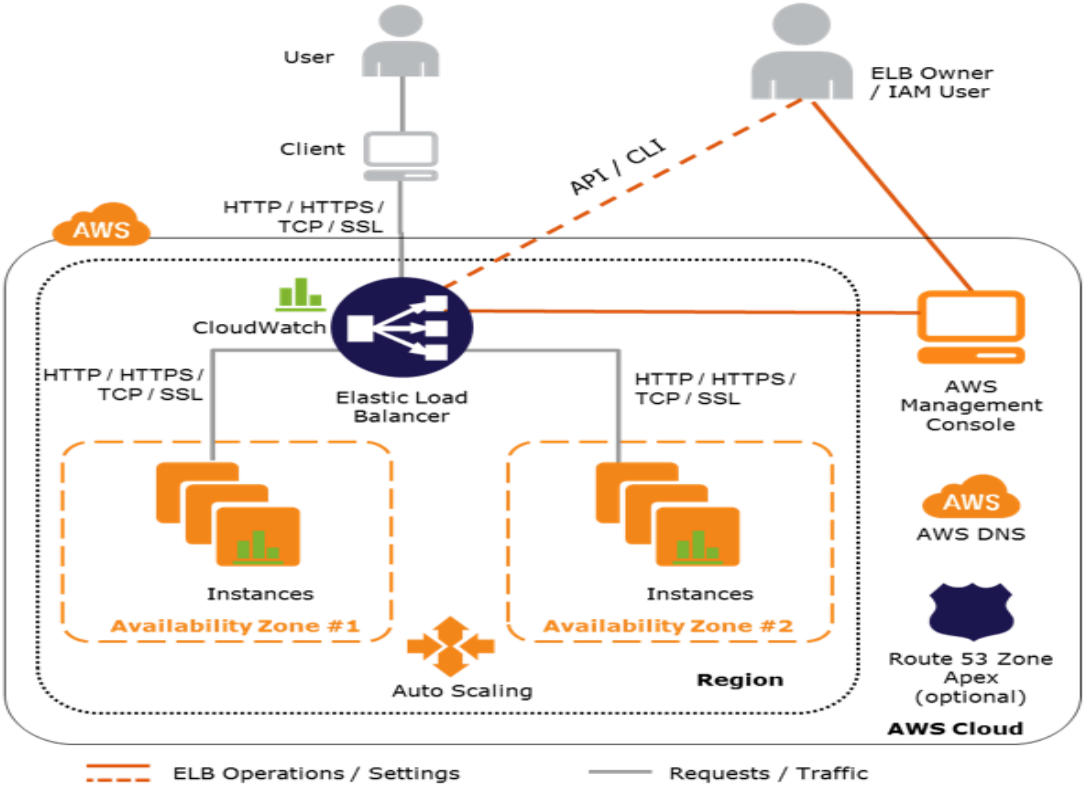
Assignment solution:

I am hosting the same server for your 2 customers on aws cloud for that I have created 2 iam users for accessing own cloud on AWS.so your customers can access the servers from the internet.

For internal communication hosting a rest api service I will give access through security group inbound rules with the help of application load balancer.

Below diagram I have taken example for one customer here you can add multiple clients.



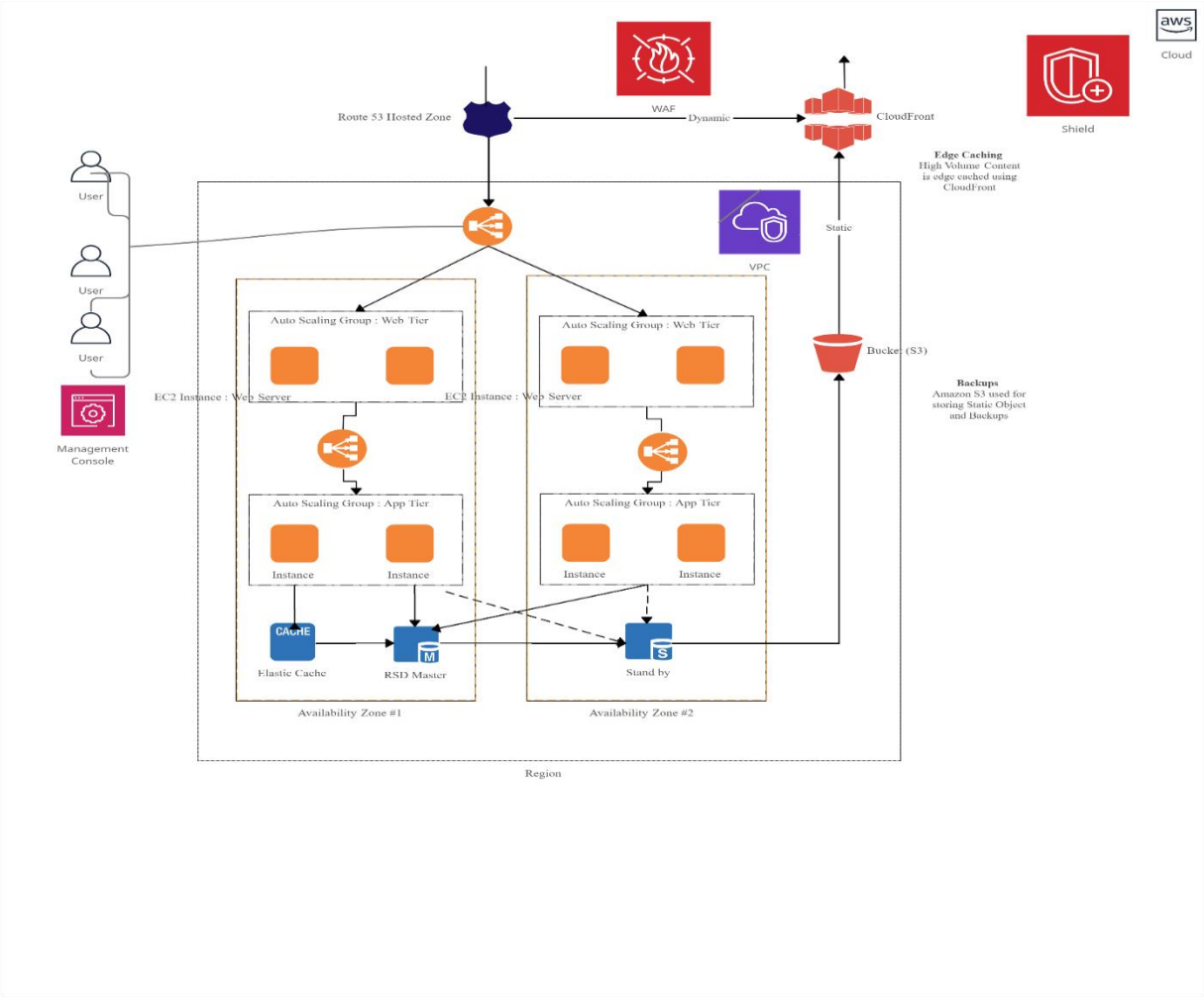
Once you create an elastic load balancer, you must configure it to accept incoming traffic and route requests to your EC2 instances.

For the billing department I can use CloudWatch logs to monitor and create a new IAM role for billing to get access to monitor the billing and cost control management.

Here I am adding the CloudFormation template for creating IAM users and hosting a server on AWS.(Not tested).

DDoS protection with AWS Shield – Safeguards your infrastructure against the most common

network and transport layer DDoS attacks automatically.



There are numerous options within the AWS Cloud for storing, accessing, and backing up your web

application data and assets. Amazon S3 provides a highly available and redundant object store. Amazon

S3 is a great storage solution for somewhat static or slow-changing objects, such as images, videos, andother static media. Amazon S3 also supports edge caching and streaming of these assets by interacting with CloudFront.

The number and sophistication of Distributed Denial of Service (DDoS) attacks are rising. Traditionally,

these attacks are difficult to fend off. They often end up being costly in both mitigation time and powerspent, as well as the opportunity cost from lost visits to your website during the attack. There are a

number of AWS factors and services that can help you defend against such attacks. One of them is the scale of the AWS network. The AWS infrastructure is quite large, and enables you to leverage our scale to optimize your defense. Several services, including Elastic Load Balancing, Amazon CloudFront, and Amazon Route 53-are effective at scaling your web application in response to a large increase in traffic. The infrastructure protection services in particular help with your defense strategy:

• AWS Shield is a managed DDoS protection service that helps safeguard against various forms of DDoS attack vectors. The standard offering of AWS Shield is free and automatically active throughout your account. This standard offering helps to defend against the most common network and transportation layer attacks. In addition to this level, the advanced offering grants higher levels of protection against your web application by providing you with near real-time visibility into an ongoing attack, as well as integrating at higher levels with the services mentioned earlier. Additionally, you get access to the AWS DDoS Response Team (DRT) to help mitigate large-scale and sophisticated attacks against your resources.

• AWS WAF (Web Application Firewall) is designed to protect your web applications from attacks that can compromise availability or security, or otherwise consume excessive resources. AWS WAF works in line with CloudFront or Application Load Balancer, along with your custom rules, to defend against attacks such as cross-site scripting, SQL injection, and DDoS. As with most AWS services, AWS WAF comes with a fully featured API that can help automate the creation and editing of rules for your AWS WAF instance as your security needs change.