For each protocol, provide the following information:

- Overview: Explain the purpose and features of the protocol in enabling secure remote access.
- Implementation: Describe how the protocol is typically implemented in organizations to ensure security and privacy during remote connections.
- Security Considerations: Discuss the potential security risks associated with each protocol and best practices to mitigate them.

SSH:

- Answer: (SSH)-The purpose of Secure Remote access is to allow different functions to be executed remotely. Features include remote administration and Secure File Transfer.
- Answer: SSH servers are configured by mapping a host of names to public keys and can be kept manually by each SSH client, along with various enterprise software products designed for SSH host key management.
- The most prevalent consideration would be a man in the middle attack. This would be a threat actor gaining credentialed access between clients and stealing data. To mitigate this issue, you make sure to be using TLS and close all ports after you are done with the remote session.

VPN

- The purpose of a VPN is to allow secure access to a server. It encrypts the user's data and masks the IP address.
- The way the VPN is implemented in ORGs, is usually in the form of Remote Access. A client or person who works for the company is working remotely. They first login to a VPN and then they are authenticated into the remote working server.
- A VPN will not keep you safe from malware or phishing and still subject man in the middle attacks as well. Mitigating the situation by being aware of the things you're downloading, and sites being visited.

RDP

- The purpose of RDP is to join a host within the local network over a remote administration protocol.
- The implementation of this technology is traditionally through SSH for terminal access. There are also many other GUI tools such as Team Viewer

that you could use. Traditionally these remote desktop products require a client app.

- Like the other Remote access protocols, RDP is also susceptible to man in the middle attacks. The best way to mitigate is using the client apps to authenticate.