AWS VPN

What?
- AWS Virtual Private Network (VPN) solutions establish secure connections between your on-premises networks, remote offices, client devices, and the AWS global network.
- AWS VPN is comprised of two services: AWS Site-to-Site VPN and AWS Client VPN.

Why?
- Because it is a cloud VPN solution, you don't need to install and manage hardware or software-based solutions, or try to estimate how many remote users to support at one time.
- Data routes over an encrypted VPN connection to help maintain the confidentiality and integrity of data in transit.

When?
- AWS Site-to-Site VPN – When you want to create encrypted tunnels between your locations (such as data centers and remote offices) and your AWS VPC or AWS Transit Gateways.
- AWS Client VPN – Your remote workforce wants to securely access resources within both AWS and your on-premises.

Where?
- Amazon side of VPN connectors (Virtual Private Gateway, Client VPN endpoint) are a regional entity.
- Customer side of VPN connectors (Customer gateway device, OpenVPN-based VPN client) run on-premises.

Who?
- AWS manages high availability and scalability for AWS side of the VPN connection. Each Site-to-Site VPN connection offers two tunnels for high availability.
- Customers manage high availability and scalability for the customer side of the VPN connection.

How?
- AWS Site-to-Site VPN – Create a VPN connection by connecting an existing Virtual Private Gateway (VPN concentrator on Amazon side) or transit gateway to the customer gateway (VPN concentrator on customer side).
- AWS Client VPN – Create a Client VPN endpoint on Amazon side and connect to it using OpenVPN-based VPN client.

Created by:

Ashish Prajapati

How much?
- AWS Site-to-Site VPN – Charged for each VPN connection-hour that your VPN connection is provisioned and available.
- AWS Client VPN – Charged per hour for the number of active client connections and the number of associated subnets.
- Standard data transfer charges apply for data transferred via the VPN.