VPC - virtual private cloud - private cloud , global , VPC network associated with them .

CLOUD ROUTER - support dynamic routing , connect gcp to non gcp network .

VPN - virtual private network - secure connection , ipsec

VPC peering - share resources between private clouds . communication links between vpc .

Share VPC - share VPC across projects , centrally managed .

CLoud interconnect - link GCP to on prem . by direct or third party carrier connection .

Firewall - control traffic flow in network and across network

Allow icmp

Allow default - tcp udp icmp across subnet

Allow rdp - access to remote desktop

Allow ssh - for linux

Routes - define the path that network traffic takes from vm to another resource .

VPC can be linked together - VPC network peering

Shared vpc - should be created in same organization

Create VPC :

Subnets can be auto , custom .

Private google access enables subnet to access google service using internal ip without need of external ip .

Flow logs - generate logs .

VPN :link on prem and gcp .

Hybrid connectivity > vpn > classic vpn / high availability vpn .

First we create a gateway . Cloud VPN gateways connect to a peer VPN gateway,

which could be another GCP cloud VPN gateway, a gateway on another cloud provider, or an on-premises VPN device.

Tunnel : tunnels are used to share traffic between networks. We also want our data to be securely encrypted, and that's why we need a tunnel. Tunnels implement IPsec,

also known as the IP security protocol. And that's used between the two VPN gateways.

Cloud router :

BGP session :

**Cloud and on prem network integration :**

VPN -

peering -

interconnect -

**IP address and CIDR :**

Ipv4 and IPv6 .

Ipv4 uses 4 octet notation

There are 2 parts in the ip address - routing prefix , device identifier .

CIDR - classless inter domain routing

For eg : 192.168.17.0/20 - 20 is cidr range for this ip .

**FIrewall rules :**

VPC network > Firewall > create rule >

Ingress / egress .

Allow / deny traffic .

**Load balancing :**

**Can be categorized based on :**

Global vs regional

External vs internal

Traffic type

Global lb : when workload are around globe and different regions , these are external lb , premium tier networking used

**There are 3 global lb :**

Http for http and https traffic

Tcp proxy for other tcp traffic

Ssl proxy for non https ssl/tls traffic

Regional lb : used when workload is within a region .

2 regional lb :

Internal tcp/udp lb for tcp udp traffic on private network in gcp

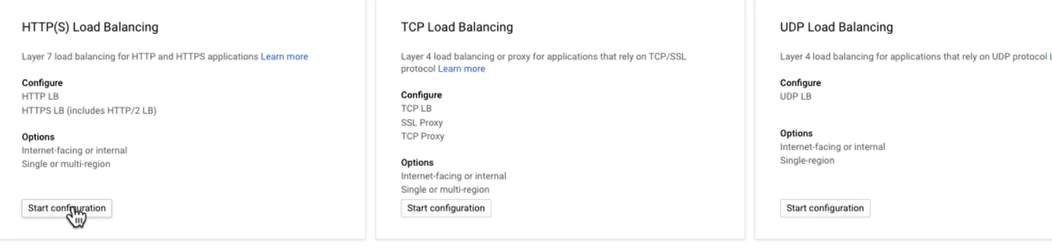
Network tcp udp for ssl or tcp traffic which is not supported by ssl proxy or tcp proxy

**Setting up lb :**

For lb we need an instance group .

Compute engine > instance group > Managed / unmanaged > Instance template .

Network services > load balancing > select type http/tcp/udp >



Http lb > network (ip)> backend service > backend type (instance group) > health check for backend > Frontend service > protocol, subnet > finalize and create .

When you create a load balancer you are providing an end point for incoming traffic to go to a single location in this case would be the load balancer and then the workload, the traffic would be routed across to instances within the instance group.

**Cloud DNS :**

Network service > DNS > DNS zone > zone name , dns name ,

And example.com, of course, is a special reserved domain name that is literally used for examples when discussing DNS.

SOA record - start of authority record .

NS record - name server record .

We add a record to provide names for our dns ip .

VPC - global resource , subnets in multiple regions , resource can communicate with private ip , we share vpc within organization , we can peer vpc across multiple organizations .

VPN - link vpc and on prem network , implemented using ipsec protocol , data is encrypted , can be routed over internet with security bcz of encryption , 3 gbps throughput

CLoud interconnect - connect gcp network from on prem dc ,

1) Direct connection between gcp and on prem - throughput 1– to 100 gbps

2) PArtnet connection - 50mbps to 10gbps

Peering - lower level network connection , linking network , traffic routed using bgp ,

Deployment manager : The Deployment Manager is a service that allows developers to create prepackaged applications that can be easily installed and run in GCP.

Deployment manager > deployment > We can deploy preconfigured applications .

Tunnels are specified when creating a VPN and the process includes configuring encryption parameters, such as the IKE version.

The HTTP(S) load balancer is a global load balancer for distributing HTTP and HTTPS traffic. Internal TCP/UDP and Network TCP/UDP are regional load balancers and can’t be used to route global traffic. SSL Proxy is a global load balancer but it is used for non-HTTPS SSL/TLS traffic.

SSH is the secure shell protocol and is used to log into remote Linux servers. FTP is a file transfer protocol. RDP is the Remote Desktop Protocol and used to log into Window servers. TLS is the transport layer security protocol, the successor to SSL.

The default configurations for VPCs create subnets in all regions. Routes are defined between subnets so subnets must be created first.

Default-allow-rdp is a firewall rule allowing connection to Windows servers using the remote desktop protocol (RDP). The ICMP firewall rule allows management traffic and the SSH rule allows for connections to Linux servers. The implied firewall rules cannot be deleted.

Both VPC Peering and Shared VPC are used to make resources in a VPC available to resources in another VPC but Shared VPCs only work with VPCs in the same organization. Cloud Interconnect and VPN are used to link on-premises networks to GCP.

Firewall rule logging can be enabled for each firewall rule. Each time the rule is applied to allow or deny traffic, a connection record is created. Connection records can be viewed in Cloud Logging.

Internal TCP/UDP Load Balancing is used for internal traffic, that is not from the internet. SSL Proxy, TCP Proxy, and Network TCP/UDP load balancing are used with external traffic.

URL maps specify direct requests to particular services. Routes are used to specify paths to destination IP addresses outside a subnet. Firewall rules control the flow of traffic on a network. Traces are used to understand performance characteristics of services in a distributed system.

Since the connected networks are in different organizations, they must use VPC Network Peering. VPC sharing is only available within a single organization. Firewall rule changes may be needed, but that is not sufficient. VPNs are used to connect GCP networks with on premises networks.