Steps for accessing the VPN

1. Before connecting make sure that you have received the ovpn configuration file. Please don't share the ovpn configuration file provided to you with others.
2. Connection to VPN could be done with two clients (either one could be chosen but option **a.** works with all operating systems)
    a. OpenVPN Client (Works in Ubuntu, Windows, MacOS, Android)
    Download from here - https://openvpn.net/download-open-vpn/
    Instructions are here -
    https://docs.aws.amazon.com/vpn/latest/clientvpn-user/connect.html
    Note - If you're using Ubuntu, please use the Command line option instead of the Network Manager option for configuration of OpenVPN client.

    b. AWS VPN Client(Works only in Windows and MacOS as on 30th July 2020)-
    https://docs.aws.amazon.com/vpn/latest/clientvpn-user/connect-aws-client-vpn-connect.html

3. Install the client mentioned in the previous step and import the ovpn configuration file provided to you and connect.
4. Check if the connection is successful by checking the status of openvpn client
5. Test by logging in (ssh) to the AWS server using its private ip (Use the existing key file and username to connect, only change the public ip to private ip).
6. Connect to the VPN only when you need to login to the servers.
7. **Disconnect** when not in use.

Note - The VPN currently uses split-tunneling, so only the traffic meant for our AWS infrastructure will pass through the VPN endpoint. Any other traffic would be routed through the ISP.