**Domain:** Cloud Security

**Question:** What are the advantages and disadvantages of using a corporate VPN, and under what

circumstances is using one appropriate?

**Answer:**

To reiterate, the question was what are the advantages and disadvantages of using a corporate VPN and under what circumstances is using one appropriate?

The advantages of using a corporate VPN is to be able to remotely have full access to a company’s internal network knowing that the network traffic is encrypted. It provides more security and reduces the chance of a security breach. We can configure the VPN to control who has access and what type of access a user is allowed to have. VPNs also allow you to bypass geo-restrictions. A VPN has the ability to “hide” or mask your IP address anonymously to prevent intruders from identifying your location or stealing sensitive data.

There are also some disadvantages such as performance and scalability. With so many employees using the corporate VPN to connect to the company, especially during a pandemic, could lead to performance issues due to the continuous workload and excessive loads. A user’s connection is through the public Internet and if their internet connection is slow, this affects their connection to the company’s internal network and could lead to frustration for that user, not to mention security issues. VPNs need to be maintained and require hardware upgrades or add-ons especially for cloud resources which leads to high-cost maintenance.

In a recent project, I created several virtual machines (VMs) within an Azure virtual network. Instead of using a VPN, I used a Jump Box VM to access these VMs. Using Azure’s network security group (NSG), I created several inbound security rules to control access from my workstation (client) to the Jump Box and from the Jump Box to the VMs. One rule was to limit the traffic from my public IP address to the internal IP address of the Jump Box using port 22.

Using a Jump Box will prevent our VMs from being exposed since we are creating the VMs without a public IP address. We can monitor and log all network activities through this one Jump Box. Since the Jump Box is exposed to the Internet, hackers can compromise it. The network setup for new VMs to a Jump Box can get complicated especially when dealing with the cloud.

A VPN might be a better solution for this project since the network traffic in a VPN is encrypted and we can use an access control list to give a group or users access to a VPN.

To implement a VPN for this project, we would need to add a ‘Virtual network gateway’ from the Azure Portal, making sure you select the virtual network you want add this VPN gateway to. In the real world, users will need an overview or training if there is a new sign-in to a system that has been changed.

Using a VPN for this project was not necessary since access to the Jump Box was limited and was only allowing traffic to 4 other virtual machines.

A VPN would be an ideal case for any business whether large or small for enhanced security or individuals that like to travel and look at foreign (their destination) content.