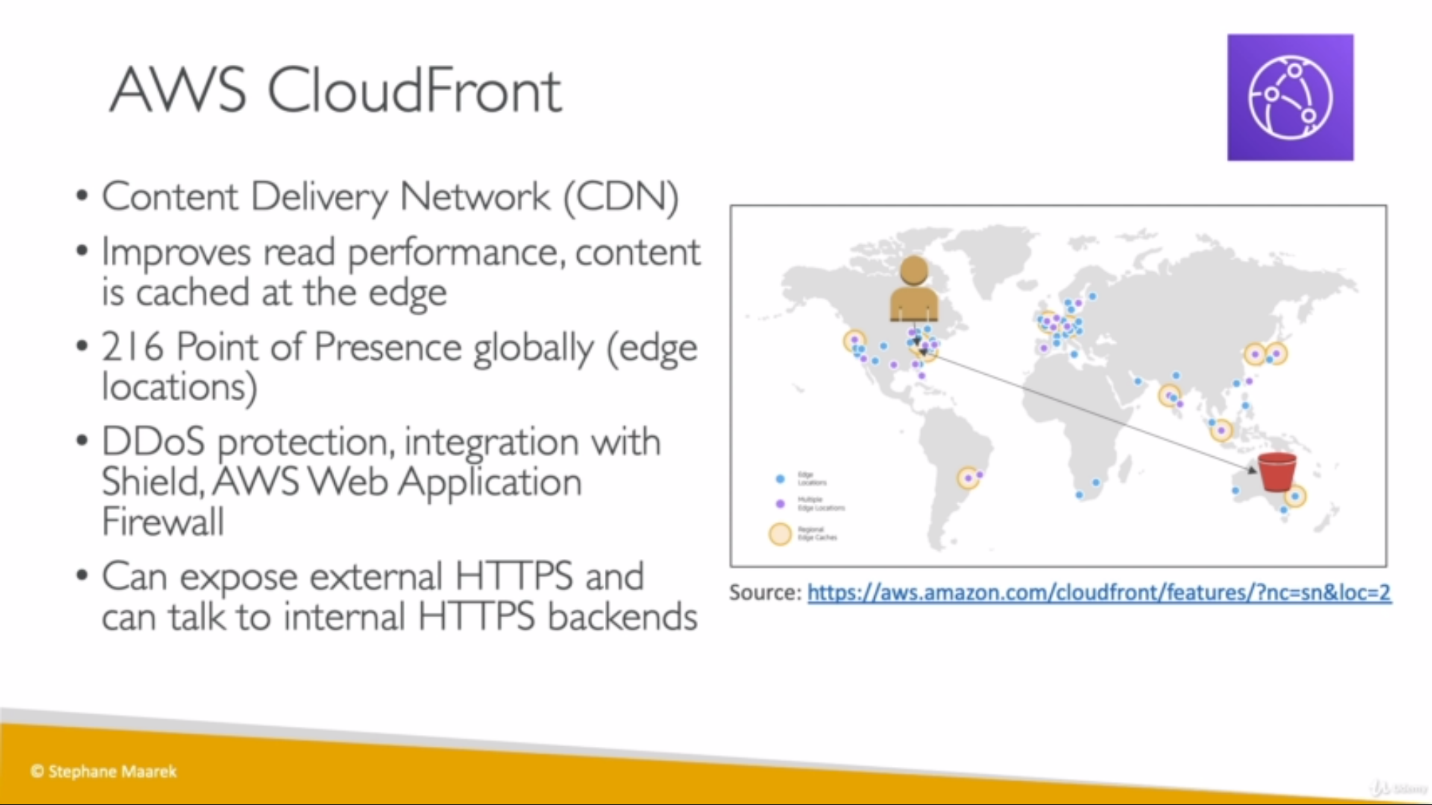
**Topic: CloudFront (CDN), CloudFront origin (S3,EC2,ALB) and edge, Geo restriction(whitelist and blacklist countries)**

**CloudFront:**

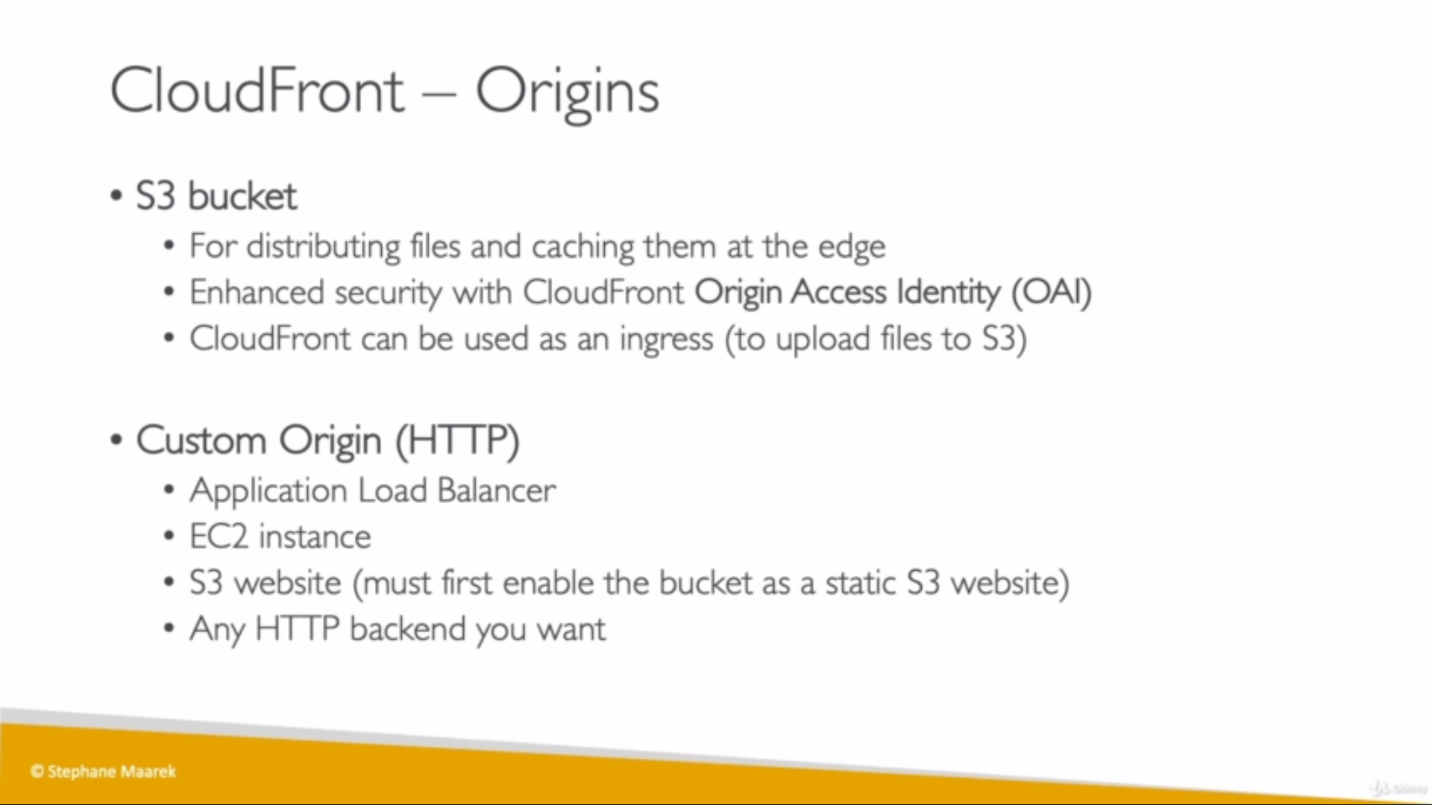
Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront is integrated with AWS – both physical locations that are directly connected to the AWS global infrastructure, as well as other AWS services. CloudFront works seamlessly with services including AWS Shield, Amazon S3, Elastic Load Balancing or Amazon EC2 as origins for our applications, and Lambda@Edge to run custom code closer to customers’ users and to customize the user experience. Lastly, if we use AWS origins such as Amazon S3, Amazon EC2 or Elastic Load Balancing, we don’t pay for any data transferred between these services and CloudFront.



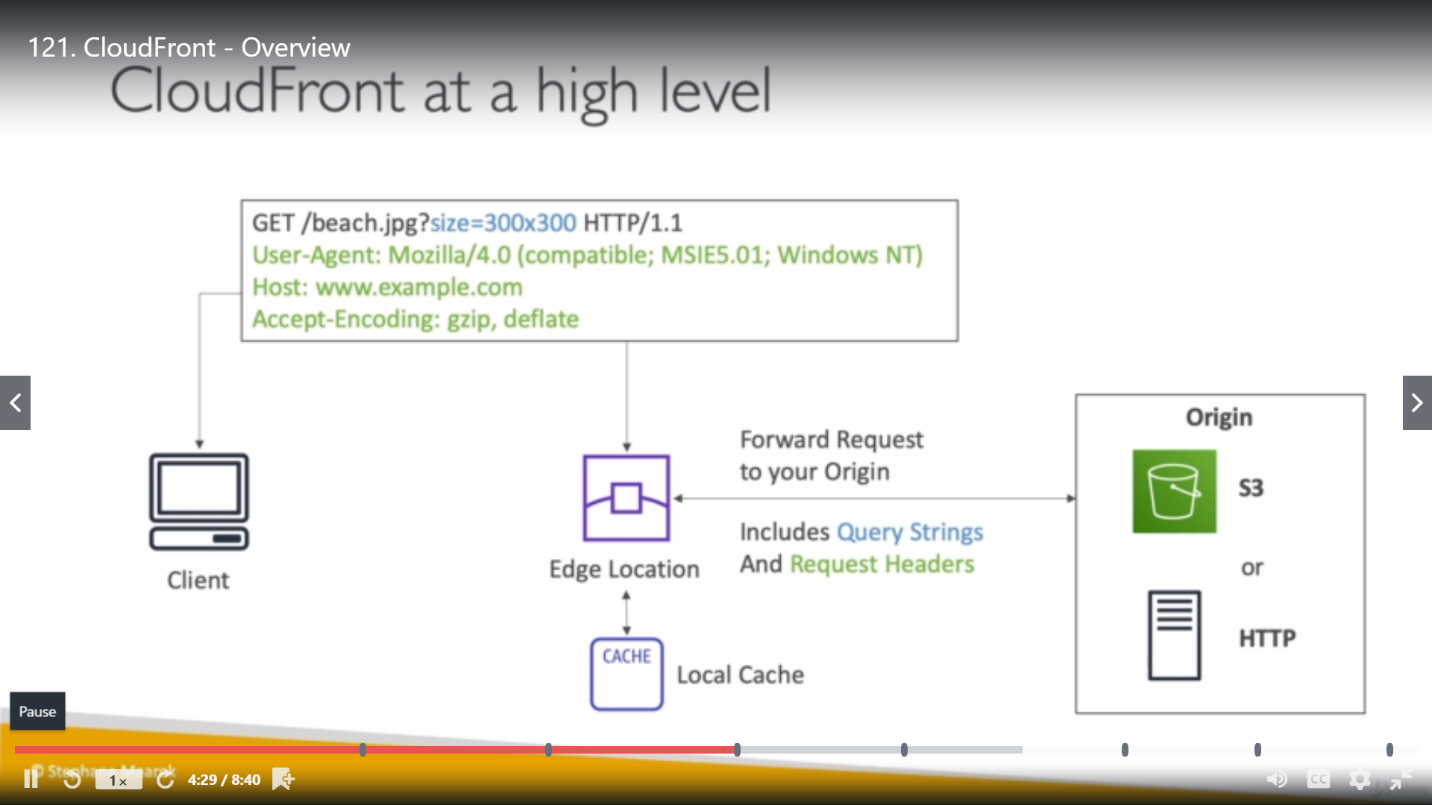
**Cloudfront Origin:**

A complex type that describes the Amazon S3 bucket, HTTP server (for example, a web server), Amazon MediaStore, or other server from which CloudFront gets our files. This can also be an origin group, if we've created an origin group. we must specify at least one origin or origin group.

Ingress: entry

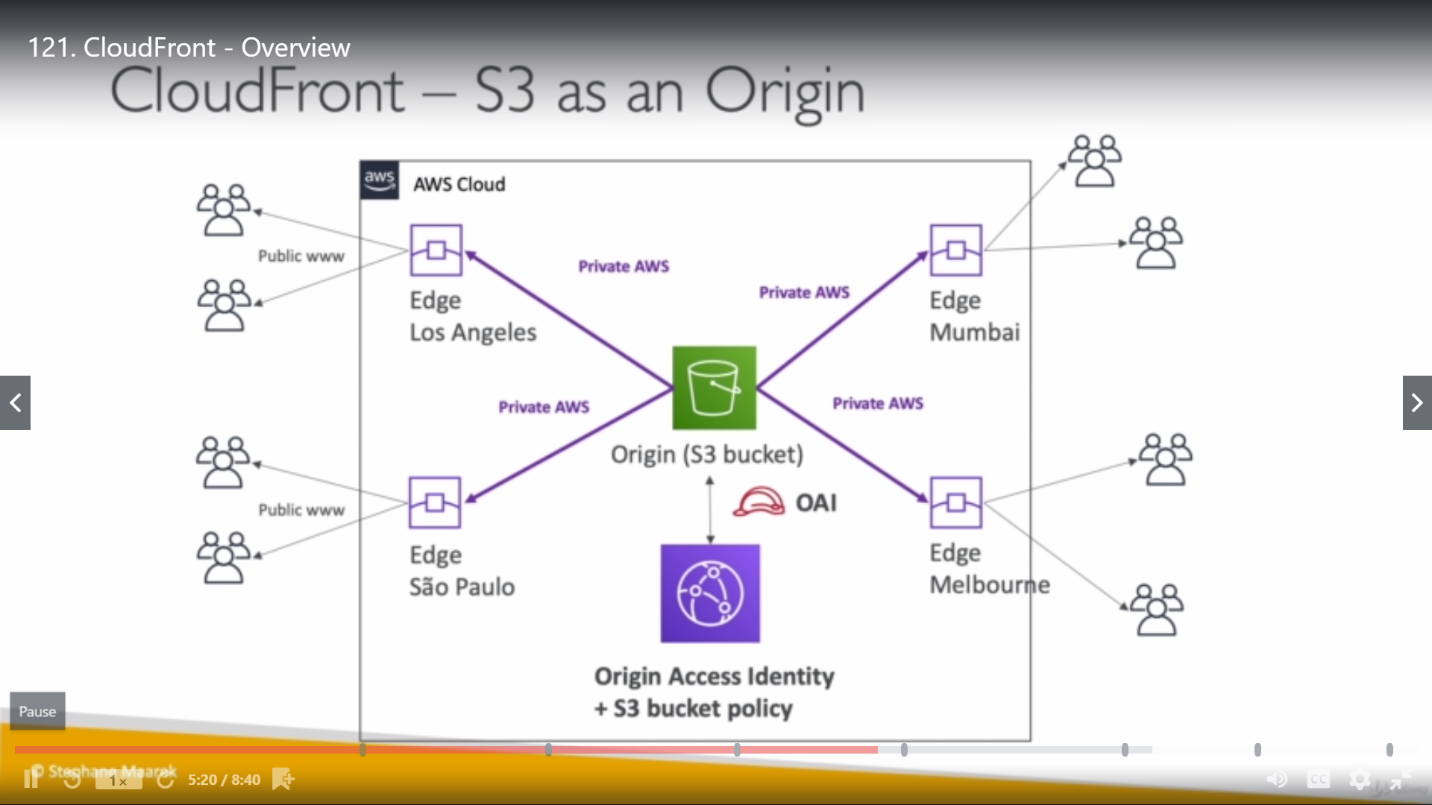


**How CloudFront origin and Edge location works:**



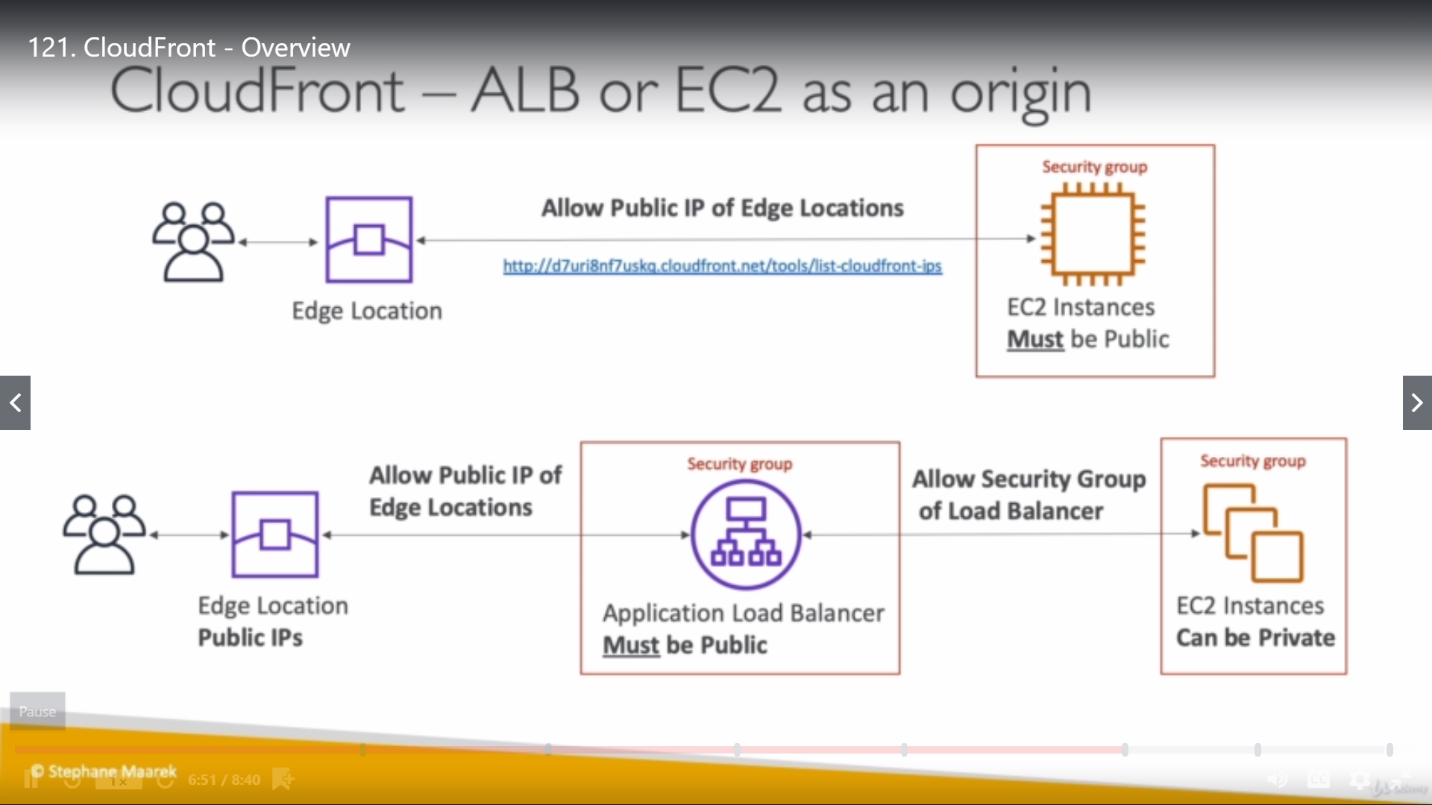
So, if next time similar request comes from any client, it won’t go to origin rather fulfilled by Local cache.

**Cloudfront S3 as origin:**



If a client wants to access S3 bucket, request will come to nearly Edge location and Edge location will communicate to S3 bucket privately. There are rules (Origin Access Identity) defined for S3 bucket which define whether request can be fulfilled or not.

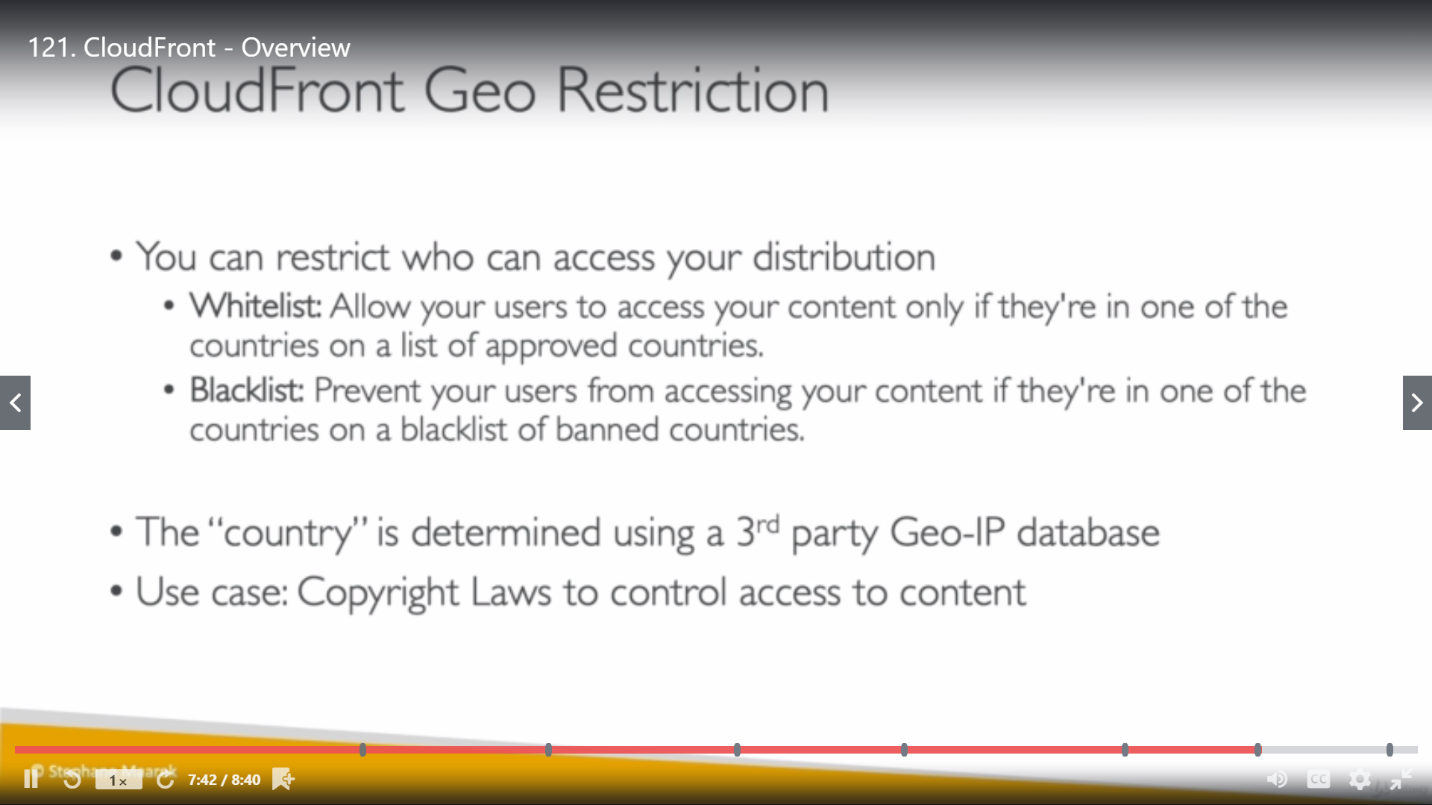
**Cloudfront EC2 or ALB as origin:**



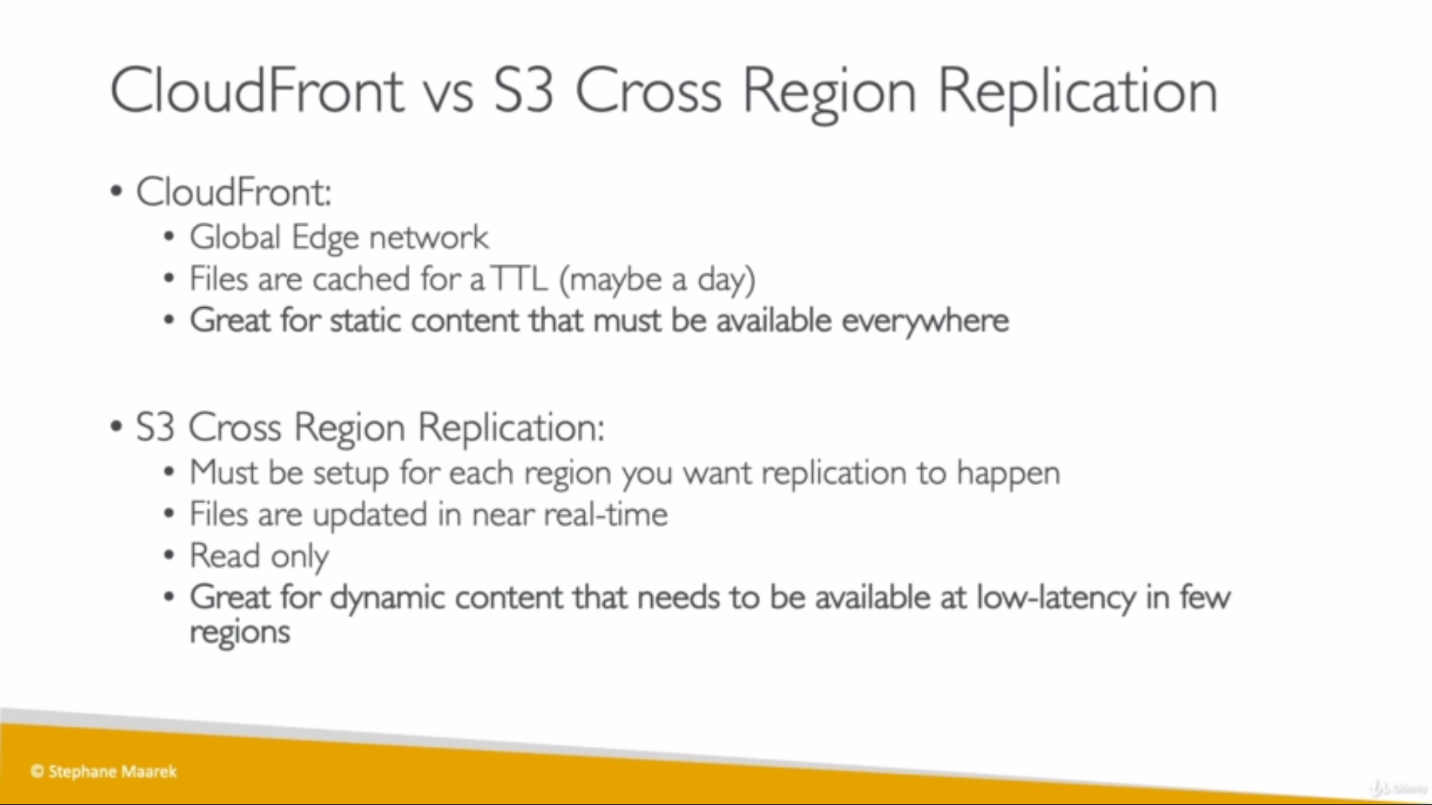
EC2 instance should be public and security group attached to it must allowed all public IPs of Edge location to access it.

In case of ALB, ALB must be public but EC2 instances can be private.

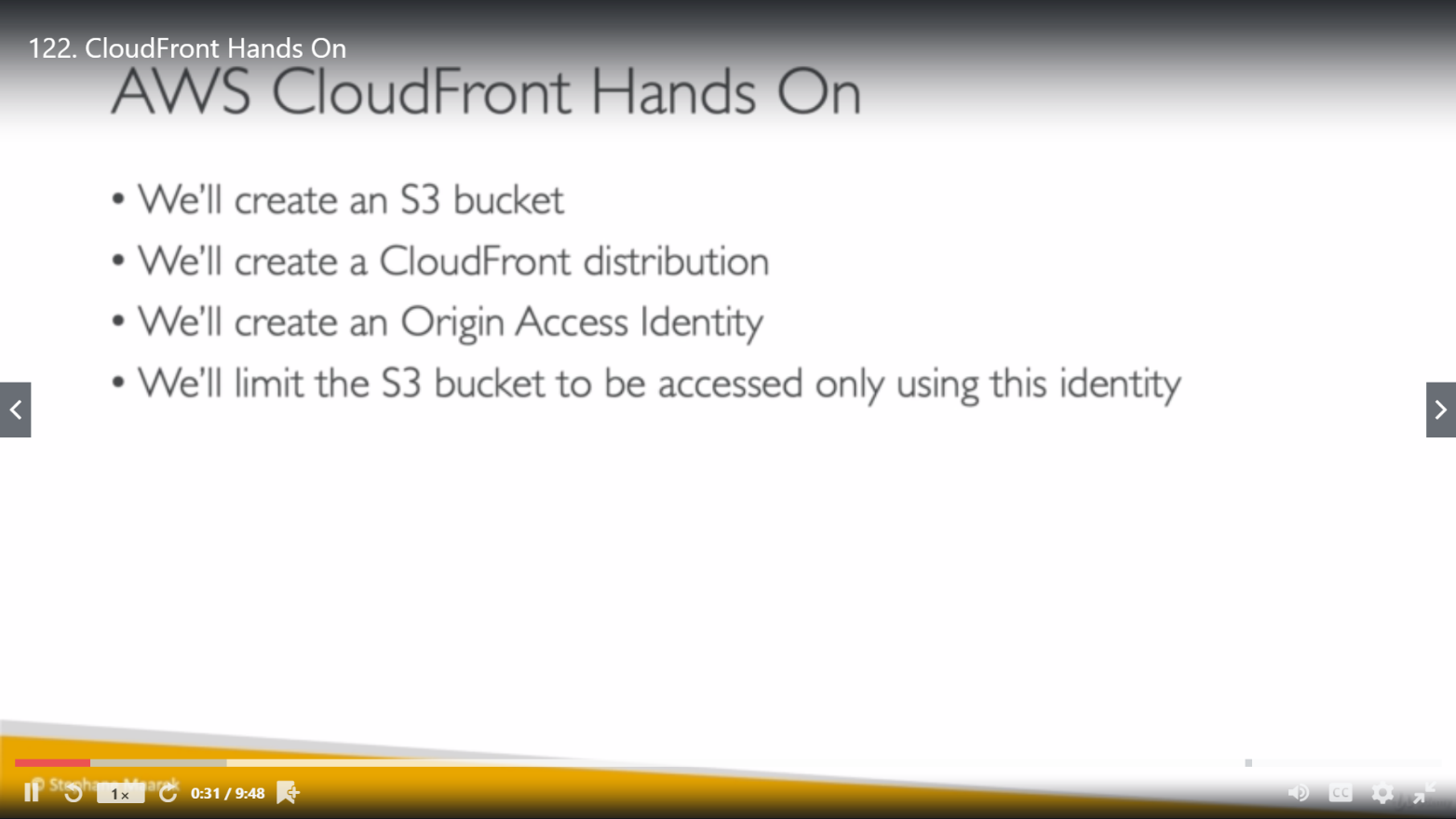
**Cloudfront Geo restriction:**



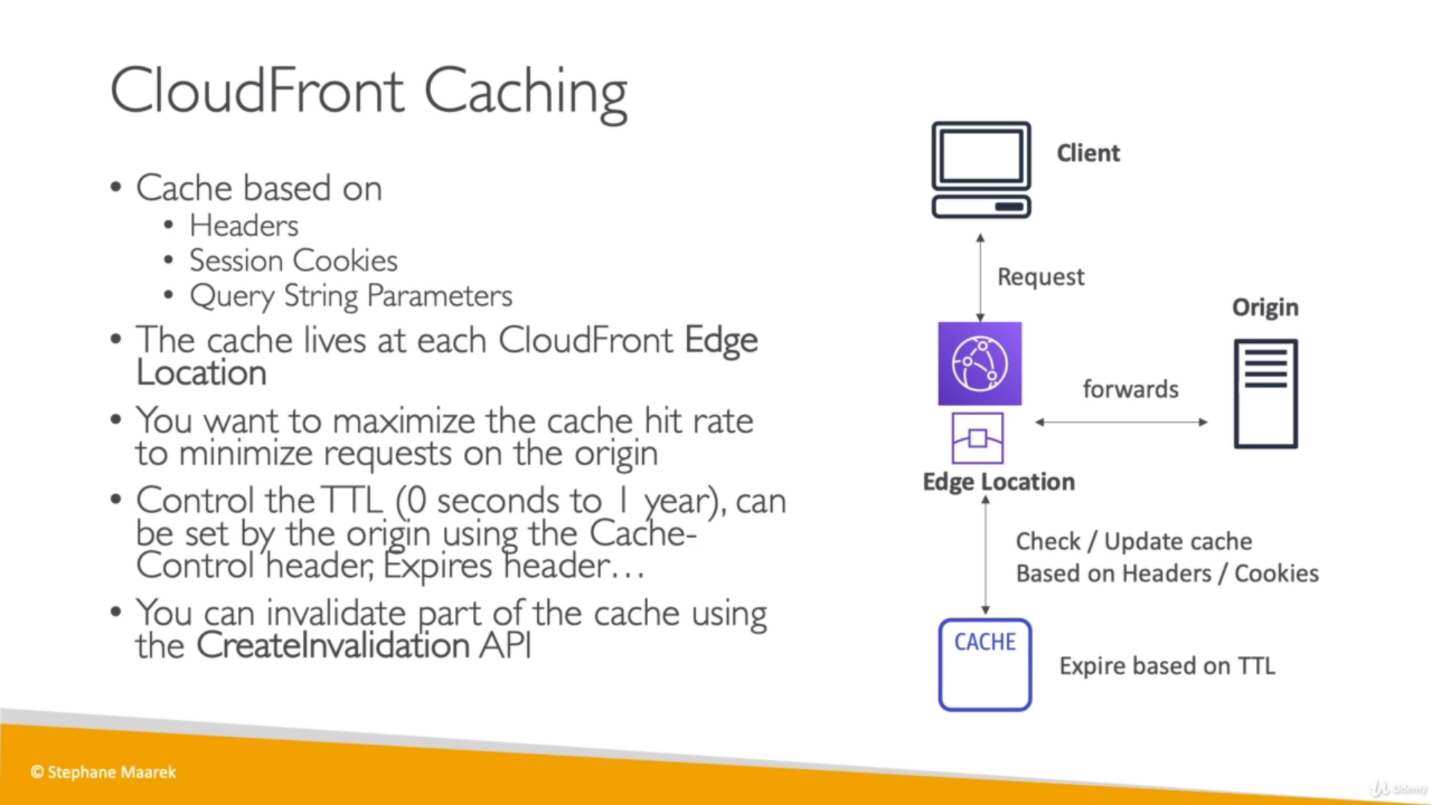
**Difference between CloudFront and Cross Region Replica:**

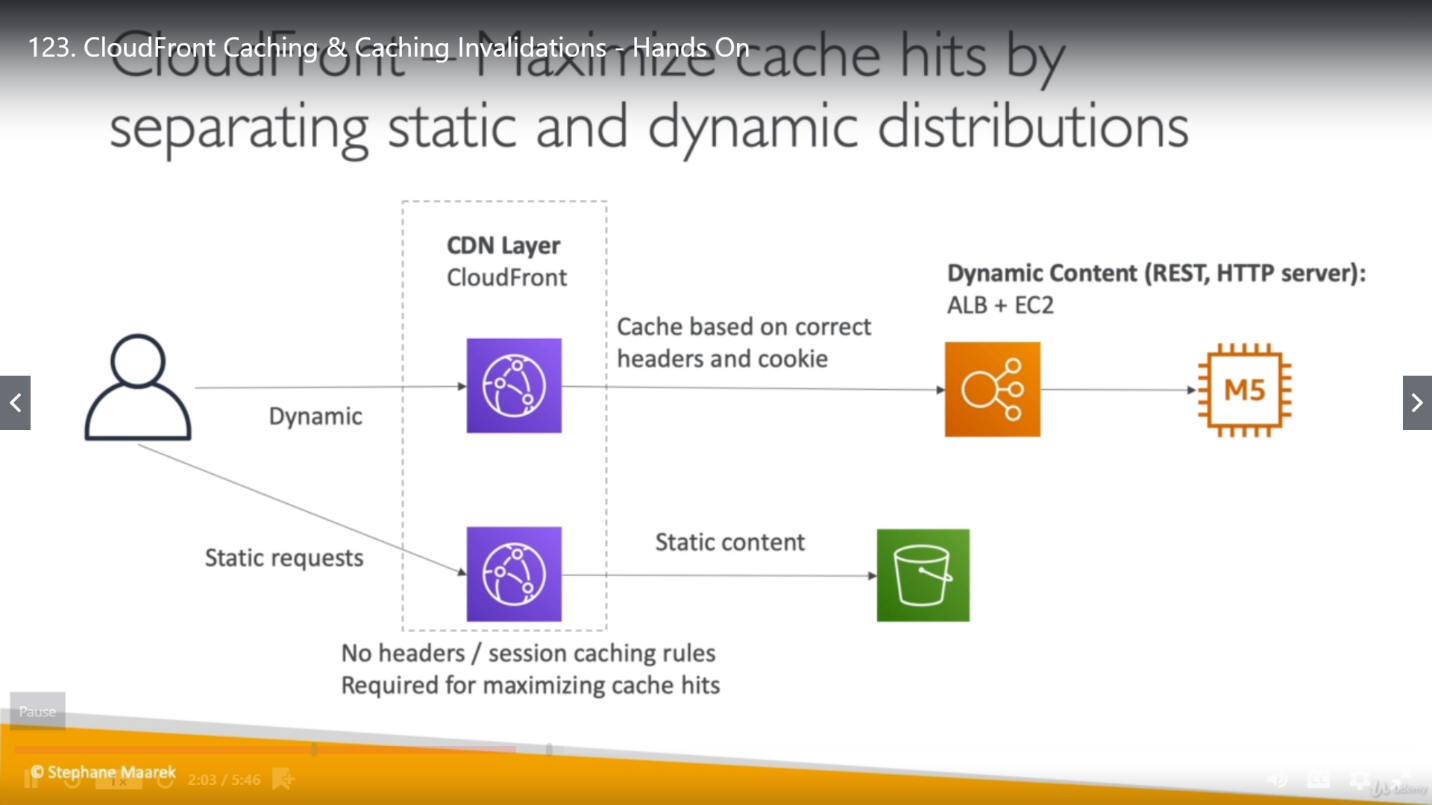


**LAB:**



**Cloudfront Cache:**



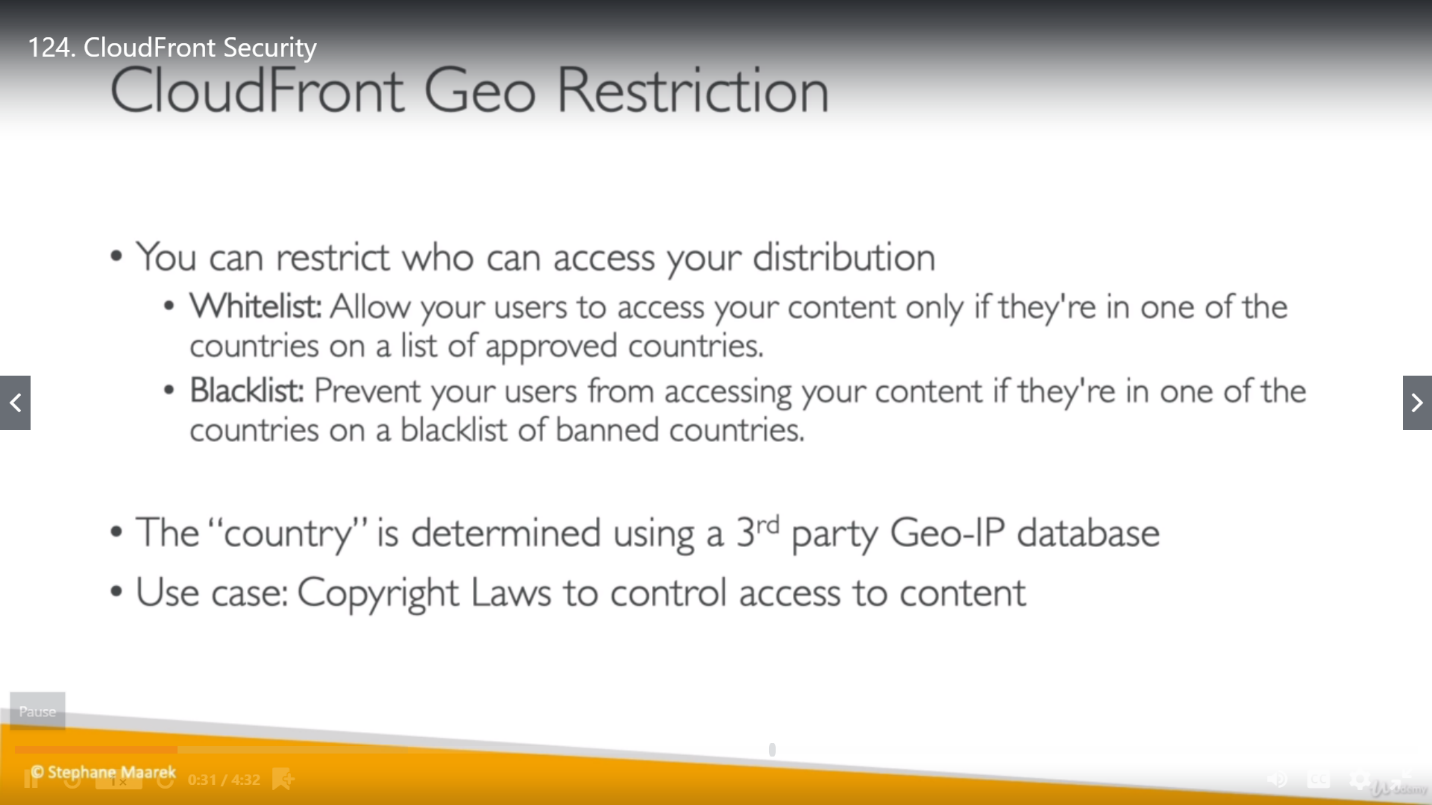


If we want to force Edge location to clear the cache data, then we can configure Invalidations under CloudFront Distribution.

**Cloudfront Security:**

1. **Geolocation restriction:**

We can setup Geolocation restriction on Cloudfront distribution to give permission who can access distribution based on geolocation (country).

****

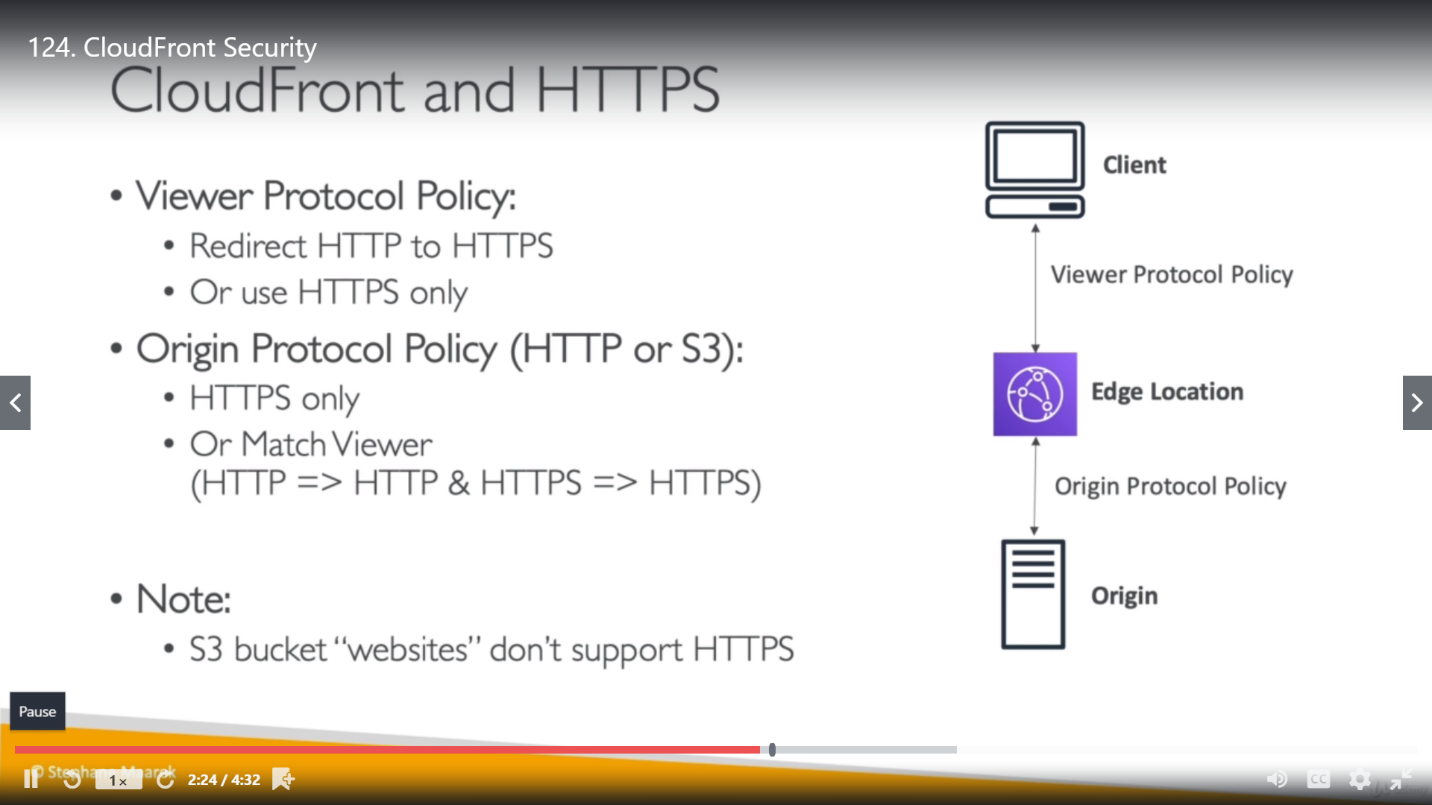
1. **HTTPS Restriction:**
2. **Viewer Protocol Policy**: We have to make sure that traffic going into CloudFront is encrypted. Choose the protocol policy that you want viewers to use to access your content in CloudFront edge locations:

* **HTTP and HTTPS:** Viewers can use both protocols.
* **Redirect HTTP to HTTPS:** Viewers can use both protocols, but HTTP requests are automatically redirected to HTTPS requests.
* **HTTPS Only:** Viewers can only access your content if they're using HTTPS.

1. **Origin Protocol Policy:** This applies only to custom origins. The protocol policy that we want CloudFront to use when fetching objects from our origin server.

Choose one of the following values:

* **HTTP Only:** CloudFront uses only HTTP to access the origin. HTTP Only is the default setting when the origin is an Amazon S3 static website hosting endpoint, because Amazon S3 doesn’t support HTTPS connections for static website hosting endpoints. The CloudFront console does not support changing this setting for Amazon S3 static website hosting endpoints.
* **HTTPS Only:** CloudFront uses only HTTPS to access the origin.
* **Match Viewer:** CloudFront communicates with our origin using HTTP or HTTPS, depending on the protocol of the viewer request. CloudFront caches the object only once even if viewers make requests using both HTTP and HTTPS protocols.



**Cloudfront Signed URL and Signed Cookies:**



