We will create three virtual networks for firewall, active directory, and express road gateway, each going to have a dedicated subnet. The clients can connect to the express gateway through VPN. This VNET will be called as management VNET

There will be two separate VNET’s for two different regions

In each virtual network of the application we going to have a separate subnet for each tier of the three-tier architecture.

Currently I am using west region as a site recovery region so when over there is a failure in east region, we will be using west region.

There will be a virtual network pairing between all the VNET’s.

The client using their VPN’s they connect via express gateway and it goes through the firewall and reaches the Azure load balancer in management VNET.

We going to have an ILB inside the application region VNET to redirect traffic to web servers coming from Azure public Load balancer (Depends on the requirement of exposing it to public) which is residing in

We going to use the internal load balancers between the three tiers, there will be an internal Load balancer between web, app, and data servers

We going to have network security group and route tables will be associated with management VNET subnets in such a way they can redirect the traffic securely to the application virtual networks.

Route tables and NSG in application VNET will help traffic go securely back to Management VNET.