Published in Google Cloud - Community

Vishal Bulbule
Mar 7 · 8 min read · Listen

Google Cloud Networking fundamentals

Introduction

Hello All, I hope you are doing great. Networking is the backbone of any cloud infrastructure. Google Cloud Networking offers a range of products and services to build and manage highly available, scalable, and performant networks in the cloud.

Based on my experience most beginners who start their cloud journey need help understanding Google cloud networking concepts. So I thought to make it easier for beginners with my small contribution to this blog. I am writing this blog with major Networking concepts and providing hands-on demo link for youtube video as well for each section.

What will we cover in this article?

— Private IP (Internal IP) vs Public IP (External IP)
— VPC
— Subnet
— CIDR Range

— Firewalls
— NAT Gateway
— Identity-Aware Proxy(IAP)
— VPC Peering
— Shared VPC
— Hybrid Connectivity
— VPN and Interconnect
— Load Balancer

Private IP vs Public IP

Whenever we create a GCE VM instance in Google Cloud it will be created with 1 Public IP and 1 Private IP by default (Unless we opt to use only internal IP). Private or Internal IP addresses are used within a local network i.e VPC in case of Cloud and are not visible or accessible from the internet. Private IP addresses fall within one of three ranges:

- Class A: `10.0.0.0` to `10.255.255.255`
- Class B: `172.16.0.0` to `172.31.255.255`
- Class C: `192.168.0.0` to `192.168.255.255`

On the other hand, public IP addresses are assigned to a device by an internet service provider (ISP) and are used to identify a device on the internet. This is the IP address that is visible to the public and is used for communication between devices on different networks. Public IP addresses are unique and can be static (never changing) or dynamic (changes periodically).

To summarize, private IP addresses are used within VPC communication, while public IP addresses are used for communication over the internet.

VPC (Virtual Private Cloud)

In Google Cloud, VPC (Virtual Private Cloud) is a service that allows you to create and manage your own virtual network in the cloud. With VPC, you can create and control your own private IP space, subnets, and routing tables within Google Cloud. You can also create firewall rules to control incoming and outgoing traffic to and from your VPC.

In Google Cloud, there are two modes for creating a VPC (Virtual Private Cloud): auto mode and custom mode.

Auto mode VPC is the default mode, and it automatically creates subnets in each region for you. Custom mode VPC, on the other hand, allows you to have more control and flexibility over your network where you can choose the desired region and CIDR IP range while creating Subnet.

> *Subnet*

In Google Cloud, Subnets are used to segment a VPC into smaller networks for better organization and management of resources. Each subnet is associated with a specific region, and the IP address range is defined by a CIDR (Classless Inter-Domain Routing) notation. You need to have a subnet available in a particular region in order to create a GCE VM instance in that region.

> *CIDR*

Classless Inter-Domain Routing (CIDR) is a range of IP addresses a network uses. A CIDR address looks like a normal IP address, except that it ends with a slash followed by a number. The number after the slash represents the number of addresses in the range. Here’s an example CIDR IP address in IPv4: 192.0.2.0/24

192.0.2.0/28 — (32–28= 4) → 2^4 = 16 IP addresses

192.0.2.0/24 — (32–24= 8) → 2^8 = 256 IP addresses

There are multiple sites and utilities available online for CIDR/IP calculation. Ex. https://www.ipaddressguide.com/cidr

> *Firewalls*

In Google Cloud, VPC firewall rules let you allow or deny traffic to or from virtual machine (VM) instances in a VPC network based on port number, tag, or protocol. Priority for each rule can be specified to control the order in which they are applied.

Ingress Firewall rules are used to control incoming traffic either allowing or denying action. On other hand Egress Firewall rules are used to control Outgoing traffic either allowing or denying action.

Overall, firewalls in Google Cloud provide a flexible and scalable solution for controlling incoming and outgoing traffic to and from virtual machine instances, providing a secure networking environment.

Please find a video demo here on how to create VPC, Subnet,Firewalls in Google Cloud

> *Identity-Aware Proxy*

An identity-Aware proxy (IAP) is used to login into the GCE VM instance without public/external IP. Identity-Aware Proxy (IAP) TCP forwarding to enable administrative access to VM instances that do not have external IP addresses or do not permit direct access over the internet.

To enable IAP we need to -

1. Enable **Cloud Identity Aware Proxy** API
2. Assign r**oles/iap.tunnelResourceAccessor** role to the user
3. Create a firewall rule to allow ssh traffic from IP range **35.235.240.0/20** this is a fixed IP range provided by google.

Overall, IAP in Google Cloud provides a way to secure access to your applications and resources based on identity. It allows you to control access to your resources with ease, reducing the risk of unauthorized access and improving your organization's overall security posture.

Please find Video demo here on How to setup IAP in Google cloud.

> *Cloud NAT*

In Google Cloud, Cloud NAT (Network Address Translation) is a service that allows you to provide Internet connectivity to instances that have only private IP addresses, without exposing those addresses to the Internet. Cloud NAT is used to translate private IP addresses to a single public IP address, allowing instances to communicate with the Internet while maintaining a secure and private network.

When an instance sends traffic to the Internet, Cloud NAT translates the private IP address to the public IP address, allowing the traffic to flow to its destination.

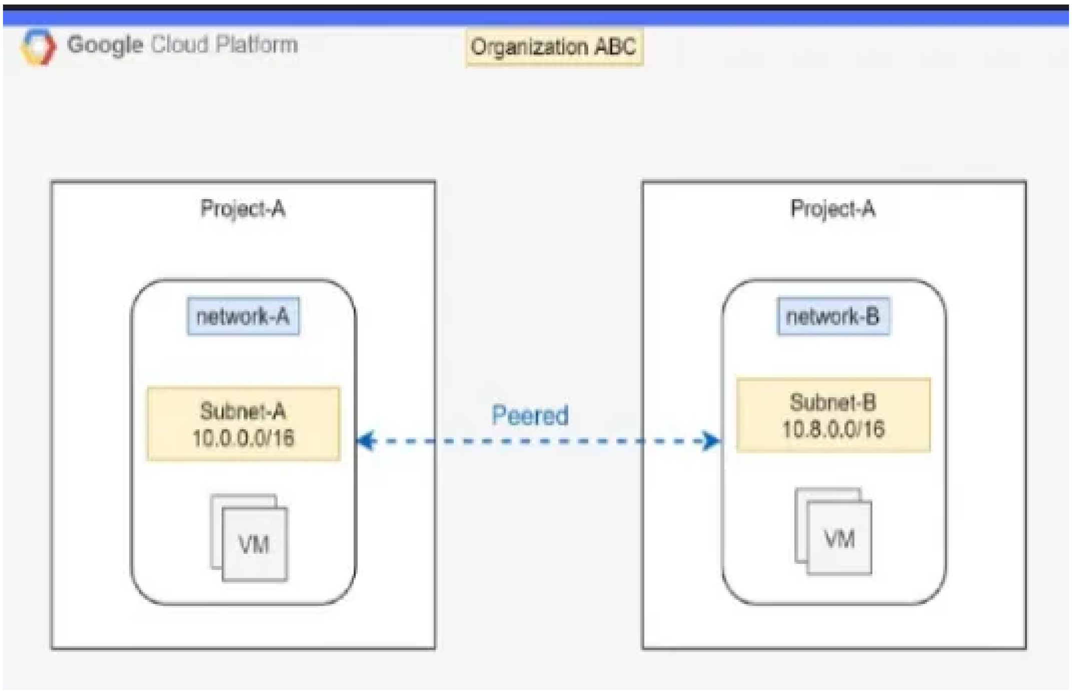
Overall, Cloud NAT in Google Cloud provides a way to provide instances with Internet connectivity while maintaining a secure and private network. It allows you to use private IP addresses for your instances, reducing the risk of exposure to the Internet and providing better security for your network.

Please find video demo here on how to create Cloud NAT

> *VPC Peering*

Google Cloud VPC Network Peering allows internal IP address connectivity across two Virtual Private Cloud (VPC) networks regardless of whether they belong to the same project or the same organization.

VPC Network Peering enables you to connect VPC networks so that workloads in different VPC networks can communicate internally. Traffic stays within Google's network and doesn't traverse the public internet.



VPC Network Peering gives you several advantages over using external IP addresses or VPNs to connect networks, including:

Network Latency: Connectivity that uses only internal addresses provides lower latency than connectivity that uses external addresses.

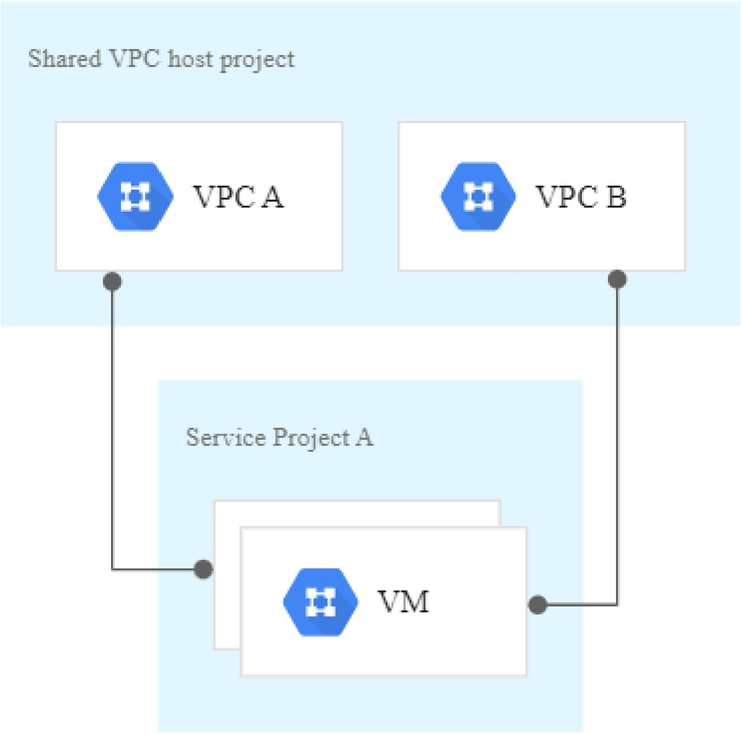
Network Security: Service owners do not need to have their services exposed to the public Internet and deal with its associated risks.

Network Cost: Google Cloud charges egress bandwidth pricing for networks using external IPs to communicate even if the traffic is within the same zone. If however, the networks have peered they can use internal IPs to communicate and save on those egress costs. Regular network pricing still applies to all traffic.

Please find video demo here on how to do VPC peering in Google Cloud.

Shared VPC

- Shared VPC allows an organization to connect resources from multiple projects to a common Virtual Private Cloud (VPC) network, so that they can communicate with each other securely and efficiently using internal IPs from that network.
- When you use Shared VPC, you designate a project as a host project and attach one or more other service projects to it. The VPC networks in the host project are called Shared VPC networks.
- Eligible resources from service projects can use subnets in the Shared VPC network.



Please find video demo here on how to create shared VPC

> *Hybrid network connectivity*

In Google Cloud, hybrid network connectivity is a service that allows you to connect your on-premises data center to your Google Cloud resources, creating a hybrid network that spans both environments. This allows you to leverage the benefits of cloud computing while still maintaining control over your on-premises resources.

Google Cloud offers several options for hybrid network connectivity, including:

1. Cloud VPN: Cloud VPN is a service that allows you to create secure, encrypted connections between your on-premises data center and your Google Cloud VPC networks. Cloud VPN uses the IPsec protocol to create a secure tunnel between your on-premises VPN gateway and the Cloud VPN gateway in Google Cloud.

2. Dedicated Interconnect: Dedicated Interconnect is a service that allows you to establish a direct physical connection between your on-premises data center and Google Cloud. Dedicated Interconnect provides a dedicated, high-bandwidth connection that is not shared with other customers, ensuring reliable and consistent network performance.

3. Partner Interconnect: Partner Interconnect is a service that allows you to connect to Google Cloud through a partner network, providing a private and secure connection to your Google Cloud resources. Partner Interconnect is ideal for customers who need to connect to Google Cloud from locations where Dedicated Interconnect is not available.

4. Cloud Router: Cloud Router is a service that allows you to dynamically exchange routes between your on-premises network and your Google Cloud VPC networks. Cloud Router enables you to create dynamic routing policies that can optimize traffic flows and ensure high availability.

> *Load Balancer*

In Google Cloud, Load Balancing is a service that enables you to distribute incoming network traffic across multiple instances of your application, improving performance, availability, and scalability.

Google Cloud offers several types of load balancers to suit different use cases and requirements.

1. HTTP(S) Load Balancer: This type of load balancer is designed for HTTP and HTTPS traffic and is ideal for web applications. It can distribute traffic to groups of backend instances running on Compute Engine, Google Kubernetes Engine, or Google Cloud Functions.

2. SSL Proxy Load Balancer: This type of load balancer is designed for SSL/TLS traffic and is ideal for non-HTTP(S) traffic, such as SMTP and MySQL. It can distribute traffic to groups of backend instances running on Compute Engine.

3. TCP/UDP Load Balancer: This type of load balancer is designed for TCP and UDP traffic and is ideal for non-HTTP(S) traffic. It can distribute traffic to groups of backend instances running on Compute Engine, Google Kubernetes Engine, or Google Cloud Functions.

4. Internal Load Balancer: This type of load balancer is designed to distribute traffic to instances within a VPC network. It can be used to balance traffic between instances in different regions or zones within a VPC network.

Conclusion

Overall, Google Cloud networking provides a powerful set of services and tools that can help you build a secure, high-performance network in the cloud. Whether you are a small startup or a large enterprise, Google Cloud networking has everything you need to build and manage your network infrastructure in the cloud.

Thank you for reading.

You can refer to my youtube channel for more interesting stuff about Google cloud and guidance on Google Cloud Certification.

TechTrapture

Managed By Vishal Bulbule Google Certified Professional Cloud Architect Google Certified Professional DevOps Engineer…

www.youtube.com