Project Report: Hybrid Cloud Integration

1. Summary

This report details the successful implementation of a secure site-to-site VPN connection between Microsoft Azure and Amazon Web Services (AWS). The project involved configuring virtual networks, gateways, and connections on both cloud platforms to establish a secure and encrypted communication tunnel. All objectives were met, resulting in a stable and connected hybrid cloud environment.

---

2. Project Goal

The primary purpose of this project was to establish a secure site-to-site VPN connection between Microsoft Azure and Amazon Web Services (AWS). This allows for secure data transfer and resource communication between the two distinct cloud environments.

---

3. Implementation Details

The project was executed in a series of steps, configuring resources on both Azure and AWS platforms.

Microsoft Azure Configuration

- **Step 1: Virtual Network and Subnet Creation**
  - A Virtual Network named `vNet-azure` was created in the `East US 2` location with an address space of `10.0.0.0/16`.
  - Two subnets were established: `GatewaySubnet` with an IP range of `10.0.1.0/24` and `subnet-01` with `10.0.2.0/24`.
- **Step 2: VPN Gateway Creation**
  - A VPN gateway named `vpn-azure-aws` was deployed in Azure to enable a secure, encrypted connection over the internet. This gateway uses a public IP address of `172.172.68.246`.
- **Step 3: Local Network Gateway Creation**
  - Two Local Network Gateways, `lng-azure-aws-01` and `lng-azure-aws-02`, were created in the `East US 2`region to represent the AWS network within Azure, ensuring that traffic is correctly routed through the VPN tunnel.
- **Step 4: Final Connection**
  - Two connections, `conn-01` and `conn-02`, were created to finalize the site-to-site IPsec tunnel, linking them to their respective local network gateway peers.

Amazon Web Services (AWS) Configuration

- **Step 1: VPC and Subnet Creation**
  - A Virtual Private Cloud (VPC) named `my-vpc-aws` was created with a CIDR block of `10.10.0.0/16`.
  - A subnet, `my-subnet-aws`, was configured within this VPC with a CIDR block of `10.10.1.0/24`.
- **Step 2: Customer Gateway Creation**
  - A Customer Gateway was created with the IP address of the Azure VPN gateway (`172.172.68.246`) and a BGP ASN of `65000` to establish the connection from the AWS side.
- **Step 3: Virtual Private Gateway Creation**
  - A Virtual Private Gateway (`vpg-azure-aws`) was created and attached to the `my-vpc-aws` VPC to manage the VPN connection. It uses an Amazon ASN of `64512`.
- **Step 4: Site-to-Site VPN Connection**
  - The site-to-site VPN connection (`site-to-site-connection`) was established to create the secure, encrypted tunnel between AWS and Azure.

---

4. Results and Verification

The hybrid cloud connection was successfully established and verified.

- **Connection Status:** The connections in Azure, `conn-01` and `conn-02`, both show a **"Connected"** status.
- **Tunnel State:** In AWS, the VPN connection details show that both Tunnels 1 and 2 have a status of **"Up"** as of March 17, 2025.

---

5. Supporting Visuals

- **vNet-azure.png:** Overview of the Azure Virtual Network.
- **subnet-azure.png:** Azure subnet configuration details.
- **vpn-gateway-azure.png:** Azure VPN Gateway status.
- **vpc-aws.png:** Overview of the AWS Virtual Private Cloud.
- **subnet-aws.png:** AWS subnet configuration details.
- **customer-gateway-aws.png:** AWS Customer Gateway pointing to Azure's public IP.
- **Virtual private gateway-aws.png:** AWS Virtual Private Gateway attached to the VPC.
- **lng_azure.png:** Local Network Gateways configured in Azure.
- **connection_azure.png:** Final connection status in Azure showing "Connected".