This scenario shows an External User accessing an on-prem service or a cloud resource through VPN.

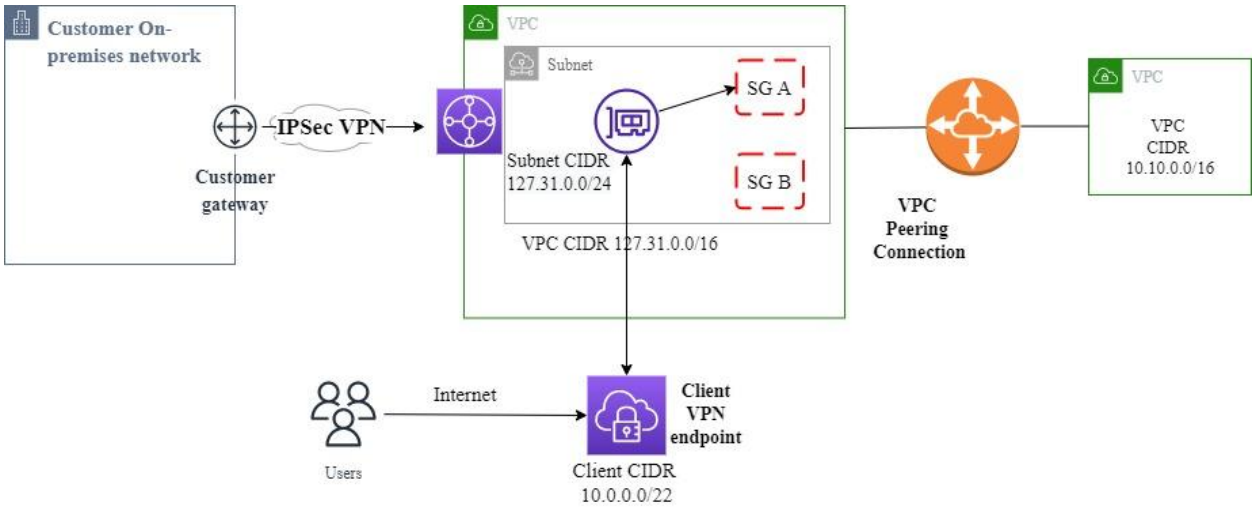

Figure A.1 : illustrate How can the external user access on-prem infrastructure and cloud infrastructure through VPN..

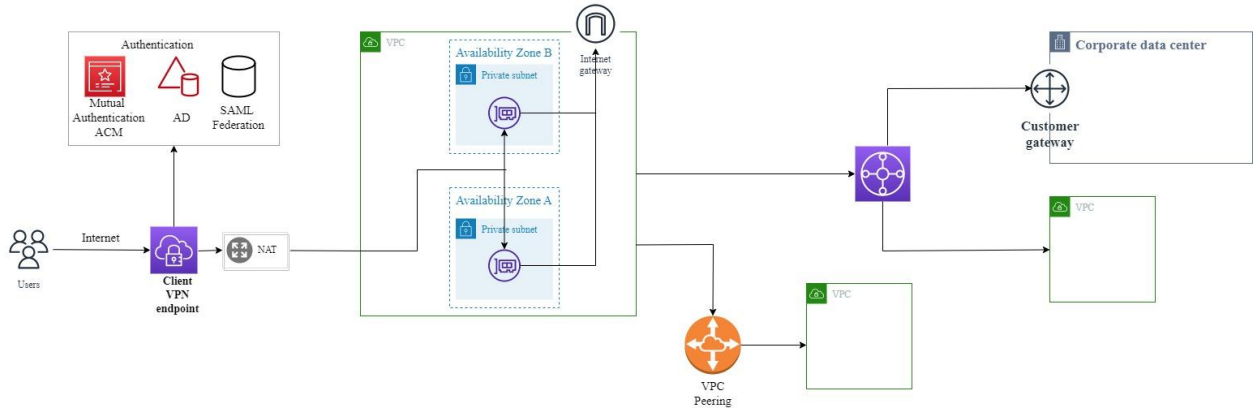

Figure A.2 : illustrate authentication of external users through VPN.

Client VPN is a service that allows you to securely access your AWS resources and resources in your on-prem network.
Client VPN can allow user to authenticate through

- Active Directory Authentication
- Mutual Authentication
- Single-Sign-On SAML-based federated authentication

~~S~~	The identity is covered by the AD, MFA (optional to use), and IAM role (mapped to OU permissions).
~~T~~	The identity is covered by AD, secure connectivity, and AD security configuration and all activities are logged and monitored.
~~R~~	The identity is governed by AD, and all activities are logged and monitored using the SIEM solution.

~~I~~	All user activities are limited by IAM role, ACL.
~~D~~	High availability and scalability are covered by AWS VPN client endpoint service.
~~E~~	The identity is governed by AD ACL, user role, and all activities are logged and monitored using the SIEM solution.