Google Cloud

# Professional Cloud Network Engineer

---

**This is the new version of the Professional Cloud Network Engineer exam guide.** If you plan to take the Professional Cloud Network Engineer exam in English on or after October 17, review this exam guide. If you plan to take the exam before October 17, review the current version.

---

## Certification exam guide

A Professional Cloud Network Engineer is responsible for the design, implementation, and management of Google Cloud network infrastructure. This includes designing network architectures for high availability, scalability, resiliency, and security. This individual is skilled in configuring and managing Virtual Private Clouds (VPCs), routing, network security services, load balancing, Cloud NAT, and Cloud DNS. Additionally, they are proficient in setting up hybrid and multi-cloud connectivity through Cloud Interconnect and Cloud VPN. Their expertise extends to diagnosing, monitoring, and troubleshooting network operations by using Google Cloud Observability and Network Intelligence Center.

### Section 1: Designing and planning a Google Cloud Virtual Private Cloud (VPC) network (~24% 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).
- Choosing a load balancer for an application or solution.
- 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.
- 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).

1.2 Designing VPC networks. Considerations include:

- Choosing the VPC type and quantity (e.g., standalone or Shared VPC, number of VPC environments).
- Determining how the networks interconnect based on requirements (e.g., VPC Network Peering, network connectivity (Mesh and Star topology) 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 addresses, managed services).
- Planning a global, regional network environment (or variations of these).
- Determining the correct MTU sizing for VPC for workloads.
- Planning third-party device insertion (e.g., network virtual appliance) with custom routes (static or policy-based) and load balancing.

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

- Designing for hybrid (e.g., on-premises and cloud, branch office) connectivity including bandwidth and security constraints (e.g., Dedicated Interconnect, Partner Interconnect, Cloud VPN, SD-WAN appliances).
- Designing for multi-cloud connectivity (e.g., Cloud VPN, Cross-Cloud Interconnect).
- Choosing when to use Direct Peering or Verified Peering Provider.
- Designing high-availability and disaster recovery connectivity strategies for multiple regions (e.g., 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 like Vertex AI and APIs privately from on-premises locations (e.g., Private Service Connect for Google APIs).
- Accessing managed services through Private Service Connect (PSC) or 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).
- Determine the correct MTU sizing for hybrid connections (Cloud Interconnect and HA VPN) for workloads.
- Understanding interconnect encryption options such as MACsec and HA VPN over Cloud Interconnect.

1.4 Designing 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.
- Planning subnets: primary and secondary ranges.
- Selecting RFC 1918, non-RFC 1918, or privately used public IP (PUPI) addresses.
- Planning for IPv6.
- Designing load balancing for GKE networking.
- Adding and managing node pool configuration.

## Section 2: Implementing a VPC network (~19% of the exam)

2.1 Configuring VPCs. Considerations include::

- Creating Google Cloud VPC resources (e.g., networks, subnets, firewall rules or policies, private services access subnet, private pools).
- Configuring VPC Network Peering.
- Creating a Shared VPC network and sharing subnets with other projects.
- Configuring access to Google APIs and Google-managed services (e.g., Private Google Access, public interfaces).
- Configuring access to Vertex AI services.
- Expanding VPC subnet ranges after creation.
- Configuring restricted Google Cloud services with VPC Service Controls perimeters.

2.2 Configuring VPC routing. Considerations include:

- Setting up static and dynamic routing (e.g. Cloud Router).
- Configuring global or regional dynamic routing.
- Implementing routing using network tags and priority.
- Designing route priorities with global dynamic routing.
- 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:

- Differentiating between spoke types (VPC Spoke, Hybrid Spoke and Producer Spoke).
- Managing VPC topology (e.g., star topology, hub and spokes, mesh topology).
- Configuring Private NAT and Private Service Connect propagation.
- Configuring IP/CIDR range filters for NCC spokes.
- Monitoring and troubleshooting NCC.

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.
- Enabling GKE Dataplane V2.
- Configuring source NAT (SNAT) and IP Masquerade policies.
- Creating GKE network policies.
- Configuring Pod ranges and service ranges.
- Deploying additional Pod ranges for GKE clusters.

## Section 3: Configuring managed network services (~16% of the exam)

3.1 Configuring load balancing. Considerations include:

- Determining the load balancing solution for your network (internal/external, regional/global, application/proxy/passthrough, etc.).
- Configuring backend services (e.g., network endpoint groups (NEGs), managed instance groups).
- Configuring various load balancers and backend settings such as the balancing method, session affinity, serving capacity, URL maps, health checks, and global access.
- Optimizing for traffic scalability by using autoscaling or manual scaling features.
- Understanding load balancers in 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 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.

3.3 Configuring Cloud DNS. Considerations include:

- Managing Cloud DNS zones and records.
- Migrating to Cloud DNS.
- Configuring Cloud DNS routing policies such as geolocation and failover policies.
- Enabling DNS Security Extensions (DNSSEC).
- Setting up self-hosted DNS integration with Cloud DNS, including configuring DNS forwarding and DNS server policies.
- Understanding DNS private and public zones and setting up split-horizon DNS.
- Setting up DNS cross-project binding and DNS peering.
- Configuring Cloud DNS and external-DNS operator for GKE.

## Section 4: Configuring and implementing hybrid and multi-cloud network interconnectivity (~15% of the exam)

4.1 Configuring Cloud Interconnect. Considerations include:

- Creating Dedicated Interconnect connections and configuring VLAN attachments.
- Creating Partner Interconnect connections, configuring VLAN attachments, and differentiating between Layer2 and Layer3 type Interconnects.
- Creating Cross-Cloud Interconnect connections and configuring VLAN attachments.
- Configuring HA VPN over Cloud Interconnect.
- Implementing 99.9% SLA and 99.99% SLA for Interconnect topologies.

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

- Configuring HA VPN towards on-premise VPN gateways.
- Configuring HA VPN towards other Google Cloud VPCs.
- 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.
- Selecting between legacy and standard best path selection at the VPC.

4.4 Configuring Network Connectivity Center. Considerations include:

- Creating hybrid spokes (e.g., VPN, VLAN attachment).
- Establishing site-to-site data transfer.
- Creating Router appliances (RAs).
- Solving common transitivity networking issues.

**Section 5: Managing, monitoring, and troubleshooting network operations (~12% of the exam)**

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

- Enabling and reviewing Cloud Logging for networking components (e.g., Cloud VPN, Cloud Router, VPC Service Controls, Cloud NGFW, Firewall Insights, VPC Flow Logs, Cloud DNS, Cloud NAT, NCC).
- Monitoring networking metrics (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.
- Managing and troubleshooting VPNs.
- Managing and troubleshooting Cloud Interconnect issues.
- 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.
- Using Flow Analyzer and VPC Flow Logs to evaluate network traffic.

**Section 6: Configuring, implementing and managing a cloud network security solution (~14% of the exam)**

6.1 Configuring Google Cloud Armor policies. Considerations include:

- Configuring and attaching edge and backend security policies.
- Implementing web application firewall (WAF) rules (e.g., SQL injection, cross-site scripting, remote file inclusion).
- Configuring advanced network distributed denial of service (DDoS) and Adaptive Protection.
- Configuring rate limiting.
- Configuring bot management.
- Applying Google Threat Intelligence.

6.2 Configuring and managing Cloud Next Generation Firewall (NGFW) policies and VPC Firewall rules. Considerations include:

- Planning the firewall strategy (e.g., VPC firewall rules, Cloud Next Generation Firewall, hierarchical firewall rules, third party integration).
- Configuring Cloud NGFW to support GKE and Cloud load balancers.
- Creating and troubleshooting VPC Cloud Firewall rules and Cloud NGFW regional/global/hierarchical policies.
- Enabling Layer 7 packet inspection with Cloud NGFW Enterprise.
- Migrating from VPC Firewall rules to Cloud NGFW Policies.
- Configuring VPC and NGFW rule criteria (e.g., rule priority, network protocols, direction (ingress and egress), source, destination) Configuring VPC and Firewall Rules Logging.
- Incorporating micro segmentation for security purposes (e.g., using metadata, (secure) Tags, service accounts, network tags).
- Differentiating between the different tiers of Cloud NGFW: Essentials, Standard and Enterprise.

6.3 Configuring and securing internet egress traffic using Public Cloud NAT and Secure Web Proxy. Considerations include:

- Configuring public Cloud NAT IP addressing and assigning automatic and manual NAT IP addresses.
- Configuring static and dynamic port allocation for Cloud NAT.
- Configuring Secure Web Proxy.

6.4 Configuring self-managed network packet inspection, IDS, and Packet Mirroring. Considerations include:

- Routing and inspecting inter-VPC traffic using multi-NIC VMs (e.g., NGFW appliances).
- Configuring an internal load balancer as a next hop for HA multi-NIC VM routing.

- Configure policy-based routes for HA multi-NIC VM routing.
- Developing a strategy for out-of-band Network Security Integration (NSI).
- Configuring the Cloud Intrusion Detection System (IDS)
- Configuring Packet Mirroring for VPC traffic towards self-managed collectors.