AWS VPC - Day 2: Advanced Networking & Connectivity

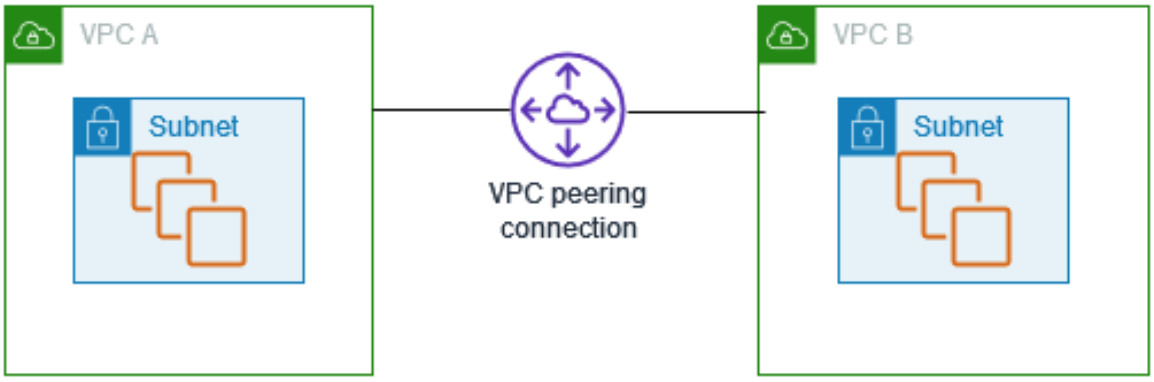
Follow me Shaik Hari Sadia Anjum for more content

1. Introduction

On **Day 1**, we covered the **fundamentals of AWS VPC**, including **subnets, route tables, internet gateways, security groups, and IP addressing**. Now, we will explore **advanced networking concepts**, focusing on **VPC Peering, Transit Gateway, PrivateLink, VPC Endpoints, hybrid cloud connectivity, and traffic analysis**.

Why is Advanced VPC Networking Important?

- Enables **secure communication** between VPCs.
- Facilitates **on-premises to AWS connectivity**.
- Ensures **efficient routing & traffic management**.
- Provides **better network isolation & security**.



2. VPC Peering & Transit Gateway

VPC Peering and Transit Gateway are **methods to connect multiple VPCs**, allowing inter-VPC communication.

2.1 VPC Peering

- Establishes a **direct network connection** between two VPCs.
- Works **within the same or different AWS accounts and regions**.
- **No bandwidth limitations** (uses AWS backbone network).

🔹 **Key Features:**
✔️ **One-to-one connection** (VPC to VPC).
✔️ No **transitive routing** (VPC A cannot communicate with VPC C through VPC B).
✔️ Supports both **IPv4 and IPv6**.

🔹 **Use Cases:**

- Connecting **VPCs in different AWS accounts** for collaboration.
- **Microservices communication** between different VPCs.

🔹 **Steps to Create VPC Peering:**

1. **Create Peering Connection** → Between two VPCs.
2. **Accept Peering Request** → Manually approve it.
3. **Update Route Tables** → Add routes to enable connectivity.
4. **Modify Security Groups** → Allow traffic between VPCs.

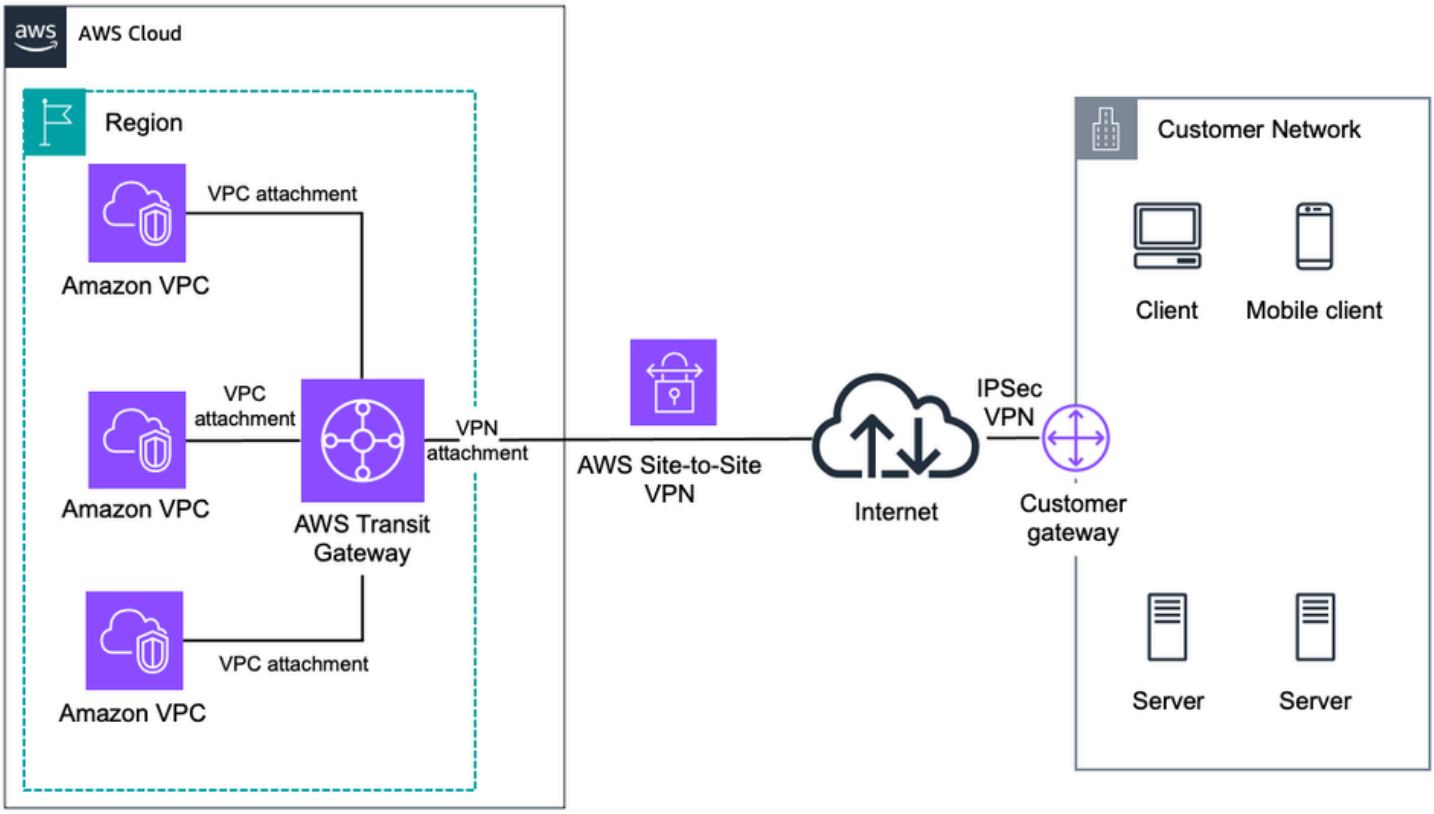
🔹 **Limitations of VPC Peering:**
❌ No support for transitive routing (each VPC needs direct peering).
❌ Limited to **125 active peering connections per VPC**.

Pricing for a VPC peering connection

There is no charge to create a VPC peering connection. All data transfer over a VPC peering connection that stays within an Availability Zone is free, even if it's between different accounts. Charges apply for data transfer over VPC peering connections that cross Availability Zones and Regions.

2.2 AWS Transit Gateway (TGW)

Transit Gateway acts as a **centralized router**, allowing multiple VPCs to communicate **efficiently**.



🔹 **Key Features:**

✔ **Hub-and-spoke model** (Connects multiple VPCs to a single gateway).

✔ Supports **transitive routing** (VPC A ⇔ Transit Gateway ⇔ VPC C).

✔ Can connect to **on-premises networks using AWS Direct Connect or VPN**.

🔹 **Use Cases:**

- **Enterprise networking** with multiple VPCs.
- **Centralized security and monitoring** across regions.
- **Hybrid cloud solutions** with VPN or Direct Connect.

🔹 **Comparison: VPC Peering vs. Transit Gateway**

Feature	VPC Peering	Transit Gateway
Scalability	Limited to 125 connections	Supports thousands of VPCs
Routing	No transitive routing	Supports transitive routing
Cost	Free (only pay for data transfer)	Charged based on attachments & traffic
Use Case	Small deployments	Large, multi-VPC architectures

3. AWS PrivateLink & VPC Endpoints

3.1 AWS PrivateLink

AWS PrivateLink enables **private connectivity** between AWS services and VPCs **without exposing data to the internet**.

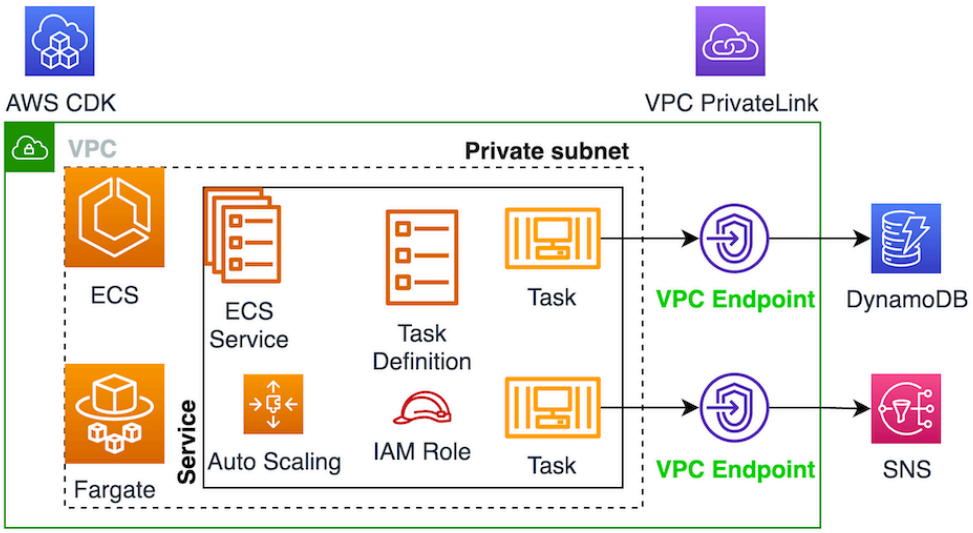
🔹 **Key Features:**
✔ Provides **secure, private connectivity**.
✔ Uses **Elastic Network Interfaces (ENIs)** inside the VPC.
✔ Reduces **exposure to public internet threats**.

🔹 **Use Cases:**

- Securely connect **AWS services (e.g., S3, DynamoDB) to a VPC**.
- **Access third-party SaaS applications** privately.

3.2 VPC Endpoints

VPC Endpoints provide **private access to AWS services**, bypassing the public internet.



🔹 **Types of VPC Endpoints:**

Type	Description	Example Services
Interface Endpoint	**Uses AWS PrivateLink for services requiring API interaction**	**S3, DynamoDB, SNS, SQS**
Gateway Endpoint	**Adds a private route to the route table**	**S3, DynamoDB**

🔹 **Benefits of VPC Endpoints:**
✔ **Eliminates public internet traffic**.
✔ **Reduces latency & enhances security**.
✔ **No extra bandwidth costs** compared to NAT Gateways.

🔹 **Steps to Create a VPC Endpoint:**

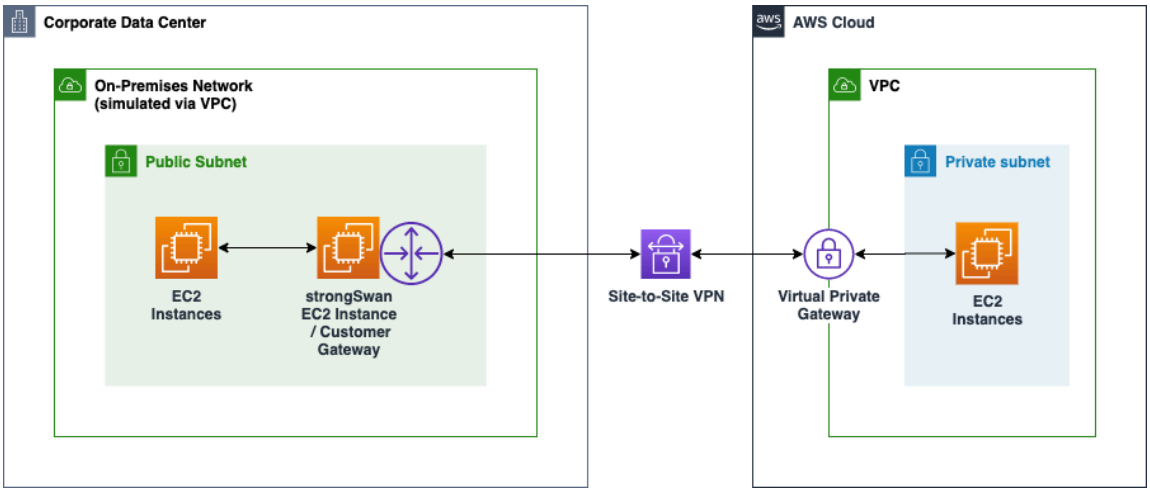
1. **Select AWS service** (e.g., S3, DynamoDB).
2. **Choose endpoint type** (Interface/Gateway).
3. **Attach it to a subnet and security group**.
4. **Update route table** for private access.

4. Hybrid Cloud Connectivity

AWS provides multiple options to **connect on-premises networks with AWS VPCs**.

4.1 AWS Site-to-Site VPN

A **secure, encrypted tunnel** between an **on-premises network** and an **AWS VPC**.



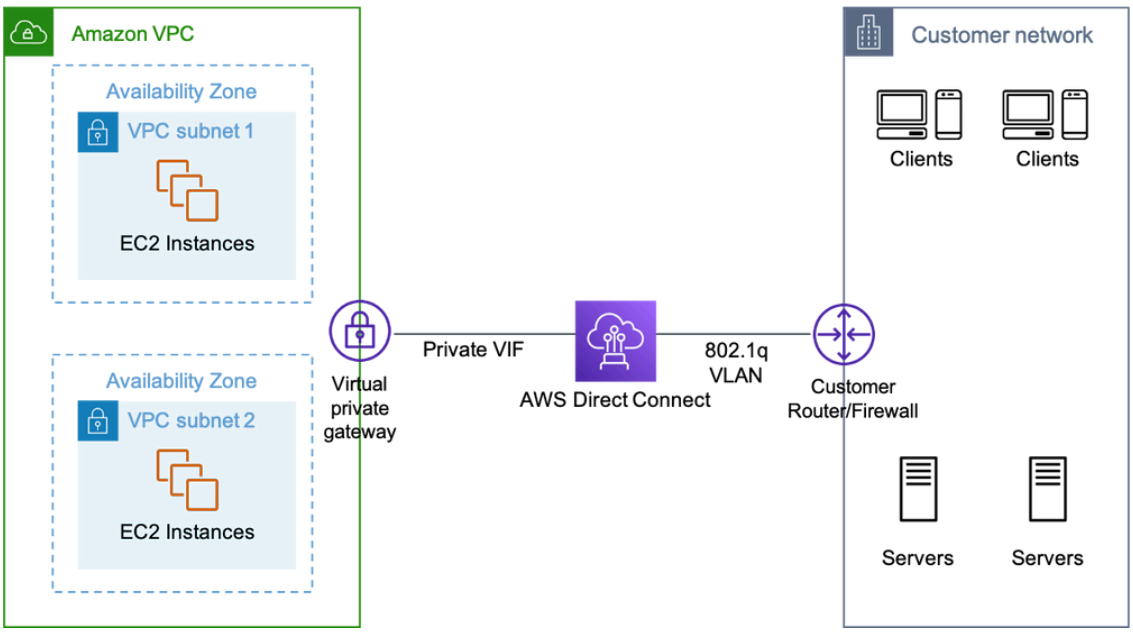
🔹 **Key Features:**
✔ Uses **IPSec encryption**.
✔ Supports **BGP for dynamic routing**.
✔ Can **failover to Direct Connect for redundancy**.

🔹 **Use Cases:**

- **Extend on-premises networks** to AWS.
- **Secure cloud migrations**.

4.2 AWS Direct Connect (DX)

AWS Direct Connect establishes a **private, dedicated** network connection between an on-premises data center and AWS.



🔹 **Key Features:**
✔ **Lower latency** compared to VPN.
✔ **Higher bandwidth** (1 Gbps – 100 Gbps).
✔ **No internet traffic** (private connection).

🔹 **Use Cases:**

- **Financial & healthcare applications** with strict compliance.
- **High-performance hybrid cloud architectures**.

🔷 Comparison: VPN vs. Direct Connect

Feature	AWS VPN	AWS Direct Connect
Encryption	Uses IPSec	Optional (can use private MPLS)
Speed	1.25 Gbps max	Up to 100 Gbps
Latency	High (internet-dependent)	Low (private connection)
Use Case	Small businesses	Large enterprises

5. Traffic Flow Analysis & Troubleshooting

5.1 VPC Flow Logs

VPC Flow Logs **capture network traffic** information.

🔹 **Key Features:**
✔️ Logs traffic **between instances, subnets, and internet**.
✔️ Helps **debug network connectivity issues**.
✔️ Stores data in **CloudWatch or S3** for analysis.

🔹 **Use Cases:**

- **Monitor security risks** and detect anomalies.
- **Analyze performance issues** in the network.

5.2 AWS Reachability Analyzer

A tool for **debugging network routing issues**.

🔹 **Use Cases:**

- Identify **blocked traffic by Security Groups or NACLs**.
- Validate **connectivity between instances**.

Conclusion

On **Day 2**, we explored **advanced VPC networking**, including:
✅ **VPC Peering vs. Transit Gateway** for multi-VPC architectures.
✅ **AWS PrivateLink & VPC Endpoints** for secure private connectivity.
✅ **Hybrid Cloud Connectivity (VPN & Direct Connect)** for on-prem to AWS networking.
✅ **Traffic Monitoring (Flow Logs, Reachability Analyzer)** for troubleshooting.