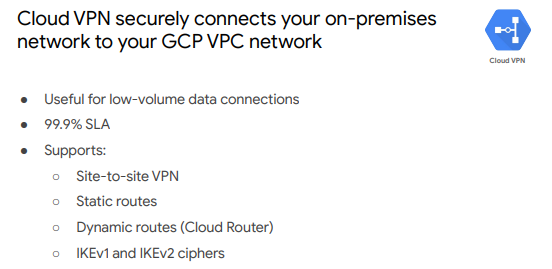
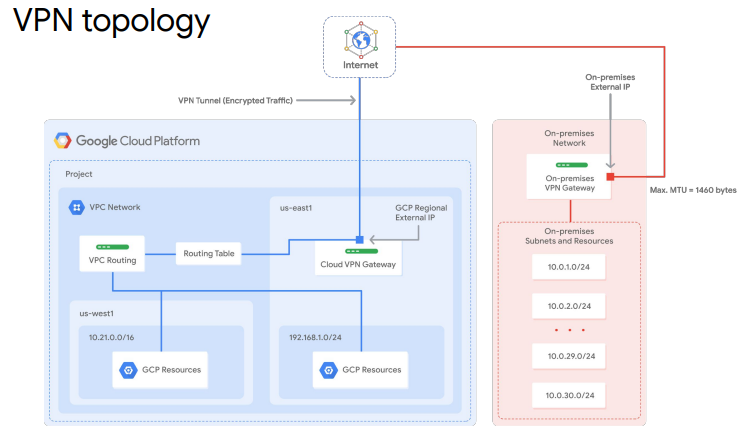
**Essential Google Cloud Infrastructure – Scaling and automation**

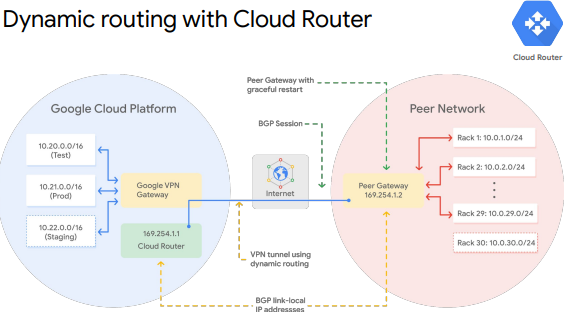
**Interconnecting networks**

Cloud VPN

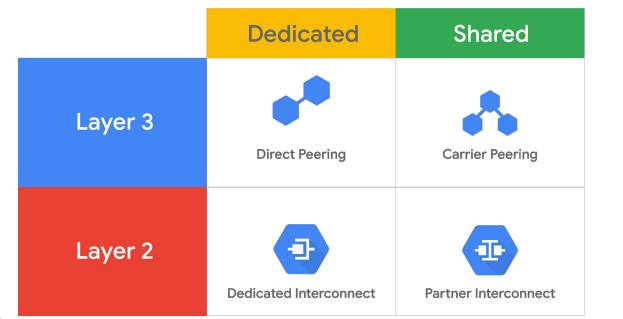


^ securely connects on-prem network to GCP VPC network through IPsec VPN. Traffic is encrypted through one gateway and decrypted by the other VPN gateway. Protecting data as it travels over the public internet. Useful for low volume data connections



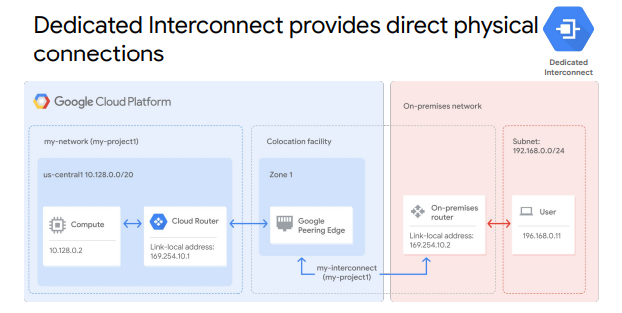


Cloud interconnect and peering



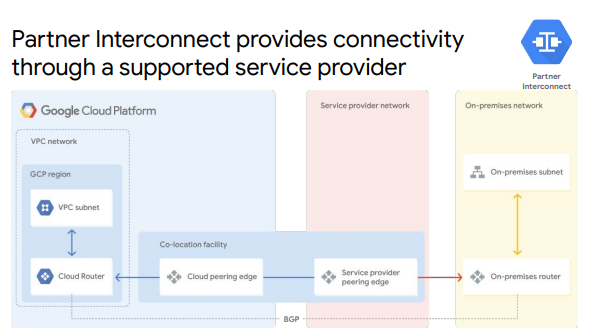
^ dedicated connections provide direct connection to Google’s network. Shared connections provide the connection through a partner. Layer 2 connections VLAN piped directly into GC environments. Layer 3 connections access to Google Workspace services, YouTube and GC APIs using public IP addresses

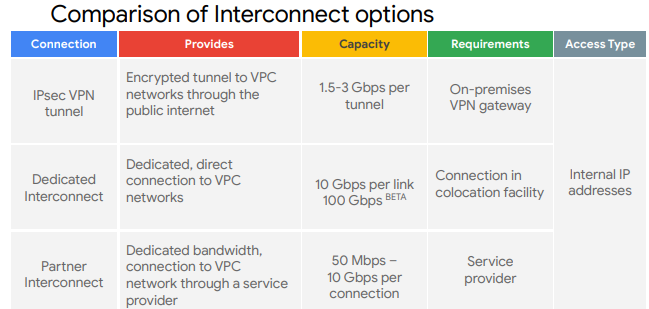
Cloud Interconnect



^ direct physical connection between on-prem and Google network. Enables transferring large amount of data between the networks. Requires your network to physically meet Google’s in supported colocation facility.

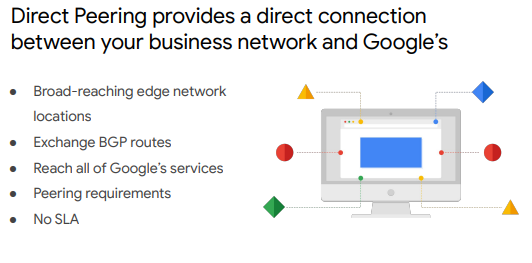
If you are too far away from a colocation facility, use partner connect

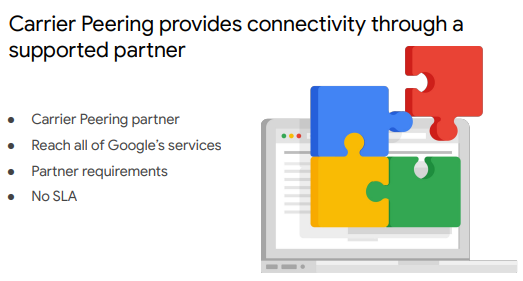




^IPsec = Cloud VPN

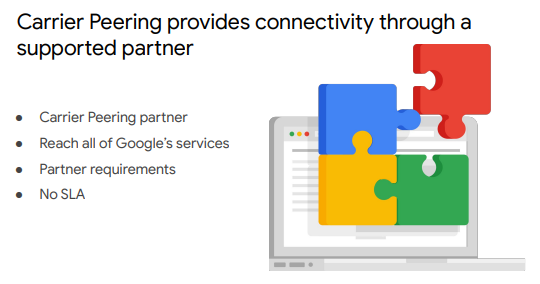
Peering

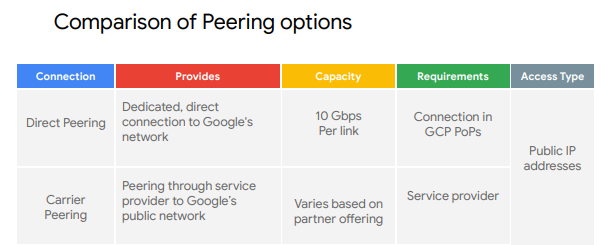




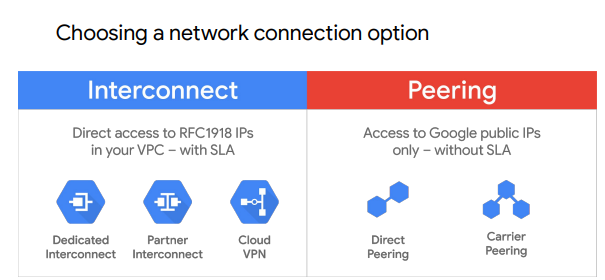
^ GCPs Edge Points of Presence (PoPs) are where Google network connects to other networks via peering.

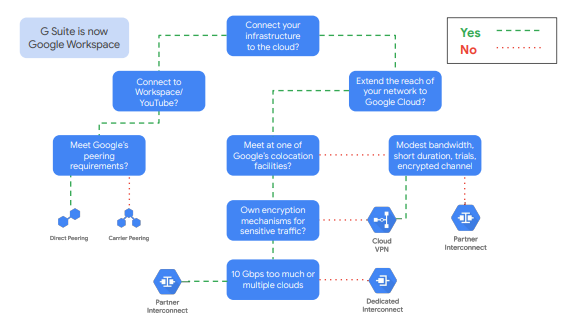
Similar to interconnect, if you are too far from a PoP you can peer via a partner





Choosing a connection

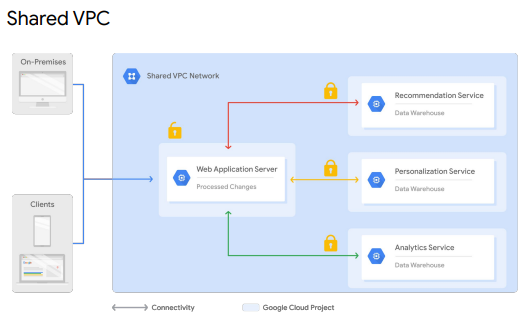




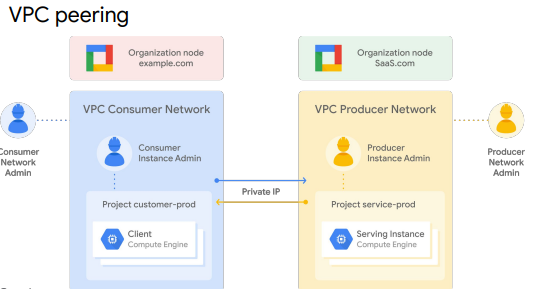
Shared VPC and VPC Peering

* Many organizations commonly deploy multiple, isolated projects with multiple VPC networks and subnets. Two configurations for sharing VPC networks across GCP projects

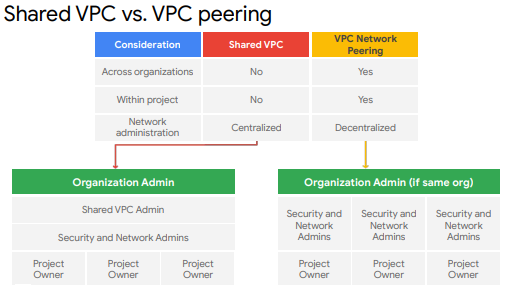
1. Shared VPC – share network across several projects in your GCP organisation
2. VPC Network Peering – configure private communication across projects in the same or different organisations



^ allows an organisation to connect resources from multiple projects to a common VPC network. Resources can then communicate securely using internal IP addresses from this network. When using shared VPC one project is designated as the host project and other projects are attached to it



^ allows connectivity across VPC networks regardless of if they belong to the same project or organisation (depending on the firewall rules that allow or deny traffic between networks). In order for it to be established, both resources most peer the network to the corresponding network. Once it is done on both sides the VPC peering becomes active and routes are exchanged. The resources can then communicate privately using internal IP addresses. VPC peering is decentralised (or distributed) because each VPC network remains under control of separate admin groups and maintains their own firewall and routing tables



**Load Balancing and Autoscaling**