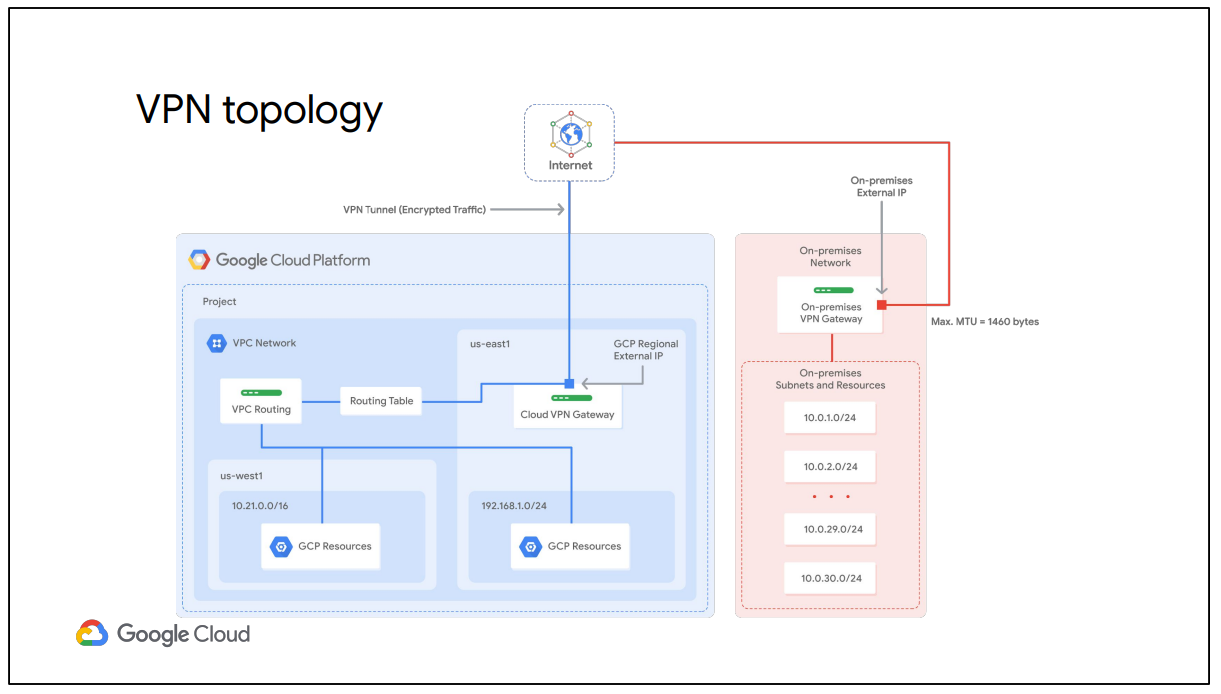
**Scaling and Automation**

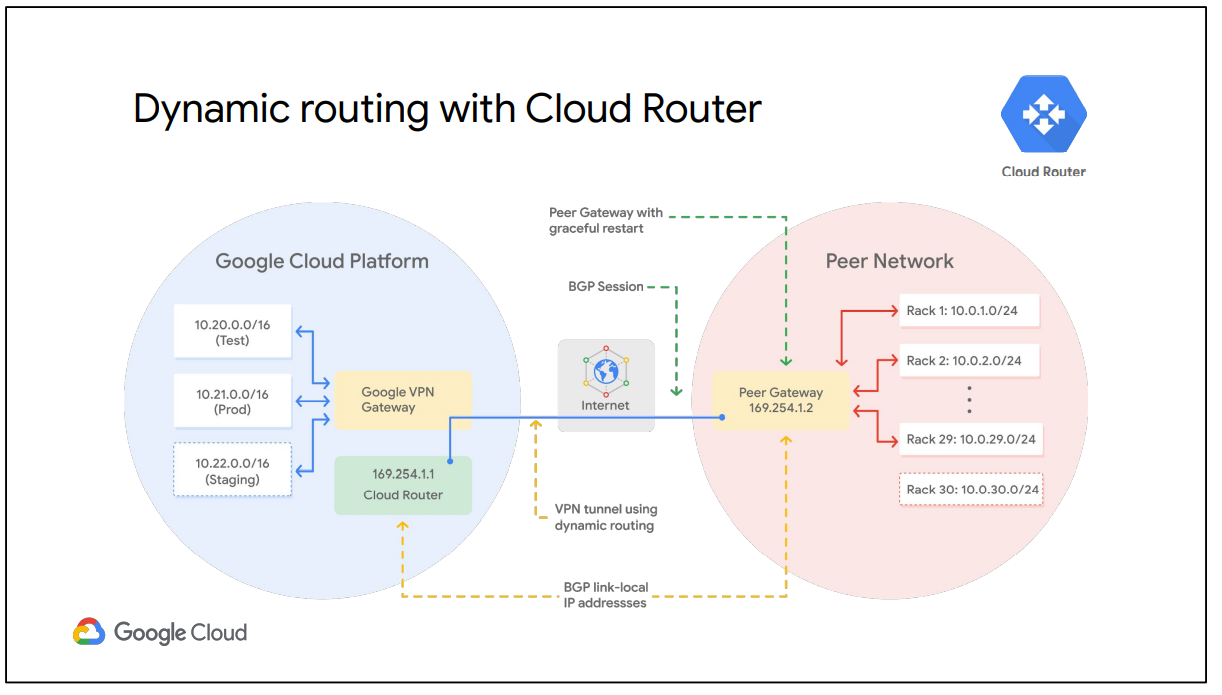
Cloud VPN securely connects your on premises network to your GCP VPC network.

* Useful for low volume data connections.
* 99.9% SLA
* Supports :
  + Site to Site VPN
  + Static routes
  + Dynamic Routes (Cloud Router)
  + IKEv1 and IKEv2 ciphers

Cloud VPN securely connects your on-premises network to your GCP VPC network through an IPsec VPN tunnel. Traffic traveling between the two networks is encrypted by one VPN gateway, then decrypted by the other VPN gateway. This protects your data as it travels over the public internet, and that’s why Cloud VPN is useful for low-volume data connections.



**Cloud Router :**

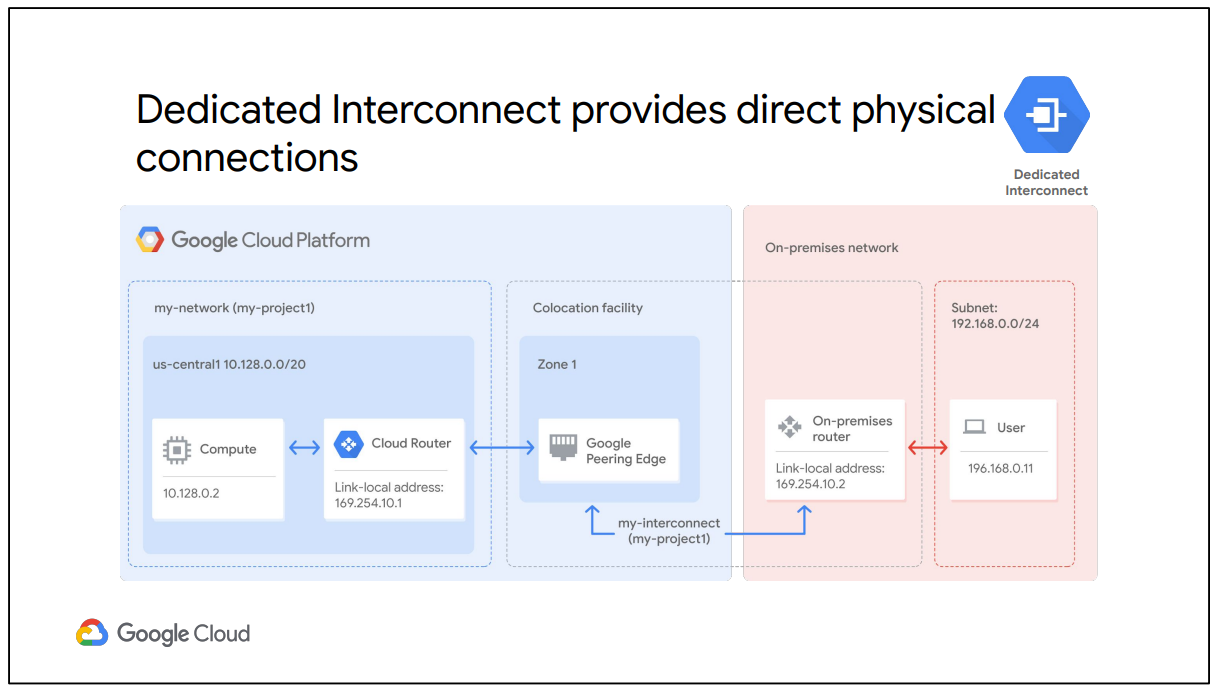


Cloud VPN supports both static and dynamic routes. In order to use dynamic routes, you need to configure Cloud Routers. Cloud Router can manage routes for a Cloud VPN tunnel using Border Gateway Protocol, or BGP. This routing method allows for routes to be updated and exchanged without changing the tunnel configuration.

how would you add a new “Staging” subnet in the GCP network and a new on-premises 10.0.30.0/24 subnet to handle growing traffic in your data center?

To automatically propagate network configuration changes, the VPN tunnel uses Cloud Router to establish a BGP session between the VPC and the on-premises VPN gateway, which must support BGP. The new subnets are then seamlessly advertised between networks. This means that instances in the new subnets can start sending and receiving traffic immediately.

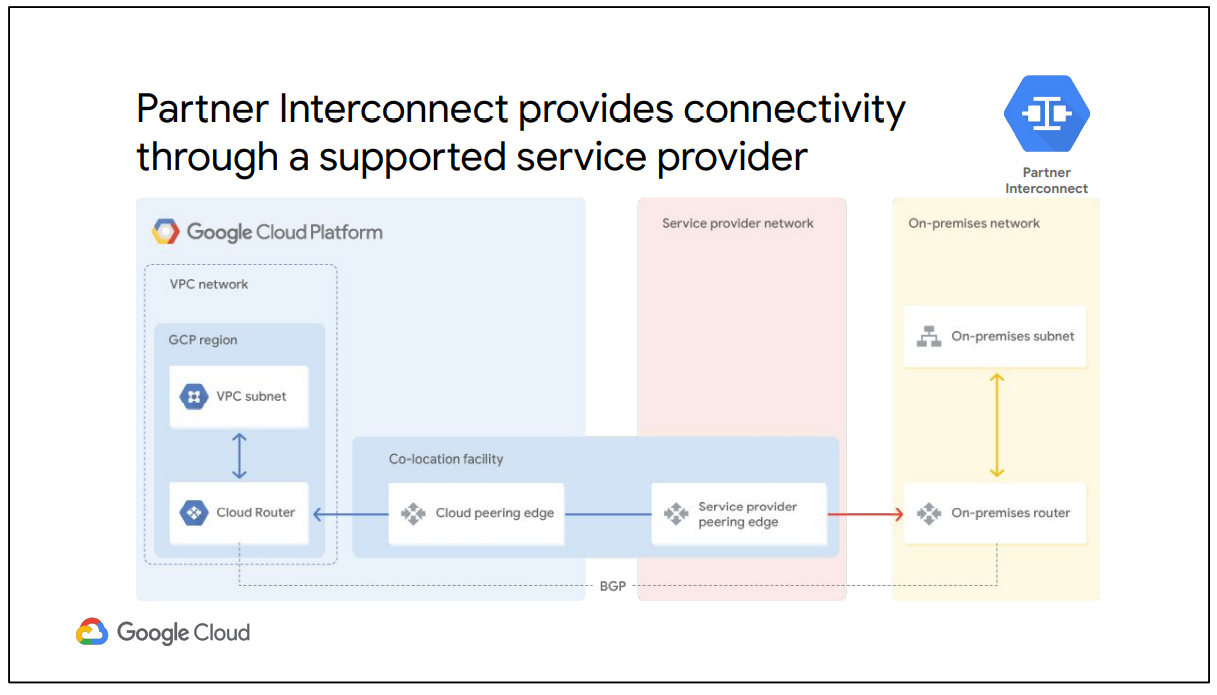
**Dedicated Interconnect :**



Dedicated Interconnect provides direct physical connections between your on-premises network and Google’s network.

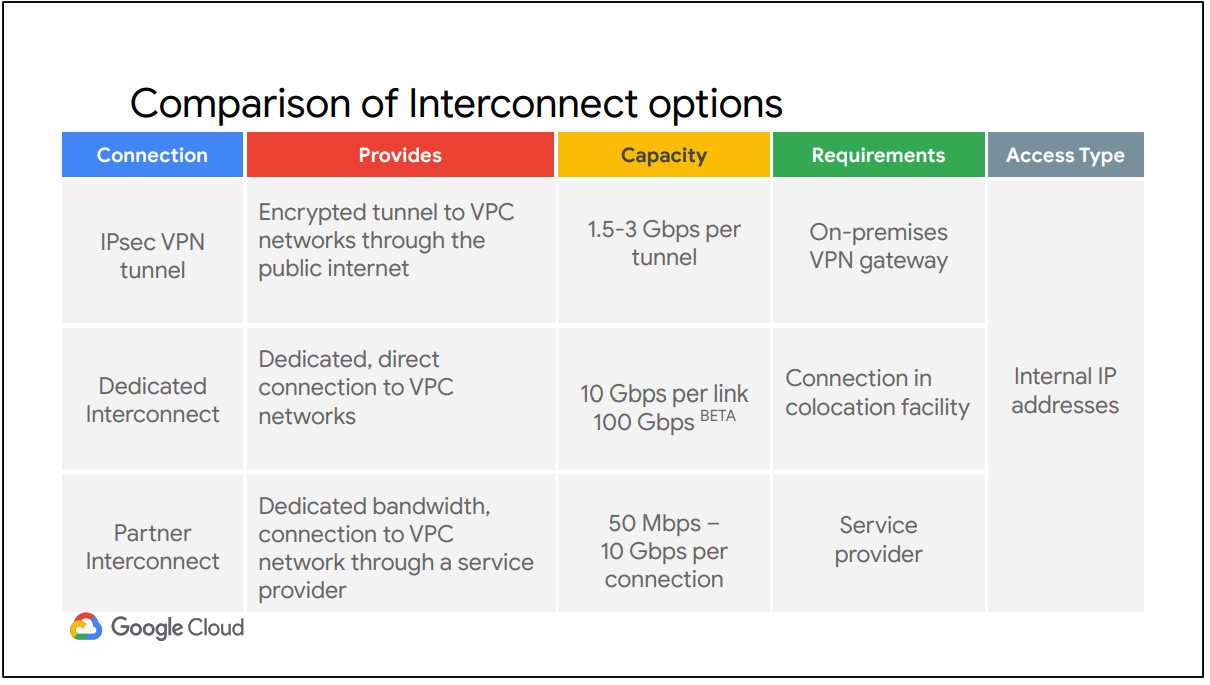
In order to use Dedicated Interconnect, you need to provision a cross connect between the Google network and your own router in a common colocation facility, as shown in this diagram. To exchange routes between the networks, you configure a BGP session over the interconnect between the Cloud Router and the on-premises router. This will allow user traffic from the on-premises network to reach GCP resources on the VPC network, and vice versa.

**Partner Interconnect :**

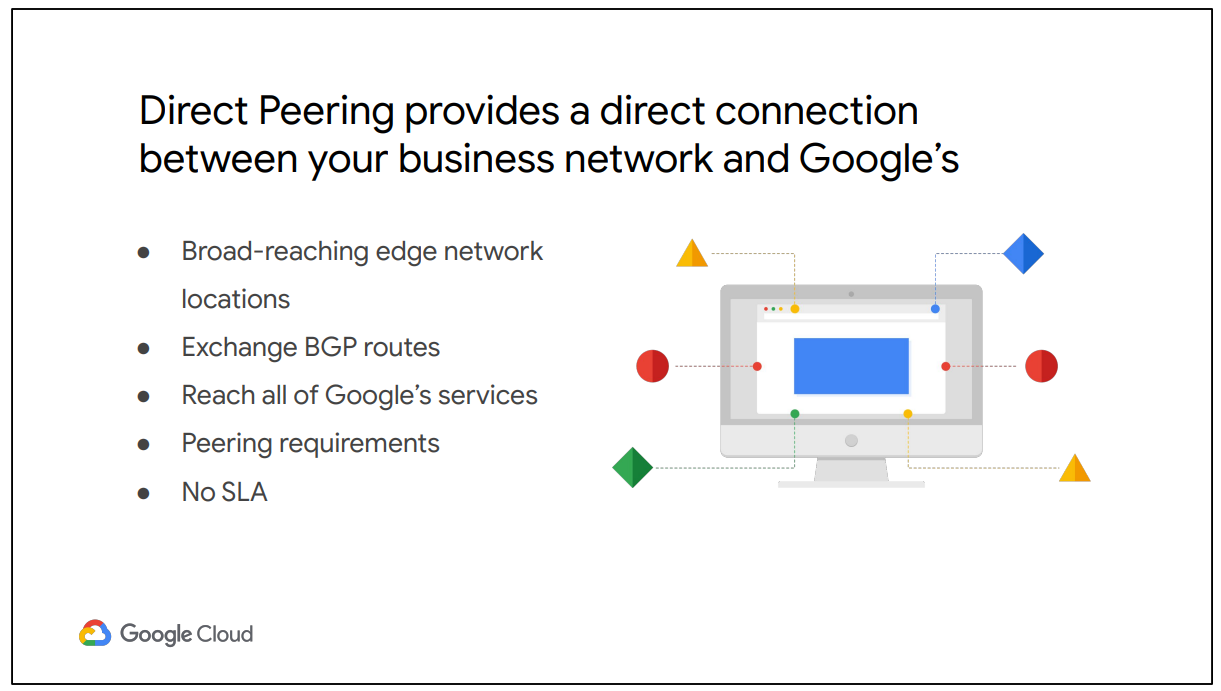


Partner Interconnect provides connectivity between your on-premises network and your VPC network through a supported service provider. This is useful if your data center is in a physical location that cannot reach a Dedicated Interconnect colocation facility or if your data needs don't warrant a Dedicated Interconnect.

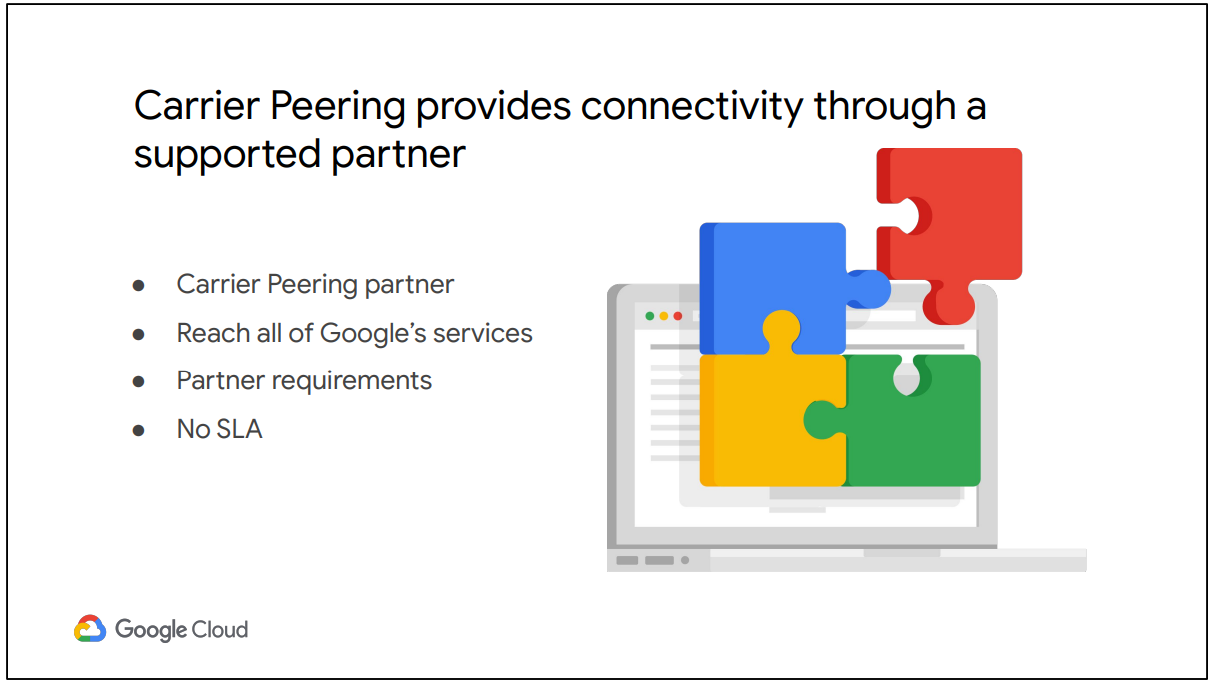
These service providers have existing physical connections to Google's network that they make available for their customers to use. After you establish connectivity with a service provider, you can request a Partner Interconnect connection from your service provider. Then, you establish a BGP session between your Cloud Router and on-premises router to start passing traffic between your networks via the service provider's network.

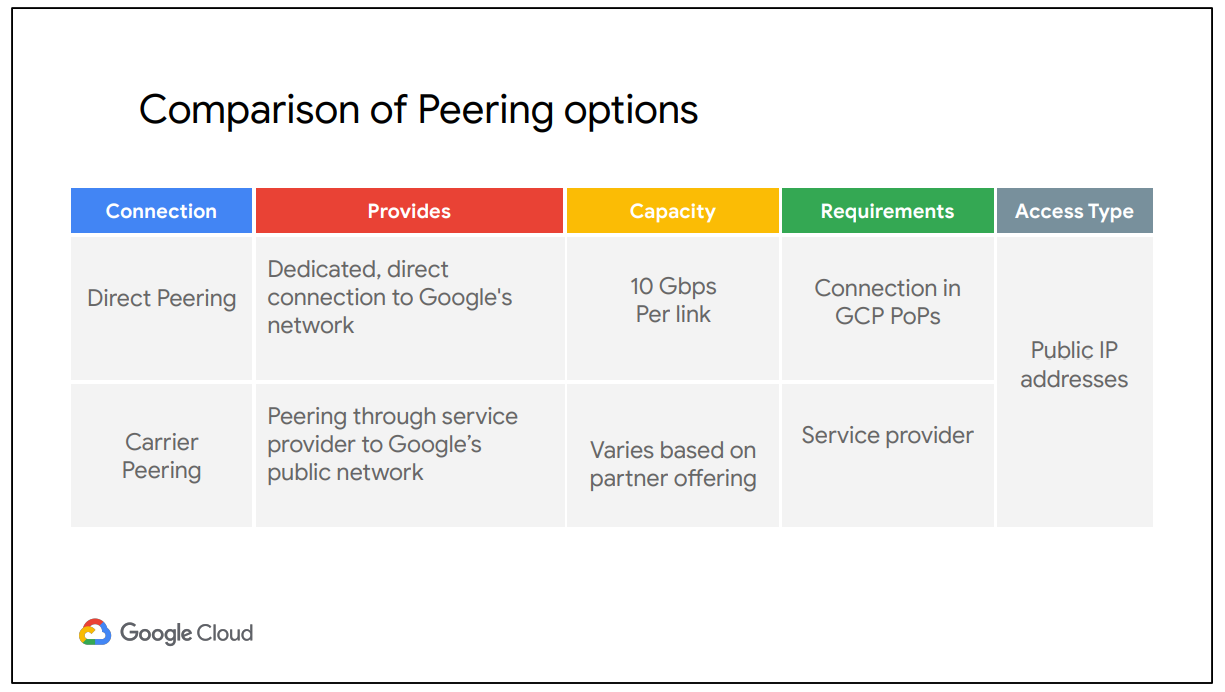


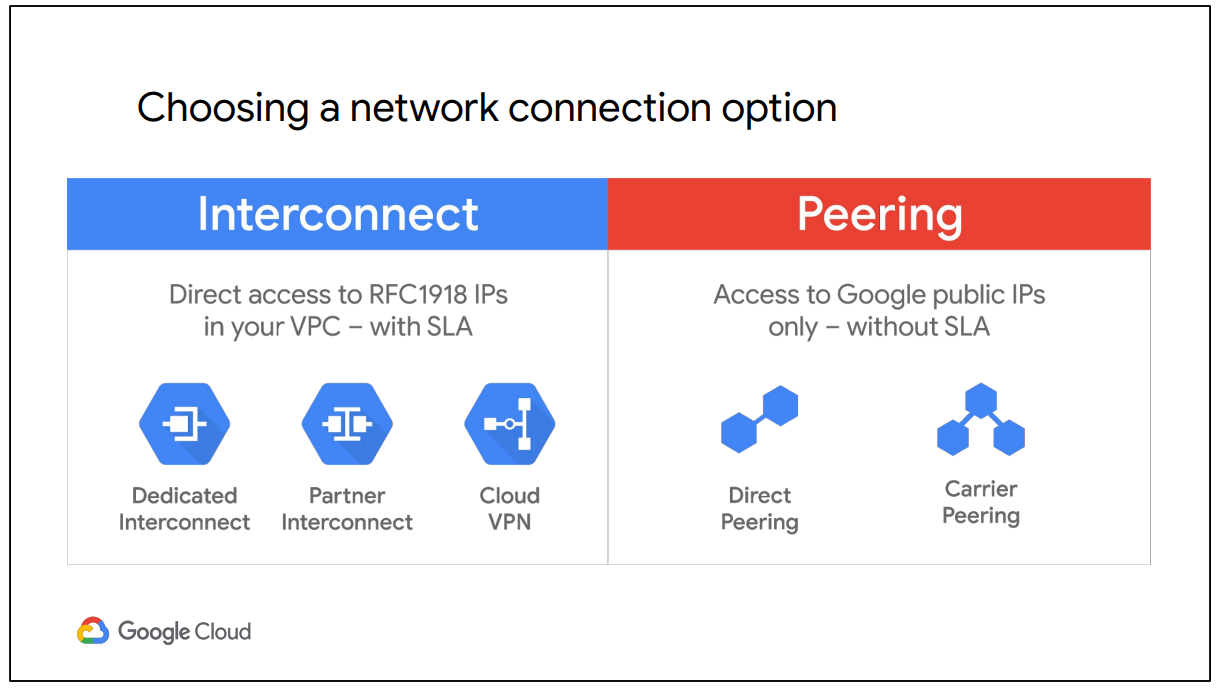
**Direct Peering :**



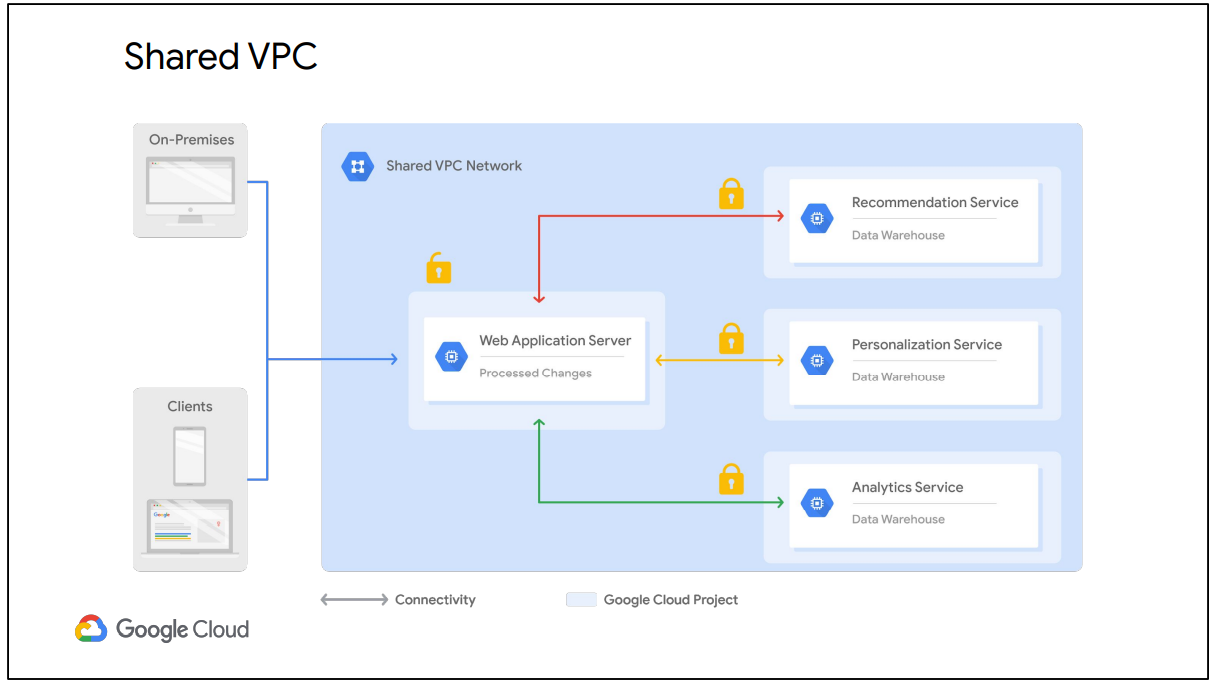
**Carrier Peering**







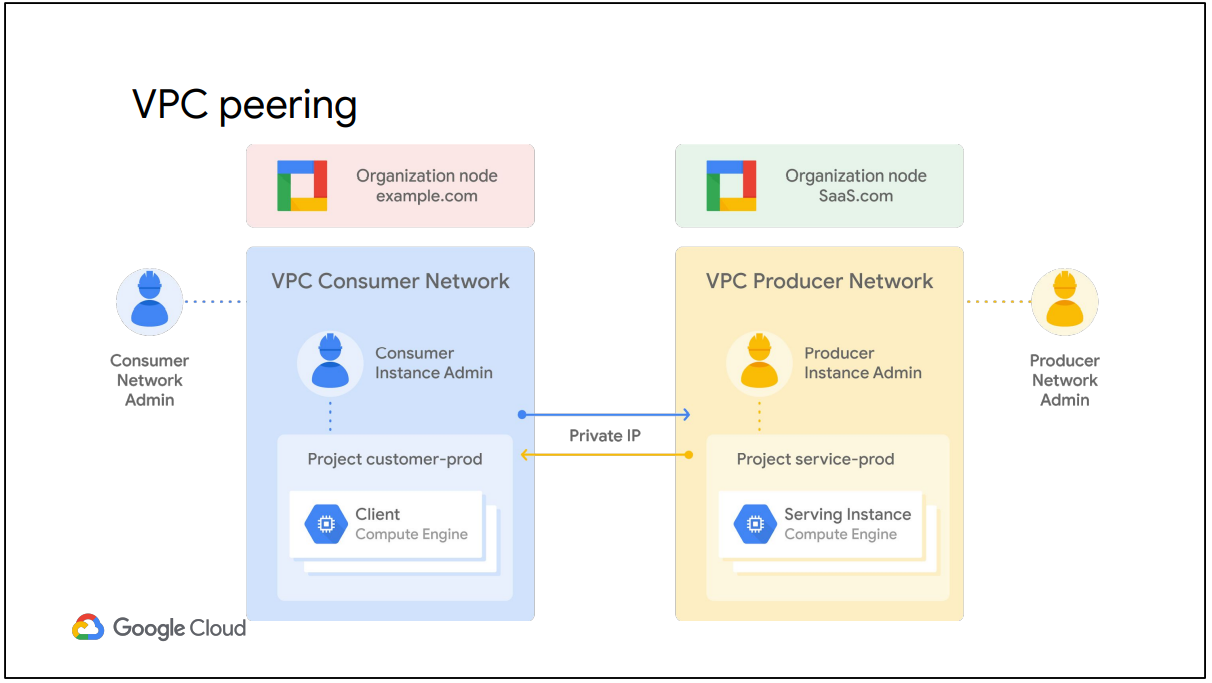
**Shared VPC :**



Shared VPC allows an organization to connect resources from multiple projects to a common VPC network. This allows the resources to communicate with each other securely and efficiently using internal IPs from that network.

For example, in this diagram there is one network that belongs to the Web Application Server’s project. This network is shared with three other projects, namely the Recommendation Service, the Personalization Service, and the Analytics Service. Each of those service projects has instances that are in the same network as the Web Application Server and allow for private communication to that server, using internal IP addresses. The Web Application Server communicates with clients and on-premises using the server’s external IP address. The backend services, in contrast, cannot be reached externally because they only communicate using internal IP addresses.

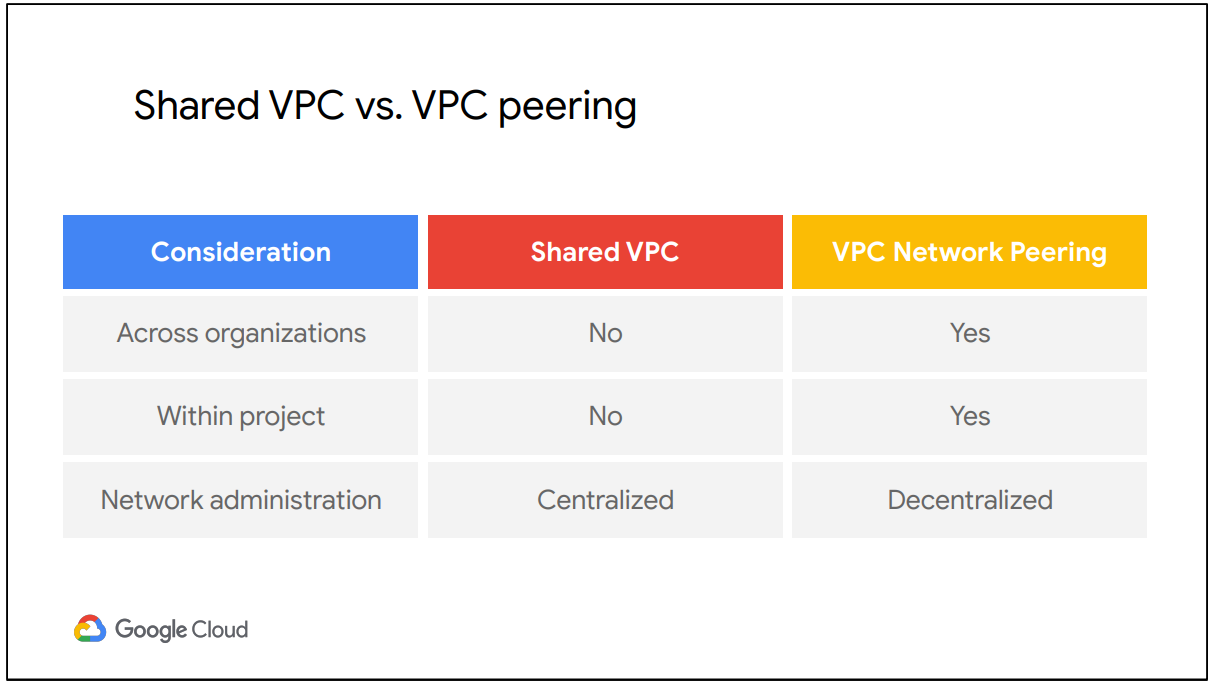
**VPC Peering :**



VPC Network Peering, in contrast, allows private RFC 1918 connectivity across two VPC networks, regardless of whether they belong to the same project or the same organization. Now, remember that each VPC network will have firewall rules that define what traffic is allowed or denied between the networks.

For example, in this diagram there are two organizations that represent a consumer and a producer, respectively. Each organization has its own organization node, VPC network, VM instances, Network Admin, and Instance Admin. In order for VPC Network Peering to be established successfully, the Producer Network Admin needs to peer the Producer Network with the Consumer Network, and the Consumer Network Admin needs to peer the Consumer Network with the Producer Network. When both peering connections are created, the VPC Network Peering session becomes Active and routes are exchanged. This allows the virtual machine instances to communicate privately using their internal IP addresses.

VPC Network Peering is a decentralized or distributed approach to multi-project networking, because each VPC network may remain under the control of separate administrator groups and maintains its own global firewall and routing tables. Historically, such projects would consider external IP addresses or VPNs to facilitate private communication between VPC networks. However, VPC Network Peering does not incur the network latency, security, and cost drawbacks that are present when using external IP addresses or VPNs.

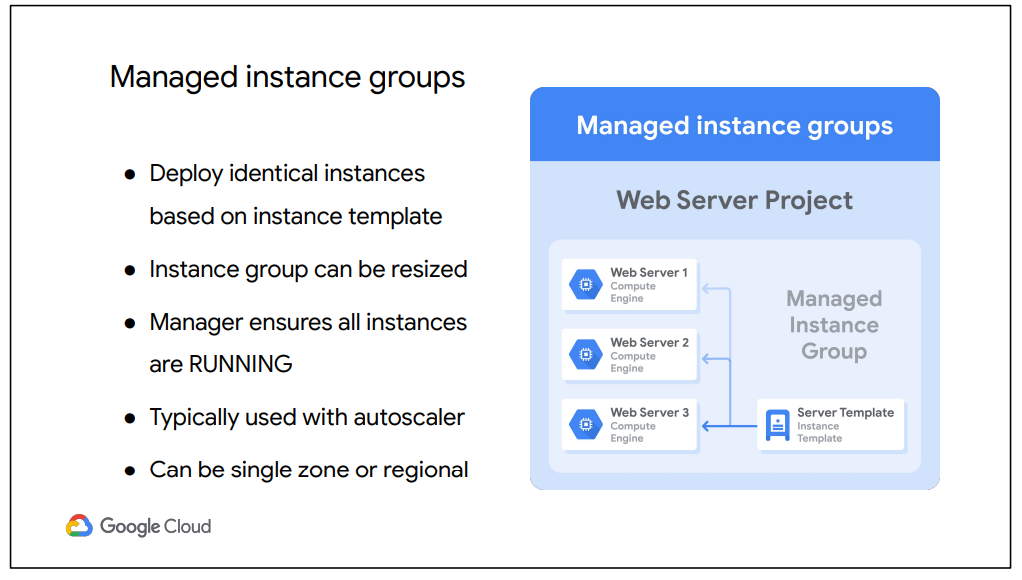


**2.**

**Cloud Load Balancers :**

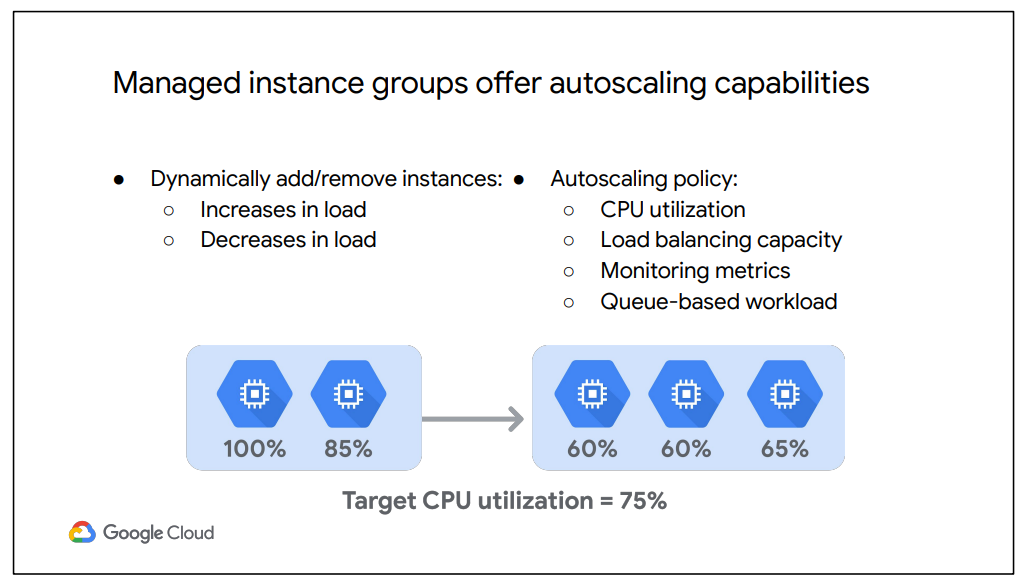
Cloud Load Balancing gives you the ability to distribute load-balanced compute resources in single or multiple regions to meet your high availability requirements, to put your resources behind a single anycast IP address, and to scale your resources up or down with intelligent autoscaling.

* **Managed Instance Group**

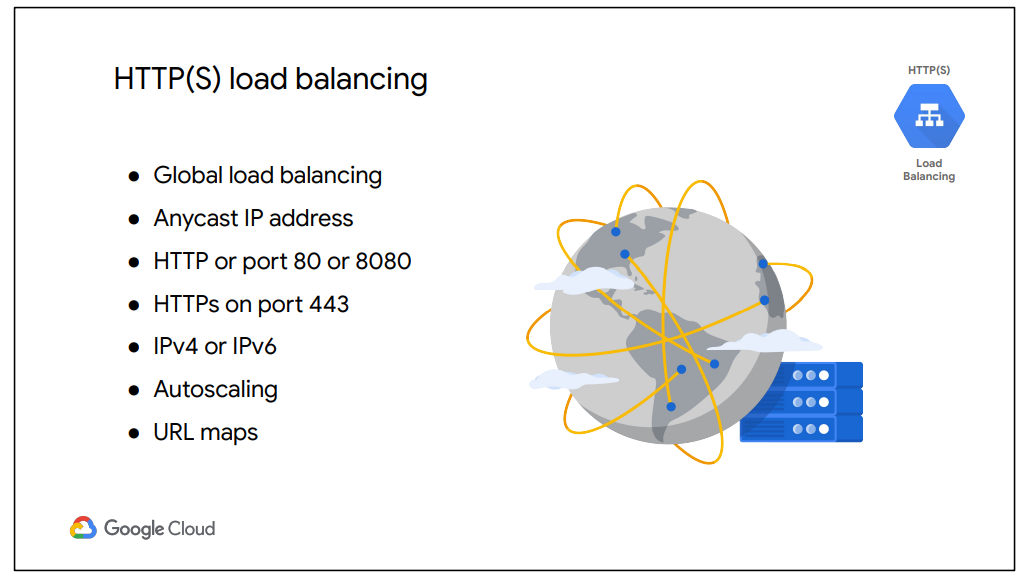


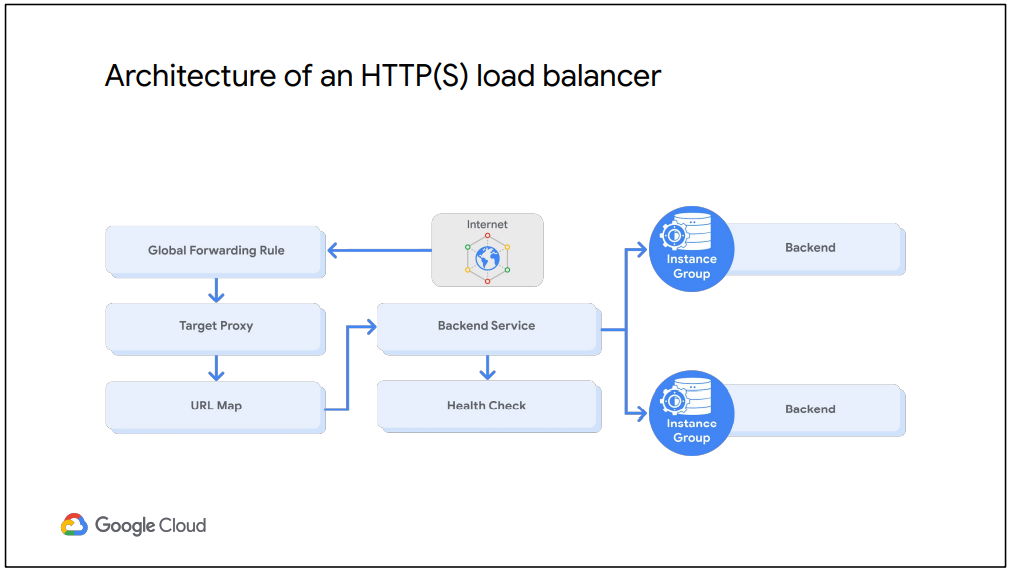
A managed instance group is a collection of identical VM instances that you control as a single entity, using an instance template. You can easily update all the instances in the group by specifying a new template in a rolling update. Also, when your applications require additional compute resources, managed instance groups can automatically scale the number of instances in the group.

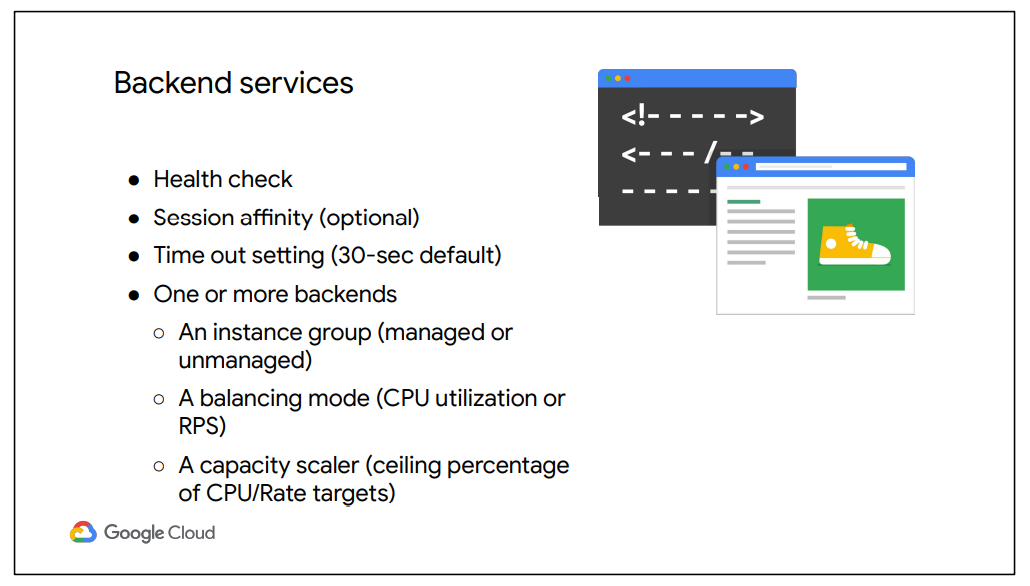
Managed instance groups can work with load balancing services to distribute network traffic to all of the instances in the group. If an instance in the group stops, crashes, or is deleted by an action other than the instance group’s commands, the managed instance group automatically recreates the instance so it can resume its processing tasks. The recreated instance uses the same name and the same instance template as the previous instance. Managed instance groups can automatically identify and recreate unhealthy instances in a group to ensure that all the instances are running optimally.



**HTTPS Load Balancer :**





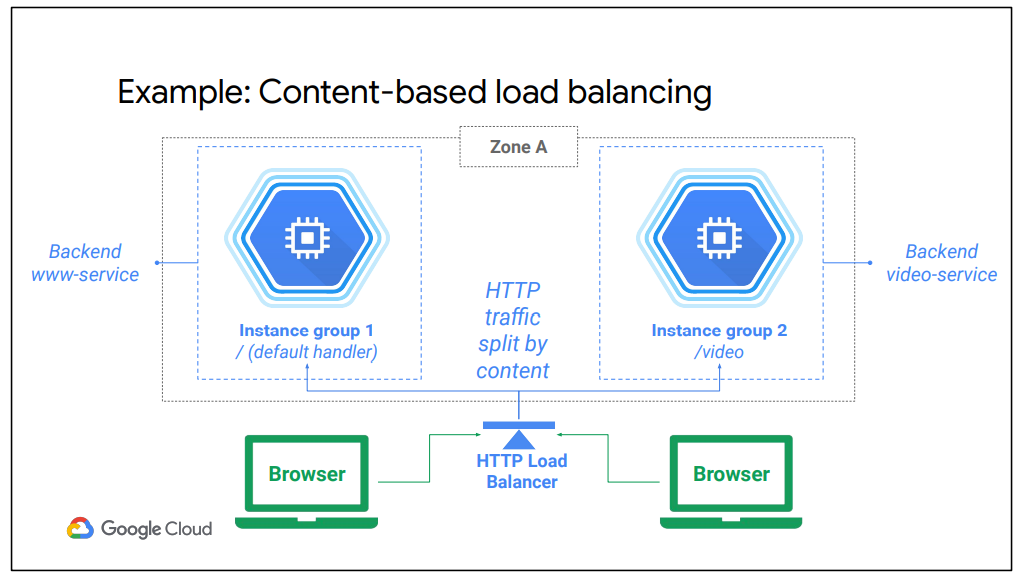


**Working :**

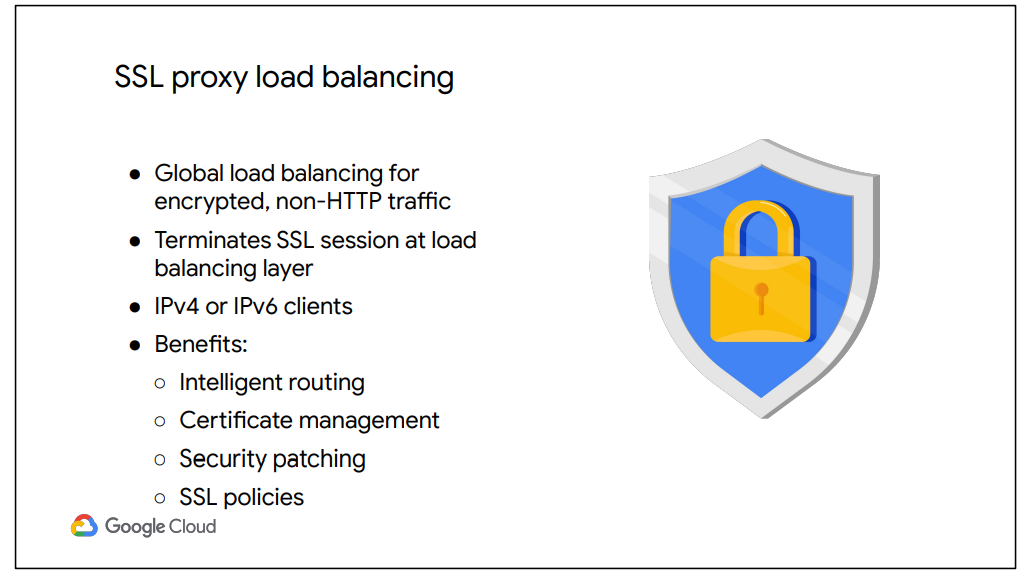
First, the global forwarding rule directs incoming requests to the target HTTP proxy. The proxy checks the URL map to determine the appropriate backend service for the request. In this case, we are serving a guestbook application with only one backend service.

The backend service has two backends: one in us-central1-a and one in europe-west1-d. Each of those backends consists of a managed instance group. Now, when a user request comes in, the load balancing service determines the approximate origin of the request from the source IP address. The load balancing service also knows the locations of the instances owned by the backend service, their overall capacity, and their overall current usage. Therefore, if the instances closest to the user have available capacity, the request is forwarded to that closest set of instances.

If there are no healthy instances with available capacity in a given region, the load balancer instead sends the request to the next closest region with available capacity. Therefore, traffic from the EMEA user could be forwarded to the us-central1-a backend if the europe-west1-d backend does not have capacity or has no healthy instances as determined by the health checker. This is referred to as cross-region load balancing.



To use HTTPS, you must create at least one SSL certificate that can be used by the target proxy for the load balancer. You can configure the target proxy with up to ten SSL certificates. For each SSL certificate, you first create an SSL certificate resource, which contains the SSL certificate information. SSL certificate resources are used only with load balancing proxies such as a target HTTPS proxy or target SSL proxy.



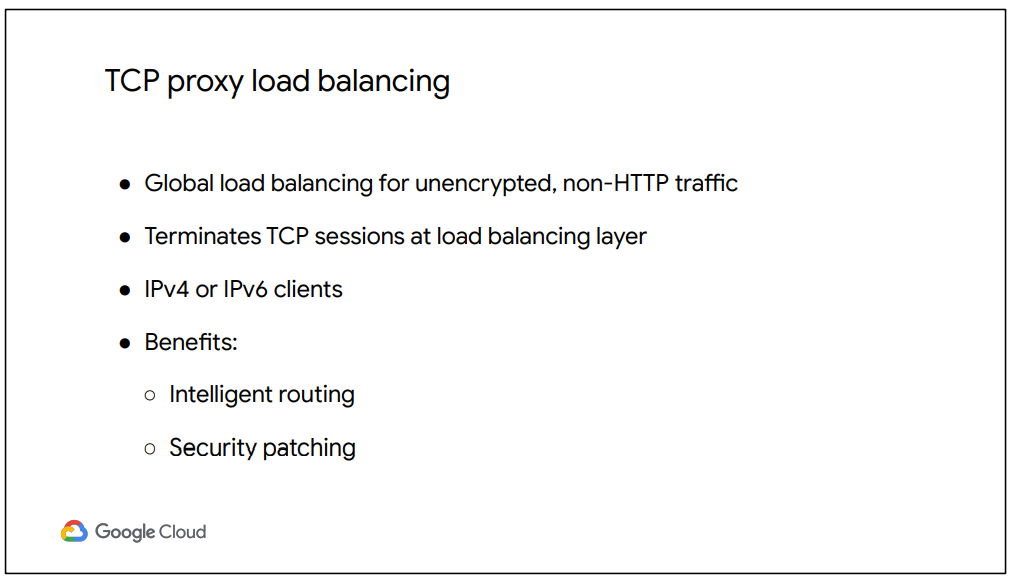
SSL proxy is a global load balancing service for encrypted, non-HTTP traffic. This load balancer terminates user SSL connections at the load balancing layer, then balances the connections across your instances using the SSL or TCP protocols. These instances can be in multiple regions, and the load balancer automatically directs traffic to the closest region that has capacity.

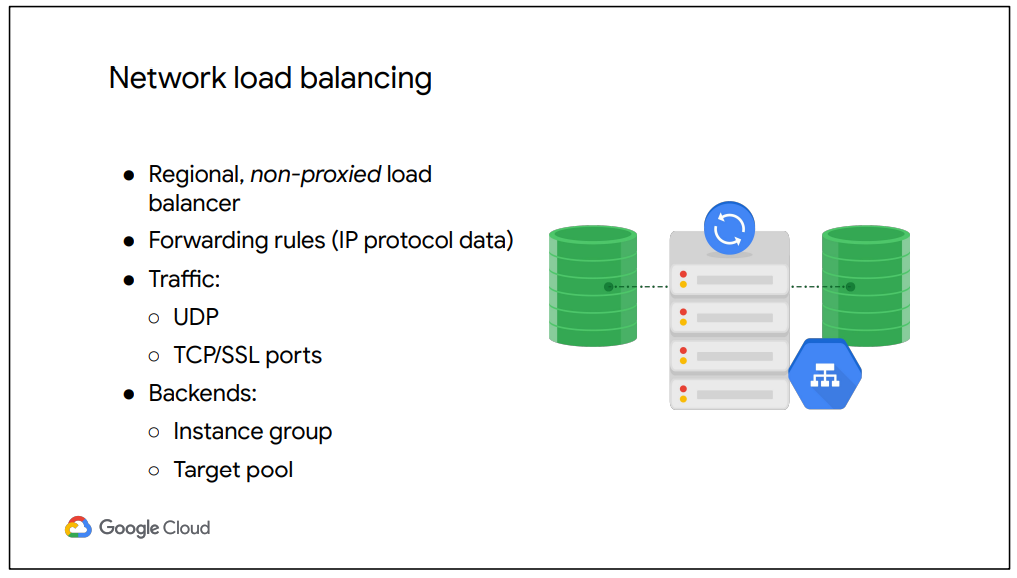
SSL proxy load balancing supports both IPv4 and IPv6 addresses for client traffic and provides Intelligent routing, Certificate management, Security patching and SSL policies.

● Intelligent routing means that this load balances can route requests to backend locations where there is capacity.

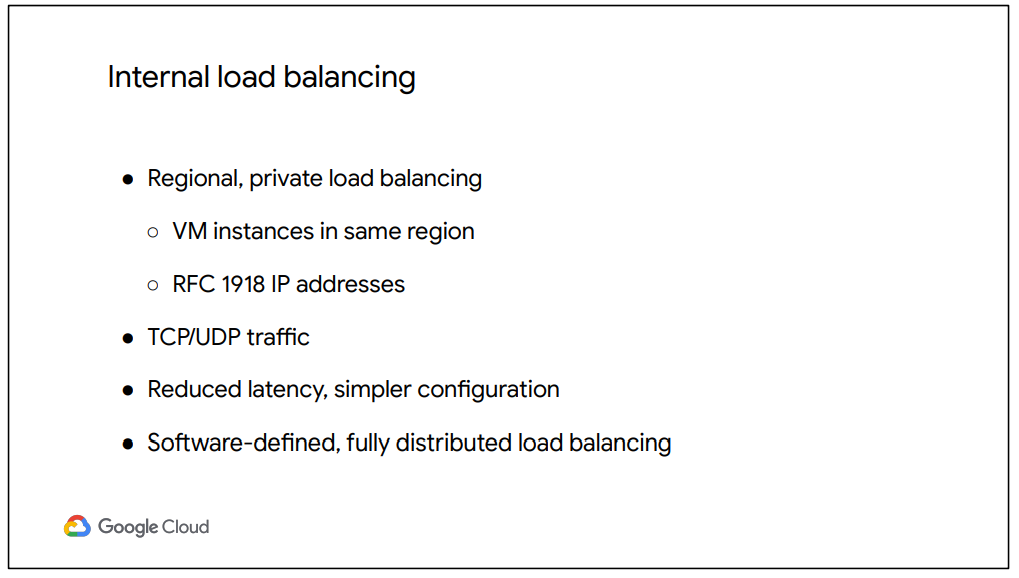
● From a certificate management perspective, you only need to update your customer-facing certificate in one place when you need to switch certificates. Also, you can reduce the management overhead for your virtual machine instances by using self-signed certificates on your instances.

● In addition, if vulnerabilities arise in the SSL or TCP stack, GCP will apply patches at the load balancer automatically in order to keep your instances safe.



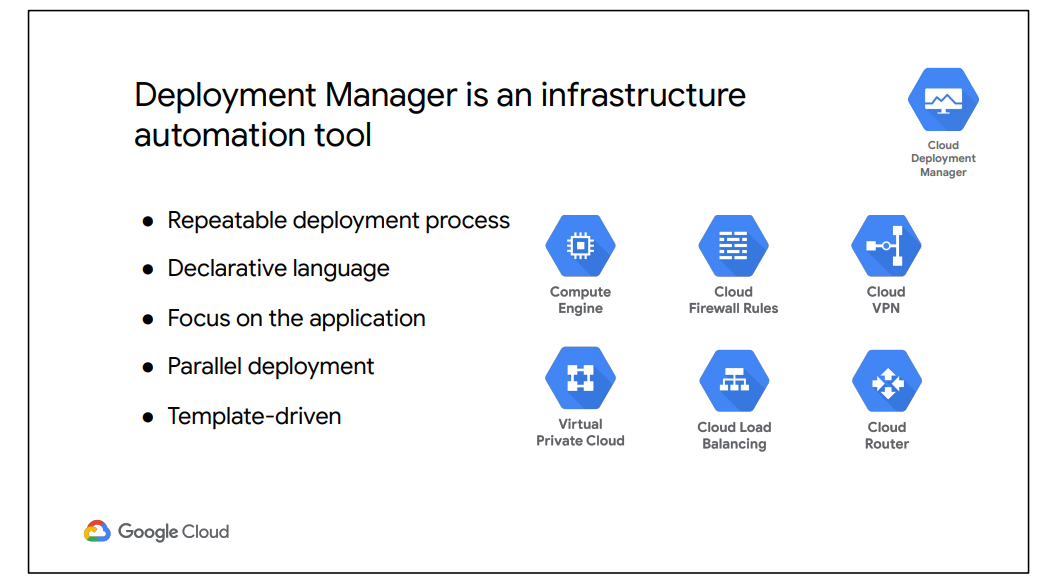


Network load balancing is a regional, non-proxied load balancing service. In other words, all traffic is passed through the load balancer, instead of being proxied, and traffic can only be balanced between VM instances that are in the same region, unlike a global load balancer.



Internal load balancing is a regional, private load balancing service for TCP- and UDP-based traffic. In other words, this load balancer enables you to run and scale your services behind a private load balancing IP address This means that it is only accessible through the internal IP addresses of virtual machine instances that are in the same region.

**3.**



Deployment Manager is an infrastructure deployment service that automates the creation and management of GCP resources for you. You just specify all the resources needed for your application in a declarative format and deploy your configuration. This deployment can be repeated over and over with consistent results, and you can delete a whole deployment with one command or click. The benefit of a declarative approach is that it allows you to specify what the configuration should be and let the system figure out the steps to take.

Instead of deploying each resource separately, you specify the set of resources which compose the application or service, allowing you to focus on the application. Unlike Cloud Shell, Deployment Manager will deploy resources in parallel. You can even abstract parts of your configuration into individual building blocks or templates that can be used for other configurations.

**4.**

