This scenario shows an Internal User Authenticating and Authorizing with AD to access internal service.

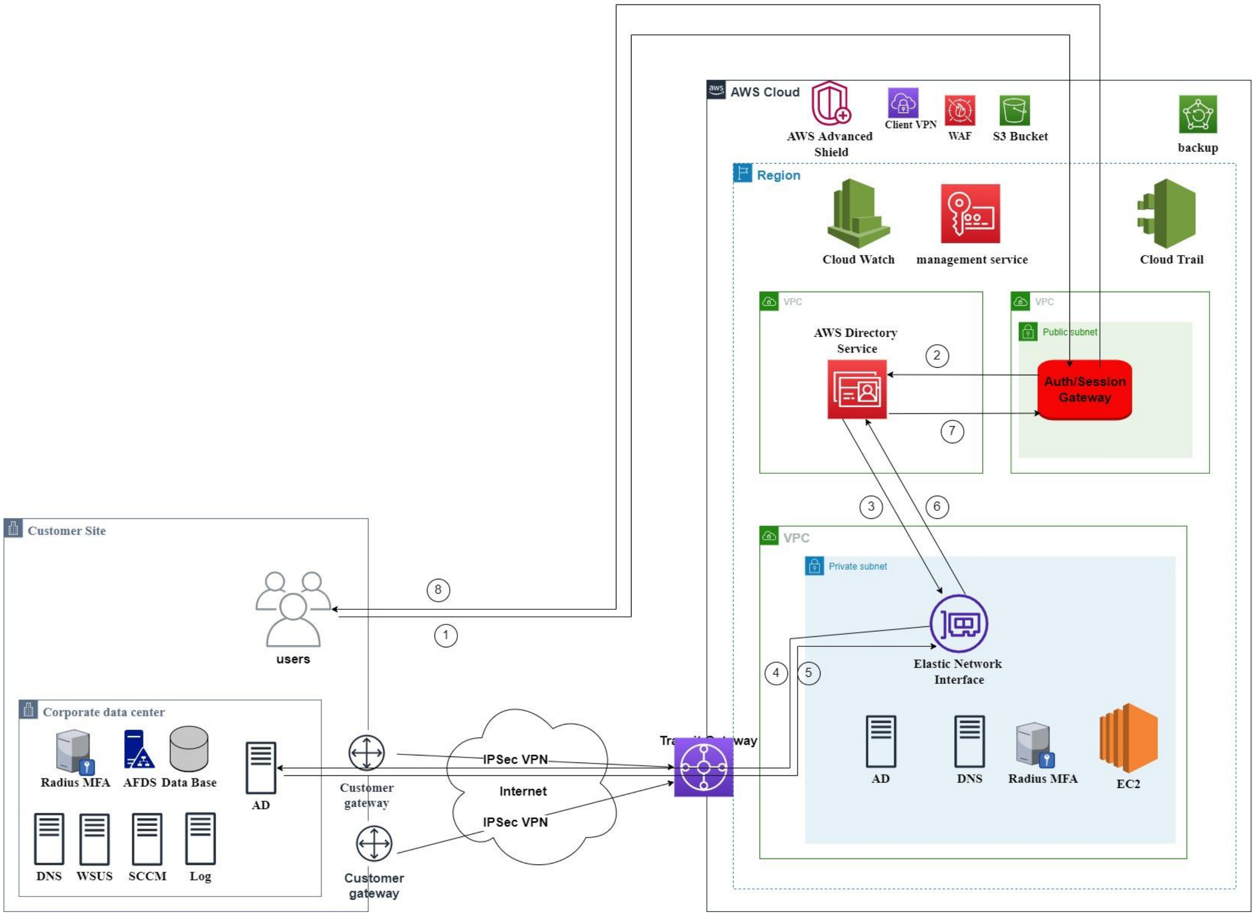

Figure A1 : illustrate authenticate internal user to AWS resource and on-prem Service

The following describes the process an internal employee will follow to authenticate with AD:

1. Internal employee requesting the AD server.
2. Internal employee requests will connect to the Auth/Session Gateway instance in AWS.
3. Auth/Session Gateway will send the request to AWS Directory Service
4. Auth/Session Gateway will communicate with on-prem AD through AWS Elastic Network Interface.
5. On-prem AD will authenticate the user and create a ticket for the user.

S	However the identity is governed by the AD, MFA (optional to use), It is highly possible if the user ticket has been compromised.
~~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	However all activities are logged and monitored using the SIEM solution, but wrong configuration for AD or vulnerability in AD server could lead for information disclosure.
~~D~~	High availability and scalability are covered by AD on-prem and another replica extended in AWS.
~~E~~	The identity is governed by AD ACL, user role, and all activities are logged and monitored using the SIEM solution.