**What is VPN?**

VPN stands for **Virtual Private Network** which is a connection made over the internet to allow organizations send and receive information as though the device used is connected locally in the organization’s network. The technique establishes an encrypted ‘pipeline’ for data transfer with the aim of preventing interception, theft or unauthorized access. VPNs are commonly employed for privacy purposes, protection and to access resources from a distant location, for instance to log into an organization’s network from a different location or to unblock geographical limitations on websites/accounts.

**How VPN will Work in the Migration:**

**Secure Connection Between On-Premises and Cloud:** During the migration, we require a secure path, to transfer data and control between the on-premise network and the cloud environment. A VPN creates an encrypted tunnel over internet which connects the on-premise data centre to cloud provider’s network like, Azure. It also guarantees secure exchange of all the information during the migration in order to avoid interception by unauthorized persons.

**Hybrid Network Architecture**: By setting up a VPN between our on-premises network and the cloud, we create a hybrid network. This allows both environments to operate as a single, integrated network. Resources in the cloud can communicate with resources on-premises as if they were on the same local network, which is useful for applications and services that need to remain interconnected during and after the migration.

**Access and Authentication**: A VPN guarantees that staff members, partners, or services can safely access the required resources from any location for teams that require access to both on-premises and cloud resources during the migration. An additional degree of security is added by its integration with authentication systems, which guarantee that only authorised users can connect.