This scenario shows that an on-prem service consumes AWS cloud resources.

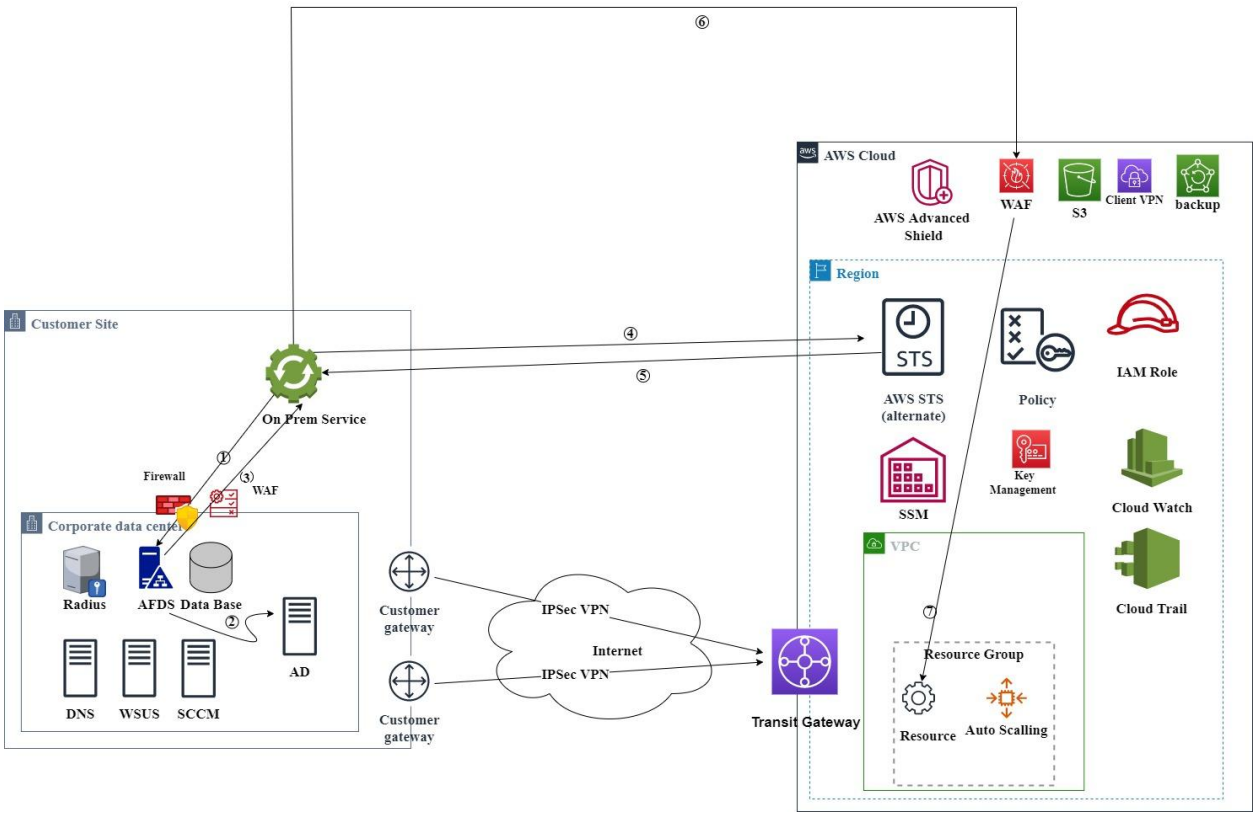

Figure A.1 : illustrate connectivity from on-prem service to AWS cloud resources

The following describes the process an on-prem service will follow to authenticate to AWS using Active Directory and ADFS as the identity provider and identity brokers:

1. The on-prem service accesses the corporate Active Directory Federation Service and provides Active Directory authentication credentials.
2. ADFS authenticate the service against AD
3. AD returns the service's information.
4. ADFS builds ARNs by using Active Directory group membership for the IAM roles and sends a signed assertion to the on-prem service with redirects to AWS STS.
5. STS AssumeRoleWithSMAL returns temporary credentials to on-prem service.
6. The on-prem service provides access to the AWS resource.

~~S~~	The identity is governed by Active Directory, ADFs, and IAM role (mapped to OU permissions).
T	However the connectivity over secure communication and there is a WAF attached to AWS, but It is possible if the integrity checks failed.
~~R~~	The identity is governed by Active Directory, ADFs, and IAM roles (mapped to OU

	permissions), and all activities are logged and monitored using cloud watch and cloud trails.
I	However there is a WAF attached to AWS but it is still possible if not handled in the on-prem's service design.
~~D~~	AWS advanced shield and auto-scaling in place.
~~E~~	The identity is governed by Active Directory, ADFs, and IAM roles (mapped to OU permissions).