Professional Cloud Network Engineer

Section 1: Designing and planning a Google Cloud network (~26% of the exam)

1.1 Designing an overall network architecture. Considerations include:

- Designing for high availability, failover, disaster recovery, and scale.
- Designing the DNS topology (e.g., on-premises, Cloud DNS).
- Designing for security and data exfiltration prevention requirements.
- Choosing a load balancer for an application.
- Designing for hybrid connectivity (e.g., Private Google Access for hybrid connectivity).
- Planning for Google Kubernetes Engine (GKE) networking (e.g., secondary ranges, scale potential based on IP address space, access to GKE control plane).
- Planning Identity and Access Management (IAM) roles including managing IAM roles in a Shared VPC environment.
- Incorporating micro segmentation for security purposes (e.g., using metadata, tags, service accounts, secure tags).
- Planning for connectivity to managed services (e.g., private services access, Private Service Connect, Serverless VPC Access).
- Differentiating between network tiers (e.g., Premium and Standard).
- Designing for VPC Service Controls.

1.2 Designing Virtual Private Cloud (VPC) networks. Considerations include:

- Choosing the VPC type and quantity (e.g., standalone or Shared VPC, number of VPC environments).
- Determining how the networks connect based on requirements (e.g., VPC Network Peering, VPC Network Peering with Network Connectivity Center, Private Service Connect).
- Planning the IP address management strategy (e.g., subnets, IPv6, bring your own IP (public advertised prefix (PAP) and public delegated prefix (PDP)), Private NAT, non-RFC 1918, managed services).
- Planning a global or regional network environment.
- Planning the firewall strategy (e.g., VPC firewall rules, Cloud Next Generation Firewall, hierarchical firewall rules).
- Planning custom routes (static or policy-based) for third-party device insertion (e.g., network virtual appliance).

1.3 **Designing a resilient and performant hybrid and multi-cloud network. Considerations include**:

- Designing for datacenter connectivity including bandwidth constraints (e.g., Dedicated Interconnect, Partner Interconnect, Cloud VPN).
- Designing for multi-cloud connectivity (e.g., Cloud VPN, Cross-Cloud Interconnect).
- Designing for branch office connectivity (e.g., IPSec VPN, SD-WAN appliances).
- Choosing when to use Direct Peering or a Verified Peering Provider.
- Designing high-availability and disaster recovery connectivity strategies.
- Selecting regional or global dynamic routing mode.
- Accessing multiple VPCs from on-premises locations (e.g., Shared VPC, multi-VPC peering and Network Connectivity Center topologies).
- Accessing Google Services and APIs privately from on-premises locations (e.g., Private Service Connect for Google APIs).
- Accessing Google-managed services through VPC Network Peering connections (e.g., private services access, Service Networking).

●Designing the IP address space across on-premises locations and cloud environments (e.g., internal ranges, planning to avoid overlaps).
●Designing the DNS peering and forwarding strategy (e.g., DNS forwarding path).

1.4 Designing an IP addressing plan for Google Kubernetes Engine (GKE). Considerations include:

●Choosing between public or private cluster nodes and node pools.
●Choosing between public or private control plane endpoints.
●Choosing between GKE Autopilot mode or Standard mode.
●Planning subnets and alias IPs.
●Selecting RFC 1918, non-RFC 1918, and/or privately used public IP (PUPI) addresses.
●Planning for IPv6.

Section 2: Implementing Virtual Private Cloud (VPC) networks (~22% of the exam)

2.1 Configuring VPCs. Considerations include:

●Creating Google Cloud VPC resources (e.g., networks, subnets, firewall rules or policy, private services access subnet).
●Configuring VPC Network Peering.
●Creating a Shared VPC network and sharing subnets with other projects.
●Configuring API access to Google services (e.g., Private Google Access, public interfaces).
●Expanding VPC subnet ranges after creation.

2.2 Configuring VPC routing. Considerations include:

●Setting up static and dynamic routing.
●Configuring global or regional dynamic routing.
●Implementing routing using network tags and priority.
●Implementing an internal load balancer as a next hop.
●Configuring custom route import/export over VPC Network Peering.
●Configuring Policy-based Routing.

2.3 Configuring Network Connectivity Center. Considerations include:

●Managing VPC topology (e.g., star topology, hub and spokes, mesh topology).
●Implementing Private NAT.

2.4 Configuring and maintaining Google Kubernetes Engine clusters. Considerations include:

●Creating VPC-native clusters using alias IPs.
●Setting up clusters with Shared VPC.
●Configuring private clusters and private control plane endpoints.
●Adding authorized networks for cluster control plane endpoints.
●Configuring Cloud Service Mesh.
●Enabling GKE Dataplane V2.
●Configuring source NAT (SNAT) and IP Masquerade policies.
●Creating GKE network policies.
●Configuring Pod ranges and service ranges, and deploying additional Pod ranges for GKE clusters.

2.5 Configuring and managing Cloud Next Generation Firewall (NGFW) rules. Considerations include:

- Creating the firewall rules and regional/global policies.
- Mapping target network tags, service accounts, and secure tags.
- Migrating from firewall rules to firewall policies.
- Configuring firewall rule criteria (e.g., rule priority, network protocols, ingress and egress rules).
- Configuring Firewall Rules Logging.
- Configuring hierarchical firewall policies.
- Configuring the intrusion prevention service (IPS).
- Implementing fully qualified domain name (FQDN) firewall objects.

Section 3: Configuring managed network services (~21% of the exam)

3.1 Configuring load balancing. Considerations include:

- Configuring backend services (e.g., network endpoint groups (NEGs), managed instance groups).
- Configuring backends and backend services with the balancing method (e.g., RPS, CPU, custom), session affinity, and serving capacity.
- Configuring URL maps.
- Configuring forwarding rules.
- Defining firewall rules to allow traffic and health checks to backend services.
- Creating health checks for backend services and target instance groups.
- Configuring protocol forwarding.
- Accommodating workload increases by using autoscaling or manual scaling.
- Configuring load balancers for GKE (e.g., GKE Gateway controller, GKE Ingress controller, NEG).
- Setting up traffic management on Application Load Balancers (e.g., traffic splitting, traffic mirroring, URL rewrites).

3.2 Configuring Google Cloud Armor policies. Considerations include:

- Configuring security policies.
- Implementing web application firewall (WAF) rules (e.g., SQL injection, cross-site scripting, remote file inclusion).
- Attaching security policies to load balancer backends.
- Configuring advanced network DDoS protection.
- Configuring edge and network edge security policies.
- Configuring Adaptive Protection.
- Configuring rate limiting.
- Configuring bot management.
- Applying Google Threat Intelligence.

3.3 Configuring Cloud CDN. Considerations include:

- Setting up Cloud CDN for supported origins (e.g., managed instance groups, Cloud Storage buckets, Cloud Run).
- Setting up Cloud CDN for external backends (internet NEGs) and third-party object storage.
- Invalidating cached content.
- Configuring signed URLs.

3.4 Configuring and maintaining Cloud DNS. Considerations include:

- Managing Cloud DNS zones and records.
- Migrating to Cloud DNS.
- Enabling DNS Security Extensions (DNSSEC).
- Configuring DNS forwarding and DNS server policies.
- Integrating on-premises DNS with Google Cloud.
- Using split-horizon DNS.
- Setting up DNS peering.
- Configuring Cloud DNS and external-DNS operator for GKE.

3.5 Configuring and securing internet egress traffic. Considerations include:

- Assigning NAT IP addresses (e.g., automatic, manual).
- Configuring port allocations (e.g., static, dynamic).
- Customizing timeouts.
- Configuring organization policy constraints for Cloud NAT.
- Configuring Private NAT.
- Configuring Secure Web Proxy.

3.6 Configuring network packet inspection. Considerations include:

- Routing and inspecting inter-VPC traffic using multi-NIC VMs (e.g., next-generation firewall appliances).
- Configuring an internal load balancer as a next hop for highly available multi-NIC VM routing.
- Enabling Layer 7 packet inspection in Cloud NGFW.

Section 4: Implementing hybrid network interconnectivity (~18% of the exam)

4.1 Configuring Cloud Interconnect. Considerations include:

- Creating Dedicated Interconnect connections and configuring VLAN attachments.
- Creating Partner Interconnect connections and configuring VLAN attachments.
- Creating Cross-Cloud Interconnect connections and configuring VLAN attachments.
- Setting up and enabling MACsec.
- Configuring HA VPN over Cloud Interconnect.

4.2 Configuring a site-to-site IPSec VPN. Considerations include:

- Configuring HA VPN.
- Configuring Classic VPN (e.g., route-based, policy-based).

4.3 Configuring Cloud Router. Considerations include:

- Implementing Border Gateway Protocol (BGP) attributes (e.g., ASN, route priority/MED, link-local addresses, authentication).
- Configuring Bidirectional Forwarding Detection (BFD).
- Creating custom advertised routes and custom learned routes.

4.4 Configuring Network Connectivity Center. Considerations include:

- Creating hybrid spokes (e.g., VPN, Cloud Interconnect).
- Establishing site-to-site data transfer.
- Creating Router appliances (RAs).

Section 5: Managing, monitoring, and troubleshooting network operations (~13% of the exam)

5.1 Logging and monitoring with Google Cloud Observability. Considerations include:

- Enabling and reviewing logs for networking components (e.g., Cloud VPN, Cloud Router, VPC Service Controls, Cloud NGFW, Firewall Insights, VPC Flow Logs, Cloud DNS, Cloud NAT).
- Monitoring metrics of networking components (e.g., Cloud VPN, Cloud Interconnect and VLAN attachments, Cloud Router, load balancers, Google Cloud Armor, Cloud NAT).

5.2 Maintaining and troubleshooting connectivity issues. Considerations include:

- Draining and redirecting traffic flows with Application Load Balancers.
- Tuning and troubleshooting Cloud NGFW rules or policies.
- Managing and troubleshooting VPNs.
- Troubleshooting Cloud Router BGP peering issues.
- Troubleshooting with VPC Flow Logs, firewall logs, and Packet Mirroring.

5.3 Using Network Intelligence Center to monitor and troubleshoot common networking issues. Considerations include:

- Using Network Topology to visualize throughput and traffic flows.
- Using Connectivity Tests to diagnose route and firewall misconfigurations.
- Using Performance Dashboard to identify packet loss and latency (e.g., Google-wide, project scoped).
- Using Firewall Insights to monitor rule hit count and identify shadowed rules.
- Using Network Analyzer to identify network failures, suboptimal configurations, and utilization warnings.