

As a sample project to deploy web application in AWS cloud is chosen

- **What services should the public cloud deployment offer to the customers?**

Main services provided by Public Clouds can be found below.

Compute (e.g Amazon EC2)

Storage (e.g Amazon S3, Amazon EBS)

Network & Content Delivery (e.g Amazon VPC, Amazon Cloudfront, Amazon Route 53, AWS Direct Connect)

Database (Amazon RDS)

- **How will the users consume those services? Will they use Internet access or will you have to provide a more dedicated connectivity solution?**

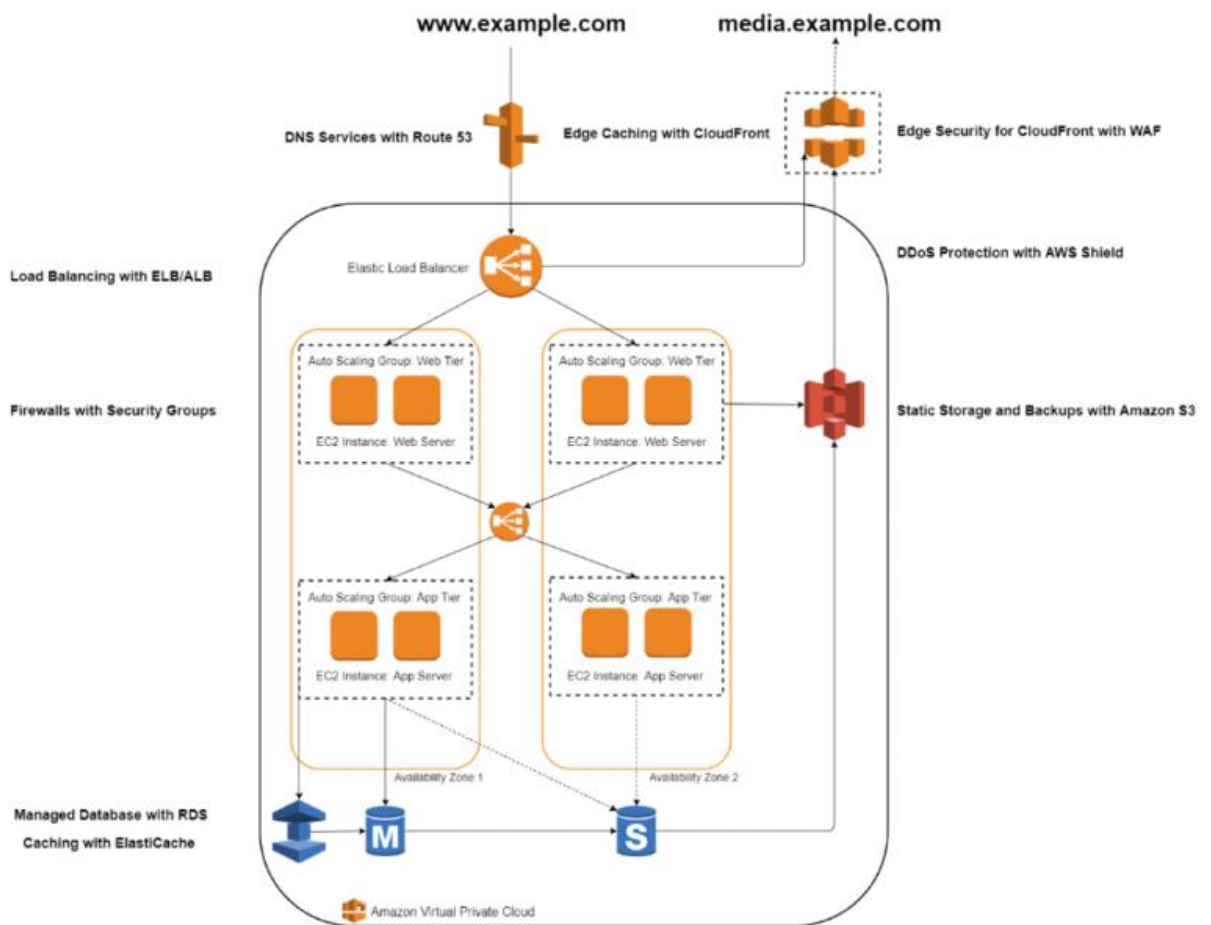
Users will access Web Application via Internet

- **Identify the data needed by the solution you're deploying. What data is shared with other applications? Where will the data reside?**

Below is the simple diagram from <https://d1.awsstatic.com/whitepapers/aws-web-hosting-best-practices.pdf> that I would like to use as a reference.

In this solution I am not going to use Cloudfront or AWS WAF or AWS Shield in this sample project.

Please note that Web and App servers (EC2 instance) can be combined into one server. Web/App Tier servers will be spread across 2 Availability Zones to provide HA. Load Balancer will be used for the same reason.



- **What are the security requirements of your application?**

To Web/App Tier: port tcp/80 and tcp/443 open from Internet, port tcp/22 open from On-Premise location (specific subnet will be provided)

To DB Server: Permit App Layer to access DB Layer

All remaining traffic will be blocked

- **What are the high availability requirements?**

Web/Application Tier servers will be spread across 2 Availability Zones, Load Balancer will allow to spread load across 2 A-Zs

- **Do you have to provide connectivity to your on-premises data center? If so, how will you implement it?**

There is a need to provide connectivity for On-Prem location – VPN Gateway will be used to establish IPsec VPN to On-Prem

- **Do you have to implement connectivity to other (customer) sites? If so, how will you implement it?**

There is no such requirement. If there is any I could use either VPN Gateway or use Direct Connect.