

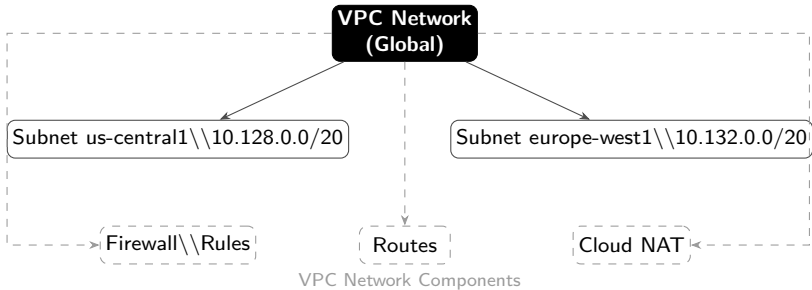


VPC & Hybrid Connectivity

GCP Professional Cloud Network Engineer | VPC Architecture, Interconnect, VPN & Cloud Router

VPC Architecture

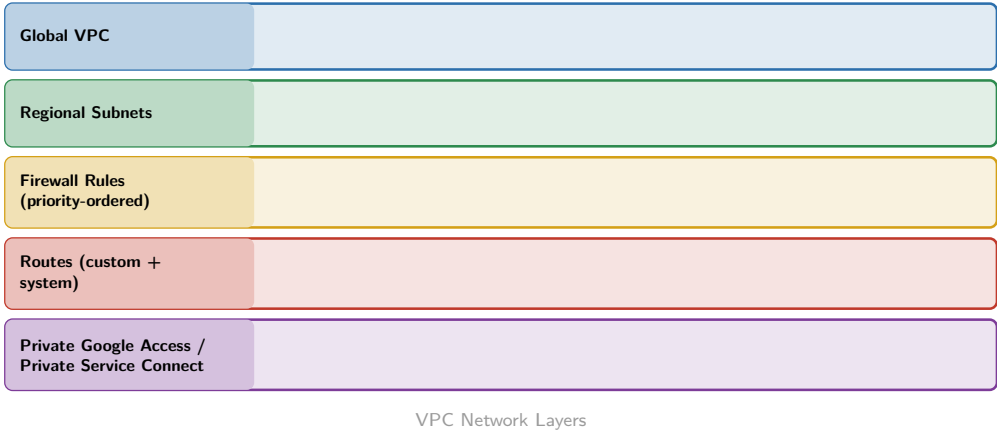
A VPC is a global, software-defined network spanning all GCP regions. Subnets are regional resources with defined CIDR ranges. VPCs provide isolation, firewall controls, routing, and connectivity to on-premises and other cloud environments.



Auto mode VPC	Automatically creates one subnet per region with predefined /20 CIDRs from 10.128.0.0/9. Simple but inflexible. Not recommended for production.
Custom mode VPC	You define subnets manually (region, CIDR). Full control over IP ranges. Required for Shared VPC, VPN, Interconnect.
Subnet secondary ranges	Alias IP ranges for GKE Pods and Services. VPC-native clusters use secondary ranges for Pod and Service CIDRs.
Routes	System-generated (default, subnet) + custom static routes. Policy-based routing with next-hop (instance, ILB, VPN tunnel).
Cloud DNS	Managed DNS. Public zones (internet-facing), private zones (internal VPC resolution). Response policies for DNS filtering.
Internal DNS	Automatic internal DNS: HOSTNAME.ZONE.c.PROJECT. internal. Zonal and global DNS resolution within VPC.

IP Addressing

Type	Scope	Use
Internal IP	VPC (RFC 1918)	Default for all instances
External IP (ephemeral)	Internet	Lost on stop, changes on restart
External IP (static)	Internet	Reserved, survives stop/start
Alias IP	Subnet secondary range	GKE Pods, multiple IPs per VM
Private Service Connect IP	VPC	Endpoint to Google APIs/services



Shared VPC & VPC Peering

Feature	Shared VPC	VPC Peering
Architecture	Host project owns network, service projects use it	Two independent VPCs connected
Transitivity	N/A (single VPC)	Non-transitive (A-B + B-C ≠ A-C)
Admin model	Network admin in host, workload in service	Independent admin per VPC
CIDR overlap	N/A (same VPC)	Not allowed
Cross-org	No (same org)	Yes
Scale limit	Per VPC quotas	25 peered networks per VPC
Best for	Org-wide centralized networking	Cross-project/org connectivity

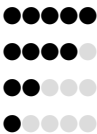
- Shared VPC: use for centralized network management, consistent firewall policies, single point of control

Shared VPC scalability

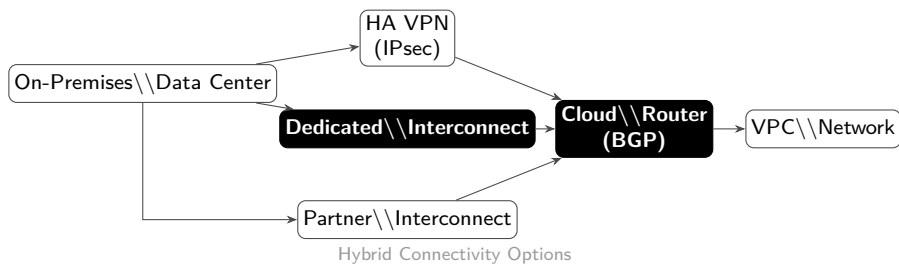
VPC Peering simplicity

Shared VPC admin overhead

VPC Peering transitivity



Hybrid Connectivity



Dedicated Interconnect	10/100 Gbps circuits at colocation facilities. VLAN attachments map to VPCs. SLA: 99.9% (single), 99.99% (redundant in 2 metros). Not encrypted by default.
Partner Interconnect	Via carrier partner. 50 Mbps to 50 Gbps. No colocation needed. SLA: up to 99.99% with redundant attachments.
HA VPN	99.99% SLA with dual-tunnel config. IPsec encrypted. BGP via Cloud Router. Up to 3 Gbps per tunnel. Good for moderate bandwidth or as Interconnect backup.
Classic VPN (deprecated)	Single tunnel, no SLA. Policy-based or route-based. Migrate to HA VPN.
Cloud Router	Managed BGP router. Learns on-prem routes, advertises VPC routes. Supports custom route advertisements and ASN.
Cross-Cloud Interconnect	Dedicated connectivity to AWS, Azure, Oracle Cloud. 10/100 Gbps. Google-managed physical connection.

Interconnect Redundancy for 99.99% SLA

- Dedicated: 4 connections (2 per metro area, 2 different metro areas)
- Partner: 4 VLAN attachments (2 per metro, 2 metros)
- HA VPN: 2 HA VPN gateways, each with 2 tunnels = 4 tunnels total
- Combine Interconnect + VPN for encrypted Interconnect traffic

Private Google Access

Private Google Access	Subnet setting. VMs without external IP reach Google APIs (storage.googleapis.com, etc.) via internal routes. Enable per subnet.
Private Google Access for on-premises	On-prem hosts access Google APIs over VPN/Interconnect using restricted.googleapis.com (199.36.153.4/30) or private.googleapis.com (199.36.153.8/30).
Private Service Connect (PSC)	Create private endpoints with internal IPs for Google APIs or published services. More granular than PGA. Supports forwarding rules and DNS.
Serverless VPC Access	Connector that allows Cloud Run, Cloud Functions, App Engine to reach VPC resources (Cloud SQL, Memorystore, internal services).

- restricted.googleapis.com: only VPC Service Controls-supported APIs. Use with VPC-SC perimeters
- private.googleapis.com: all Google APIs. Use when VPC-SC is not needed
- Private Service Connect supports consumer-producer model for internal service publishing
- DNS zones for googleapis.com must be configured to resolve to private endpoints

Cloud NAT

How it works	Regional managed NAT gateway. Maps internal IPs to NAT IPs for outbound internet. No inbound connections. No VM required.
Static NAT IPs	Reserve external IPs for predictable source addresses. Required for allowlisting by external services.
Dynamic port allocation	Automatically adjusts ports per VM based on connection needs. Reduces port exhaustion.
Logging	NAT logs show translations, errors, and dropped connections. Export to Cloud Logging for analysis.

- Applies to VMs, GKE nodes, and serverless VPC Access connectors
- Configure per subnet or for all subnets in a region
- Minimum ports per VM: 64 (default). Increase for VMs with many connections
- Cloud NAT does not apply to Cloud Interconnect or VPN traffic

High Bandwidth + Low Latency • Dedicated Interconnect • Cross-Cloud Interconnect	Moderate Bandwidth + Flexible • Partner Interconnect • HA VPN
Private Access + No Peering • Private Service Connect • Private Google Access	Internal + Managed • Cloud NAT • Serverless VPC Access

Connectivity Option Selection

99.99%
HA VPN SLA
Requires dual-tunnel configuration with Cloud Router BGP

Official resources

⚠ Check the current exam guide

Google Cloud is updating its exams to the products announced at Google Cloud Next '26 (Gemini Enterprise Agent Platform, the data and analytics stack), per the certification hub checked 2026-10-05: read the current exam guide before these sheets.

[1] Professional Cloud Network Engineer exam guide

Google Cloud · accessed 2026-10-05 · services.google.com/fh/files/misc/042426_pro...ork_engineer_exam_guide_english.pdf
Supports: domains and topics

[2] Professional Cloud Network Engineer certification page

Google Cloud · accessed 2026-10-05 · cloud.google.com/learn/certification/cloud-network-engineer
Supports: format, price, sample questions link, renewal

[3] Professional Cloud Network Engineer learning path

Google Skills · accessed 2026-10-05 · skills.google/paths/14
Supports: Google Skills (ex Cloud Skills Boost)

[4] gcloud CLI cheat sheet

Google Cloud · accessed 2026-10-05 · cloud.google.com/sdk/docs/cheatsheet
Supports: the commands on one page

[5] VPC documentation

Google Cloud · accessed 2026-10-05 · cloud.google.com/vpc/docs
Supports: VPC, subnets, routes, firewall rules

[6] Cloud Interconnect documentation

Google Cloud · accessed 2026-10-05 · cloud.google.com/network-connectivity/docs/interconnect
Supports: Dedicated and Partner

[7] Cloud VPN documentation

Google Cloud · accessed 2026-10-05 · cloud.google.com/network-connectivity/docs/vpn
Supports: HA VPN, BGP

[8] Cloud Load Balancing documentation

Google Cloud · accessed 2026-10-05 · cloud.google.com/load-balancing/docs
Supports: choose a load balancer

8 sources · 2 publishers · last accessed 2026-10-05