What Is a Bastion Host?

A **bastion host** (also known as a jump server) is a **special-purpose instance** that acts as a **secure gateway** between a trusted network (like your local environment) and an **internal/private network**, such as private subnets in your AWS Virtual Private Cloud (VPC). It is commonly used to:

- **Securely manage** instances in private subnets via SSH or RDP.
- Provide **controlled access** to infrastructure.
- **Log and monitor** access attempts.

Think of it as a "guard tower" – you enter the AWS network through this host, and from there, you access internal resources that are otherwise unreachable from the public internet.

Characteristics of a Bastion Host

- **Public IP address**: So it can be accessed from the internet.
- **Minimal software**: To reduce the attack surface.
- **Strict security rules**: Like IP whitelisting and multi-factor authentication (MFA).
- **Monitoring and logging**: Often integrated with AWS CloudTrail, CloudWatch, or third-party tools.

How to Set Up a Bastion Host in AWS

Here’s a high-level step-by-step guide:

1. Create a VPC (if not already existing)

Set up your AWS Virtual Private Cloud with at least:

- One **public subnet** (for the bastion host).
- One or more **private subnets** (for internal resources like EC2, RDS, etc.).

2. Launch an EC2 Instance in the Public Subnet

- Use an Amazon Linux AMI (or your preferred OS).
- Ensure it has:
  - A **public IP address**.
  - An appropriate **security group**.

3. Configure the Security Groups

- **Bastion Host Security Group**:
  - Allow **inbound SSH (port 22)** from your IP address.
  - Block all other inbound traffic.
  - Allow **outbound SSH** to private subnet CIDR.
- **Private Instances' Security Group**:
  - Allow **inbound SSH** only from the bastion host's **security group**.

4. Access Your Private Resources

Connect to the bastion host:

```
ssh -i my-key.pem ec2-user@<bastion-public-ip>
```

Then from the bastion:

```
ssh -i my-key.pem ec2-user@<private-instance-ip>
```