Domain: Cloud Security

Question 2: Corporate VPN

I believe there are advantages and disadvantages of using a corporate VPN, but I think it's a good tool to use when you have multiple people on one network. During the project I only had 2 VM’s that were connected to the network, I would use the security groups tools like shh or http to control access to the network. Instead of using a VPN I was using a ssh key to gain access to the network. Only disadvantage I see in not using a VPN is if someone was able to access your ssh key they would have access to the network, and I see using ssh key gives you more control over the network.

I would think if I were to use a VPN it would meet the access control requirements, because it's just another way to access the network. I dont think a VPN would protect the network, it would just add another Ip address to the network.

To set up a VPN you would go to the connections tab in the azure portal, add info into profile. The best way to get users onto the VPN network is to set them up with a network key with a username access and password that they will only know.

I dont think a VPN should be an appropriate access control because someone could get ahold of the clients username and password and would be able to access the network. I think its best used for corporations who want to give access to their network without them being close to the network. VPN’s are a good solution for companies who have alot of employees who work from home or work abroad who wants to have access to the network.