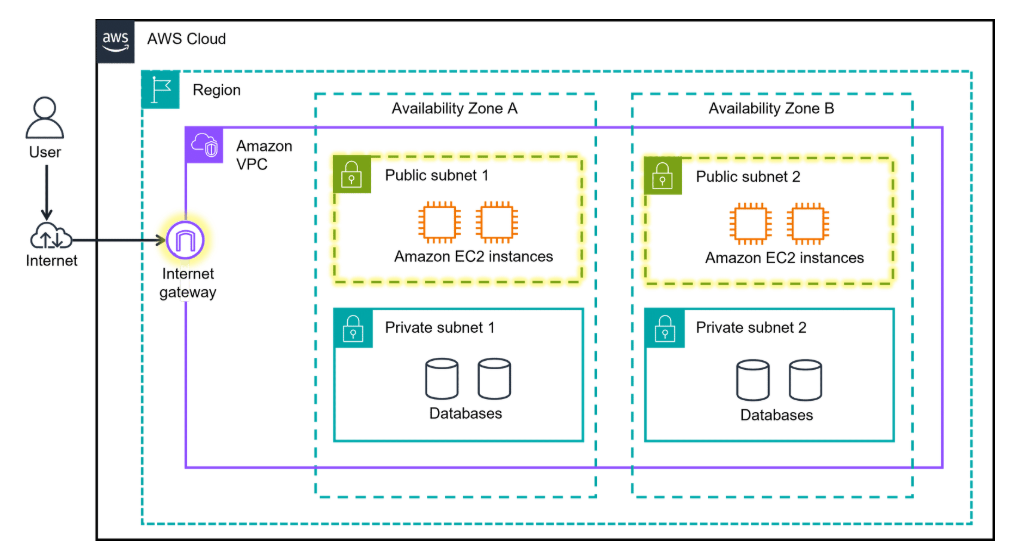
Networking - The term *networking* refers to interconnected devices that can exchange data and resources.

Amazon Virtual Private Cloud (Amazon VPC) - An Amazon VPC lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define.

Subnet - Subnets are used to organize your resources and can be made publicly or privately accessible. A private subnet is commonly used to contain resources like a database storing customer or transactional information. A public subnet is commonly used for resources like a customer-facing website.

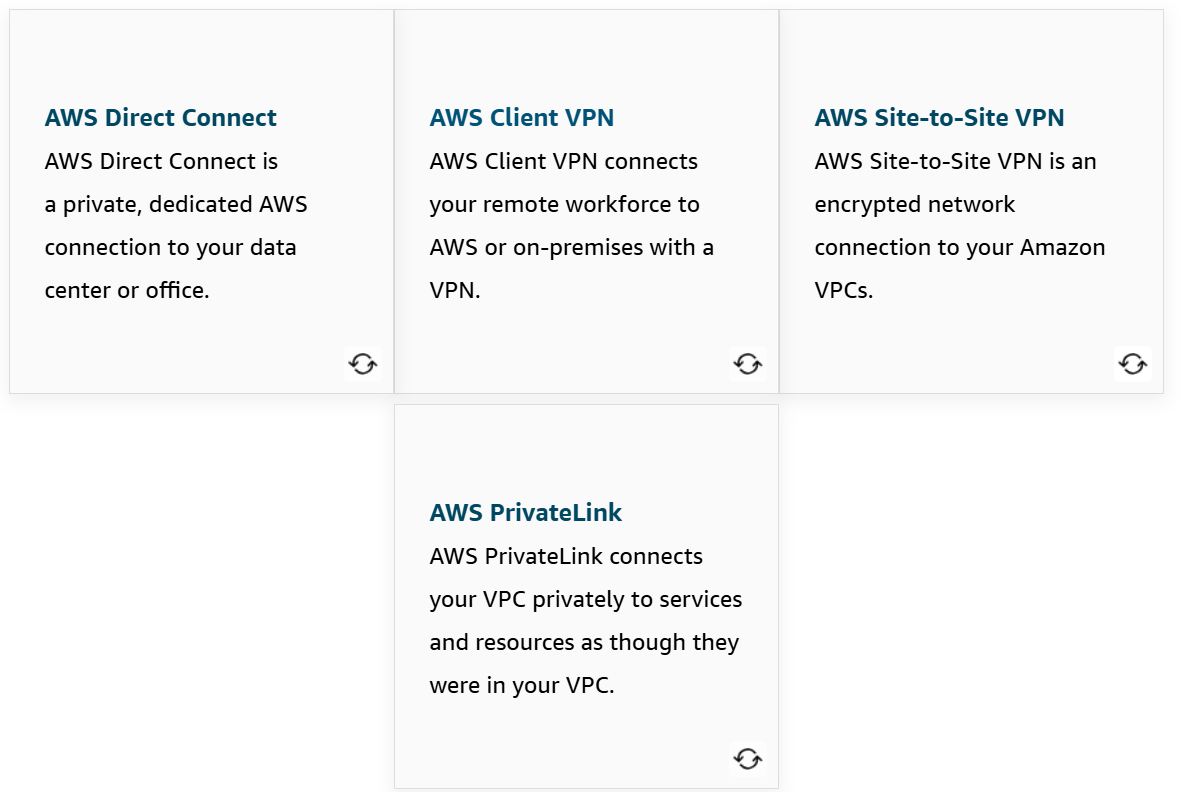




Internet Gateway -  An internet gateway is a connection between a VPC and the internet. Without an internet gateway, no one can access the resources within your VPC.



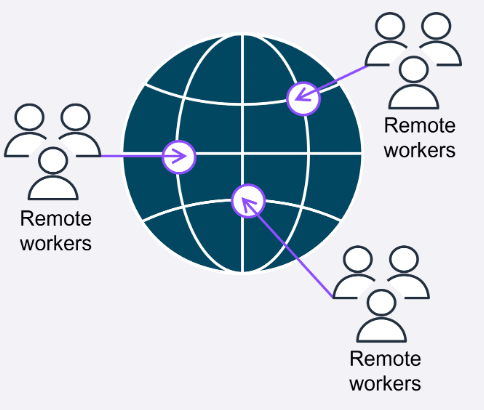
**Connecting to the AWS Cloud**

****

**AWS Client VPN –**

**Benefits:** AWS Client VPN provides advanced authentication, remote access. It is elastic and fully managed.

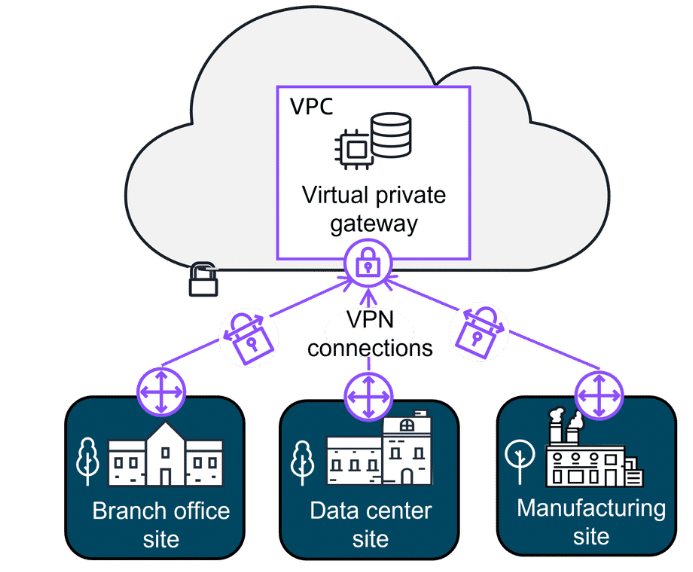
**Use case:** It can be used to quickly scale remote-worker access.



**AWS Site-to-Site VPN -**

**Benefits:** Site-to-Site VPN provides high availability, secure and private sessions, and accelerates applications.

**Use cases:**It can be used for application migration and secure communication between remote locations.



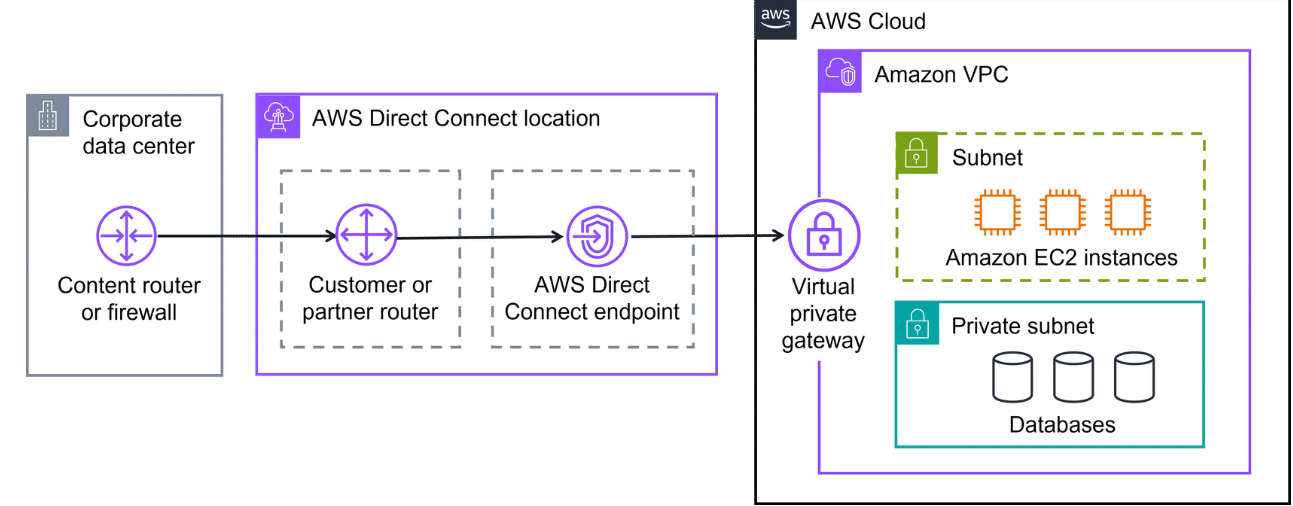
**AWS PrivateLink –**

**Benefits:**AWS PrivateLink helps you secure your traffic and connect with simplified management rules.

**Use case:**It is used for connecting your clients in your VPC to resources, other VPCs, and endpoints.

**AWS Direct Connect –**

**Benefits:** AWS Direct Connect reduces network costs and increases amount of bandwidth.



Subnet - A **subnet** is a section of a VPC in which you can group resources based on security or operational needs. Subnets can be public or private.

Public subnet - **Public subnets**contain resources that need to be accessible by the public, such as an online store’s website.

Private subnet - **Private subnets** contain resources that should be accessible only through your private network, such as a database that contains customers’ personal information and order histories.

Network ACLs - A network ACL is a virtual firewall that controls inbound and outbound traffic at the subnet level.

Stateless packet filtering - Network ACLs perform stateless packet filtering. They remember nothing and check packets that cross the subnet border each way: inbound and outbound.

Security groups - It is a virtual firewall that controls inbound and outbound traffic for specific AWS resources, like Amazon EC2 instances. By default, a security group denies all inbound traffic and allows all outbound traffic.

Stateful packet filtering - Security groups perform stateful packet filtering. They remember previous decisions made for incoming packets.

