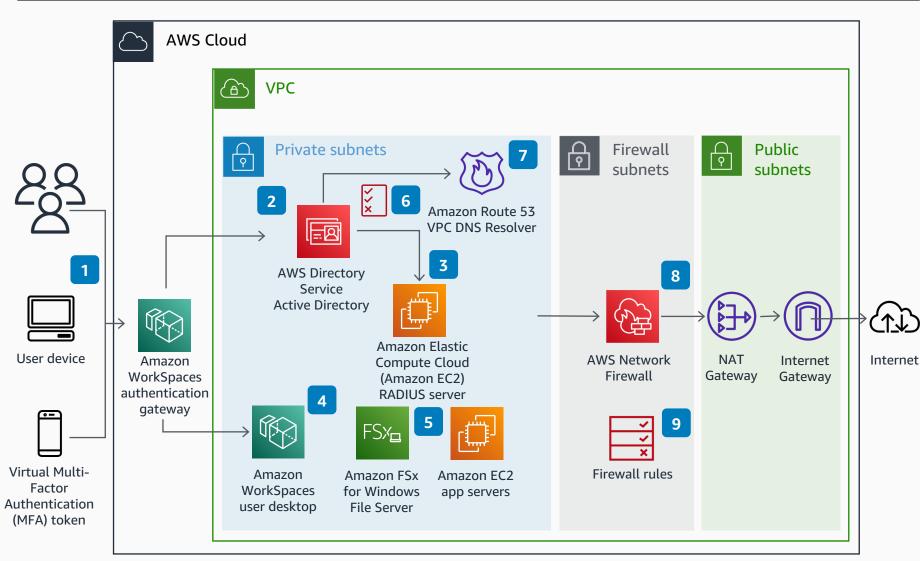
Secure Remote Worker Environment

Build a secure desktop environment for remote workers to access key line of business applications and data.



- Users connect to their desktop using the Amazon WorkSpaces application by supplying a username, password, and MFA code
- Amazon WorkSpaces authentication gateway authenticates against Directory Service.
- MFA code is authenticated against MFA service's RADIUS server. For example, OneLogin.
- Users are connected to their desktop through **Amazon WorkSpaces.**
- Users access core systems and files hosted on Amazon EC2 and Amazon FSx.
- Group policy is implemented in Active
 Directory to prevent unwanted activities,
 such as printing to local printers from
 Amazon WorkSpaces.
- 7 Domain Controller DNS forwards to Amazon Route 53 VPC DNS resolver with applied Route 53 Resolver DNS Firewall rules.
- Outbound internet traffic is filtered first by AWS Network Firewall, then sent through a NAT gateway and internet gateway to the public internet.
- Firewall rules are set up to block outbound traffic to unwanted sites (such as filesharing platforms) to prevent data leaks.