1. Sample application

Frontend – it has public access, can use any framework for it like python, angular js etc.

So, it has direct public endpoint access.

Backend – we must protect backend services from direct access, it will have protected access. Front will be inside the subnet and that subnet will have access to the backend. And our DB is also not allowed to be accessed on user end point. We will take backend subnet and allow to access the DB. Communication with backend is done by frontend only.

Communication here will be done by azure backbone/subnet.

backend

frontend

DB  
(restricted access via service endpoint)

Public access

Restricted access

user

To setup the application in 3 tier through terraform, we can follow the steps

1. initialise terraform with command - **terraform init**
2. we have to create the terraform configuration, for that we have to make main.tf file (can be found in challenge1 folder).
3. Apply the Terraform Configuration with command - **terraform apply**
4. Now we have to Define and Create Resources for Each Tier (presentation, application, and data) within the respective subnets.

This can include VM, DBs, web applications, etc.

We'll need to create separate Terraform configurations for each tier's resources.

1. We have to Configure network security groups, route tables, and any other networking and security settings as needed for our specific use case.
2. Deploy our applications on the appropriate resources within each tier.
3. Test and validate our 3-tier environment to ensure that it functions as expected.