How to Connect to a Private EC2 Instance

In AWS, a private EC2 instance does not have a public IP, so it cannot be accessed directly from the internet. There are multiple ways to connect to such instances securely, such as using a Bastion Host (Jump Server), AWS Systems Manager (SSM), or VPN/Direct Connect.

1. Using Bastion Host (Jump Server)

- Launch a Bastion Host in a public subnet with a public IP.
- Configure Security Groups: Bastion SG allows SSH from your IP; Private Instance SG allows SSH only from Bastion SG.
- SSH into Bastion Host: ssh -i my-key.pem ec2-user@
- From Bastion, SSH into the private instance: ssh -i my-key.pem ec2-user@
- Alternatively, use ProxyCommand for one-step connection: ssh -i my-key.pem -o ProxyCommand="ssh -i my-key.pem -W %h:%p ec2-user@" ec2-user@

2. Using AWS Systems Manager (SSM)

- Ensure SSM Agent is installed on the private EC2 instance.
- Attach IAM Role with AmazonSSMManagedInstanceCore policy.
- Ensure instance has internet access via NAT Gateway or VPC Endpoint.
- Install AWS CLI on your system.
- Start session using: aws ssm start-session --target

3. Using VPN or Direct Connect

- Connect to your organization's VPN or AWS Direct Connect.
- Once connected, access the private EC2 instance directly with: ssh -i my-key.pem ec2-user@

The most common method is using a Bastion Host or AWS SSM Session Manager. For corporate environments, VPN or Direct Connect may also be used. Choose the method that best matches your infrastructure and security requirements.