

This scenario shows an MSSP user accessing on-prem and cloud's resources through the RD gateway.

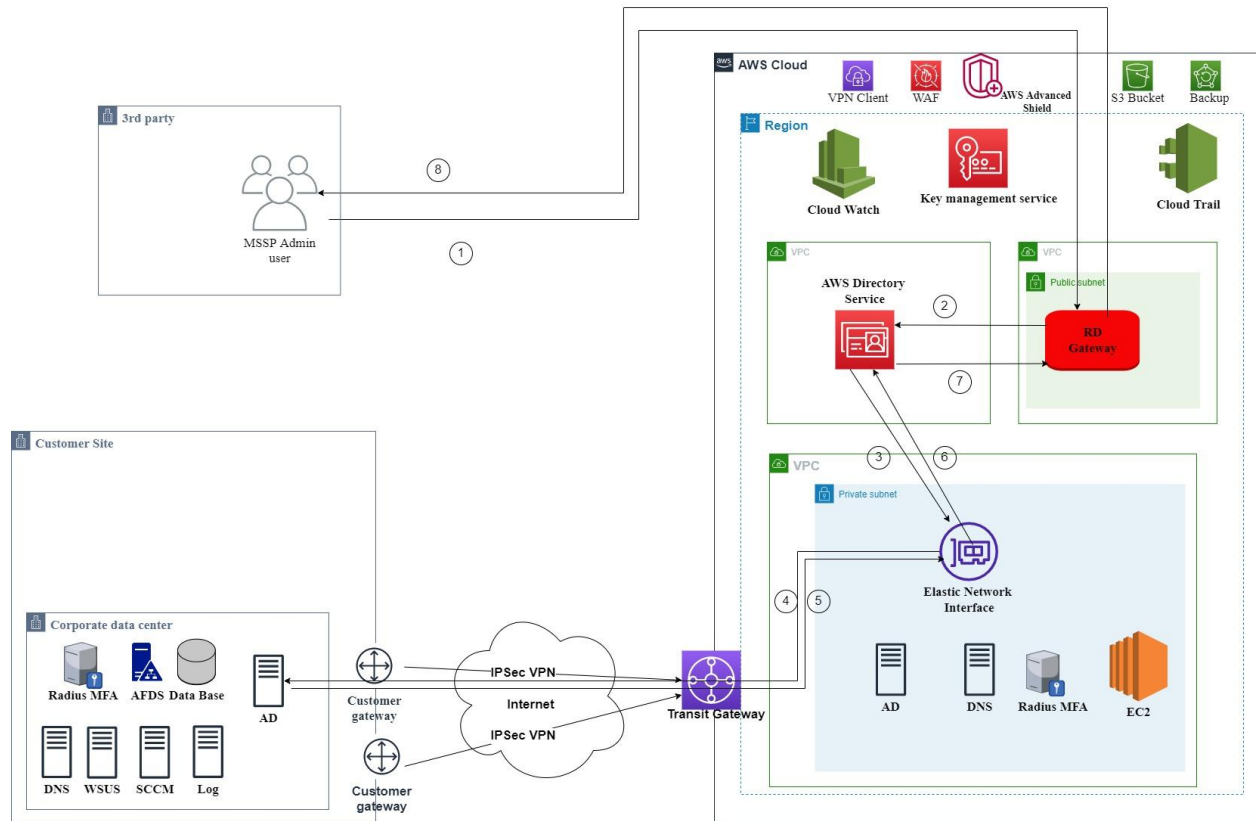


Figure A.1 : illustrate authenticate MSSP user to AWS resource and on-prem Service

The following describes the process an MSSP user will follow to authenticate with AD:

1. MSSP user trying to login to machine through RDP.
2. MSSP user requests will connect to the RD Gateway instance in AWS.
3. RD Gateway will send the request to AWS Directory Service
4. RD Gateway will communicate with on-prem AD through AWS Elastic Network Interface.
5. On-prem AD will authenticate the MSSP user and create a ticket for the MSSP user.

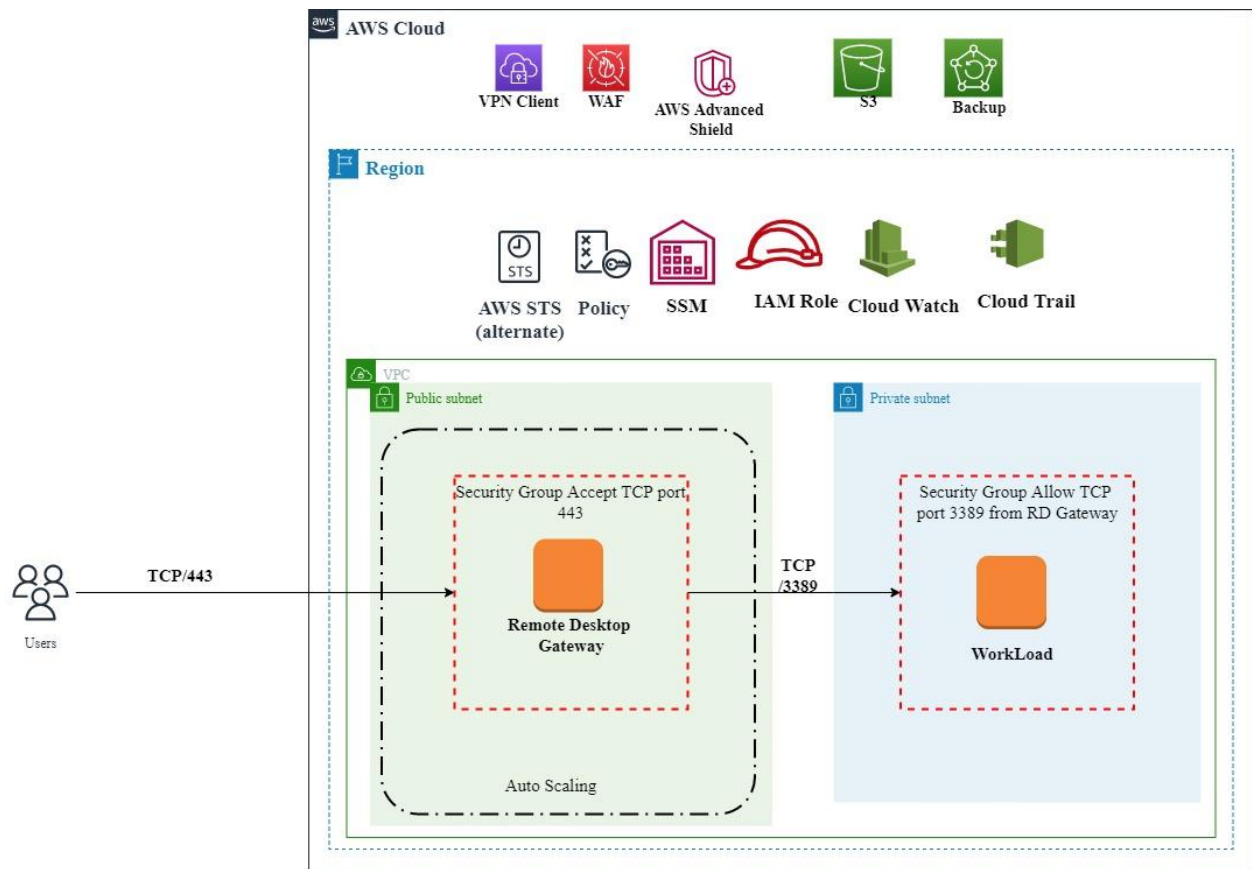


Figure A.2 : illustrate how MSSP users will access AWS resources and on-prem Service through the RDP.

RD Gateway is a service that provides Remote Desktop over HTTPS to establish a secure, encrypted connection between remote users and EC2 instances running Microsoft Windows, without needing to configure a virtual private network (VPN).

S	The identity is governed by Active Directory, MFA ,ADFs, and IAM roles (mapped to OU permissions).
T	However the connectivity over secure communication, It is Highly 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	Highly possible if not handled in the service design.
D	AWS advanced shield and auto-scaling in place.

✚ The identity is governed by Active Directory, ADFs, and IAM role (mapped to OU permissions).