AWS to GCP Site-to-Site VPN

Clean technical case study prepared by Hariharan J

Executive Summary

This case study describes a hybrid connectivity pattern between AWS and Google Cloud using site-to-site VPN. It highlights VPC planning, tunnel configuration, routing, firewall controls, and validation steps for secure cross-cloud communication.

Primary services	AWS VPC, GCP VPC, VPN Gateway, Cloud Router, BGP/static routing
Goal	Enable private communication between workloads across AWS and GCP
Security focus	Encrypted tunnel, scoped routes, firewall rules, and validation

Architecture

```
AWS VPC subnet -> AWS VPN gateway/customer gateway -> encrypted tunnel -> GCP HA VPN gateway
-> Cloud Router/GCP VPC subnet. Firewall rules allow only required traffic.
```

Implementation Steps

- Plan non-overlapping CIDR ranges for AWS and GCP networks.
- Create VPN gateways and configure tunnel parameters consistently on both sides.
- Configure BGP or static routes for private subnet reachability.
- Apply firewall and security group rules for only required protocols.
- Validate private connectivity using ping, traceroute, and service-level tests.

Validation

- Confirm tunnel status is up on both cloud providers.
- Check route tables and learned/advertised routes.
- Test private IP communication between controlled test instances.

Risks and Controls

- CIDR overlap can make routing impossible; mitigate with address planning.
- Mismatched tunnel parameters can keep VPN down; mitigate with configuration checklist.
- Overly broad firewall rules increase exposure; mitigate with least-privilege network access.

Interview Talking Points

- Why hybrid VPN is useful for private migration and multi-cloud operations.
- How routing and firewall controls work together.
- How to troubleshoot tunnel status and reachability issues.