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

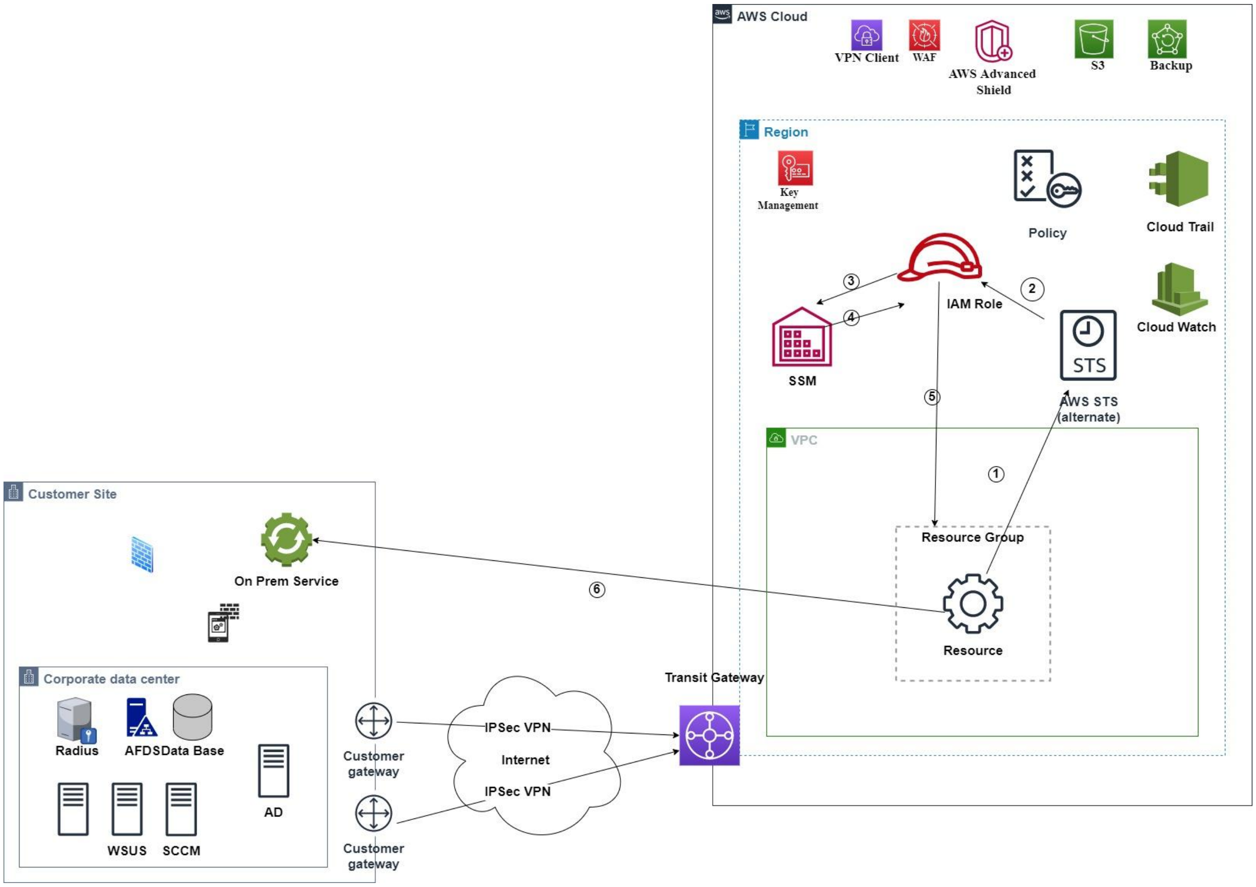

Figure A.1 : illustrate connectivity from AWS resource to on-prem Service

The following describes the process an AWS resource will follow to authenticate to on-prem service using the service's credentials stored in AWS Secret Manger :

1. AWS resources will request the STS to AssumeRole to access the SSM.
2. STS will request an IAM role to query the SSM with the credentials for on-prem service.
3. The IAM role will send the credentials to the AWS resource.
4. AWS resource will connect to on-prem service through Transit Gateway + VPN

~~S~~ The identity is governed by the AWS Secret Manager, IAM role (mapped to OU permissions) and firewall and WAF deployed on-prem .

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 AWS Secret Managery, and IAM roles (mapped to OU permissions), and all activities are logged and monitored using the SIEM solution.
I	Highly possible if not handled in the AWS Resource’s service design.
D	On-prem infrastructure is affected by DoS.
~~E~~	The identity is governed by AWS Secret Managery, IAM role (mapped to OU permissions), and ACL.