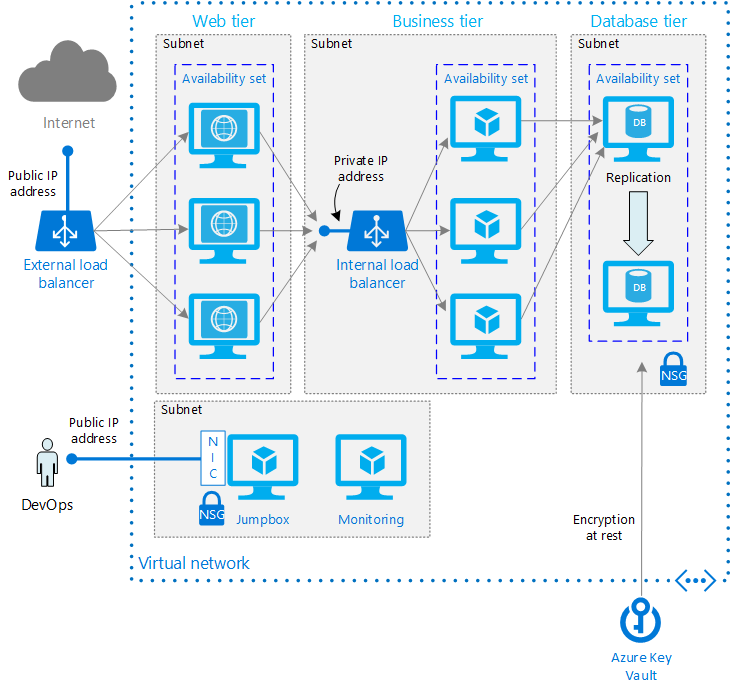
**The Below Azure Architecture is an example of 3 Tier architecture:**

* **Web tier.** Handles incoming HTTP requests. Responses are returned through this tier.
* **Business tier.** Implements business processes and other functional logic for the system.
* **Data tier.** Provides persistent data storage.

**Architecture diagram**



* **Availability Sets.** Create an [Availability Set](https://github.com/uglide/azure-content/blob/master/articles/virtual-machines/virtual-machines-windows-manage-availability.md#configure-each-application-tier-into-separate-availability-sets) for each tier, and provision at least two VMs in each tier. This approach is required to reach the availability [SLA](https://azure.microsoft.com/en-us/support/legal/sla/virtual-machines/v1_0/) for VMs.
* **Subnets.** Create a separate subnet for each tier. Specify the address range and subnet mask using CIDR notation.
* **Load balancers.** Use an [Internet-facing load balancer](https://github.com/uglide/azure-content/blob/master/articles/load-balancer/load-balancer-internet-overview.md) to distribute incoming Internet traffic to the web tier, and an internal load balancer to distribute network traffic from the web tier to the business tier.
* **Jumpbox**. A jumpbox, also called a [bastion host](https://en.wikipedia.org/wiki/Bastion_host), is a VM on the network that administrators use to connect to the other VMs. The jumpbox has an NSG that allows remote traffic only from whitelisted public IP addresses. The NSG should permit remote desktop (RDP) traffic if the jumpbox is a Windows VM, or secure shell (SSH) requests if the jumpbox is a Linux VM.
* **Monitoring**. Monitoring software such as [Nagios](https://www.nagios.org/), [Zabbix](http://www.zabbix.com/), can give us insight into response time, VM uptime, and the overall health of your system. Install the monitoring software on a VM that's placed in a separate management subnet.
* **NSGs**. Use [network security groups](https://github.com/uglide/azure-content/blob/master/articles/virtual-network/virtual-networks-nsg.md) (NSGs) to restrict network traffic within the VNet. For example, in the 3-tier architecture shown here, the data tier does not accept traffic from the web front end, only from the business tier and the management subnet.
* **Key Vault**. Use [Azure Key Vault](https://azure.microsoft.com/services/key-vault.md) to manage encryption keys, for encrypting data at rest.

The Azure Components used in the 3 tier Architecture are :

1. A single Virtual Network.
2. 3 subnets in that Virtual Network.
3. 1 webtier subnet, 1 app tier subnet, 1 db tier subnet.
4. 3 Virtual Machine should be deployed on each subnet.
5. 3 Network Security Group to restrict the Virtual Machine access.
6. 1 Azure KeyVault
7. 1 Azure Load Balancer .