A VPN stands for ‘Virtual Private Network” ensuring your data stays encrypted, your location stays private, and you can surf the web anonymously. VPNs are often used for remote access. Direct access VPNs allow users to access private networks via a public network. Access over a public network is a core security concern with VPNs. With more people working from home and connecting to company networks has become a popular attack vector on VPNs. When you sent your information online, a VPN creates a tunnel. Different tunneling protocols encapsulate and encrypt the traffic to protect the data from unauthorized disclosure. The tunnel prevents anyone from reading the data transferred through it. In contrast to the previous outlook on control access protocols, we will be using the same Azure cloud configuration to dissect the best practice use case on VPN technologies.

These days spreading our risks and our capabilities throughout multiple cloud vendors with the use of Azure AD as our application proxy. AD allows our employees and users on-premise applications from a remote client. A proxy acts on behalf of a request connection to the internal resources. We don't have to expose our website to the internet, but the proxy is exposed instead with no open inbound firewall ports. Leveraging Azure AD as authentication provides internal and guest access to the site.

By now moving to the cloud, things are now different compare to the domain directory of passwords. With SSO Azure active directory functioning as our identity provider, it now works as a different authentication mechanism. In the SSO implementation, the client signs in once and therefore do not need to sign in again until after their token has expired. Adopting Azure AD instrument to use SSO which also gives us the benefit of using password hash sync.

Azure Bastion allows us to connect to our virtual machines without exposing our VMs to the public internet. Using the Bastion host can help limit threats such as port scanning and other types of malware targeting the companies’ VMs. Bastion gives us seamless RDP and SSH access to VM through the Azure portal SSL without any exposure through public IP addresses. In summary, the Azure Bastion is specifically designed to provision at the perimeter of your network in order to precisely guard your VMs.

Azure VPN Gateway is an infrastructure as a service. Providing and allowing your components to connect to the cloud. Using the virtual network also allows traffic between Azure and on-premise infrastructures. Even if you have different components in a different region, using the VPN Gateway will be favorable in cross-regional communication between your virtual networks.

WVD Windows Virtual Desktop is a group of technologies from Azure that simply creates a windows virtual desktop. Launched recently that became the evolution of Microsoft remote desktop services or RDS. a flexible approach to desktop virtualization without compromising control. Built-in centralized security, management, and scalability. Still able to maintain full control over service configuration and management with lots of options for deploying services, implementing identity, and file storage. Azure Virtual Desktop is flexible and configurable to tailor towards any employee or client. Allowing the preference to choose from hundreds of VMs sizes and performance options to various densities of users in your VMs base on the workload.

Azure Remote Desktop is the virtualization application that runs fully on cloud. Giving the chance to run multi-session Windows 11 with full scalability. Connecting to full on app experience. “Use the Azure portal, Azure CLI, PowerShell and REST API to configure the host pools, create app groups, assign users, and publish resources.”

Azure certification is the Microsoft cloud-level expertise that an individual can obtain after passing the examination. With the certification, it validates your creditability to employees looking to hire in your select domain. Increase in higher salary package upon completion. Allowing you to pursue a wide range of career options. Ensuring that users are up-to-date on their level of comprehensive knowledge about the Azure platform.

By default most VPN providers automatically use the best protocol suited for your network. Thankfully most VPN providers grant control over letting you configure your protocols whether it is PPTP, L2TP/IPSec, or SSL/TLS. PPTP has long been the standard protocol for corporate network VPN. However, it is not a secure VPN protocol and can be easily decrypted by malicious 3rd parties. L2TP is a better-graded version of PPTP. It is simple and easy to set up since it's built-in for all modern operating systems. Although it does not provide encryption on its own. Usually implemented with IPsec authentication suite. SSL is the hybrid cryptography to send secure information. Both private and public certification which help you shield information by encrypting data as you browse through the web servers.

(n.d.). Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal?pivots=portal.