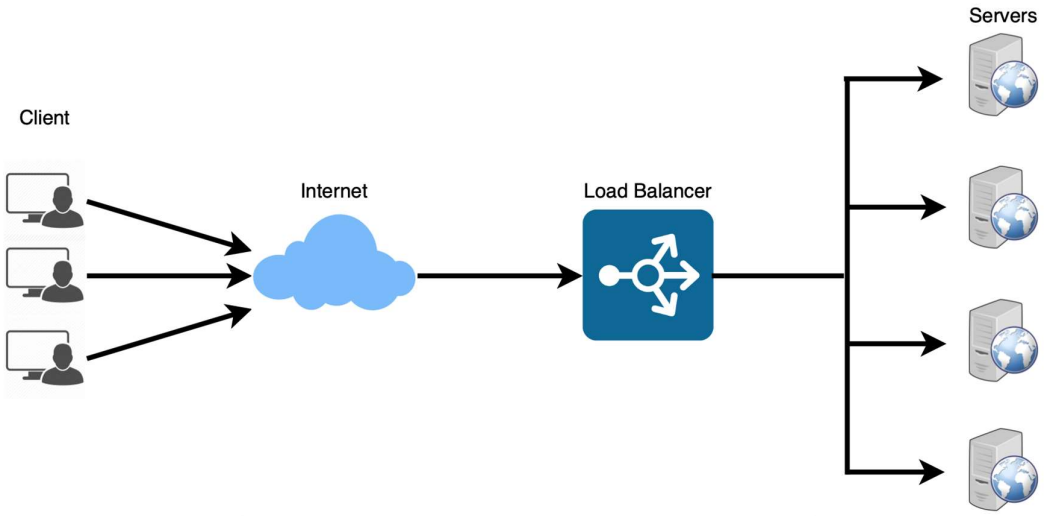
**Elastic Load Balancing:**

- Load balancing is the process of distributing workload evenly across multiple servers.
- This helps spread the traffic across a cluster of servers to enhance applications, websites responsiveness and availability.
- Load Balancers also detect the health of back end resource and do not send traffic to servers, which cannot achieve requests, along these lines load balancers can improve network and application performance by controlling and handling applications and network sessions automatically by using various algorithms.
- Load balancers can help Minimize the risk of denial-of-service attacks in addition to providing simple distributed service to multiple servers, grant legitimate users to access services without interruption, protect against single-point failures and avoid network traffic bottlenecks.
- Therefore, we can say that the LB is first line of defense against DDOS.
- ELB automatically distributes your incoming application traffic across all the EC2 instances that you are running.




Elastic Load Balancing provides four types of load balancers that can be used.

**Application Load Balancer:**

- Routes and load balances at the application layer (HTTP/HTTPS), and supports path-based routing.
- An Application Load Balancer can route requests to ports on one or more registered targets, such as EC2 instances, in your virtual private cloud (VPC).

**Network Load Balancer:**

- Routes and load balances at the transport layer (TCP/UDP Layer-4), based on address information extracted from the Layer-4 header.
- Network Load Balancers can handle traffic bursts, retain the source IP of the client, and use a fixed IP for the life of the load balancer.

**Gateway Load Balancer:**

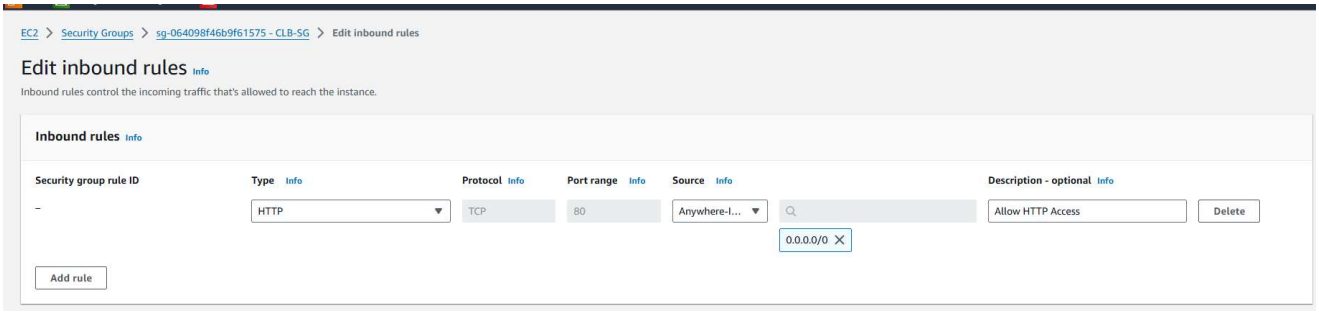
- Gateway Load Balancers work with virtual appliances that support the GENEVE protocol.

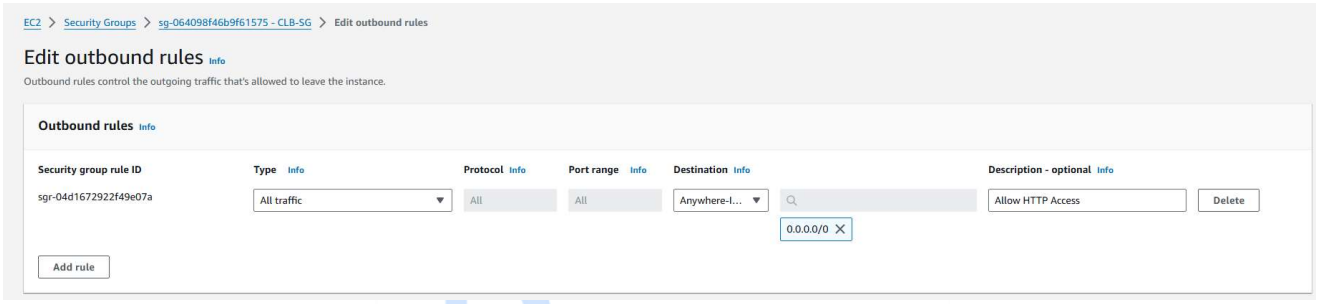
**Classic Load Balancer:**

- Routes and load balances either at the transport layer (TCP/SSL), or at the application layer (HTTP/HTTPS).

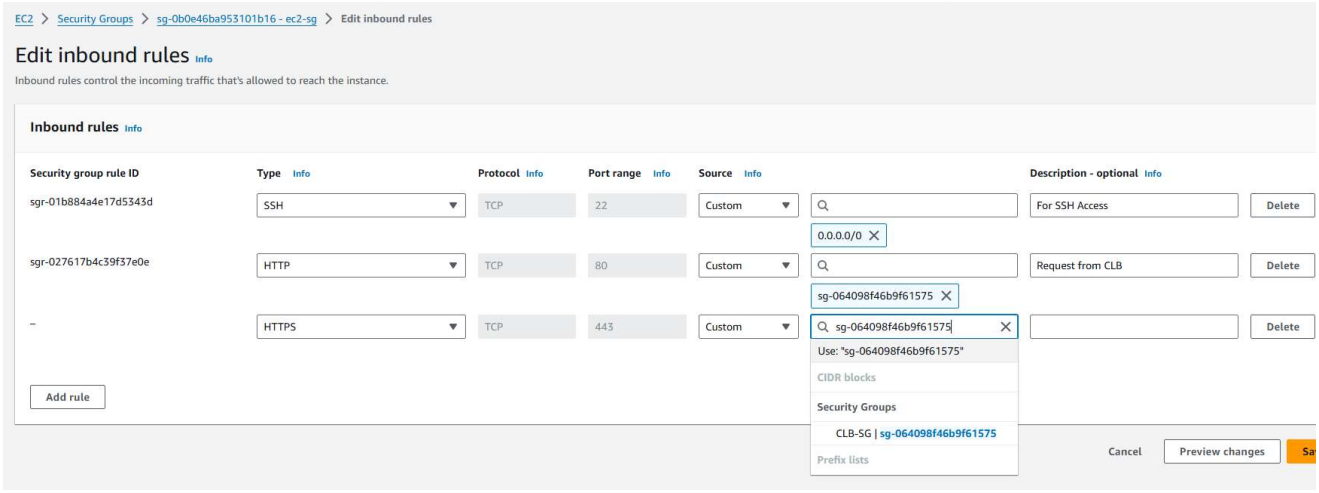
**Create a Classic Load Balancer:**

1. Login to AWS Console.
2. Go to EC2.
3. Create a security group for CLB. Here we should allow **only HTTP access** under inbound rule and allow **all traffic** under outbound rule.




4. Before creating a CLB, let's create 3 EC2 instances, on top of which we will create a CLB.
5. Create a separate Security Group for EC2 instances. For the EC2 instances, we will allow both HTTP and HTTPS access.




6. While launching EC2 instances, add following script under user data section.

```
#!/bin/bash
apt-get update
apt-get install nginx -y
echo "<h1> This is $(hostname) </h1>" > /var/www/html/index.html
```