GCP Network Security & Firewall Strategy

1. VPC Segmentation & Firewall Policies

- Implement separate VPCs for production, development, and testing environments.

- Enforce deny-all ingress and allow-only necessary traffic.

- Use Identity-Aware Proxy (IAP) for access to internal applications.

2. Security Perimeter & Access Restrictions

- Implement VPC Service Controls to restrict data movement between services.

- Use Private Google Access to prevent public internet exposure.

3. DDoS & Intrusion Protection

- Enable Cloud Armor to mitigate large-scale attacks.

- Use Security Command Center to monitor and respond to threats.

4. Zero Trust Networking

- Require context-aware access based on device, identity, and location.

- Use BeyondCorp principles to enforce continuous authentication.