What are the advantages and disadvantages of using a corporate VPN, and under what circumstances is using one appropriate?

How would using a corporate VPN secure or be a vulnerability? Is it appropriate to use a corporate VPN?

1. Provide a Concrete Example Scenario
   * In Project 1, which VMs did you have on the network? I built a JumpBox, three Web VMs, and ELK-Stack.
   * Which tools did you use to control access to and from the network? First I denied all traffic while building this cloud infrastructure. I only allowed SSH (22) access to all the virtual machines.
   * If you didn't use a VPN, what did you use? Only implemented port 22 to gain access.
   * What disadvantage(s) did your non-VPN solution have? I believe that VPNs impedes scalability.
   * What advantage(s) did your non-VPN solution have? Its low cost and protect users more.
2. Explain the Solution Requirements
   * Would a VPN meet the access control requirements you had for Project 1? No, It would not, That employee could be socially engineered to give up that VPN
   * How would a VPN protect the network just as well, or better, than your current solution? It could add another layer of protection.
3. Explain the Solution Details
   * Which Azure tools would you use to implement a VPN to your Project 1 network? By setting up a VM and going to the networking tab, go to vnet gateway, then click create and select VPN.
   * How would you onboard users to the new VPN system? Dashboard, enterprise apps Azure VPN, conditional access, and the set users and groups.
4. Identify Advantages and Disadvantages of the Solution
   * In Project 1, would a VPN have been an appropriate access control solution? Yes
   * Under what circumstances is a VPN a good solution? It would be a good solution for the public wifi
   * When, if ever, is a VPN "overkill"? when its not a quality VPN.