ELASTIC LOAD BALANCER(ELB)

1/ Your Browser requests the IP address of the Load Balancer from DNS.
2/ DNS returns the IP address of the Load Balance.
3/ Your Browser uses the IP address to request the html page via HTTP from the Load Balancer.
4/ AWS perimeter devices checks and forwards the request to the Load Balancer.
5/ The Load Balancer finds an active web server and forwards the HTTP request.
5/ The web server returns the requested html file via the Load Balancer.
6/ Your Browser processes the HTML file and paints a graphical representation on your screen.

Separately/ The Load Balancer checks the health of each web server by reading the healthcheck.html at the frequency & interval set.
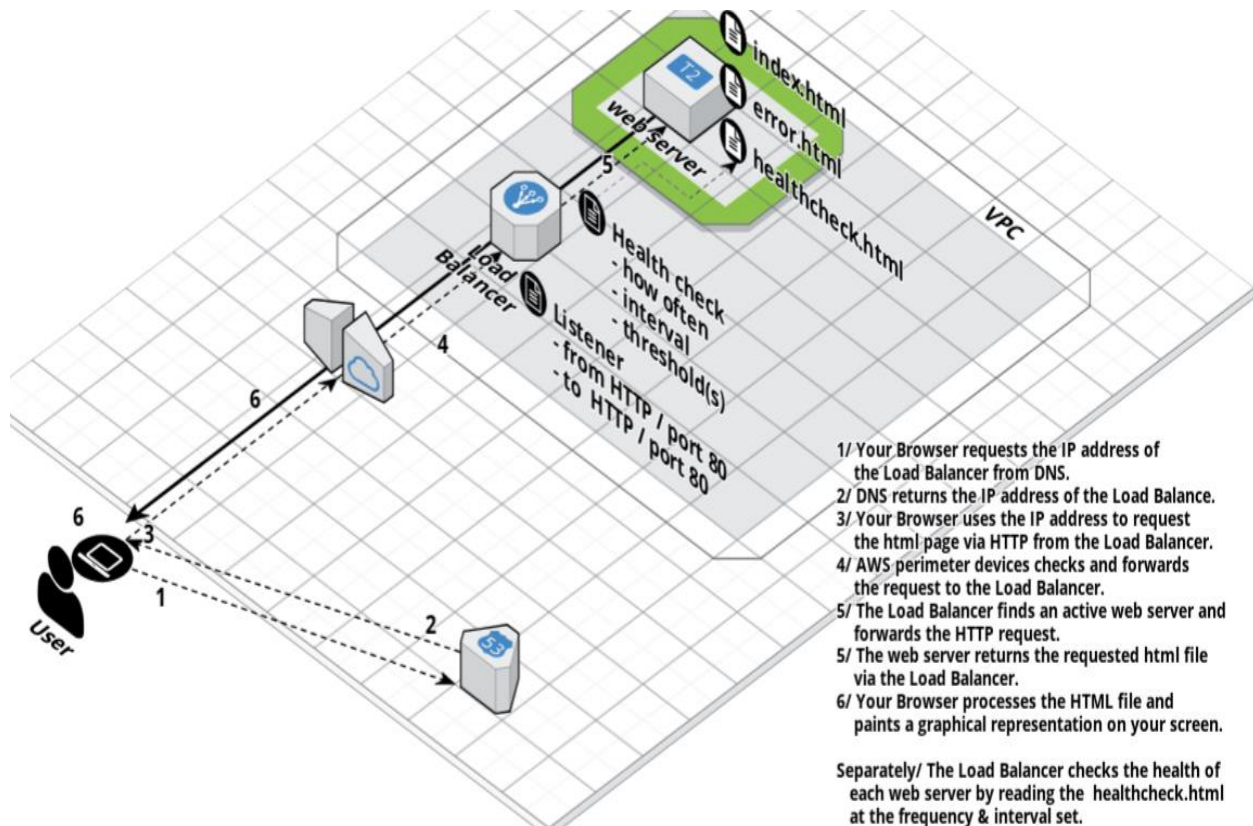
http://clusterfrak.com/notes/certs/aws_saa_notes/

Elastic Load Balancing offers two types of load balancers that both feature high availability, automatic scaling, and robust security. These include the Classic Load Balancer that routes traffic based on either application or network level information, and the Application Load Balancer that routes traffic based on advanced application level information that includes the content of the request.

- When configuring ELB health checks, bear in mind that you may want to create a file like healthcheck.html or point the ping path of the health check to the main index file in your application.
- Remember the health check interval is how often a health check will occur.
- Your Healthy/Unhealthy thresholds are how many times either will check before marking the origin either healthy or unhealthy

  - Health Check Interval: 10 seconds
  - Unhealthy Threshold: 2
  - Healthy Threshold: 3
  - This means that if the health check interval occurs twice without success, then the source will be marked as unhealthy. This is 2 checks @ 10 seconds per check, so basically after 20 seconds the origin will be marked unhealthy

- o Likewise, if the healthy threshold is marked at 3, then it would be 3 x health check interval or 10 seconds being 30 seconds. After 30 seconds with 3 consecutive success checks, the origin will be marked as healthy.
- Enable Cross-Zone Load Balancing will distribute load across all back-end instances, even if they exist in different AZ's.
- ELBs are NEVER given public IP Addresses, only a public DNS name.
- ELBs can be In Service or Out of Service depending on health check results.
- Charged by the hour and on a per GB basis of usage.
- Must be configured with at least one listener.
- A listener must be configured with a protocol and a port for front end (client to ELB connection), as well as a protocol and port for backed end (ELB to instances connection)
- ELBs support HTTP, HTTPS, TCP, and SSL (Secure TCP).
- ELBs support all ports (1-65535).
- ELBs do not support multiple SSL certificates.
- Classic ELBs support the following ports:
    - o 25 (SMTP)
    - o 80 (HTTP)
    - o 443 (HTTPS)
    - o 465 (SMTPS)
    - o 587 (SMTPS)
    - o 1024-65535
- HTTP Error Codes:
    - o 200 - The request has succeeded
    - o 3xx - Redirection
    - o 4xx - Client Error (404 not found)
    - o 5xx - Server Error

Application Load Balancer Limit	Default Limit
Load balancers per region:	20
Target groups per region:	50
Listeners per load balancer:	10
Targets per load balancer:	1000
Subnets per Availability Zone per load balancer:	1
Security groups per load balancer:	5

Application Load Balancer Limit	Default Limit
Rules per load balancer (excluding defaults:	10
No. of times a target can be registered per LB:	100
Load balancers per target group:	1
Targets per target group :	1000
Classic Load Balancer Limit	**Default Limit**
Load balancers per region:	20
Listeners per load balancer:	100
Subnets per Availability Zone per load balancer:	1