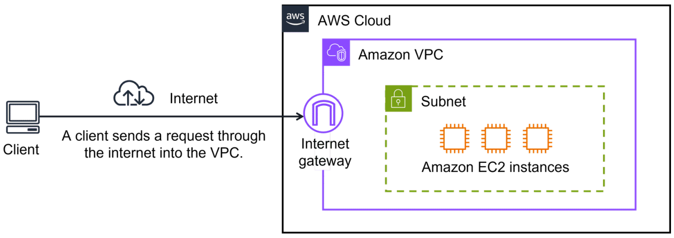
Module 5: Networking

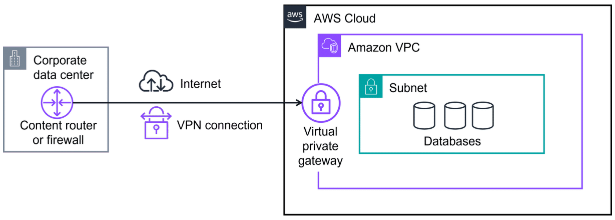
Amazon Virtual Private Cloud (Amazon VPC):

- Provision a logically isolated section of AWS Cloud where you can launch AWS resources in a virtual network that you define.

Subnet: - Sections of VPC - Chunks of IP Addresses

Internet gateway: Connection between VPC and internet





Virtual Private Gateway:

- Connect protected traffic to enter VPC.
- Establish **VPN** connection between VPC and a private network, such as an **on-premises data center** or **internal corporate network.**
- Allows traffic into VPC only if coming from approved network.

*****VPN can cause slower bandwidth. For Dedicated Connection, use AWS Direct Connect*****

AWS Direct Connect:

- Completely Private & Dedicated Connection

AWS Client VPN:

- Connect remote workers and on-premises networks to AWS cloud
- Uses OpenVPN-based client
- Works with **Global** Regions

AWS Site-to-Site VPN:

- Creates a secure connection **between data center/branch offices and AWS Cloud resources.**
- Used for application migration and secure communication between remote locations.

AWS PrivateLink:

- Privately connect VPC to resources as if in VPC.
- No internet gateway, Direct Connect connection, or AWS Site-to-Site VPN
- Used for connecting your clients in your VPC to resources, other VPCs, and endpoints.

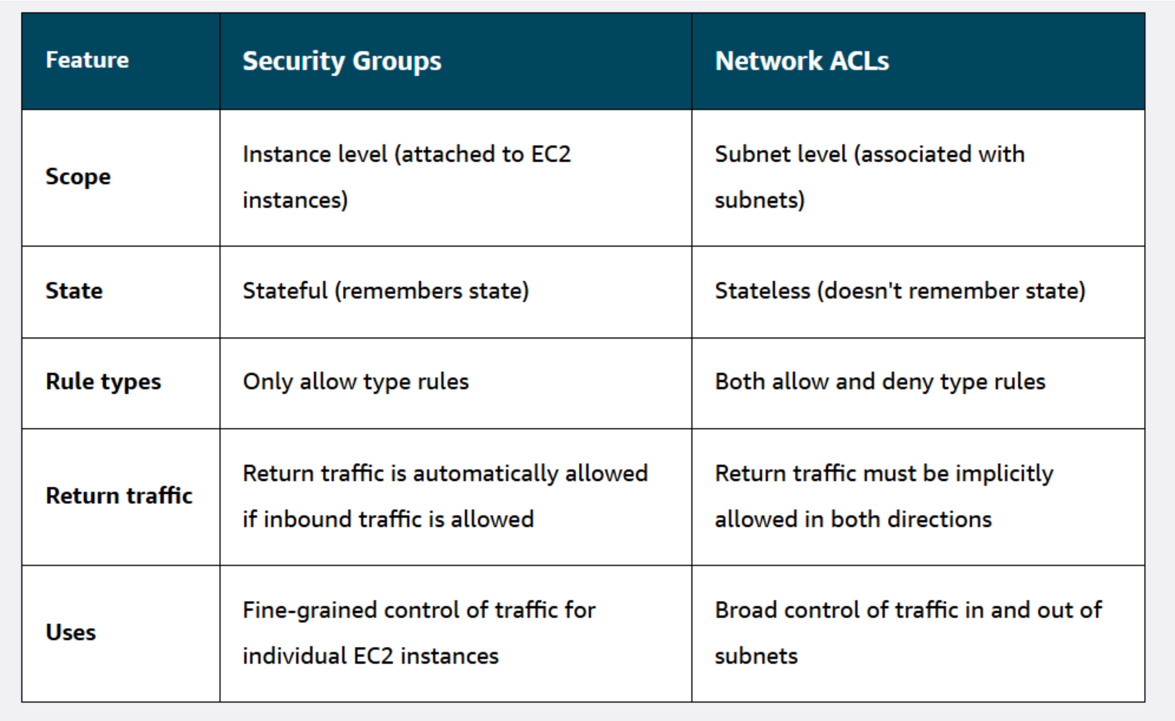
AWS Transit Gateway:

- Connect Amazon VPCs and on-premises networks through a **central hub.**

Network Address Translation (NAT) Gateway:

- Instances in private subnet can connect to services outside VPC **BUT** external services can't initiate a connection with those instances.

Amazon API Gateway: Creating, publishing, maintaining, monitoring, and securing APIs at any scale



Feature	Security Groups	Network ACLs
Scope	Instance level (attached to EC2 instances)	Subnet level (associated with subnets)
State	Stateful (remembers state)	Stateless (doesn't remember state)
Rule types	Only allow type rules	Both allow and deny type rules
Return traffic	Return traffic is automatically allowed if inbound traffic is allowed	Return traffic must be implicitly allowed in both directions
Uses	Fine-grained control of traffic for individual EC2 instances	Broad control of traffic in and out of subnets