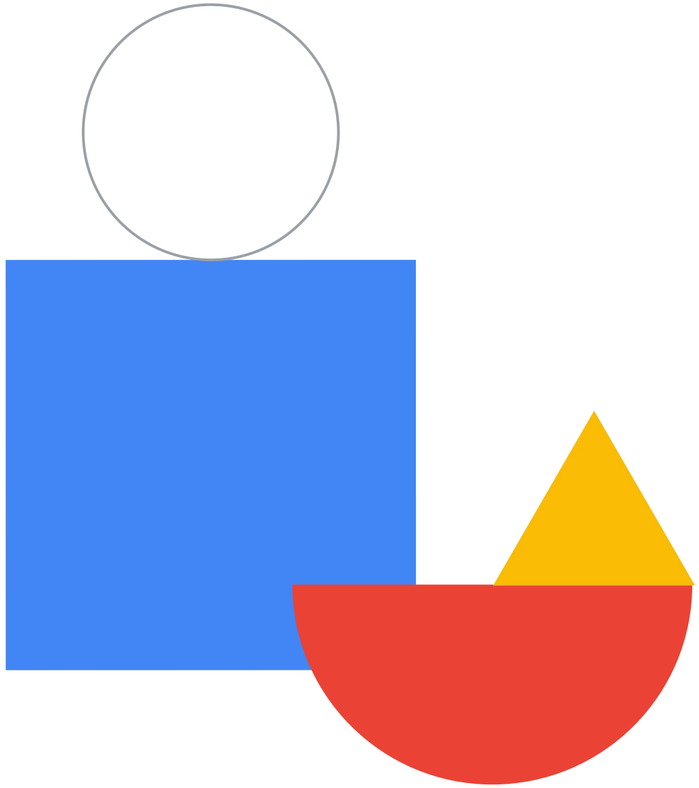
Google Cloud



Preparing for Your Professional Cloud Security Engineer Journey

Module 2 : Configuring Network Security

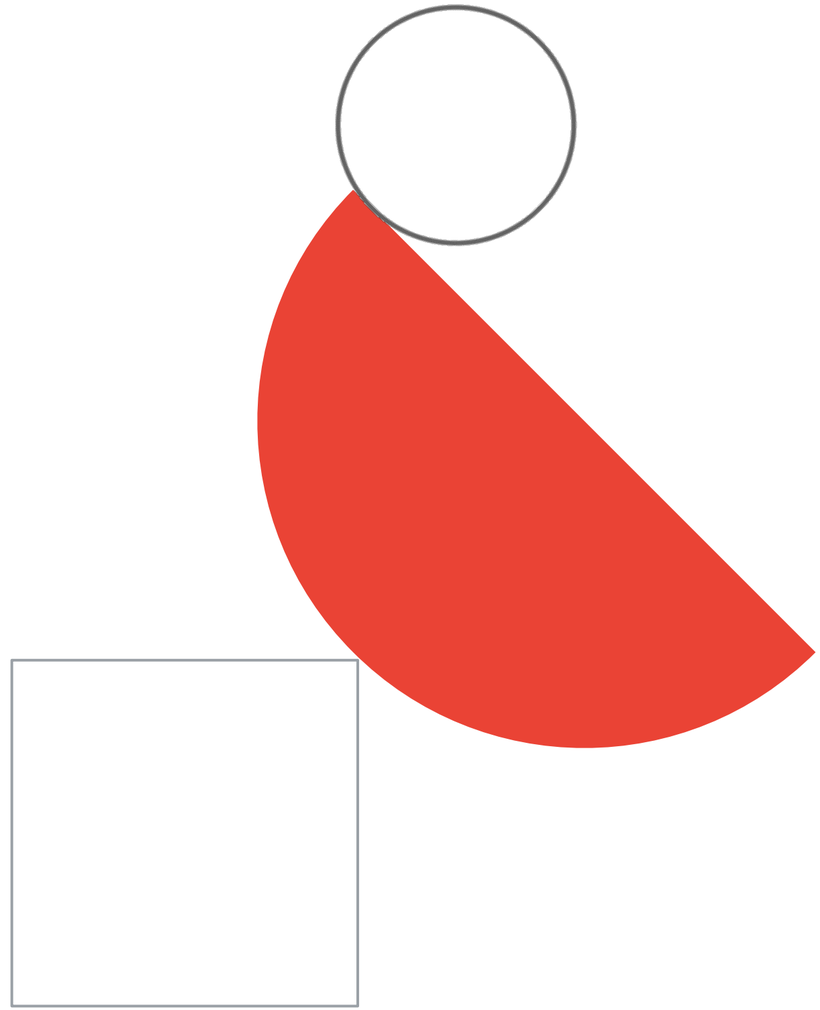
Module agenda

01 Securing Cymbal Bank’s network resources

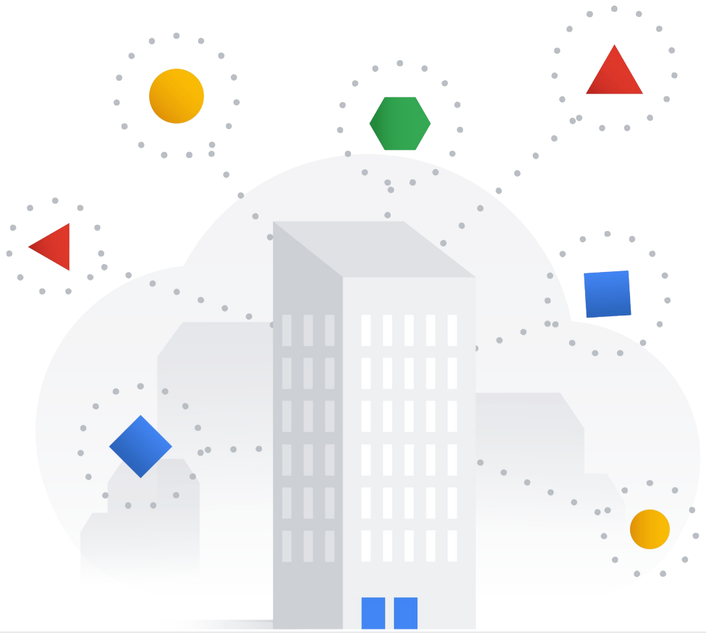
02 Diagnostic questions

03 Review and study planning

Securing Cymbal Bank's network resources



Securing Cymbal Bank's network resources



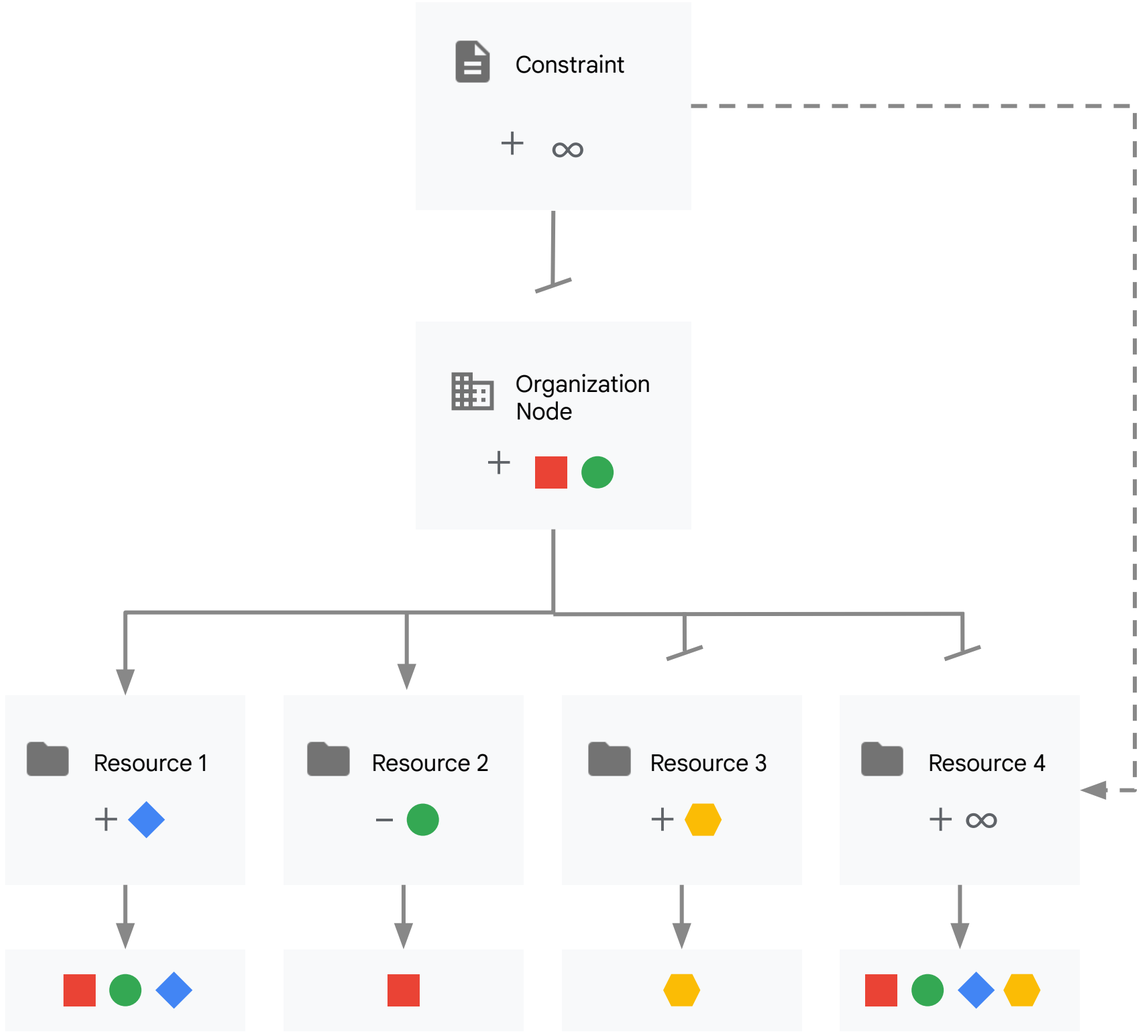
- Designing network security
- Configuring network segmentation
- Establishing private connectivity

Cymbal Bank

Organization policy helps restrict to authorized usage

Organization policies composed of a set of organizational policy constraints can be bound at multiple levels of hierarchy

- Large number of optional constraint types across various Google cloud services
- Policies may be configured for inheritance down hierarchy or not
- With inheritance, ancestor policy constraints can be overridden or merged



Organization Policy vs IAM Policy

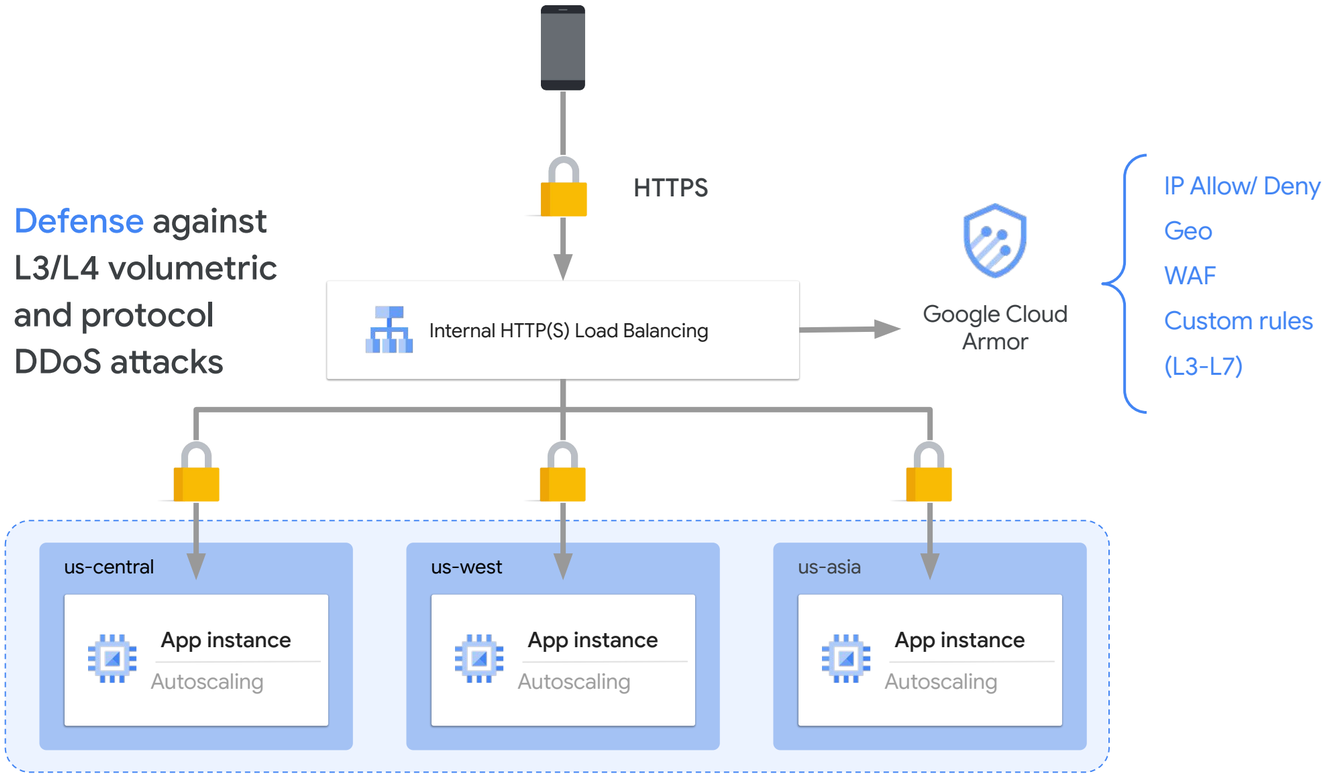
Organization Policies	IAM Policies
Constraints that allow you to: • Limit resource sharing based on domain. • Limit the usage of Identity and Access Management service accounts. • Restrict the physical location of newly created resources.	Effectively they're bindings which specify what access should be granted to principal on resources.
Focuses on "what". Allows to set restrictions on specific resources to determine how they can be configured	Focuses on "who". Let's you authorize who can take action on specific resources based on permissions
Can be set on different levels (org, folder, project), propagate down but lower-level policy overwrites a higher-level one.	Effective IAM Policy on each level is a SUM of all privileges (* with an exception of "deny policies", which are not covered on the exam as of Q1 '23)
Both should be used as part of a security posture! It's NOT one or the other.	

Most common Organization Policy constraints

Policy Constraint	Description
compute.vmExternalIpAccess	A list of project/zone/instance names that are allowed to have external IP addresses and deny all others. Attempts to create any other VMs with an external IP address will fail.
compute.trustedImageProjects	A list of projects that contain trusted images that can be used as the basis for a VM and deny all others. Attempting to instantiate a VM with an image from another project is denied.
compute.skipDefaultNetworkCreation	Disables the creation of default VPC when creating a project. The default VPC uses auto mode subnetworks and includes default firewall rules which are often incompatible with production deployments.
iam.disableServiceAccountKeyCreation	This boolean constraint disables the creation of service account external keys where this constraint is set to `True`.
compute.restrictVpcPeering	This list constraint defines the set of VPC networks that are allowed to be peered with the VPC networks belonging to this project, folder, or organization.
serviceuser.services	This list constraint defines the set of services and their APIs that can be enabled on this resource and below. By default, all services are allowed.
gcp.resourceLocations	BETA: This list constraint defines the set of locations where location-based GCP resources can be created. Policies for this constraint can specify multi-regions such as asia and europe, regions such as us-east1 or europe-west1, or individual zones such as europe-west1-b as allowed or denied locations.
sql.restrictPublicIp	This boolean constraint restricts configuring Public IP on Cloud SQL instances where this constraint is set to True. This constraint is not retroactive, Cloud SQL instances with existing Public IP access will still work even after this constraint is enforced. By default, Public IP access is allowed to Cloud SQL instances.
sql.disableDefaultEncryptionCreation	BETA: Restrict default Google-managed encryption on Cloud SQL instances
compute.requireShieldedVm	This boolean constraint, when set to True, requires that all new Compute Engine VM instances use Shielded disk images with Secure Boot, vTPM, and Integrity Monitoring options enabled. Secure Boot can be disabled after creation, if desired. Shielded VM features add verifiable integrity and exfiltration resistance to your VMs.
compute.restrictSharedVpcHostProjects	Restrict Shared VPC Host Projects This list constraint defines the set of Shared VPC host projects that projects at or below this resource can attach to. By default, a project can attach to any host project in the same organization, thereby becoming a service project.
iam.allowedPolicyMemberDomains	This list constraint defines the set of members that can be added to Cloud IAM policies. By default, all user identities are allowed to be added to Cloud IAM policies. The allowed/denied list must specify one or more Cloud Identity or G Suite customer IDs. If this constraint is active, only identities in the allowed list will be eligible to be added to Cloud IAM policies.

Configure HTTPS load balancers and Google Cloud Armor

- Supports variety of load balancers:
  - Global external HTTP(S)
  - Global external HTTP(S) (classic)
  - External TCP proxy
  - External SSL proxy

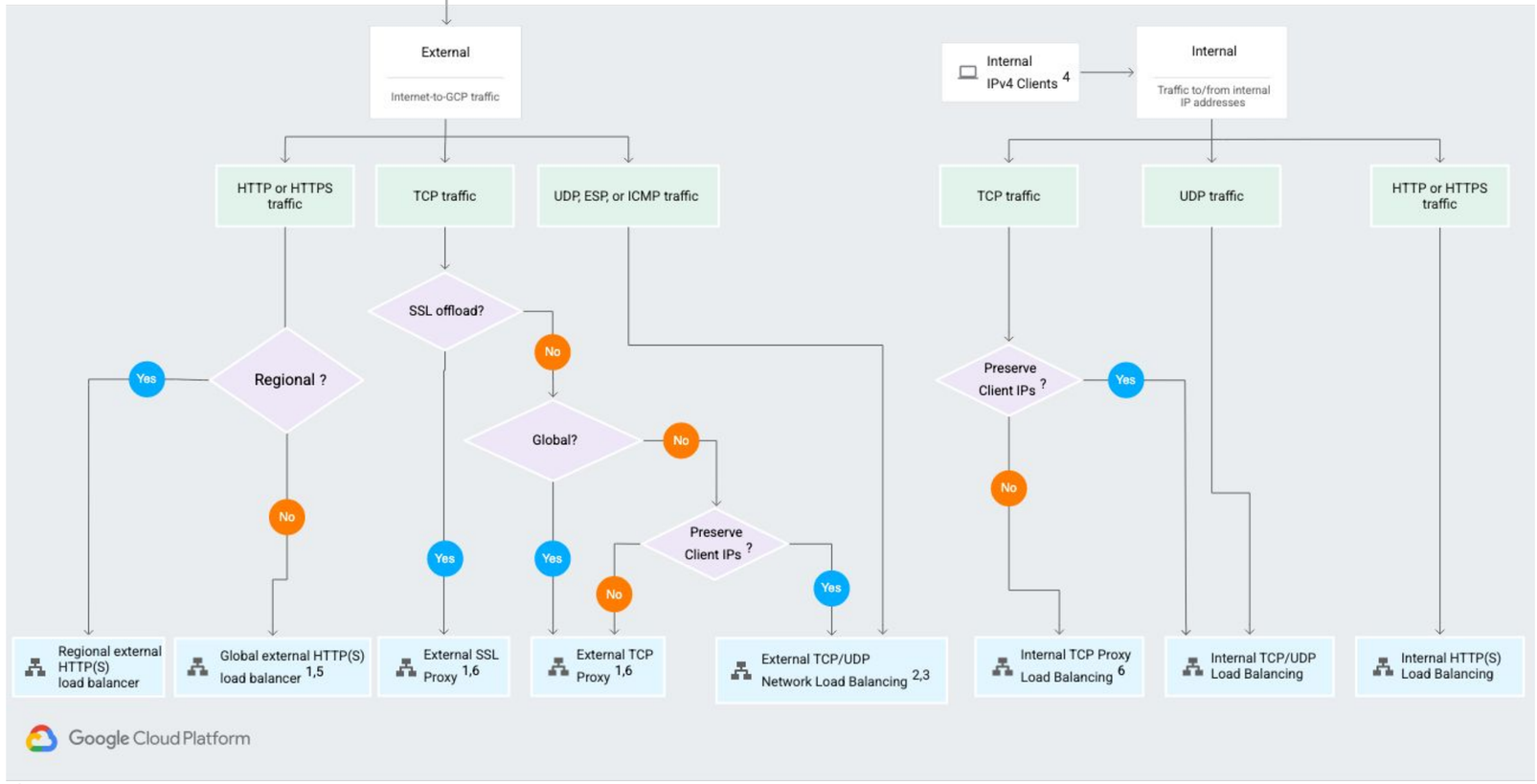


- Provide Layer 7 DDoS defense
- Protect against SQL injection attacks
- Protect against XSS injection attacks
- Configure rules for filtering traffic

Exam Tip: *you need to know which Load Balancers can be used with Cloud Armor and how it works with IAP*

Types of load balancers

Exam Tip: *Google's Load Balancers can also load balance traffic across non-GCP backends!*



[1] IPv6 termination is available if you configure the load balancer in Premium Tier.

[2] Choose external TCP/UDP network load balancing if you need to ensure that the load balancer is located in a particular region, or if you want to configure IPv6 load balancing (with dual-stack backends). The latter is only available for backend service-based network load balancers.

[3] External TCP/UDP network load balancers use regional external IP addresses that are accessible by clients anywhere.

[4] Clients in a VPC network or in a network connected to a VPC network.

[5] The global external HTTP(S) load balancer (classic) can be configured to be effectively regional in Standard Tier.

[6] Client source IP preservation is available in certain configurations by using the PROXY protocol.

Traffic type

The type of traffic that you need your load balancer to handle is another factor in determining which load balancer to use:

- **HTTP and HTTPS traffic**:
  - Global external HTTP(S) load balancer
  - Global external HTTP(S) load balancer (classic)
  - Regional external HTTP(S) load balancer
  - Internal HTTP(S) Load Balancing
- **SSL traffic**:
  - External SSL Proxy Load Balancing
- **TCP traffic**:
  - External TCP Proxy Load Balancing
  - External TCP/UDP Network Load Balancing
  - Internal TCP/UDP Load Balancing
- **UDP traffic**:
  - External TCP/UDP Network Load Balancing
  - Internal TCP/UDP Load Balancing
- **ESP or ICMP traffic**:
  - Network Load Balancing

Exam Tip: *source here.*

Configure policy

Name *
cloud-armor-policy
Lowercase letters, numbers, hyphens allowed

Description

Policy type

- (•) Backend security policy
- ( ) Edge security policy

Default rule action

- ( ) Allow
- (•) Deny

Deny status
403 (Forbidden)

NEXT STEP

Apply policy to targets (optional)

Targets are Google Cloud Platform resources that you want to control access to.
You can only use non-CDN HTTP(S) load balancer backend services as targets.

Type 1
Load balancer backend ser...

Backend Service target 1 *

Filter Type to filter

web-backend
Load balancer: web-lb

+ ADD TARGET

You can also add/edit targets after the p

NEXT STEP

RULES | TARGETS | LOGS

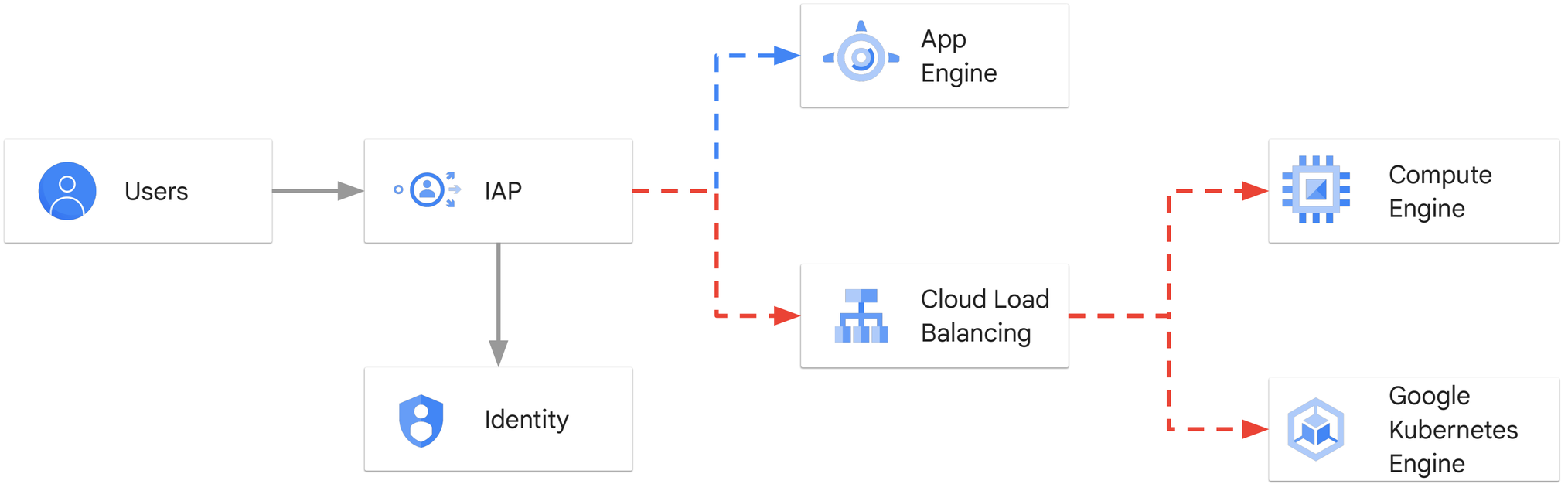
Rules are evaluated by priority: Lower numbers are evaluated first. Learn more

ADD RULE | DELETE | MORE

Filter Enter property name or value

Action	Type	Match	Description	Priority
Deny (403)	IP addresses/ranges	* (All IP addresses)	Default rule, higher priority overrides it	2,147,483,647

Connect through Identity-Aware Proxy



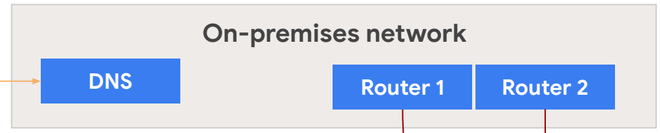
Exam Tip: *It's a best practise to also use IAP to enable administrative access to VMs (ssh, rdp) which do not have external IPs.*

Reference architecture

Hub-and-spoke with VPC peering - Segmentation based on environments

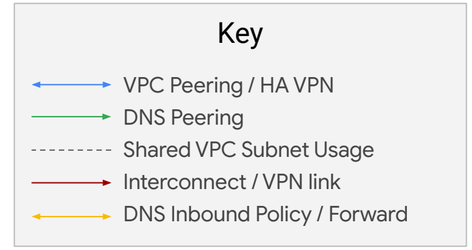
Network security control
- Centralized network security administration
- Central services (NAT, DNS, etc.) deployed in Shared VPC

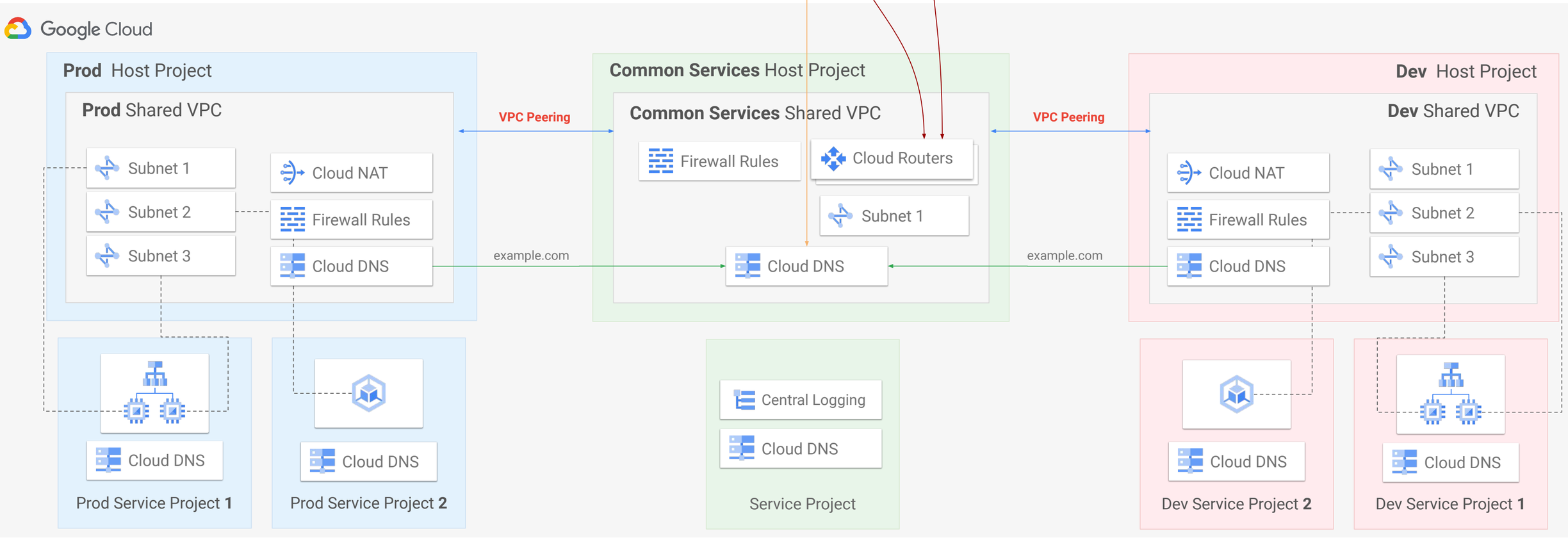
Scalability
- **Up to 25 spokes**, per VPC peering limitations
- Each spoke can have a high number of service projects



Spokes isolation
- Spokes are isolated as VPC peering is **non-transitive**

Central control versus autonomy
- Full networking autonomy for spokes, based on a separate shared VPC network

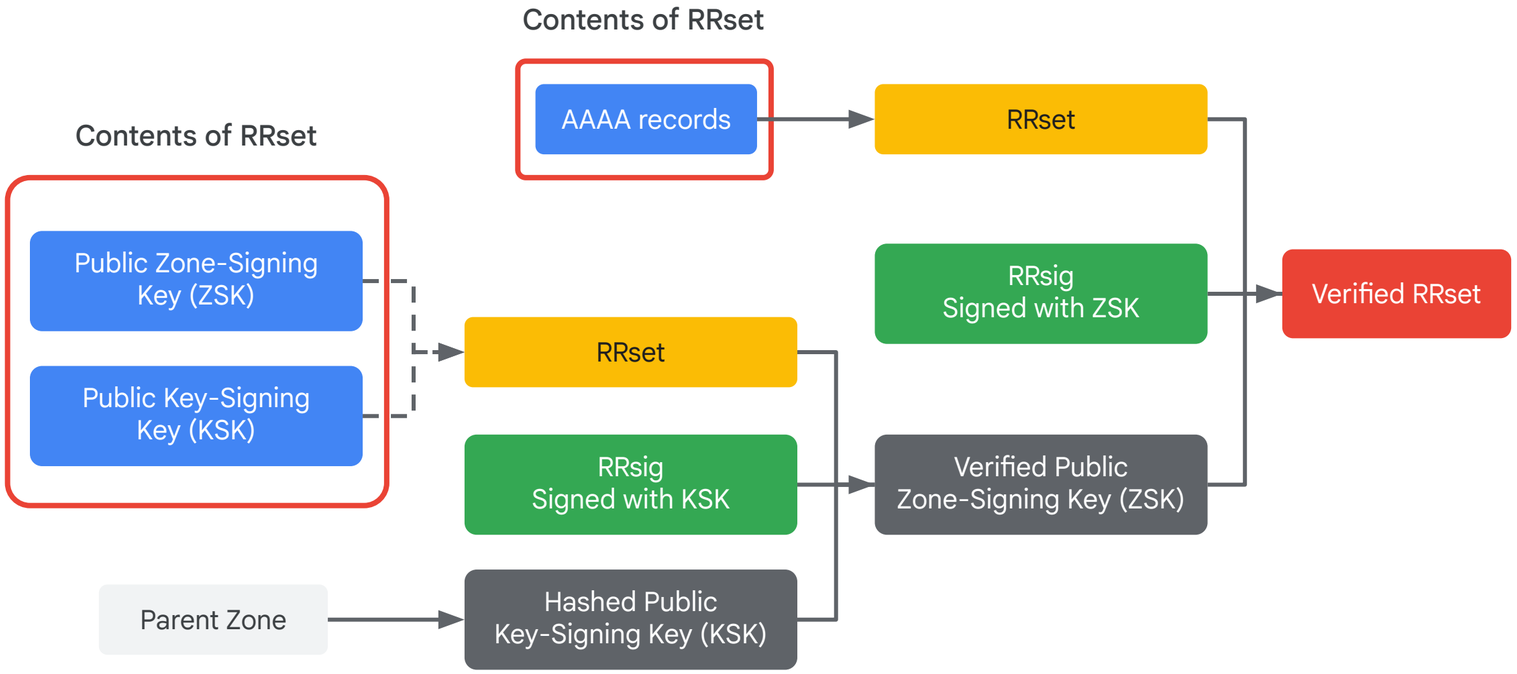




Protect public DNS zones

Cloud DNS supports DNSSEC to secure the DNS resources and prevent attackers from manipulating DNS responses.

- Ensures authenticated DNS responses to DNS requests
- Automatically manages DNSSEC related DNS records
- Integrates with DNSSEC at the domain registrar level

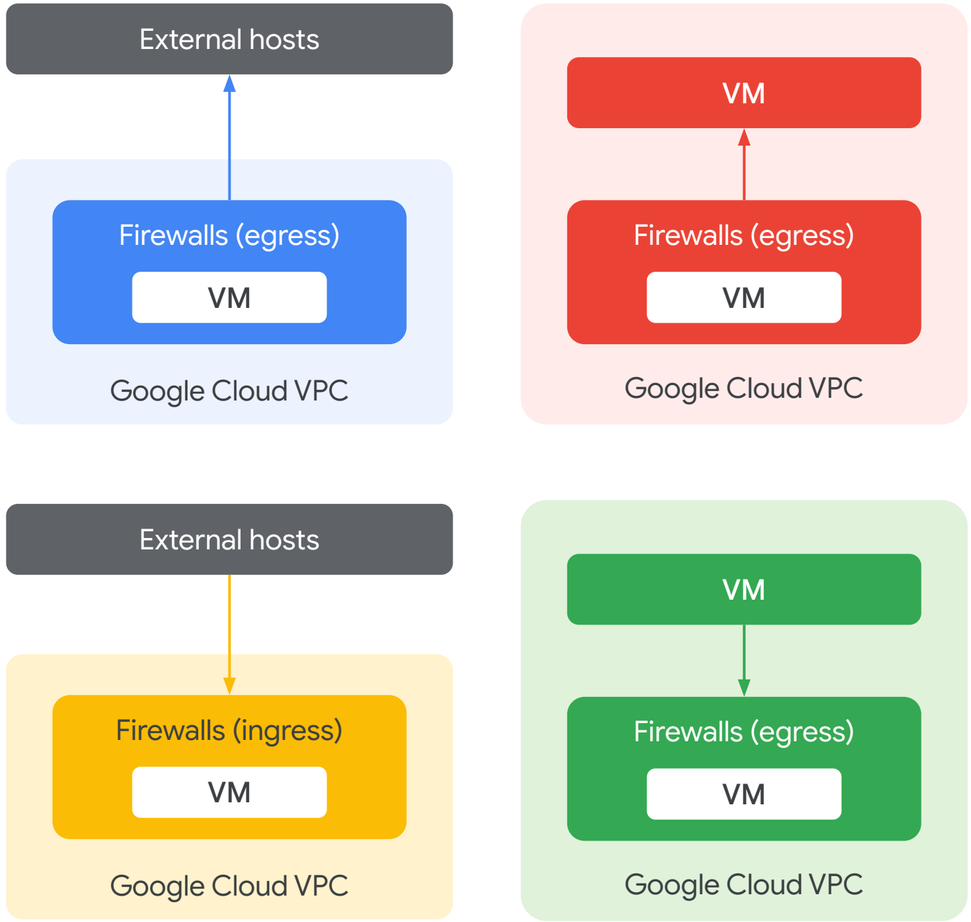


[Know how to migrate DNSSEC-signes zones to Cloud DNS]

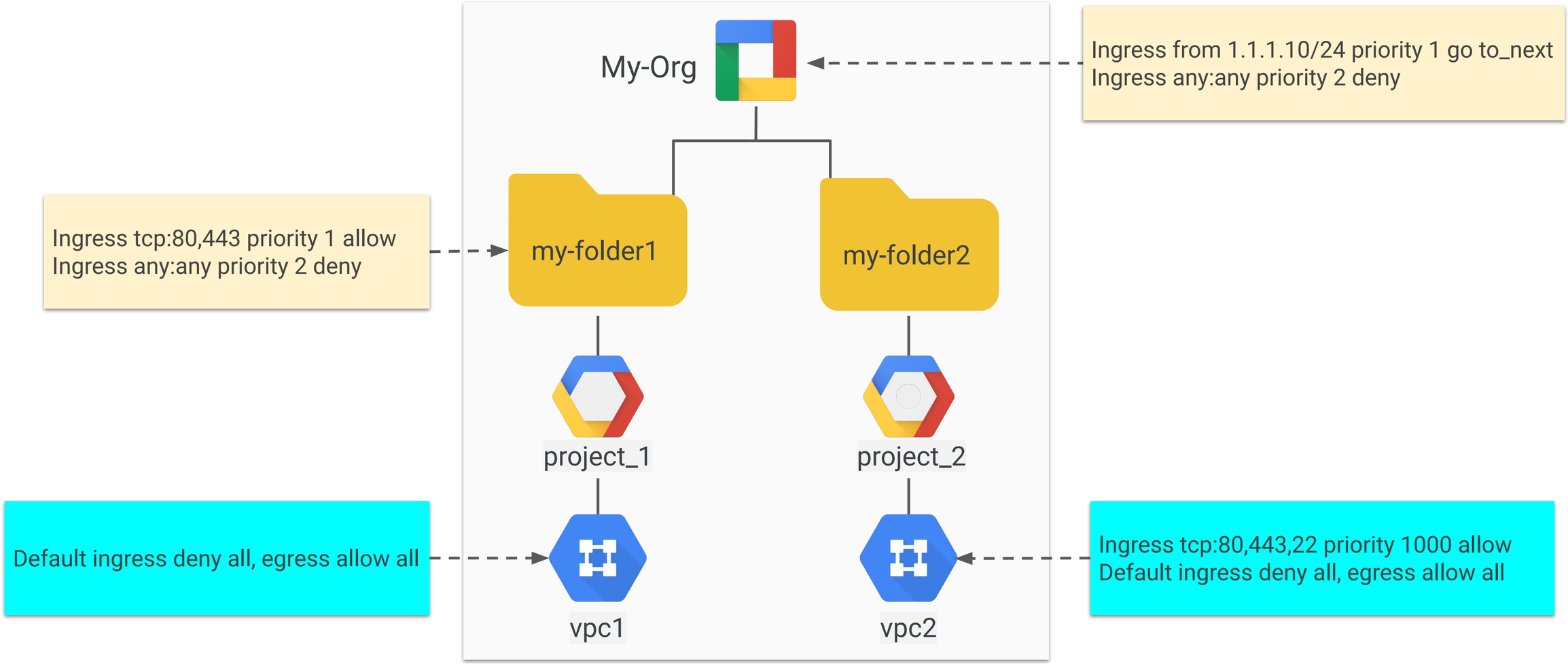
Limit VPC traffic with Firewall rules

Cymbal Bank will use firewall rules to only allow valid and expected traffic between workloads, and block all other traffic.

- Stateful rules handle requests in either the ingress or egress direction.
- Firewall rules can defined from source service accounts to target service accounts.
- Firewall rules can be applied in a hierarchical manner to ensure uniform application across projects.



Hierarchical firewall **policies** (yeah… another policy…)



Google Cloud

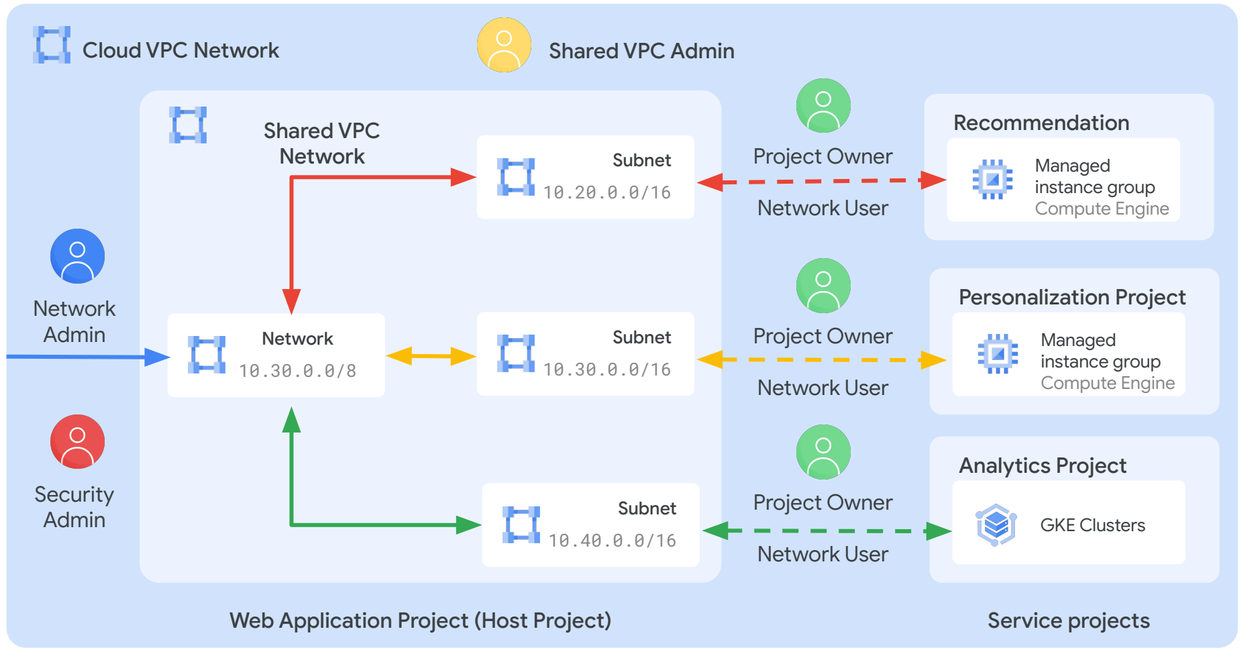
Firewall Policy vs. VPC Firewall Rules

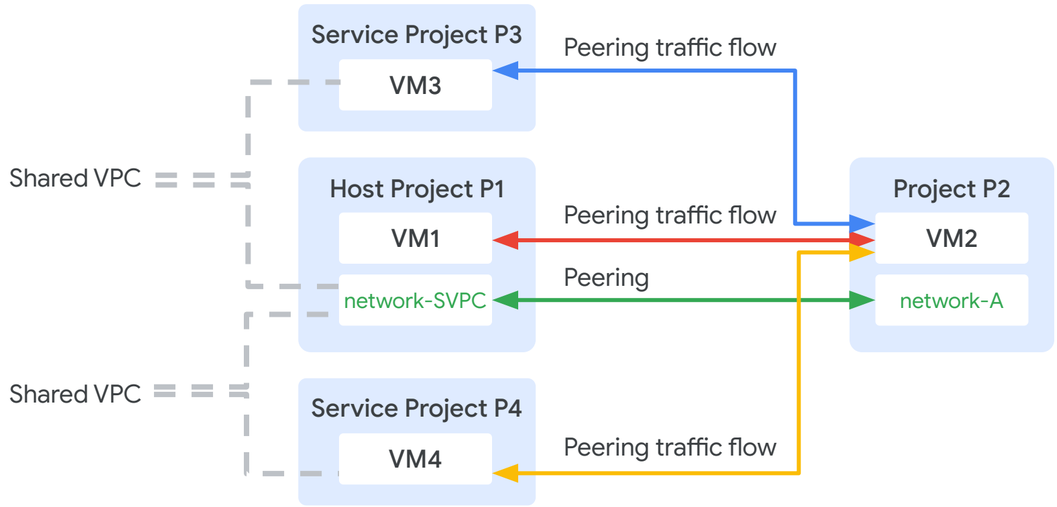
Rules in Firewall Policies are similar to VPC Firewall Rules with a few differences:

	VPC Firewall Rules	Firewall Policy Rules
Action Supported	Allow/deny	Allow/deny/**goto_next**
Service Account	Yes	**Target** only
Network Tag	Yes	**No**
Rule Name	mandatory	optional
Quota	Rule count	**Attribute** count
Priority	Duplication allowed	**No duplication** allowed

Isolate networks to secure workloads

Cymbal Bank will connect privately across projects using shared VPC and VPC peering.





Shared VPC vs VPC Network Peering

Consideration	Shared VPC	VPC Network Peering
Across organizations	No	Yes
Within project	No	Yes
Network Administration	Centralized	Decentralized

Organization Admin		
Shared VPC Admin		
Security and Network Admins		
Project Owner	Project Owner	Project Owner

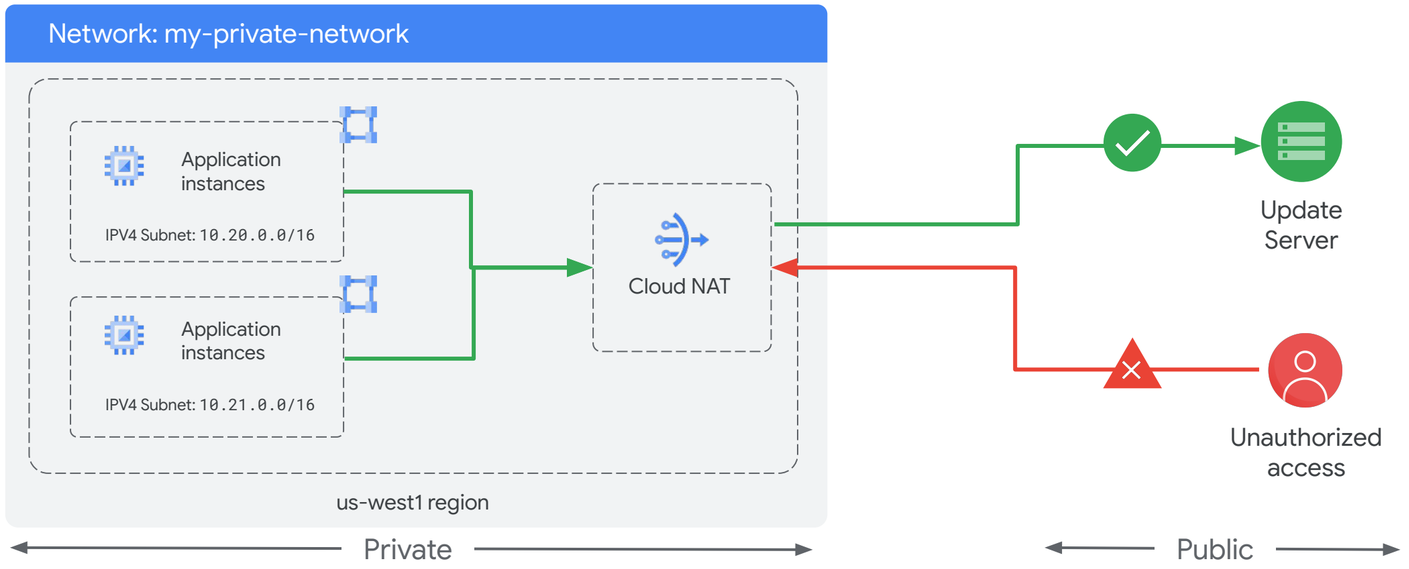
Organization Admin (if same org)		
Security and Network Admins	Security and Network Admins	Security and Network Admins
Project Owner	Project Owner	Project Owner

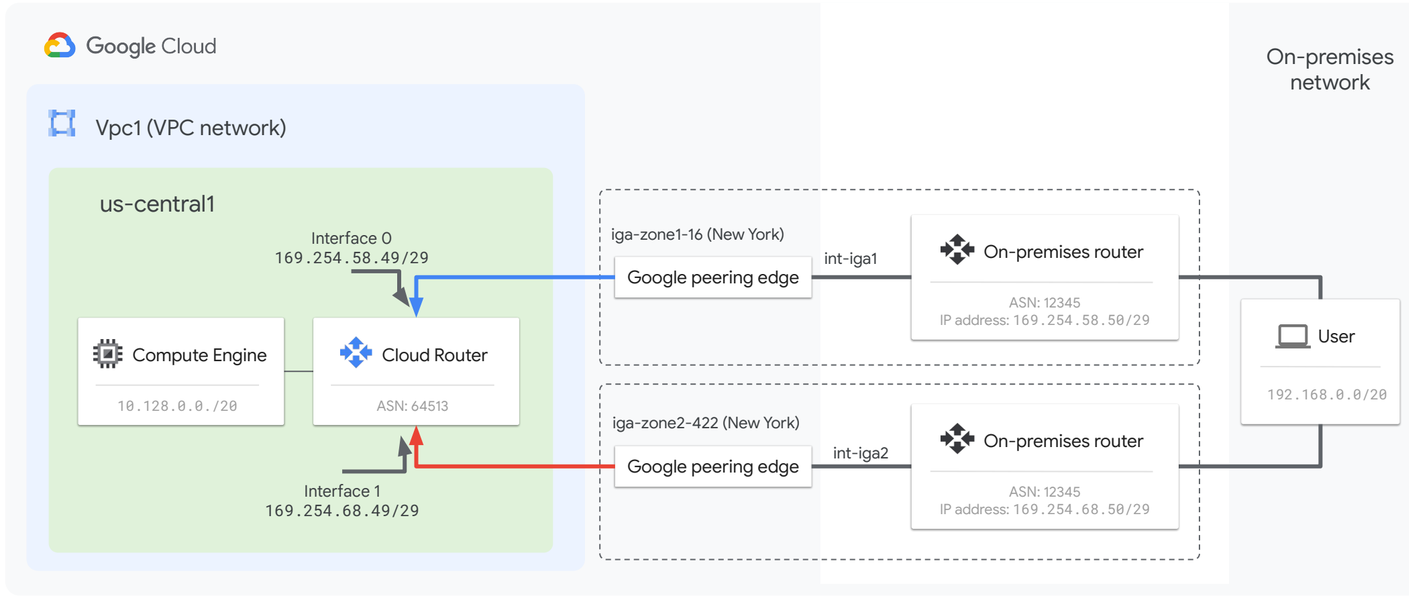
Keep traffic private where possible

Cymbal Bank will connect privately from on-premises into Google Cloud to Google APIs or the wider Internet.

You will use:

- Cloud VPN and Interconnect
- Google private access
- Cloud NAT





Private service connectivity

Managed services connectivity methods

Private Google Access (PGA)	Private Services Access (PSA) with VPC Peering	Private Service Connect (PSC) for Google APIs and Google Managed Services (future direction)	VPC Serverless Connectors
Access Google APIs (ex: Cloud Storage or BigQuery) privately, from Google Cloud or on-prem	Privately connect producer and consumer VPCs via VPC peering (e.g.: Google managed VPC for Cloud SQL)	Privately connect producer and consumer VPCs with Private Service Connect (scales to hundreds or thousands of services shared)	Provides connectivity to Google Cloud Serverless services (App Engine Standard, Cloud Function, Managed Cloud Run) to resources in your VPC

- Private Google Access
- Private Service Access
- Serverless VPC Access
- Private Service Connect

You need to know when to use which one!

Private Google access

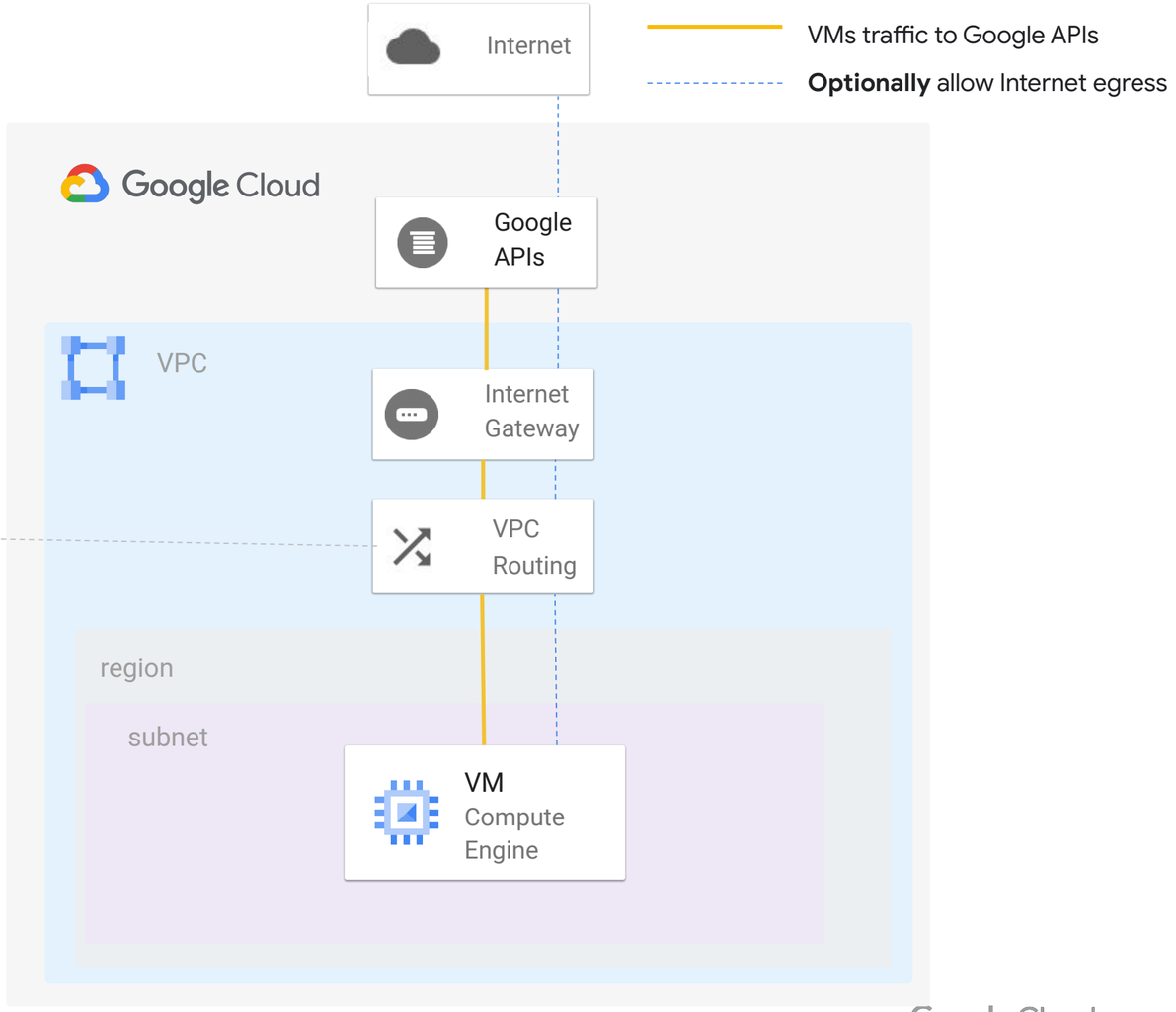
Allow Google Cloud VMs to reach API endpoints, without Internet access.

Problem:

Instances without access to the Internet can't access Google Cloud public API endpoints.

Solution:

Enable **Private Google Access** in the subnetwork the instance is attached to.



Example of Google API based managed services:

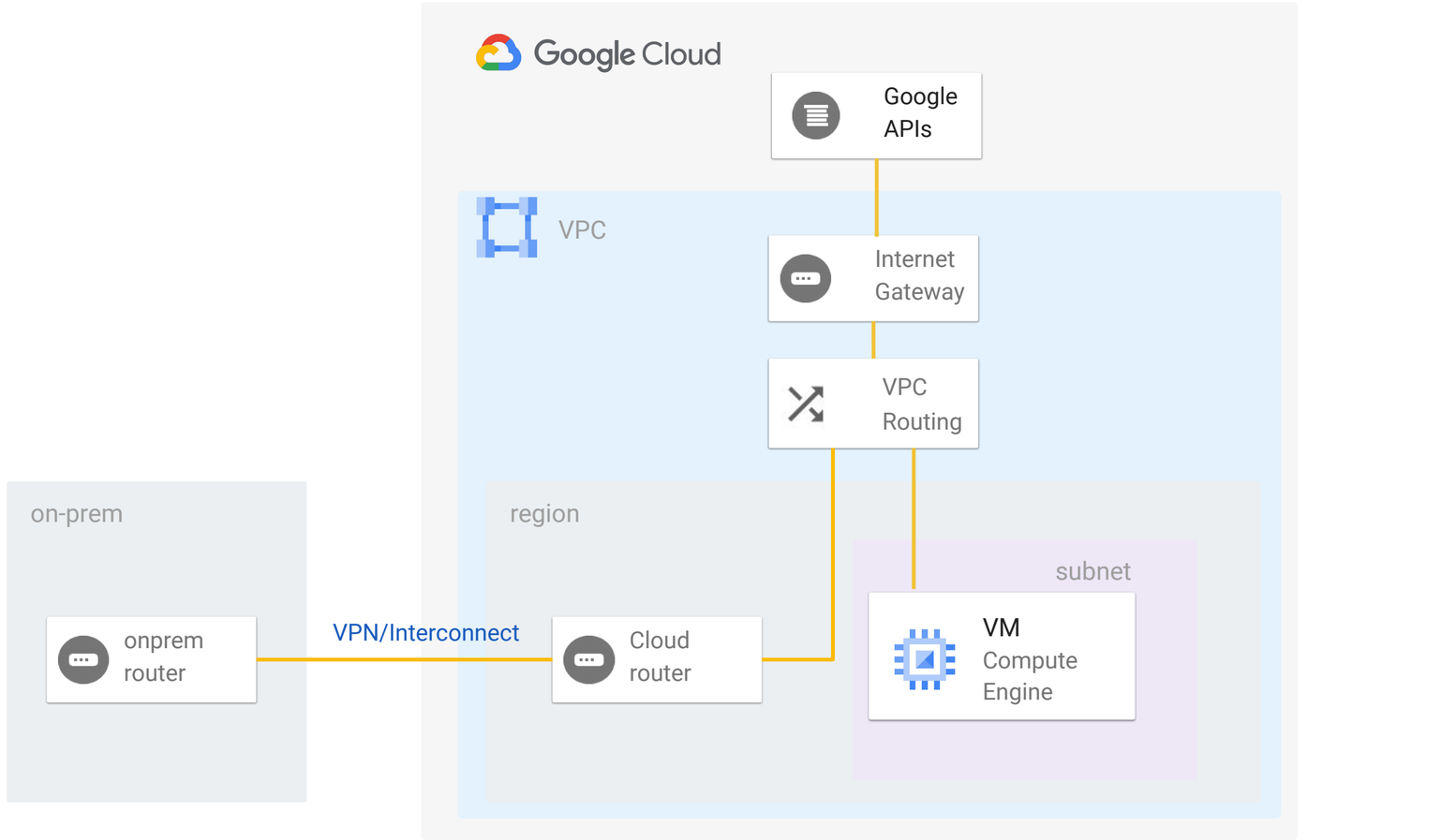
- Google Cloud Storage
- Big Query
- Pub/Sub
- ...

Private Google access for on-premises

Private Google Access for on-premises hosts

On-premises hosts can reach Google APIs and services over a Cloud VPN or Cloud Interconnect connection from your data center to Google Cloud.

The configuration uses DNS overrides to send API traffic to specific VIPs.



https://cloud.google.com/vpc/docs/private-access-options#pga

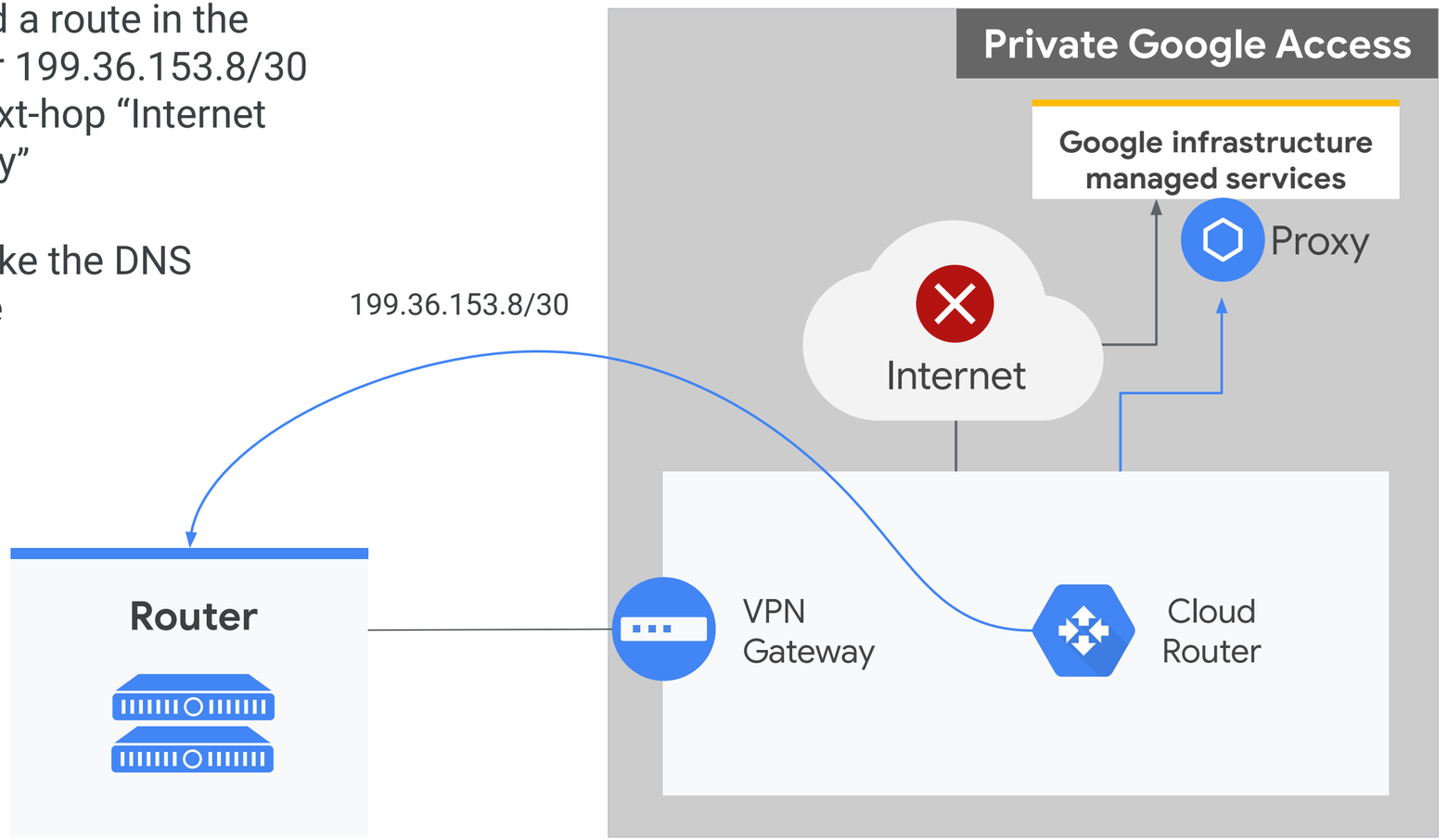
Example of configuration

01. Remove Public IP on VMs AND Activate google access per subnet

02. Add a route in the VPC for 199.36.153.8/30 with next-hop “Internet gateway”

03. BGP announce: 199.36.153.8/30

04. Make the DNS Change



Internal API endpoints for on-prem
(or VPCs without a default route to the Internet Gateway)

Not using VPC SC or need to access more APIs not supported by VPC SC

PRIVATE DNS

private.googleapis.com

restricted.googleapis.com

ROUTES

199.36.153.8/30

199.36.153.4/30

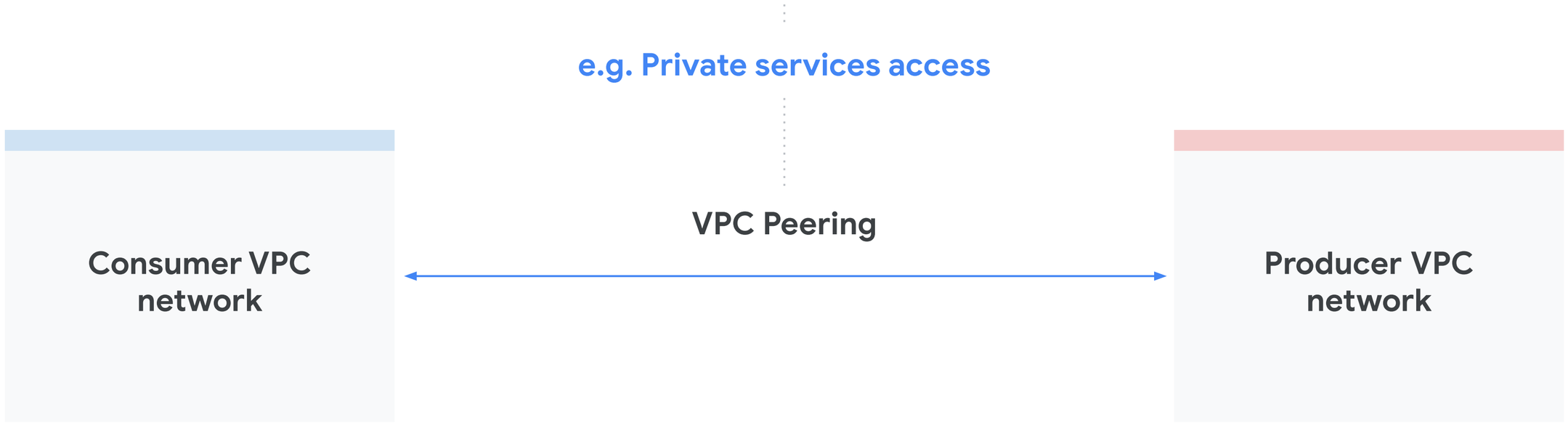
Internet Gateway

Use to **ONLY** reach APIs protected by **VPC SC**

Alternatively, the default Internet Gateway route can be used

Typical Consumer/Producer Networking Setup

- Operational burden, i.e. IP address coordination to avoid overlap between VPCs
- Developers constrained by networking requirements
- Different models for different services, i.e. Private Google Access vs Private services access
- VPC Peering considerations, i.e. quotas and limits, non-overlapping CIDRs, no route filtering



Private Service Access (PSA)

Allows Google Cloud VMs and on-prem networks to access Google Managed Services

Problem:

Instances or on-prem hosts need to reach Google Services deployed in a Google managed VPC

Solution:

Enable **Private Service Access** in the VPC to create a VPC Peering to the Google managed VPC.

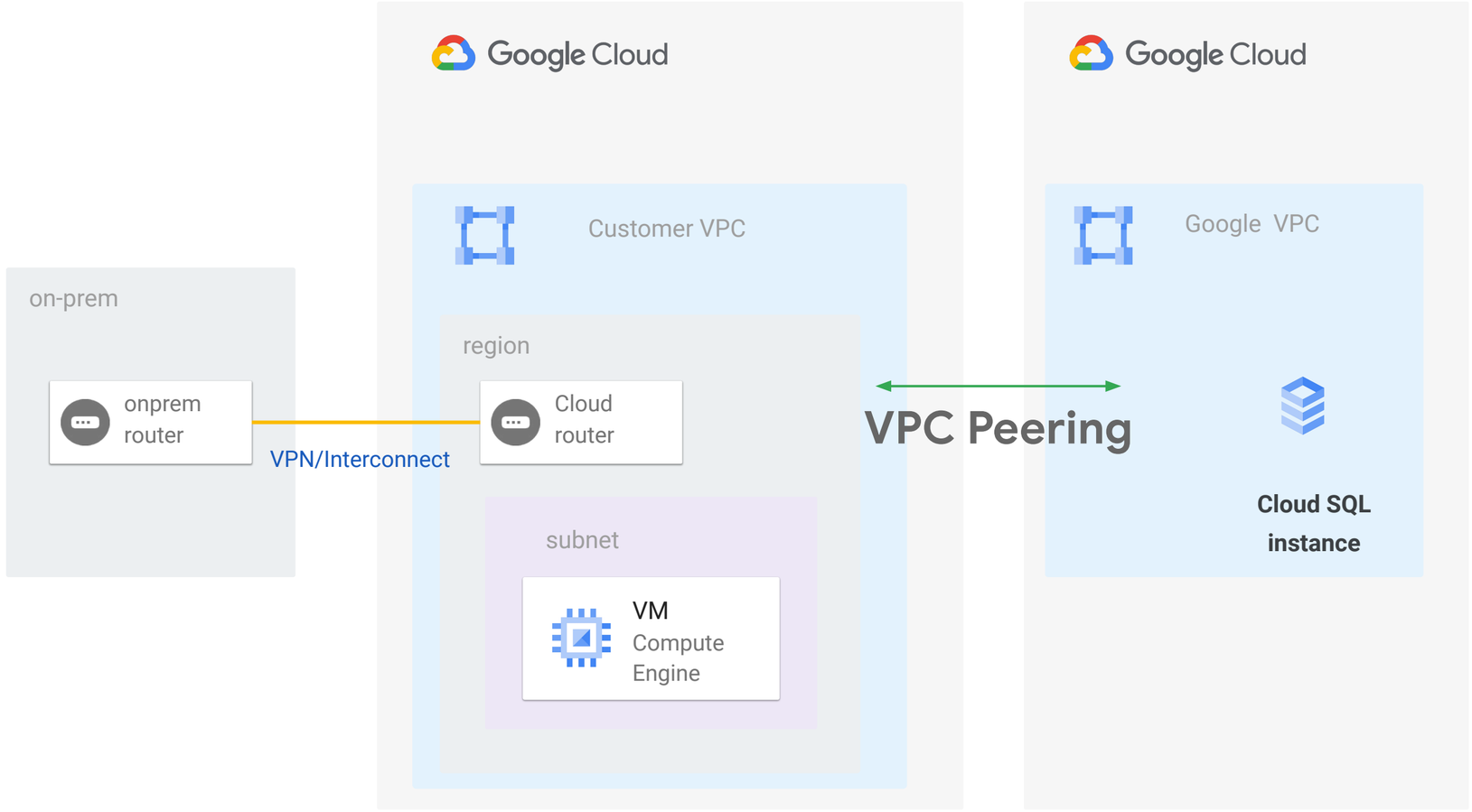
Example of PSA based managed services:

- Cloud SQL
- Memcache
- Cloud IDS
- ...

Private Service Access

Private Service Access for on-premises hosts

Google Cloud and On-premises hosts (via hybrid connectivity) can reach certain Google managed services over shared VPC peerings.



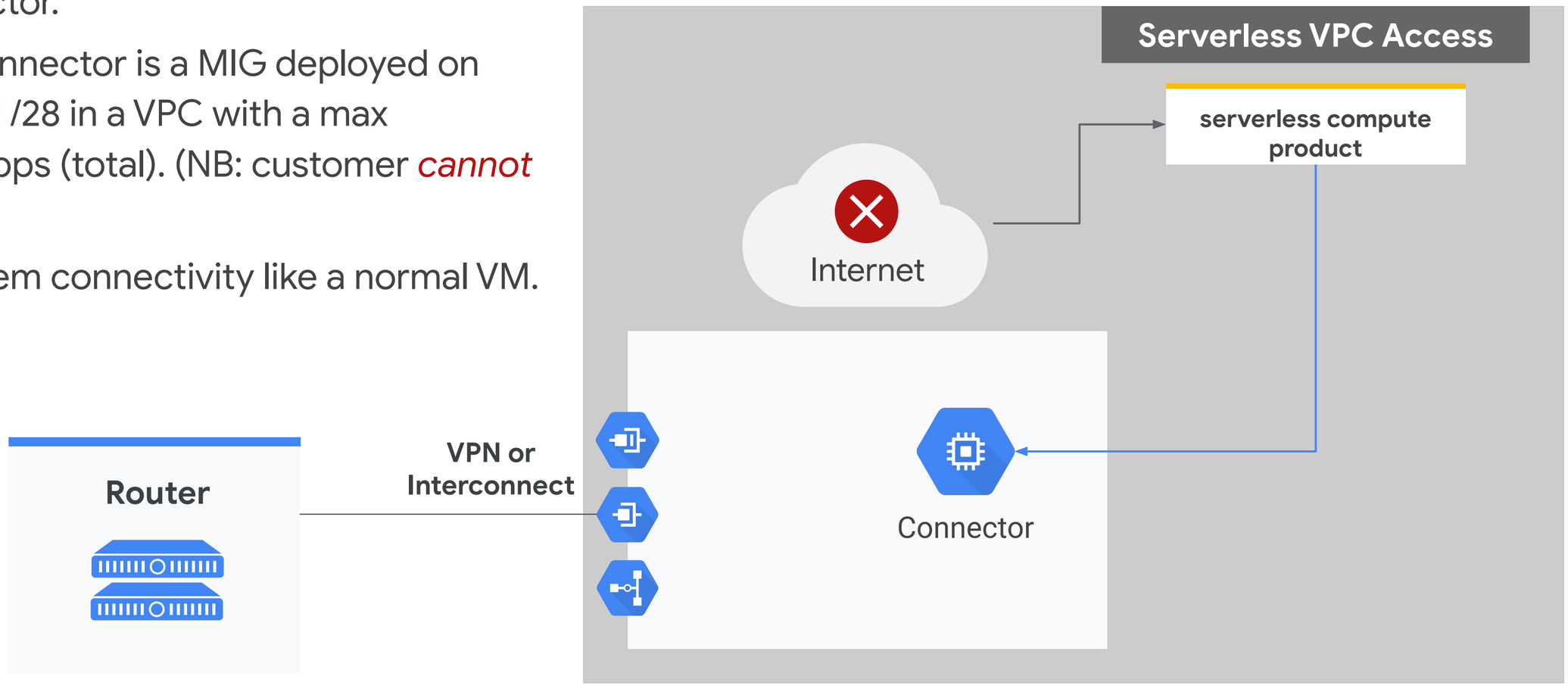
Serverless VPC Access

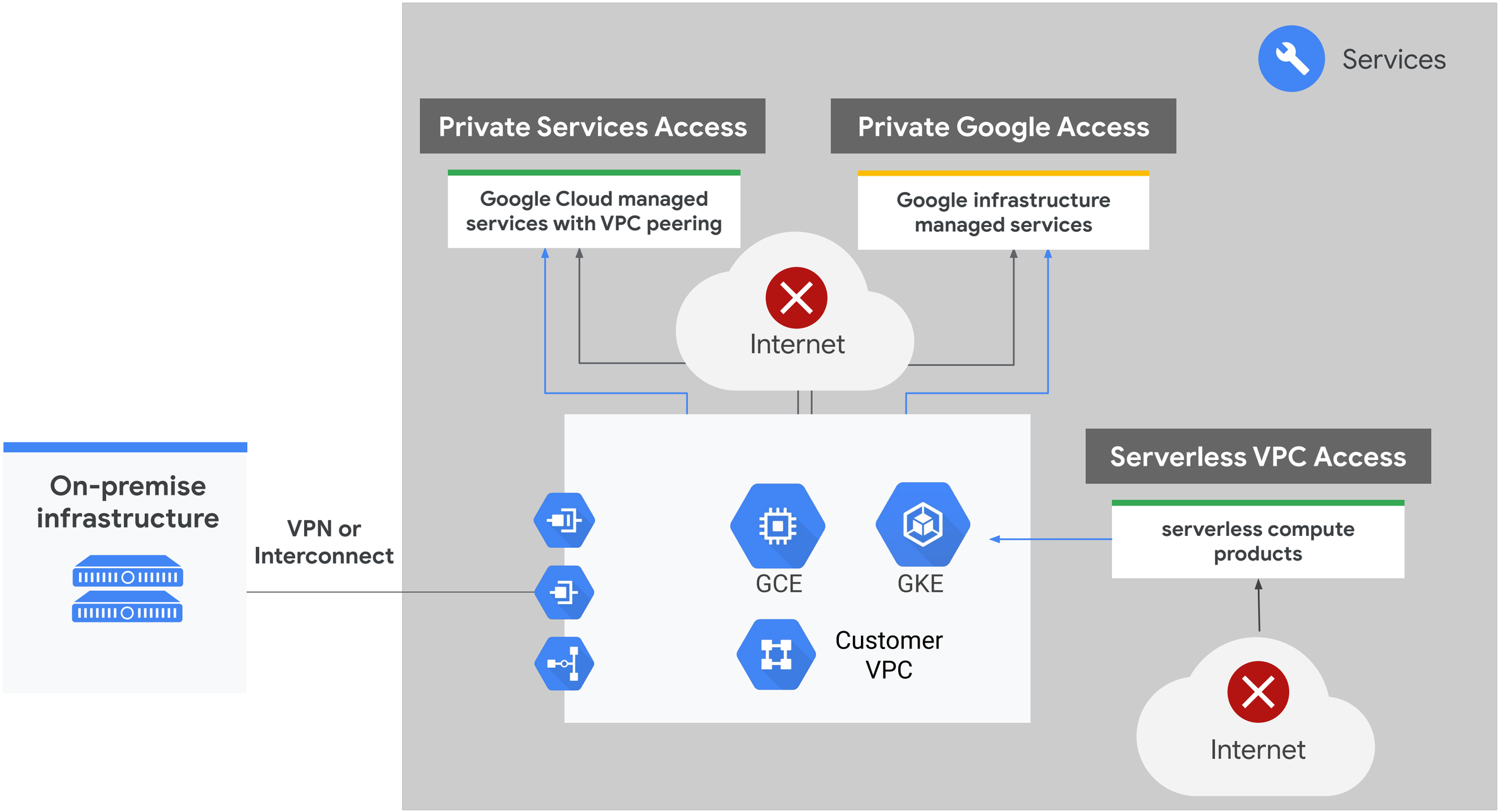
Cloud Function, Cloud Run, AppEngine standard

Traffic *initiated* from serverless product is routed through the connector.

Under the hood, connector is a MIG deployed on customer-provided /28 in a VPC with a max throughput of ~1 Gbps (total). (NB: customer *cannot* see MIG today)

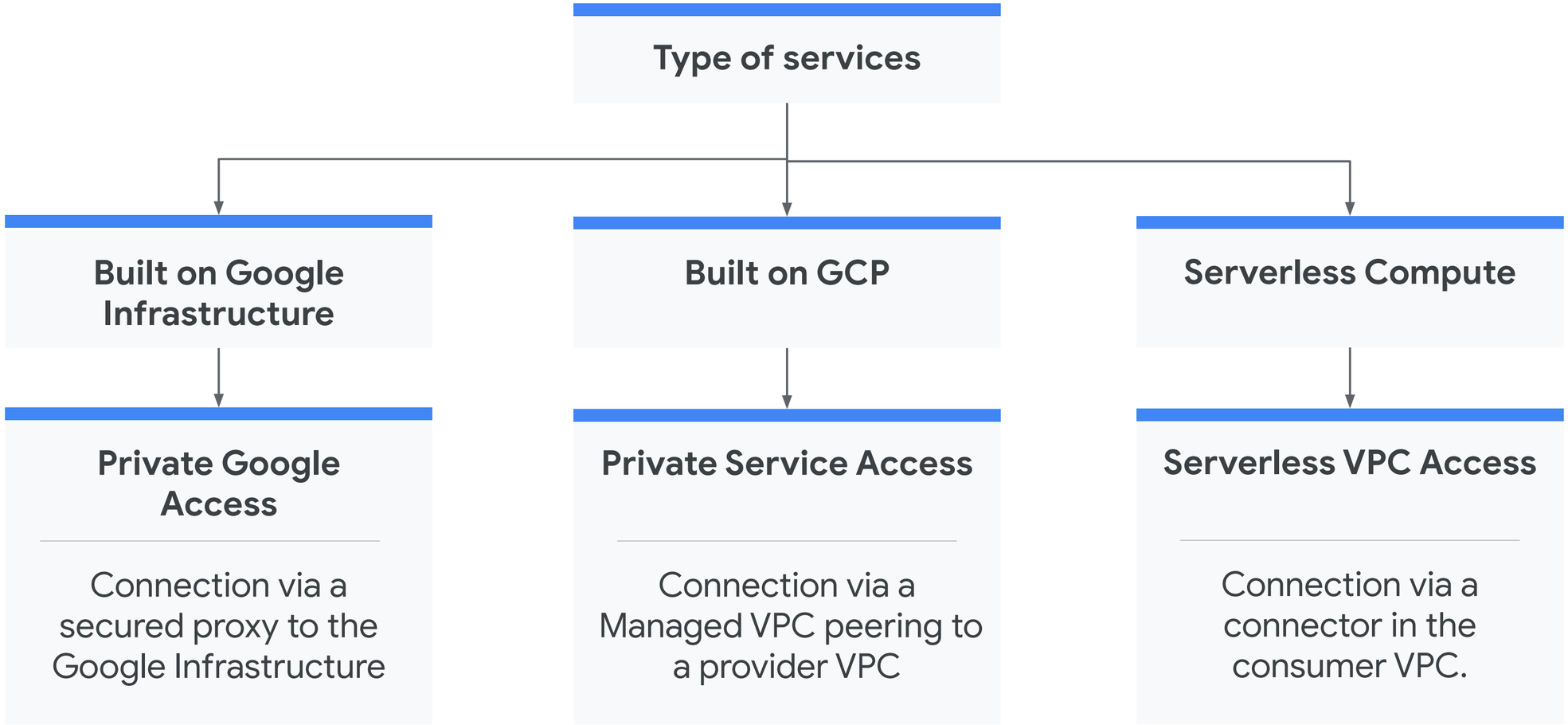
Internet and On-prem connectivity like a normal VM.





Solutions Summary

Full list of services:https://cloud.google.com/vpc/docs/private-access-options



A new solution to simplify this area is coming: Private Service Connect

Why Private Service Connect

Consume Services Faster

- Consumer and Producers operate independently
- Support for Single-Tenant and Multi-Tenant Services

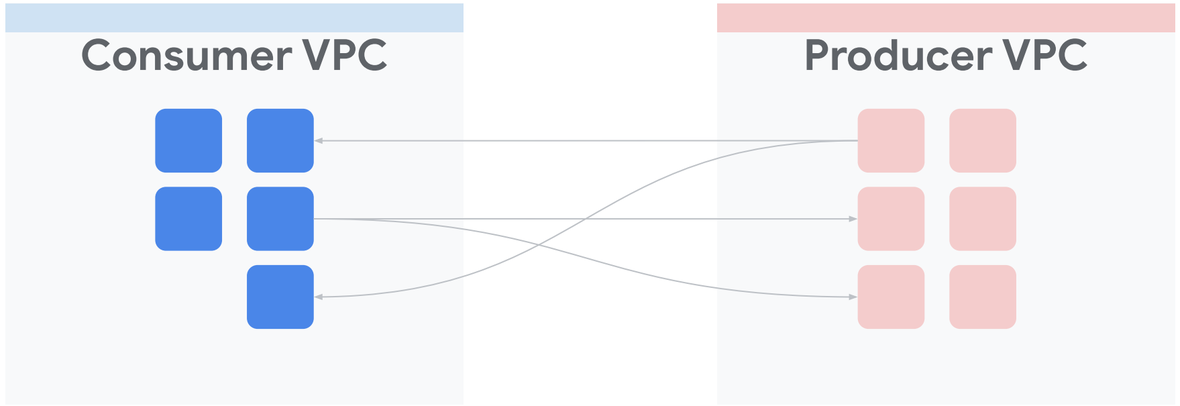
Private and Seamless Connectivity

- Private End to End Connectivity
- Create an Endpoint on the Consumer Network

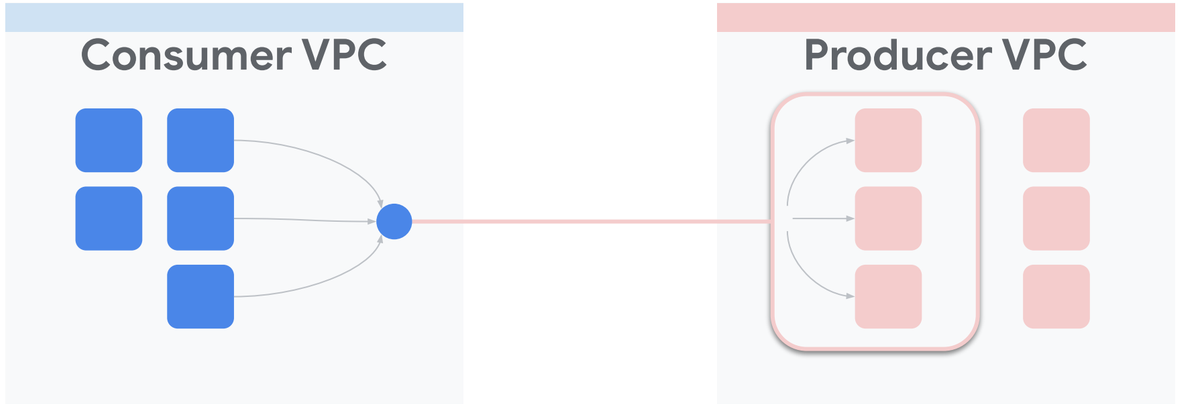
Accelerate Cloud Consumptions

- 1st Party, 3rd Party and Customer Owned Services

VPC Peering (Private Service Access)

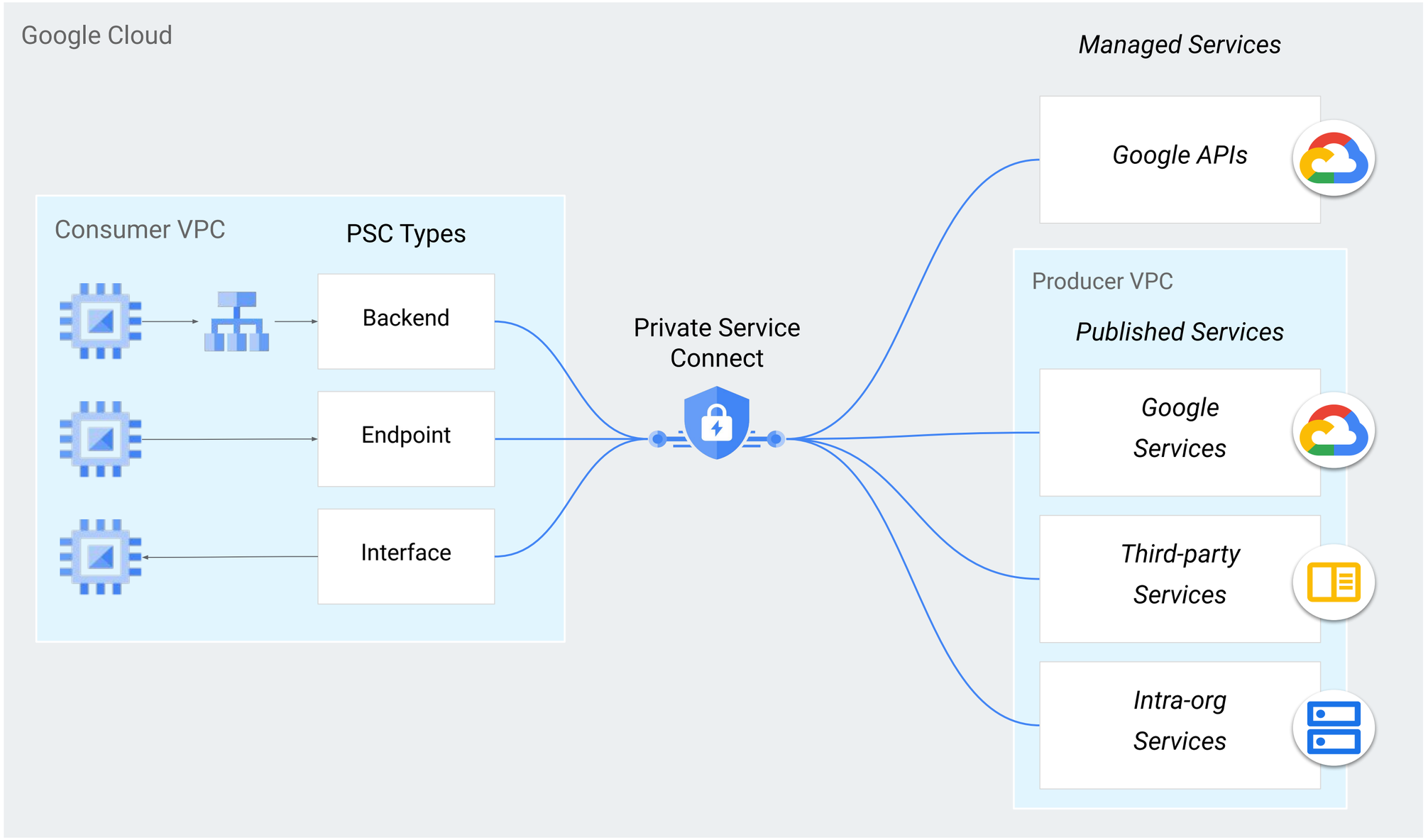


Private Service Connect



Google Cloud

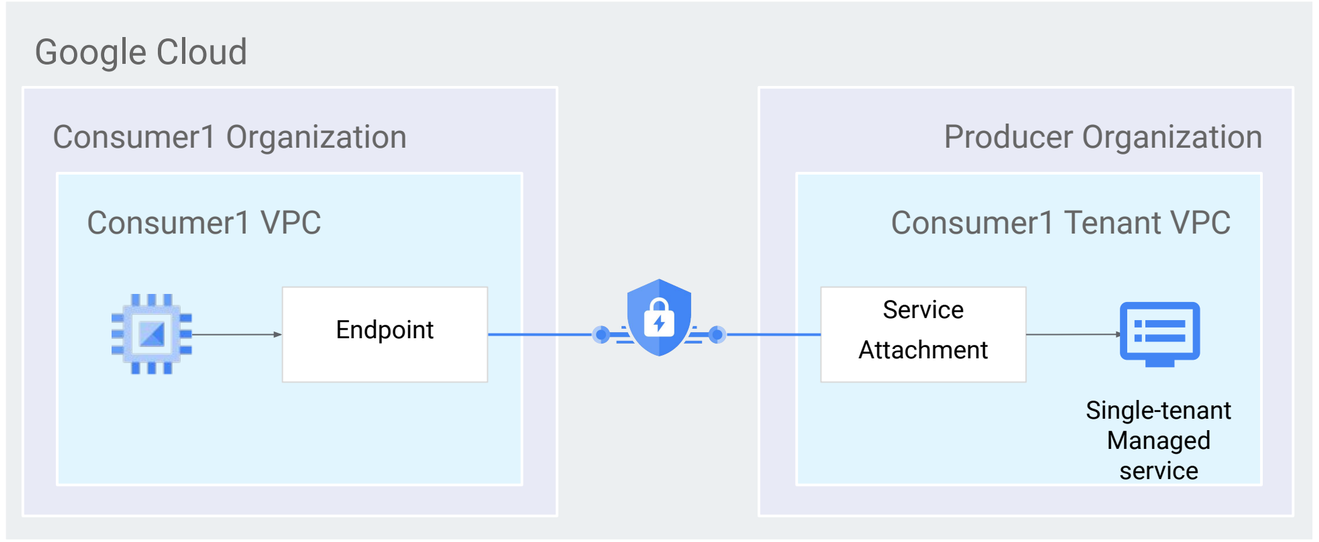
PSC for ...


Google Cloud
Managed Services
Google APIs
Consumer VPC
PSC Types
Backend
Endpoint
Interface
Private Service Connect
Producer VPC
Published Services
Google Services
Third-party Services
Intra-org Services

PSC Topologies

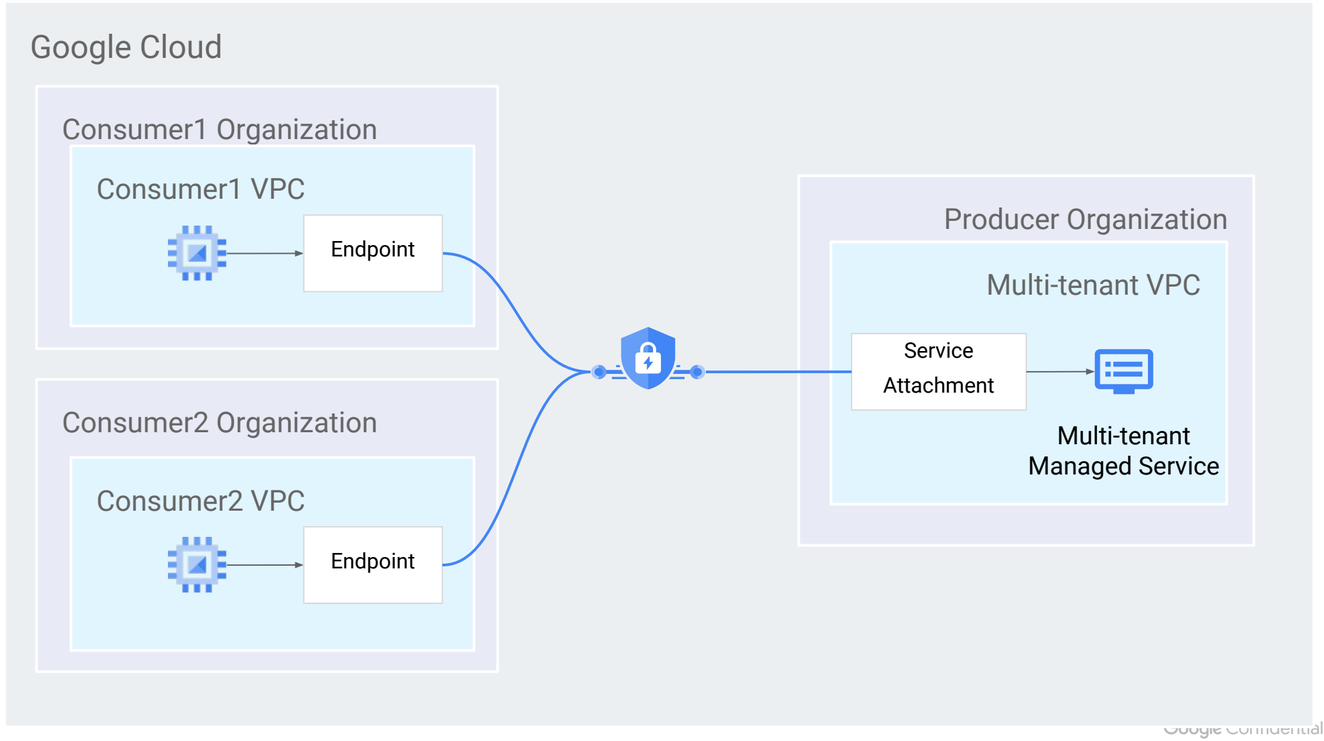
Single-tenant Managed Services

Managed services which are consumed by a single consumer.



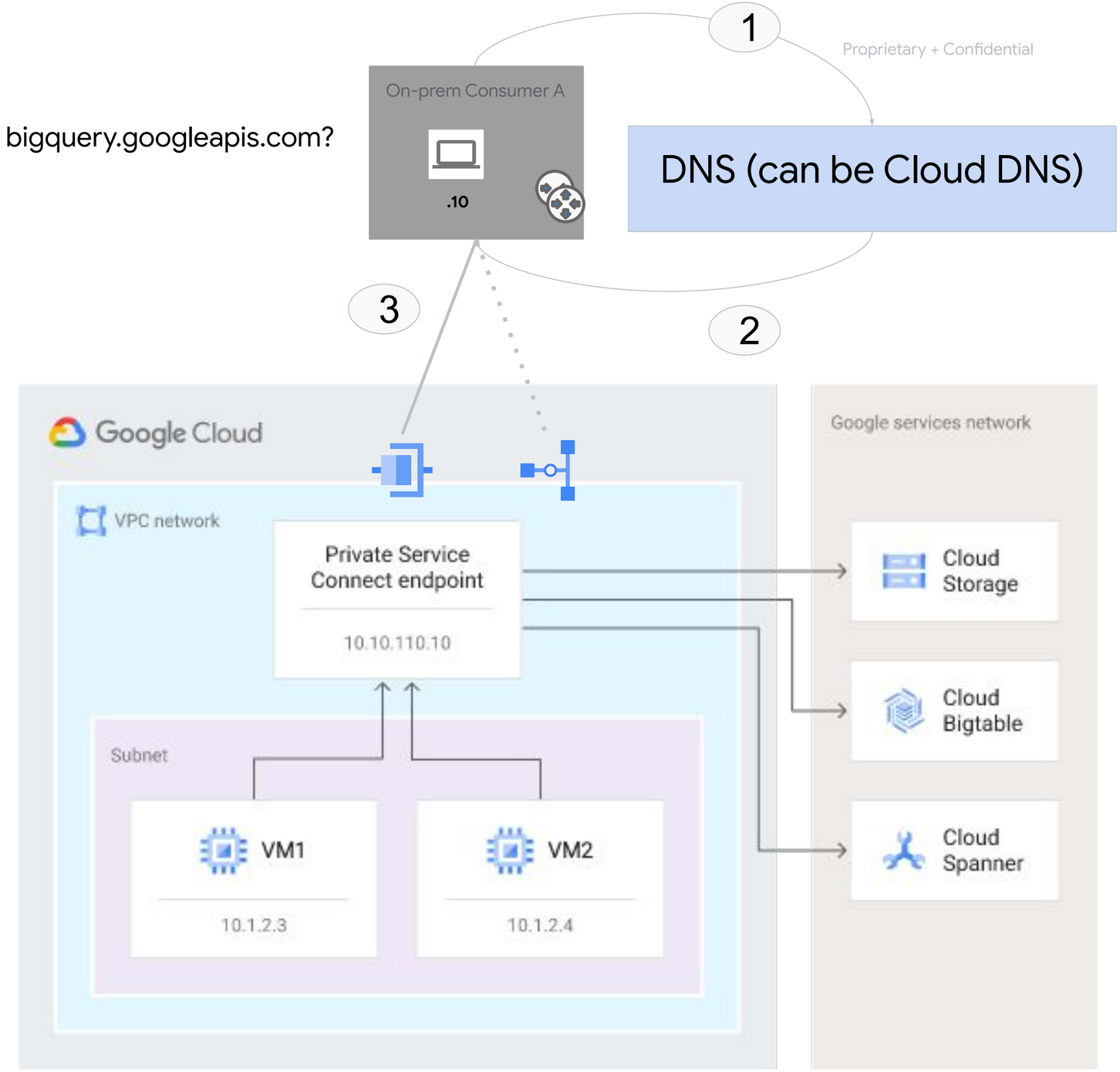
Multi-tenant Managed Services

Managed services which are consumed by multiple different consumers. Multiple PSC connections terminate on a single service attachment.

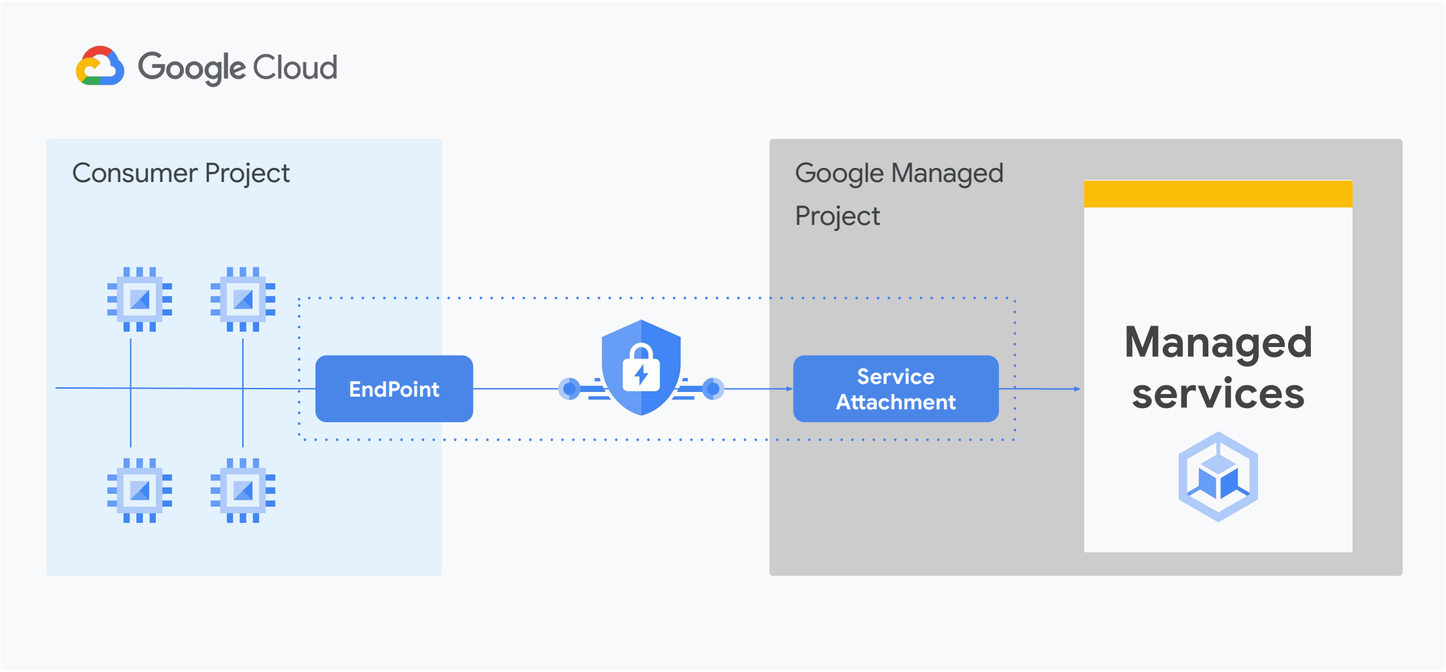


PSC for Google APIs

- Private endpoints IP addresses front-ending Google APIs
- Can be accessed from VPC and on-premises networks (via Interconnect/VPN)
    - Prior to PSC for Google APIs, if on-prem wanted to reach googleapis via IC or VPN, they needed to use (non publicly reachable) public IP ranges
- Enables using customer-defined private endpoints using *.p.googleapis.com
- Compatible with VPC Service Controls



PSC for Google Managed Services

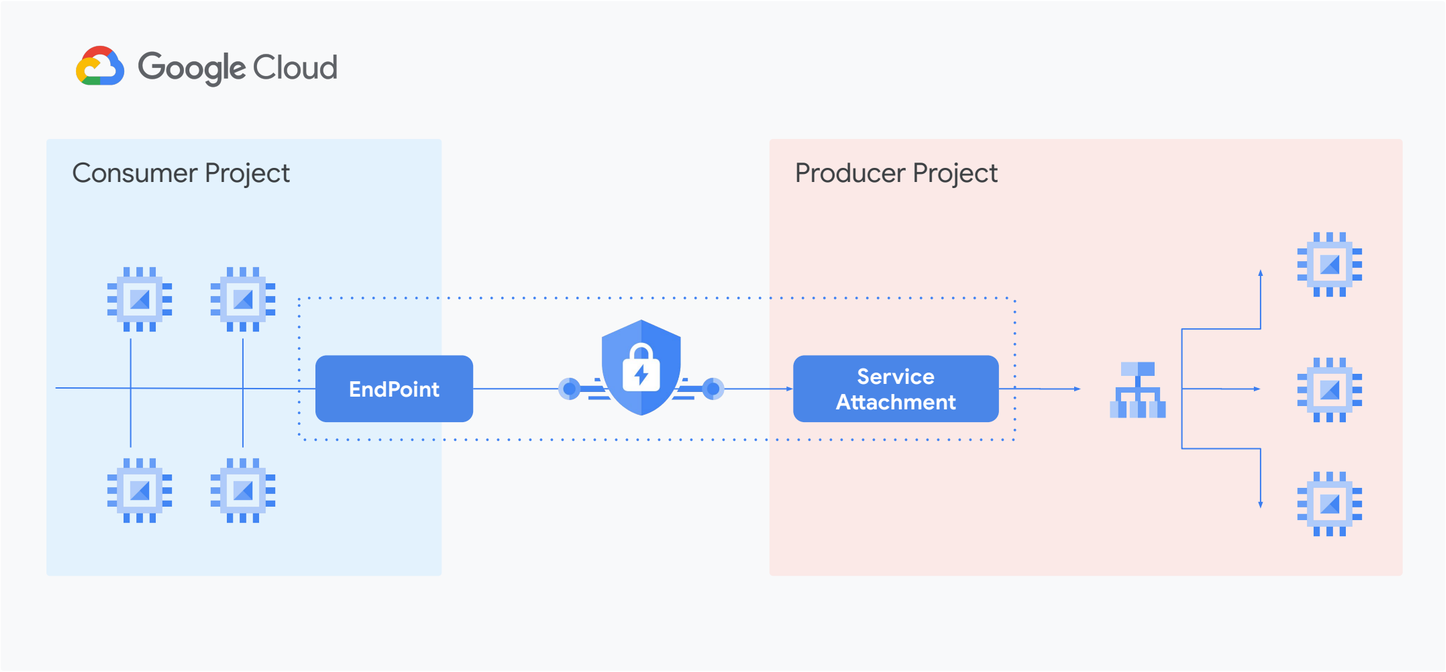


Consumer defines its own IP range for endpoint

Allows for access to some Google Managed services without the use of PSA or other VPC peering

Adoption based on a per product basis

PSC for Internal Load Balancing



Consumer defines its own IP range for endpoint

Allows for overlapping IP space between consumer and producer

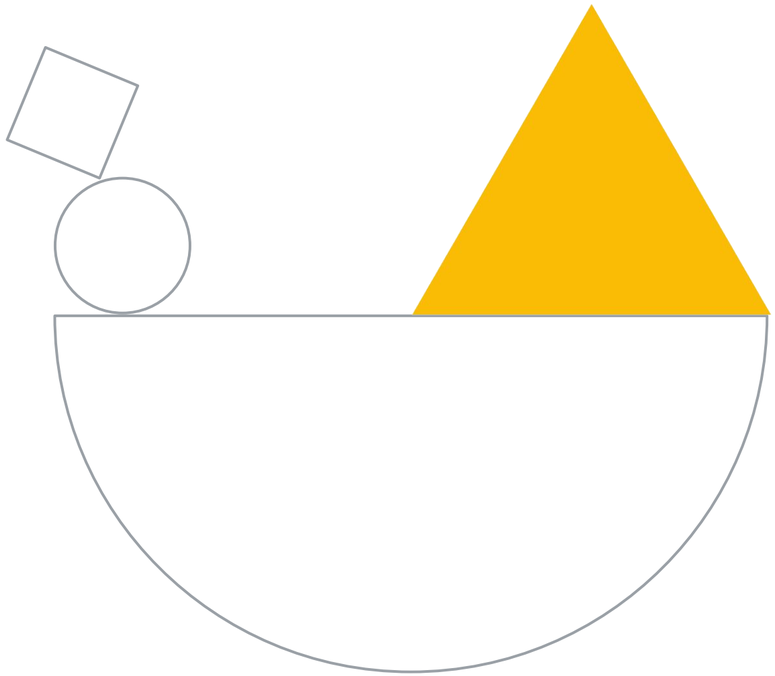
Producer resource is placed behind an Internal Load Balancer

Works across projects or organizations

Support for Single-Tenant and **Multi-Tenant Services**

Does not require VPC peering, VPN or Multi-NIC appliance

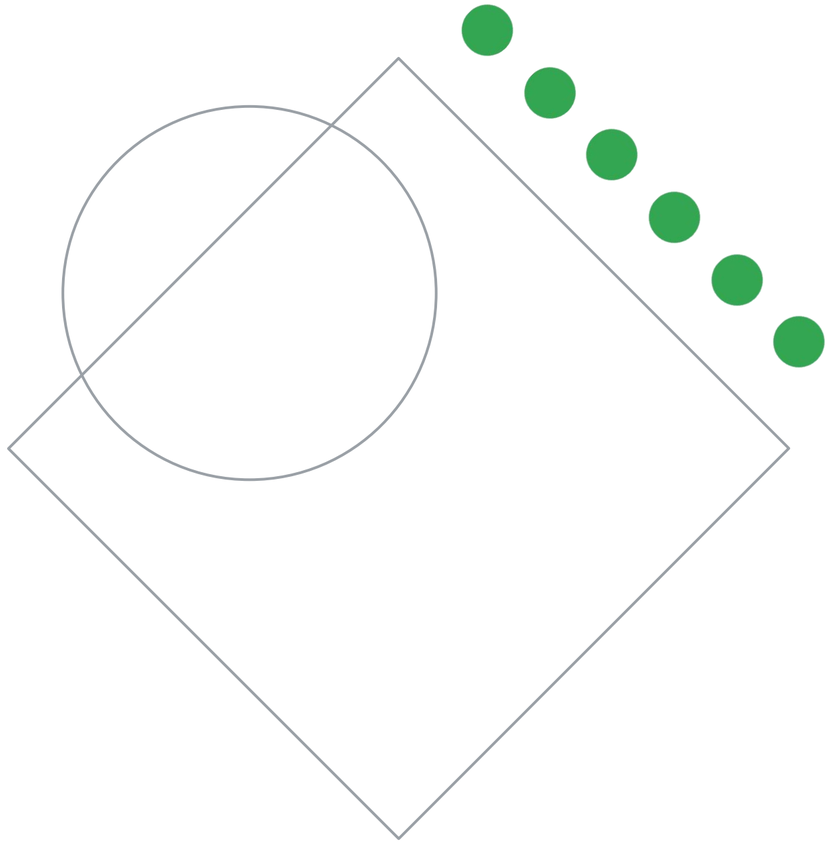
Diagnostic questions



Please complete the diagnostic questions now

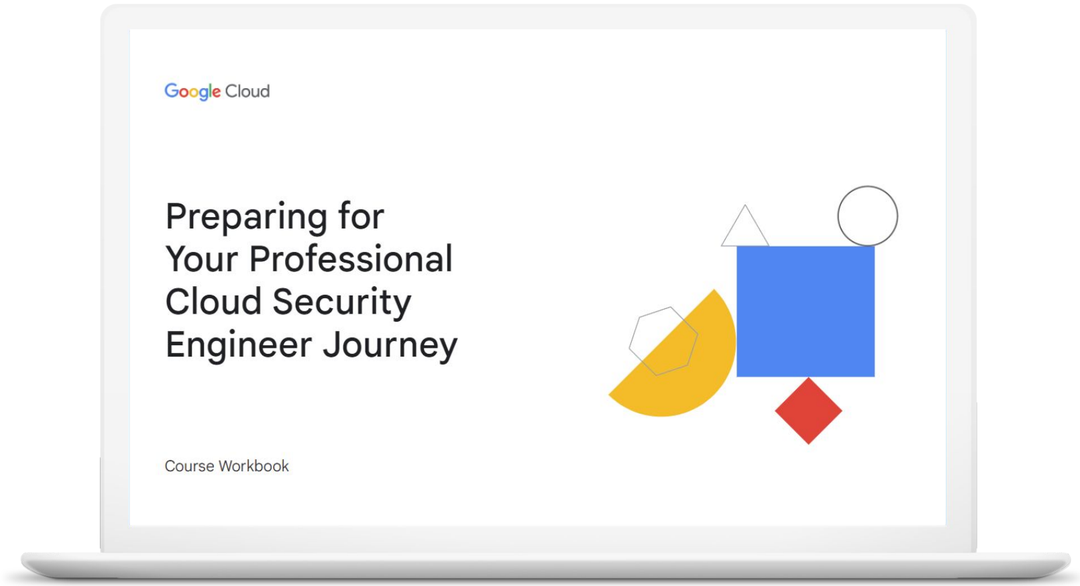
- Forms are provided for you to answer the diagnostic questions
- The instructor will provide you a link to the forms
- The diagnostic questions are also available in the workbook

Review and study planning



Your study plan:

Configuring network security



2.1 Designing network security

2.2 Configuring network segmentation

2.3 Establish private connectivity

2.1 Designing network security

Considerations include:

- Configuring network perimeter controls (firewall rules; Identity-Aware Proxy (IAP))
- Configuring load balancing (global, network, HTTP(S), SSL Proxy, and TCP Proxy load balancers)
- Identifying Domain Name System Security Extensions (DNSSEC)
- Identifying differences between private versus public addressing
- Configuring web application firewall (Google Cloud Armor)
- Configuring Cloud DNS

2.1 Diagnostic Question 01 Discussion

Cymbal Bank has published an API that internal teams will use through the HTTPS load balancer. You need to limit the API usage to 200 calls every hour. Any exceeding usage should inform the users that servers are busy.

Which gcloud command would you run to throttle the load balancing for the given specification?

A. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=throttle
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=allow
--exceed-action=deny-429
--enforce-on-key=HTTP-HEADER

B. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=throttle
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=60
--conform-action=deny
--exceed-action=deny-404
--enforce-on-key=HTTP-HEADER

C. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=rate-based-ban
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=deny
--exceed-action=deny-403
--enforce-on-key=HTTP-HEADER

D. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges="<source range>"
--action=rate-based-ban
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=allow
--exceed-action=deny-500
--enforce-on-key=IP

2.1 Diagnostic Question 01 Discussion

Cymbal Bank has published an API that internal teams will use through the HTTPS load balancer. You need to limit the API usage to 200 calls every hour. Any exceeding usage should inform the users that servers are busy.

Which gcloud command would you run to throttle the load balancing for the given specification?

A. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=throttle
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=allow
--exceed-action=deny-429
--enforce-on-key=HTTP-HEADER

B. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=throttle
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=60
--conform-action=deny
--exceed-action=deny-404
--enforce-on-key=HTTP-HEADER

C. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=rate-based-ban
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=deny
--exceed-action=deny-403
--enforce-on-key=HTTP-HEADER

D. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges="<source range>"
--action=rate-based-ban
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=allow
--exceed-action=deny-500
--enforce-on-key=IP

2.1 Diagnostic Question 02 Discussion

Cymbal Bank is releasing a new loan management application using a Compute Engine managed instance group. External users will connect to the application using a domain name or IP address protected with TLS 1.2. A load balancer already hosts this application and preserves the source IP address. You are tasked with setting up the SSL certificate for this load balancer.

What should you do?

A. Create a Google-managed SSL certificate. Attach a global dynamic external IP address to the internal HTTPS load balancer. Validate that an existing URL map will route the incoming service to your managed instance group backend. Load your certificate and create an HTTPS proxy routing to your URL map. Create a global forwarding rule that routes incoming requests to the proxy.

B. Create a Google-managed SSL certificate. Attach a global static external IP address to the external HTTPS load balancer. Validate that an existing URL map will route the incoming service to your managed instance group backend. Load your certificate and create an HTTPS proxy routing to your URL map. Create a global forwarding rule that routes incoming requests to the proxy.

C. Import a self-managed SSL certificate. Attach a global static external IP address to the TCP Proxy load balancer. Validate that an existing URL map will route the incoming service to your managed instance group backend. Load your certificate and create a TCP proxy routing to your URL map. Create a global forwarding rule that routes incoming requests to the proxy.

D. Import a self-managed SSL certificate. Attach a global static external IP address to the SSL Proxy load balancer. Validate that an existing URL map will route the incoming service to your managed instance group backend. Load your certificate and create an SSL proxy routing to your URL map. Create a global forwarding rule that routes incoming requests to the proxy.

2.1 Diagnostic Question 02 Discussion

Cymbal Bank is releasing a new loan management application using a Compute Engine managed instance group. External users will connect to the application using a domain name or IP address protected with TLS 1.2. A load balancer already hosts this application and preserves the source IP address. You are tasked with setting up the SSL certificate for this load balancer.

What should you do?

A. Create a Google-managed SSL certificate. Attach a global dynamic external IP address to the internal HTTPS load balancer. Validate that an existing URL map will route the incoming service to your managed instance group backend. Load your certificate and create an HTTPS proxy routing to your URL map. Create a global forwarding rule that routes incoming requests to the proxy.

B. Create a Google-managed SSL certificate. Attach a global static external IP address to the external HTTPS load balancer. Validate that an existing URL map will route the incoming service to your managed instance group backend. Load your certificate and create an HTTPS proxy routing to your URL map. Create a global forwarding rule that routes incoming requests to the proxy.

C. Import a self-managed SSL certificate. Attach a global static external IP address to the TCP Proxy load balancer. Validate that an existing URL map will route the incoming service to your managed instance group backend. Load your certificate and create a TCP proxy routing to your URL map. Create a global forwarding rule that routes incoming requests to the proxy.

D. Import a self-managed SSL certificate. Attach a global static external IP address to the SSL Proxy load balancer. Validate that an existing URL map will route the incoming service to your managed instance group backend. Load your certificate and create an SSL proxy routing to your URL map. Create a global forwarding rule that routes incoming requests to the proxy.

2.1 Diagnostic Question 03 Discussion

Your organization has a website running on Compute Engine. This instance only has a private IP address. You need to provide SSH access to an on-premises developer who will debug the website from the authorized on-premises location only.

How do you enable this?

A. Set up Cloud VPN. Set up an unencrypted tunnel to one of the hosts in the network. Create outbound or egress firewall rules. Use the private IP address to log in using a gcloud ssh command.

B. Use SOCKS proxy over SSH. Set up an SSH tunnel to one of the hosts in the network. Create the SOCKS proxy on the client side.

C. Use the default VPC's firewall. Open port 22 for TCP protocol using the Google Cloud Console.

D. Use Identity-Aware Proxy (IAP). Set up IAP TCP forwarding by creating ingress firewall rules on port 22 for TCP using the gcloud command.

2.1 Diagnostic Question 03 Discussion

Your organization has a website running on Compute Engine. This instance only has a private IP address. You need to provide SSH access to an on-premises developer who will debug the website from the authorized on-premises location only.

How do you enable this?

A. Set up Cloud VPN. Set up an unencrypted tunnel to one of the hosts in the network. Create outbound or egress firewall rules. Use the private IP address to log in using a gcloud ssh command.

B. Use SOCKS proxy over SSH. Set up an SSH tunnel to one of the hosts in the network. Create the SOCKS proxy on the client side.

C. Use the default VPC's firewall. Open port 22 for TCP protocol using the Google Cloud Console.

D. Use Identity-Aware Proxy (IAP). Set up IAP TCP forwarding by creating ingress firewall rules on port 22 for TCP using the gcloud command.

2.1 Designing network security

Courses

Networking in Google Cloud

- M2 Controlling Access to VPC Networks
- M4 Load balancing

Security in Google Cloud

- M4 Configuring VPC for Isolation and Security
- M7 Application Security: Techniques and Best Practices
- M9 Protecting Against DDoS Attacks

Networking in Google Cloud: Defining and implementing networks

- M2 Controlling Access to VPC Networks
- M4 Load balancing

Managing Security in Google Cloud

- M4 Configuring VPC for Isolation and Security

Security Best Practices in Google Cloud

- M3 Application Security: Techniques and Best Practices

Mitigating Security Vulnerabilities in Google Cloud

- M1 Protecting Against DDoS Attacks

Skill Badges

Google Cloud

Build and Secure Networks in Google Cloud Quest

Google Cloud

Ensure Access and Identity in Google Cloud Quest

Documentation

gcloud compute security-policies rules update | Cloud SDK Documentation

gcloud compute security-policies | Cloud SDK Documentation

Setting up an global external HTTP(S) load balancer (classic) with a Compute Engine backend | Load Balancing | Google Cloud

Using Google-managed SSL certificates | Load Balancing

Using IAP for TCP forwarding | Identity-Aware Proxy | Google Cloud

Securely connecting to VM instances | Compute Engine Documentation | Google Cloud

2.2 Configuring network segmentation

Considerations include:

- Configuring security properties of a VPC Network, VPC Peering, Shared VPC, and Firewall Rules
- Configuring network isolation and data encapsulation for N tier application design
- Configuring app-to-app security policy

2.2 Diagnostic Question 04 Discussion

Cymbal Bank has two engineering teams (T1 and T2) working on two different Projects (P1 and P2). Both P1 and P2 use custom VPCs. T2 needs to request and verify DNS records for T1's domain that are internal to P1's Compute Engine Instance. After the records are verified, T2 will access and look up more records in this Compute Engine Instance.

How would you enable the lookup access to ensure that the requests are always authenticated and are protected against exfiltration?

A. Create a forwarding zone with P1 and P2's VPCs in the VPC network list. Add P2's IP addresses in the private forwarding targets list. Then enable DNSSEC with `gcloud dns managed-zones update zone-name -dnssec-state` on.

B. Create a peering zone. Set P1 as producer network and P2 as consumer network. Then enable DNSSEC with `gcloud dns managed-zones update zone-name -dnssec-state` on.

C. Create a managed reverse lookup private zone with P1 and P2's VPCs in the VPC network list. Keep visibility as private. Add the required domain names in dns-names while creating the managed zone.

D. Create a cross-project binding zone by creating a private zone with the URL of P2's VPC network. Then enable DNSSEC with `gcloud dns managed-zones update zone-name -dnssec-state` on.

2.2 Diagnostic Question 04 Discussion

Cymbal Bank has two engineering teams (T1 and T2) working on two different Projects (P1 and P2). Both P1 and P2 use custom VPCs. T2 needs to request and verify DNS records for T1's domain that are internal to P1's Compute Engine Instance. After the records are verified, T2 will access and look up more records in this Compute Engine Instance.

How would you enable the lookup access to ensure that the requests are always authenticated and are protected against exfiltration?

A. Create a forwarding zone with P1 and P2's VPCs in the VPC network list. Add P2's IP addresses in the private forwarding targets list. Then enable DNSSEC with `gcloud dns managed-zones update zone-name -dnssec-state` on.

B. Create a peering zone. Set P1 as producer network and P2 as consumer network. Then enable DNSSEC with `gcloud dns managed-zones update zone-name -dnssec-state` on.

C. Create a managed reverse lookup private zone with P1 and P2's VPCs in the VPC network list. Keep visibility as private. Add the required domain names in dns-names while creating the managed zone.

D. Create a cross-project binding zone by creating a private zone with the URL of P2's VPC network. Then enable DNSSEC with `gcloud dns managed-zones update zone-name -dnssec-state` on.

2.2 Diagnostic Question 05 Discussion

Cymbal Bank needs to connect its employee MongoDB database to a new human resources web application on the same network. Both the database and the application are autoscaled with the help of Instance templates. As the Security Administrator and Project Editor, you have been tasked with allowing the application to read port 27017 on the database.

What should you do?

A. Create service accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow TCP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-service-account

A. Create service accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow ICMP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-service-account

A. Create a user account for the database admin and a service account for the application. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow TCP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-admin-user-account

A. Create user accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--deny UDP:27017
--source-service-accounts web-application-user-account
--target-service-accounts database-admin-user-account

2.2 Diagnostic Question 05 Discussion

Cymbal Bank needs to connect its employee MongoDB database to a new human resources web application on the same network. Both the database and the application are autoscaled with the help of Instance templates. As the Security Administrator and Project Editor, you have been tasked with allowing the application to read port 27017 on the database.

What should you do?

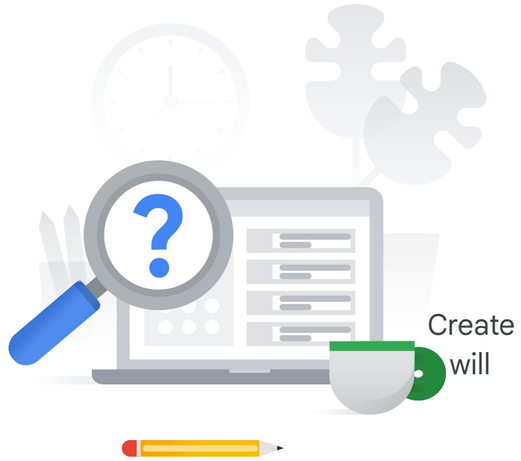
A. Create service accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow TCP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-service-account

A. Create service accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow ICMP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-service-account

A. Create a user account for the database admin and a service account for the application. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow TCP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-admin-user-account

A. Create user accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--deny UDP:27017
--source-service-accounts web-application-user-account
--target-service-accounts database-admin-user-account

2.2 Diagnostic Question 06 Discussion



Cymbal Bank has designed an application to detect credit card fraud that will analyze sensitive information. The application that's running on a Compute Engine instance is hosted in a new subnet on an existing VPC. Multiple teams who have access to other VMs in the same VPC must access the VM. You want to configure the access so that unauthorized VMs or users from the internet can't access the fraud detection VM.

What should you do?

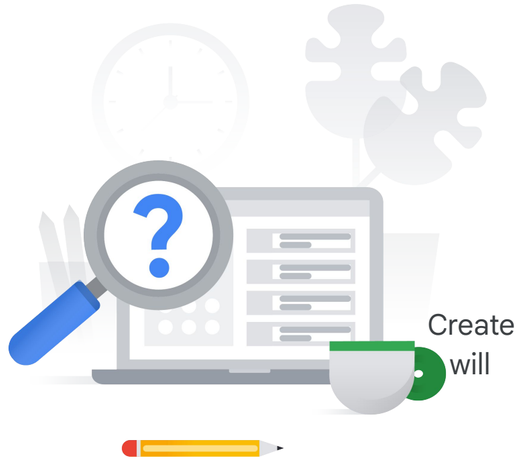
A. Use subnet isolation. Create a service account for the fraud detection VM. Create one service account for all the teams' Compute Engine instances that will access the fraud detection VM. Create a new firewall rule using:
gcloud compute firewall-rules create ACCESS_FRAUD_ENGINE
--network <network name>
--allow TCP:80
--source-service-accounts <one service account for all teams>
--target-service-accounts <fraud detection engine's service account>

B. Use target filtering. Create two tags called 'app' and 'data'. Assign the 'app' tag to the Compute Engine instance hosting the Fraud Detection App (source), and assign the 'data' tag to the other Compute Engine instances (target). Create a firewall rule to allow all ingress communication on this tag.

C. Use subnet isolation. Create a service account for the fraud detection engine. Create service accounts for each of the teams' Compute Engine instances that will access the engine. Add a firewall rule using:
gcloud compute firewall-rules create ACCESS_FRAUD_ENGINE
--network <network name>
--allow TCP:80
--source-service-accounts <list of service accounts>
--target-service-accounts <fraud detection engine's service account>

D. Use target filtering. Create a tag called 'app', and assign the tag to both the source and the target. Create a firewall rule to allow all ingress communication on this tag.

2.2 Diagnostic Question 06 Discussion



Cymbal Bank has designed an application to detect credit card fraud that will analyze sensitive information. The application that's running on a Compute Engine instance is hosted in a new subnet on an existing VPC. Multiple teams who have access to other VMs in the same VPC must access the VM. You want to configure the access so that unauthorized VMs or users from the internet can't access the fraud detection VM.

What should you do?

A. Use subnet isolation. Create a service account for the fraud detection VM. Create one service account for all the teams' Compute Engine instances that will access the fraud detection VM. Create a new firewall rule using:
gcloud compute firewall-rules create ACCESS_FRAUD_ENGINE
--network <network name>
--allow TCP:80
--source-service-accounts <one service account for all teams>
--target-service-accounts <fraud detection engine's service account>

B. Use target filtering. Create two tags called 'app' and 'data'. Assign the 'app' tag to the Compute Engine instance hosting the Fraud Detection App (source), and assign the 'data' tag to the other Compute Engine instances (target). Create a firewall rule to allow all ingress communication on this tag.

C. Use subnet isolation. Create a service account for the fraud detection engine. Create service accounts for each of the teams' Compute Engine instances that will access the engine. Add a firewall rule using:
gcloud compute firewall-rules create ACCESS_FRAUD_ENGINE
--network <network name>
--allow TCP:80
--source-service-accounts <list of service accounts>
--target-service-accounts <fraud detection engine's service account>

D. Use target filtering. Create a tag called 'app', and assign the tag to both the source and the target. Create a firewall rule to allow all ingress communication on this tag.

2.2 Configuring network segmentation

Courses

[Networking in Google Cloud]

- M2 Controlling Access to VPC Networks

[Security in Google Cloud]

- M4 Configuring VPC for Isolation and Security

[Networking in Google Cloud: Defining and implementing networks]

- M2 Controlling Access to VPC Networks

[Managing Security in Google Cloud]

- M4 Configuring VPC for Isolation and Security

Skill Badges

Google Cloud

Build and Secure Networks in Google Cloud Quest

Documentation

DNS zones overview | Google Cloud

Using firewall rules | VPC | Google Cloud

Best practices and reference architectures for VPC design

Best practices and reference architectures for VPC design

Best practices for securing service accounts | Cloud IAM Documentation

2.3 Establishing private connectivity

Considerations include:

- Designing and configuring private RFC1918 connectivity between VPC networks and Google Cloud Projects (Shared VPC, VPC Peering)
- Designing and configuring private RFC1918 connectivity between data centers and VPC network (IPSEC and Cloud Interconnect)
- Establishing private connectivity between VPC and Google APIs (Private Google Access, Private Google Access for on-premise hosts, Private Services Access)
- Configuring Cloud NAT

2.3 Diagnostic Question 07 Discussion

The data from Cymbal Bank's loan applicants resides in a shared VPC. A credit analysis team uses a CRM tool hosted in the App Engine standard environment. You need to provide credit analysts with access to this data. You want the charges to be incurred by the credit analysis team.

What should you do?

A. Add egress firewall rules to allow TCP and UDP ports for the App Engine standard environment in the Shared VPC network. Create either a client-side connector in the Service Project or a server-side connector in the Host Project using the IP Range or Project ID of the target VPC. Verify that the connector is in a READY state. Create an egress rule on the Shared VPC network to allow the connector using Network Tags or IP ranges.

B. Add egress firewall rules to allow SSH and/or RDP ports for the App Engine standard environment in the Shared VPC network. Create a client-side connector in the Service Project using the IP range of the target VPC. Verify that the connector is in a READY state. Create an egress rule on the Shared VPC network to allow the connector using Network Tags or IP ranges.

C. Add ingress firewall rules to allow NAT and Health Check ranges for the App Engine standard environment in the Shared VPC network. Create a client-side connector in the Service Project using the Shared VPC Project ID. Verify that the connector is in a READY state. Create an ingress rule on the Shared VPC network to allow the connector using Network Tags or IP ranges.

D. Add ingress firewall rules to allow NAT and Health Check ranges for App Engine standard environment in the Shared VPC network. Create a server-side connector in the Host Project using the Shared VPC Project ID. Verify that the connector is in a READY state. Create an ingress rule on the Shared VPC network to allow the connector using Network Tags or IP ranges.

2.3 Diagnostic Question 07 Discussion

The data from Cymbal Bank's loan applicants resides in a shared VPC. A credit analysis team uses a CRM tool hosted in the App Engine standard environment. You need to provide credit analysts with access to this data. You want the charges to be incurred by the credit analysis team.

What should you do?

A. Add egress firewall rules to allow TCP and UDP ports for the App Engine standard environment in the Shared VPC network. Create either a client-side connector in the Service Project or a server-side connector in the Host Project using the IP Range or Project ID of the target VPC. Verify that the connector is in a READY state. Create an egress rule on the Shared VPC network to allow the connector using Network Tags or IP ranges.

B. Add egress firewall rules to allow SSH and/or RDP ports for the App Engine standard environment in the Shared VPC network. Create a client-side connector in the Service Project using the IP range of the target VPC. Verify that the connector is in a READY state. Create an egress rule on the Shared VPC network to allow the connector using Network Tags or IP ranges.

C. Add ingress firewall rules to allow NAT and Health Check ranges for the App Engine standard environment in the Shared VPC network. Create a client-side connector in the Service Project using the Shared VPC Project ID. Verify that the connector is in a READY state. Create an ingress rule on the Shared VPC network to allow the connector using Network Tags or IP ranges.

D. Add ingress firewall rules to allow NAT and Health Check ranges for App Engine standard environment in the Shared VPC network. Create a server-side connector in the Host Project using the Shared VPC Project ID. Verify that the connector is in a READY state. Create an ingress rule on the Shared VPC network to allow the connector using Network Tags or IP ranges.

2.3 Diagnostic Question 08 Discussion

Cymbal Bank's Customer Details API runs on a Compute Engine instance with only an internal IP address. Cymbal Bank's new branch is co-located outside the Google Cloud points-of-presence (PoPs) and requires a low-latency way for its on-premises apps to consume the API without exposing the requests to the public internet.

Which solution would you recommend?

A. Use a Content Delivery Network (CDN). Establish direct peering with one of Google's nearby edge-enabled PoPs.

B. Use Carrier Peering. Use a service provider to access their enterprise grade infrastructure to connect to the Google Cloud environment.

C. Use Partner Interconnect. Use a service provider to access their enterprise grade infrastructure to connect to the Google Cloud environment.

D. Use Dedicated Interconnect. Establish direct peering with one of Google's nearby edge-enabled PoPs.

2.3 Diagnostic Question 08 Discussion

Cymbal Bank's Customer Details API runs on a Compute Engine instance with only an internal IP address. Cymbal Bank's new branch is co-located outside the Google Cloud points-of-presence (PoPs) and requires a low-latency way for its on-premises apps to consume the API without exposing the requests to the public internet.

Which solution would you recommend?

A. Use a Content Delivery Network (CDN). Establish direct peering with one of Google's nearby edge-enabled PoPs.

B. Use Carrier Peering. Use a service provider to access their enterprise grade infrastructure to connect to the Google Cloud environment.

C. Use Partner Interconnect. Use a service provider to access their enterprise grade infrastructure to connect to the Google Cloud environment.

D. Use Dedicated Interconnect. Establish direct peering with one of Google's nearby edge-enabled PoPs.

2.3 Diagnostic Question 9 Discussion

An external audit agency needs to perform a one-time review of Cymbal Bank's Google Cloud usage. The auditors should be able to access a Default VPC containing BigQuery, Cloud Storage, and Compute Engine instances where all the usage information is stored. You have been tasked with enabling the access from their on-premises environment, which already has a configured VPN.

What should you do?

A. Use a Cloud VPN tunnel. Use your DNS provider to create DNS zones and records for private.googleapis.com. Connect the DNS provider to your on-premises network. Broadcast the request from the on-premises environment. Use a software-defined firewall to manage incoming and outgoing requests.

B. Use Partner Interconnect. Configure an encrypted tunnel in the auditor's on-premises environment. Use Cloud DNS to create DNS zones and A records for private.googleapis.com.

C. Use a Cloud VPN tunnel. Use Cloud DNS to create DNS zones and records for *.googleapis.com. Set up on-premises routing with Cloud Router. Use Cloud Router custom route advertisements to announce routes for Google Cloud destinations.

D. Use Direct Interconnect. Configure a VLAN in the auditor's on-premises environment. Use Cloud DNS to create DNS zones and records for restricted.googleapis.com and private.googleapis.com. Set up on-premises routing with Cloud Router. Add custom static routes in the VPC to connect individually to BigQuery, Cloud Storage, and Compute Engine instances.

2.3 Diagnostic Question 9 Discussion

An external audit agency needs to perform a one-time review of Cymbal Bank's Google Cloud usage. The auditors should be able to access a Default VPC containing BigQuery, Cloud Storage, and Compute Engine instances where all the usage information is stored. You have been tasked with enabling the access from their on-premises environment, which already has a configured VPN.

What should you do?

A. Use a Cloud VPN tunnel. Use your DNS provider to create DNS zones and records for private.googleapis.com. Connect the DNS provider to your on-premises network. Broadcast the request from the on-premises environment. Use a software-defined firewall to manage incoming and outgoing requests.

B. Use Partner Interconnect. Configure an encrypted tunnel in the auditor's on-premises environment. Use Cloud DNS to create DNS zones and A records for private.googleapis.com.

C. Use a Cloud VPN tunnel. Use Cloud DNS to create DNS zones and records for *.googleapis.com. Set up on-premises routing with Cloud Router. Use Cloud Router custom route advertisements to announce routes for Google Cloud destinations.

D. Use Direct Interconnect. Configure a VLAN in the auditor's on-premises environment. Use Cloud DNS to create DNS zones and records for restricted.googleapis.com and private.googleapis.com. Set up on-premises routing with Cloud Router. Add custom static routes in the VPC to connect individually to BigQuery, Cloud Storage, and Compute Engine instances.

2.3 Establish private connectivity

Courses

[Networking in Google Cloud](#)

- M5 Hybrid Connectivity
- M7 Network Design and Deployment

[Security in Google Cloud](#)

- M4 Configuring VPC for Isolation and Security
- M5 Securing Compute Engine: Techniques and Best Practices

[Networking in Google Cloud: Hybrid Connectivity and Network Management](#)

- M1 Hybrid Connectivity
- M3 Network Design and Deployment

[Managing Security in Google Cloud](#)

- M4 Configuring VPC for Isolation and Security

[Security Best Practices in Google Cloud](#)

- M1 Securing Compute Engine: Techniques and Best Practices

Skill Badges

Google Cloud

[Build and Secure Networks in Google Cloud Quest](#)

Google Cloud

[Ensure Access and Identity in Google Cloud Quest](#)

Documentation

[Configuring Serverless VPC Access | Google Cloud](#)

[Overview of VPC Service Controls | Google Cloud](#)

[Choosing a Network Connectivity product | Google Cloud](#)

[Private Google Access | VPC](#)

[Manage zones | Cloud DNS](#)

[Private Google Access for on-premises hosts | VPC](#)

[Simplifying cloud networking for enterprises: announcing Cloud NAT and more | Google Cloud Blog](#)

[Example GKE setup | Cloud NAT](#)

[Cloud NAT overview](#)

Knowledge Check 1

Which tool will Cymbal Bank use to enforce authentication and authorization for services deployed to Google Cloud?

A. Identity-aware proxy

B. HTTP(S) Load balancer

C. Cloud Armor

D. Firewall rules

Knowledge Check 1

Which tool will Cymbal Bank use to enforce authentication and authorization for services deployed to Google Cloud?

A. Identity-aware proxy

B. HTTP(S) Load balancer

C. Cloud Armor

D. Firewall rules

Knowledge Check 2

How will Cymbal Bank enable resources with only internal IP addresses to make requests to the Internet?

A. Shared VPC

B. Google private access

C. Dedicated Interconnect

D. Cloud NAT

Knowledge Check 2

How will Cymbal Bank enable resources with only internal IP addresses to make requests to the Internet?

A. Shared VPC

B. Google private access

C. Dedicated Interconnect

D. Cloud NAT

Additional content

QUIZ week 2

(the one we went through during the meeting)

Reminder:

- NOT as complex as questions on the exam
- Technical knowledge validation (No business context)

Additional content 1

[READING]

- VPC network overview - Security properties of a VPC network, VPC peering, shared VPC, and firewall rules
- Best practices and reference architectures for VPC design - Network isolation and data encapsulation for N tier application design
- DNS Security Extensions (DNSSEC) overview - Use of DNSSEC
- Manage DNSSEC configuration (especially focus on migrating DNSSEC-signed zones to Cloud DNS)
- Cloud Armor overview - Tip: know which Load Balancers are supported by Cloud Armor; know preview mode
- VPC firewall rules overview
- Identity-Aware Proxy overview
- IAP for on-premises apps
- Hierarchical firewall policies overview - that's another "policy" topic, but it's NOT related to IAM Policies or Organization Policies
- Choosing a load balancer
- Load balancer features - don't try to memorize all, but rather know high-level of most important ones only (proxy/pass-through, protocols, session affinity, security)
- Shared VPC overview
- VPC Network Peering overview
- Choosing a Network Connectivity product

Additional content 2

- Private access options for services - overview of different options to reach GCP APIs and managed services
  a. Private Google Access:
     i. Private Google Access - overview
     ii. Configuring Private Google Access - differenciate between private.googleapis.com and restricted.googleapis.com!
  b. Private Services Access
     i. Private services access - overview
     ii. Configuring private services access
  c. [new service] Private Service Connect, which solves some difficulties (mainly: non-transitivity of VPC Peering for managed services)
     i. Private Service Connect - overview
     ii. How to publish managed services using Private Service Connect
     iii. How to access managed services using Private Service Connect
  d. Serverless VPC Access
     i. How to access VPC resources from serverless services?
     ii. How to configure Serverless VPC Access
- Cloud NAT overview - with special focus on NAT subnet IP ranges and NAT rules.
- [IMPORTANT] VPC Service Controls. What is a service perimeter and perimeter bridge.

Additional content 3

[VIDEOS]

- Great demo of how to centralize network management and set up Shared VPC in GCP: Level Up From Zero Episode 4: Shared VPC
- Private Service Connect (new service that might solve issues with transitivity when Private Google Access / Private Service Access is being used): What is Private Service Connect?
- IAP as a way to control access to your internal apps (most real IAP use-cases in a single video!): Centralize access to your organization's websites with Identity Aware Proxy (IAP)
- If IAP is not granular enough and application-based auth is needed, you can use GCP Identity Platform Learn to add authentication and identity management to your own apps
- How do I protect my applications from DDoS attacks with Google Cloud Armor?
- Learn about Serverless VPC Connector: Connecting to private GCE instances
- Learn to isolate containerized workloads with Google Cloud - Superb video explaining GKE Sandbox in 5 mins
- How do I provide organizational wide security control using Hierarchical Firewall Policies

[PODCASTS]

- Preparing for Cloud Migrations from a CISO Perspective, Part 2
- Scaling Google Kubernetes Engine Security

BONUS CONTENT: Cloud DNS *

* if you want to understand Cloud DNS better. It’s more related to Network Engineer exam, but with PCSE, you might still get 1 or 2 questions where you should differentiate between different options Cloud DNS gives you.

Quick Overview of DNS Terminology*

These are common terms used in discussing DNS, not just at Google

Recursive Resolver
Acts as a middleman between a client and a DNS name server

Name Server
A computer designated to translate domain names into IP addresses

A/AAAA Records
Records that map a host to an IP address either IPv4 (A) or IPv6 (AAAA)

PTR Record
Opposite of A/AAAA record, used to map an IP address to an associated name

CNAME
Define an alias for canonical name for your server (one defined by an A or AAAA record)

Zone File
Zone files are the way that name servers store information about the domains they know about

Registrar
Organization that manages the reservation of Internet domain names. A registrar must be accredited by a generic top-level domain (gTLD) registry or a country code top-level domain (ccTLD) registry.

Google Cloud

*More terminology can be found in RFC7719 documentation

DNS Primer

How DNS Works (overly simplified)

Step 1
A client makes DNS request

Step 2
Recursive resolver responds to request

OR

Step 2
Recursive resolver redirects request to other servers

Step 3
Other server responds to request

Step 4
Information is sent to client

Google Cloud

DNS options

An internal metadata server acts as DNS resolver, and is automatically set as such as part of DHCP leases.

Internal DNS

Records are automatically created for VMs primary and internal IP's with the following FQDN:

- [INSTANCE_NAME].[ZONE].c.[PROJECT_ID].internal

Used for resolution within the same project and VPC

Cloud DNS

Scalable, reliable (**100% SLA**), and managed authoritative DNS service for public and private records offering

Private: Used for providing a namespace that is only visible inside the VPC

Public: Used for providing authoritative DNS resolution to clients on the public internet.

Public vs Private DNS Zone

Private Zone

- Used for providing a namespace that is only visible inside the VPC or hybrid network environment.
- Example - a business organization has a domain dev.gcp.example.com, reachable only from within the company intranet.

Public Zone

- Used for providing authoritative DNS resolution to clients on the public internet.
- Example - a business has an external website, example.com accessible directly from the Internet.
- Not to be confused with Google Public DNS (8.8.8.8) which is just a public recursive resolver

Google Cloud

DNS Forwarding

What it is

DNS forwarding is the process by which particular sets of DNS queries are handled by a designated server, rather than being handled by the initial server contacted by the client.

How is it setup

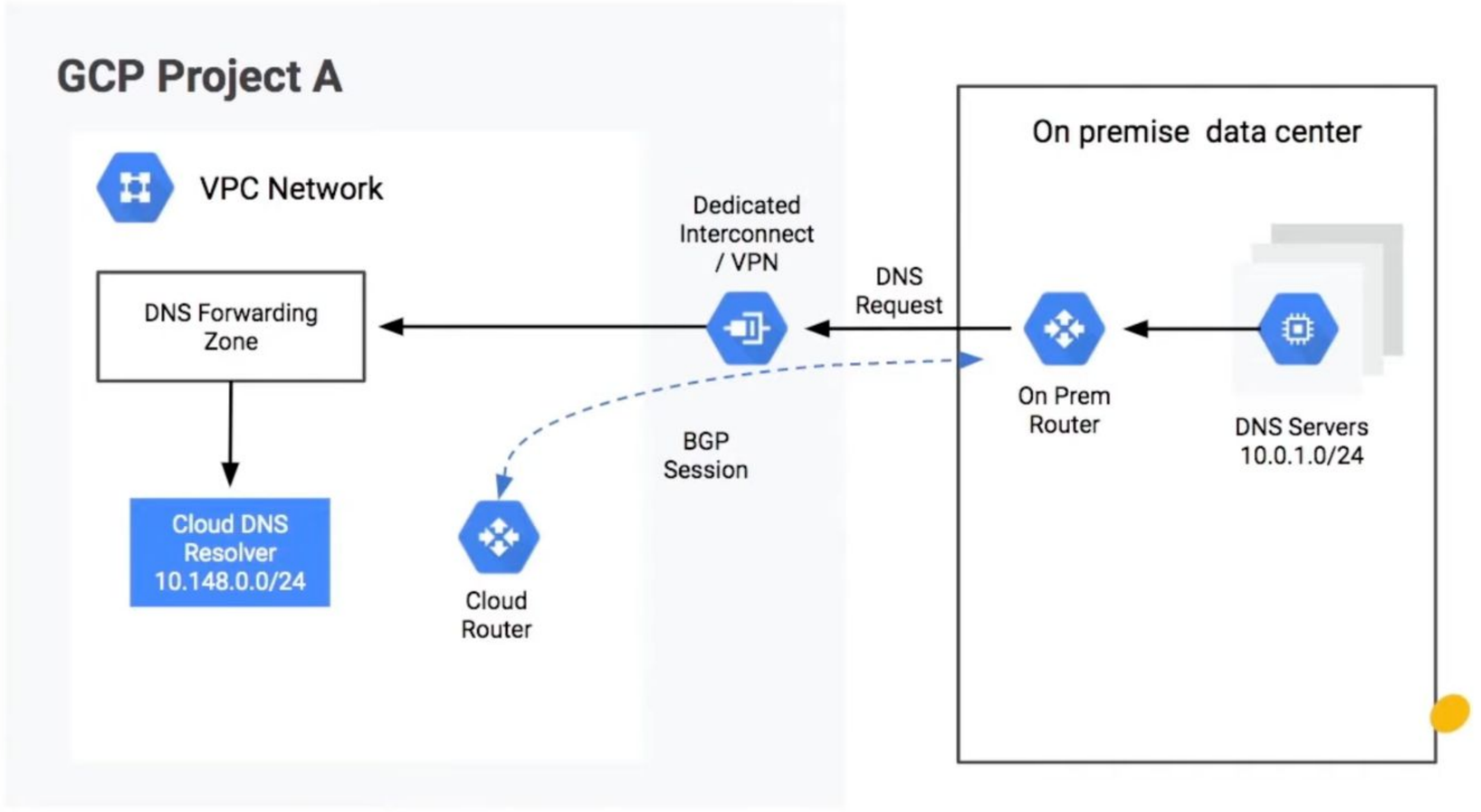
Two types of DNS forwarding

- Outbound zone: from GCP to on-prem
- Inbound policy: from on-prem to GCP

Notes and Caveats on DNS Forwarding

- Cannot setup forwarding to another VPC, must involve on-prem environment as either the source or destination.
- Uses Google proxies (35.199.192.0/19 block) for all outbound forwarding (note, while this is a public IP block, it is not routed publically on the Internet, and only used within GCP Cloud environments).

DNS Inbound Forwarding Architecture*



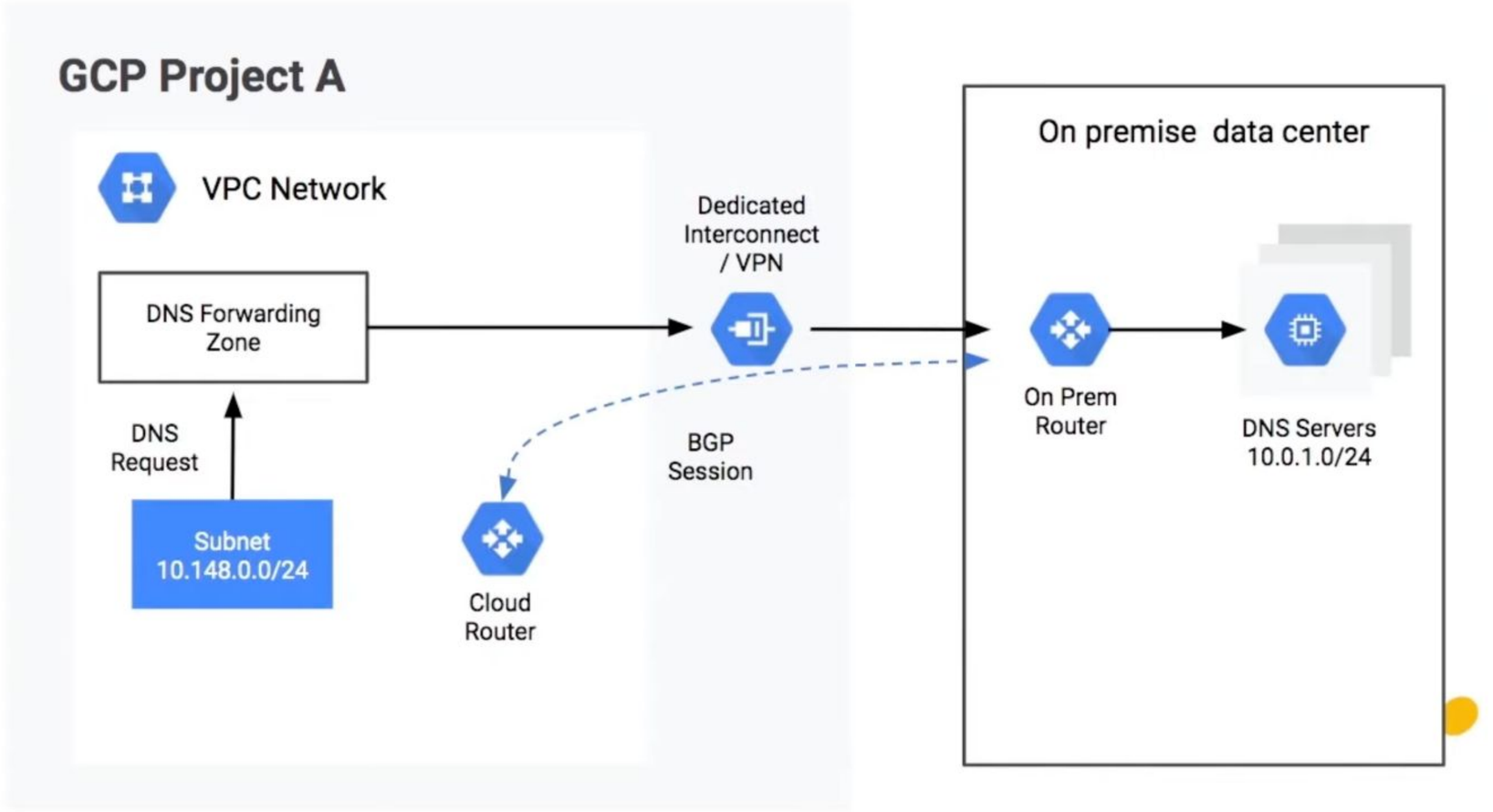
Configuration Notes

- Setup DNS Policy for Inbound Forwarding
- Obtain IP address established for inbound forwarding
- Google CR should be learning 10.0.1.0/24 route from on prem router
- Verify no firewall rules are blocking the 10.148.0.0/24 IP block at your on prem environment.
- Verify no firewall rules are blocking the 10.148.0.0/24 IP block at your on prem environment.
- Google CR should be advertising 10.148.0.0/24 block to on prem router

Google Cloud

*More detailed configuration instructions can be found here

DNS Outbound Forwarding Architecture*



Configuration Notes

- Setup an outbound forwarding zone to use an on prem DNS Server for a particular domain.
- Google CR should be learning 10.0.1.0/24 route from on prem router
- Verify no firewall rules are blocking the 35.199.192.0/19 IP block at your on prem environment.
- Setup a custom route advertisement for 35.199.192.0/19 advertising to on prem router.

Google Cloud

*More detailed configuration instructions can be found here

Alternative Name Servers (ANS)

What it is

Another mechanism for forwarding DNS requests outside of GCP. With ANS, **ALL** requests are forwarded to the specified name servers, not just specific domains.

How is it setup

- Specify an IPv4 address for the Alternative Name Server.
- Ensure the routing is setup so the alternative name server is reachable from within your VPC network.
- Verify no firewall rules are blocking the 35.199.192.0/19 IP block at your on prem environment.
- Ensure your on prem environment has a route that directs traffic destined to 35.199.192.0/19 back to your VPC network, through your Cloud VPN tunnel, Dedicated Interconnect VLAN, or Partner Interconnect VLAN.

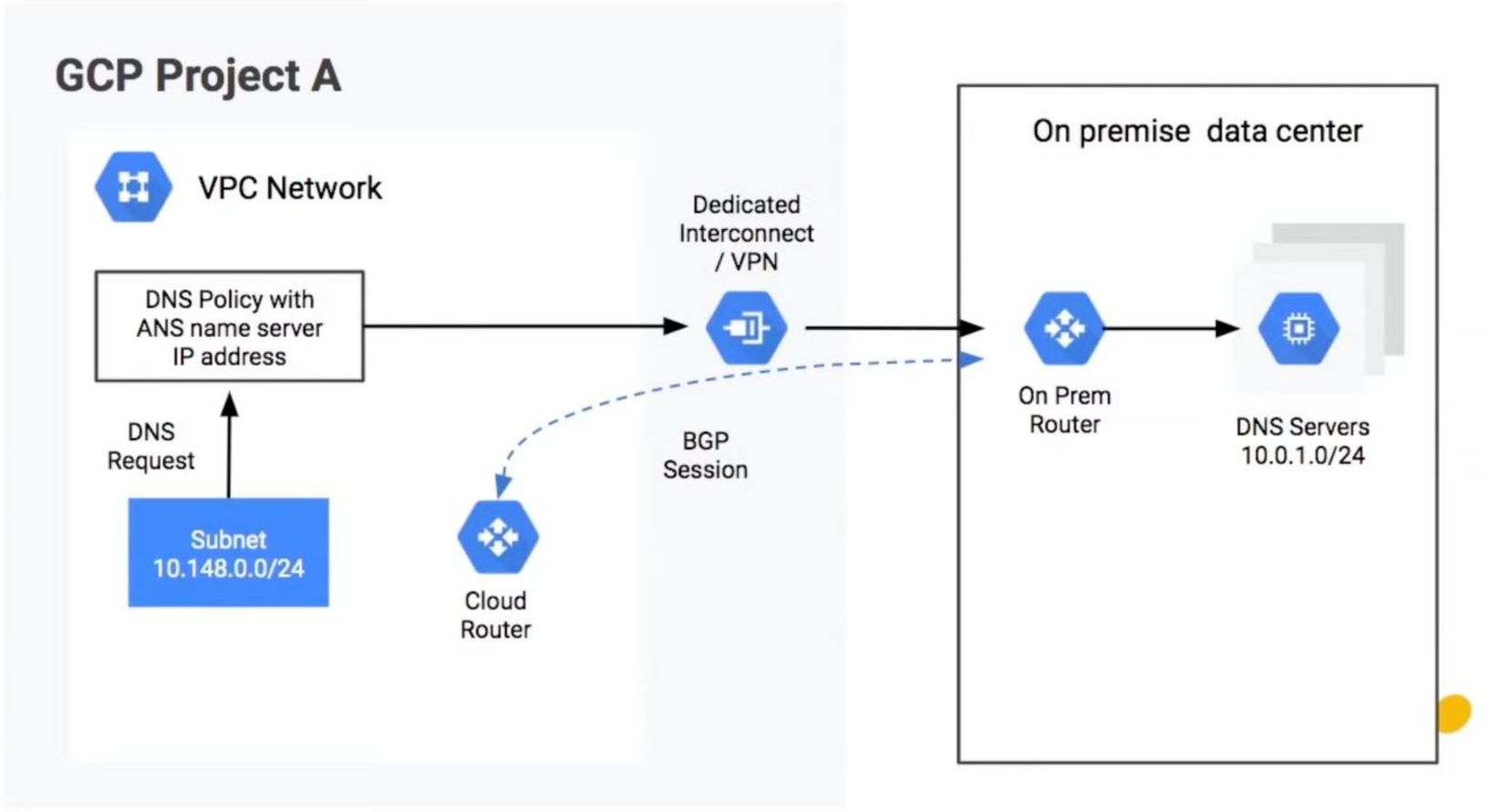
Notes and Caveats on Alternative Name Servers

- The alternative name server that receives the request must be the one that sends the reply to 35.199.192.0/19
- Use to completely bypass Google Cloud DNS: Infoblox, on prem BIND, etc....
- In contrast, outbound forwarding is specific to a zone, e.g onprem.example.com

Google Cloud

Google Cloud

Alternative Name Architecture*



Configuration Notes

- Setup DNS Policy to use ANS servers
- Google CR should be learning 10.0.1.0/24 route from on prem router
- Verify no firewall rules are blocking the 35.199.192.0/19 IP block at your on prem environment.
- Setup a custom route advertisement for 35.199.192.0/19 advertising to on prem router.

Google Cloud

More detailed configuration instructions can be found here

DNS Peering

What it is

DNS Peering allows DNS queries to be sent to another VPC for resolution

How is it setup

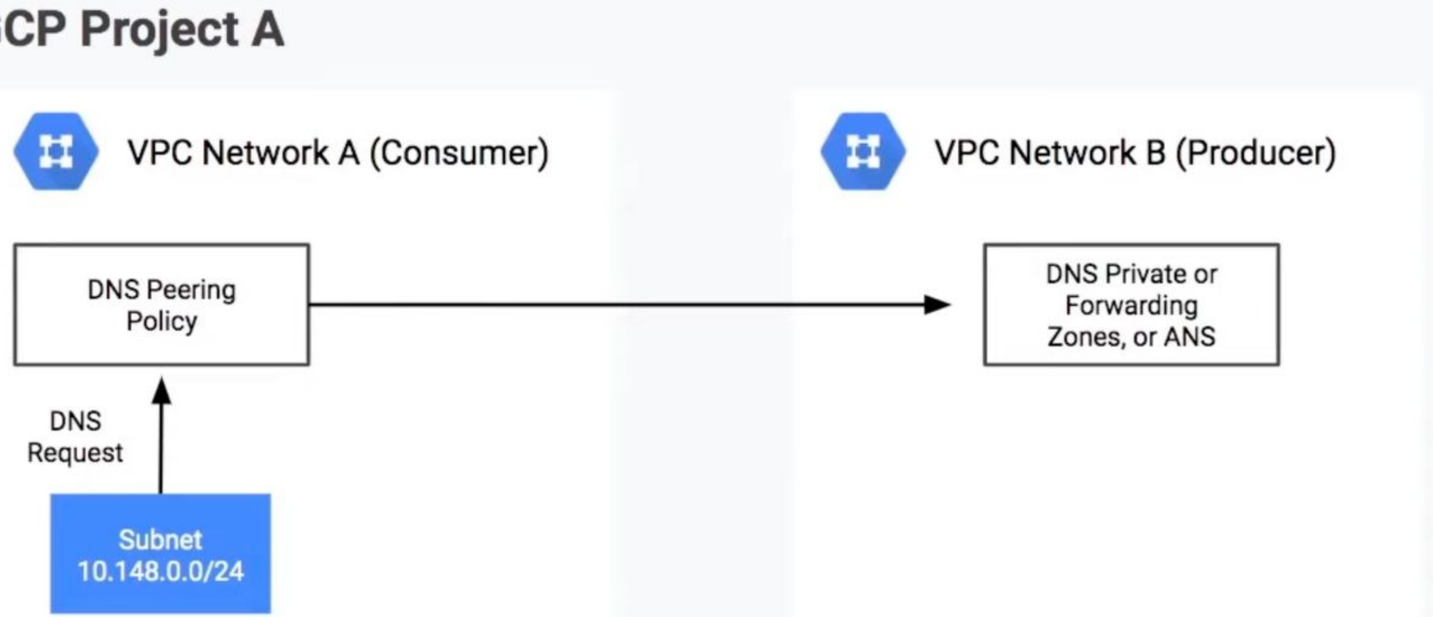
- Configure a zone that is peered to another network
- Once DNS request is received, final resolution is done via a private zone, forwarding zone, or ANS (see next slide) attached to the targeted (Provider) network

Notes and Caveats on DNS Peering

- DNS Peering is important for SaaS providers (eg Cloud AD, Mongo)
- Used in conjunction with forwarding to alleviate the issue with multiple forwarding zones to an on-prem environment.
- DNS Peering alongside DNS Forwarding resembles a hub & spoke networking model

Google Cloud

DNS Peering Architecture*



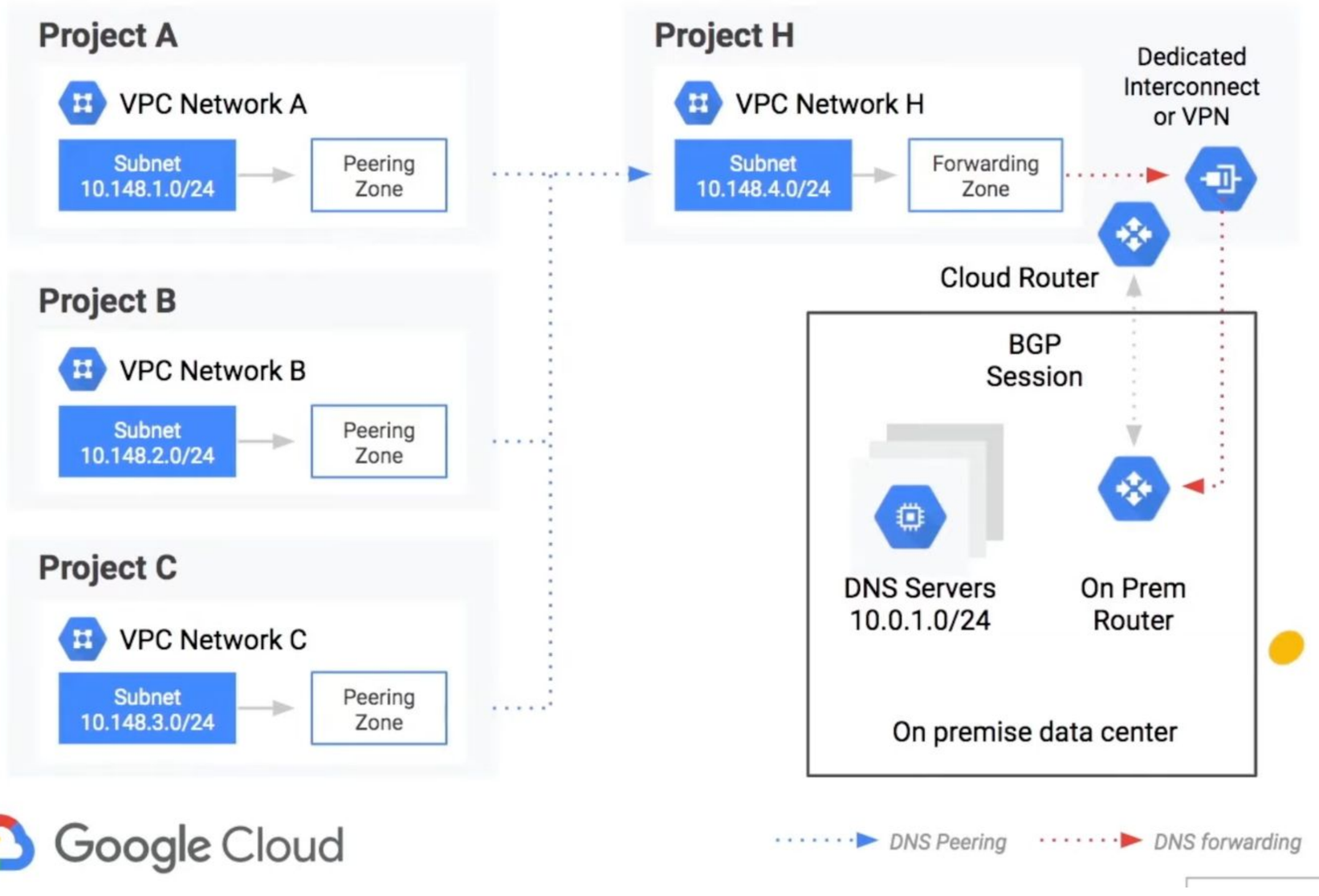
Configuration Notes

- Setup Private Zone, Forwarding Zone, or ANS policy in Producer network
- Setup DNS Peering Policy in Consumer network to to point to VPC Network B.

More detailed configuration instructions can be found here

Cloud DNS Deployment Design Options

Multiple VPCs Resolving to On Premise

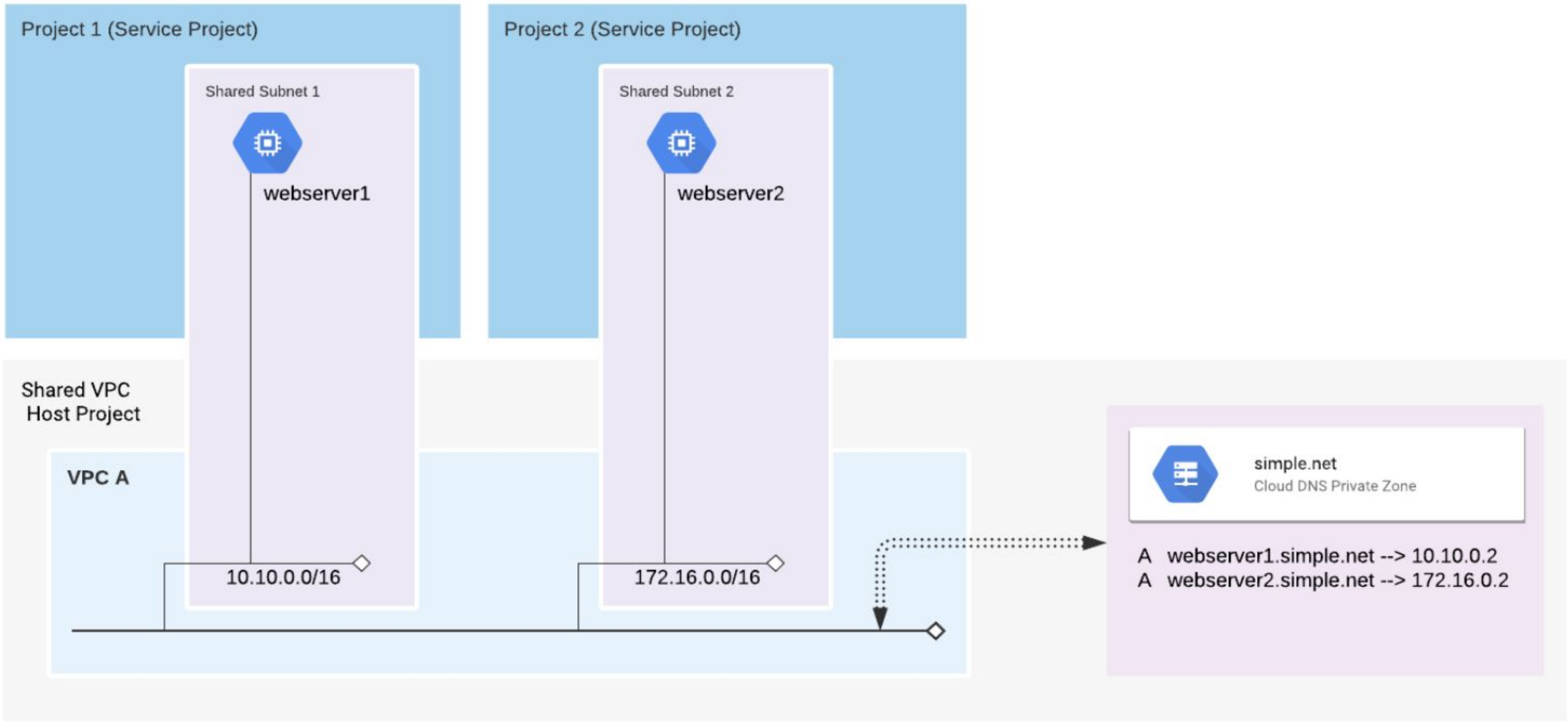


Configuration Notes

- Setup DNS Forwarding Zone in VPC Network H
- Setup DNS Peering Zones in Networks A, B, and C to point to Network H.
- Google CR in Network H should be learning 10.0.1.0/24 route from on prem router
- Verify no firewall rules are blocking the 35.199.192.0/19 IP block at your on prem environment.
- Setup a custom route advertisement In Network H for 35.199.192.0/19 advertising to on prem router.

Google Cloud

Cloud Native: Shared VPC

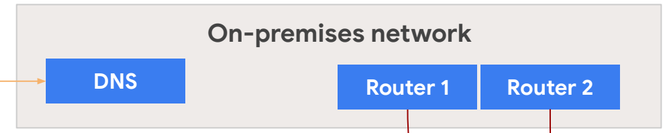


Reference architecture (final version)

Hub-and-spoke with VPC peering - Segmentation based on environments

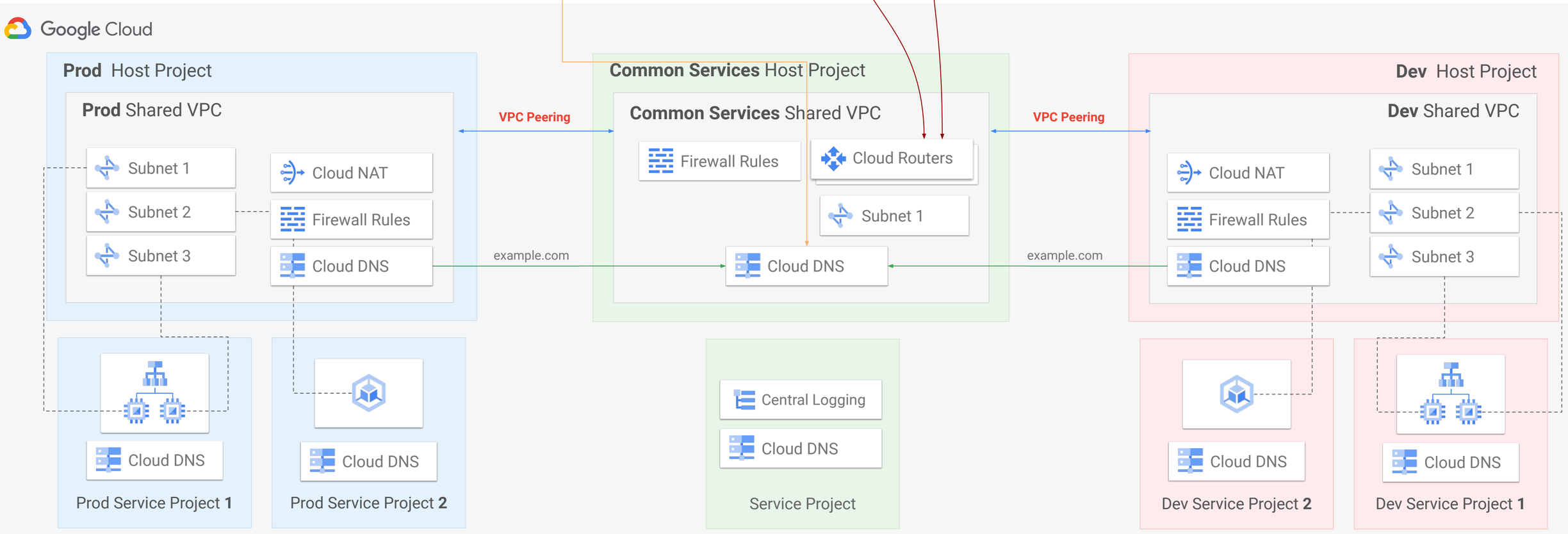
Network security control
- Centralized network security administration
- Central services (NAT, DNS, etc.) deployed in Shared VPC

Scalability
- **Up to 25 spokes**, per VPC peering limitations
- Each spoke can have a high number of service projects



Spokes isolation
- Spokes are isolated as VPC peering is **non-transitive**

Central control versus autonomy
- Full networking autonomy for spokes, based on a separate shared VPC network



Key
- VPC Peering / HA VPN
- DNS Peering
- Shared VPC Subnet Usage
- Interconnect / VPN link
- DNS Inbound Policy / Forward

Cloud DNS Toolkit For Hybrid Setup

Default Private Zones

- In-VPC private zone.
- Used with Private IP addresses and non-RFC 1918 address.
- Not reachable via the Internet
- Can be used in Hybrid deployments.
- Fully controllable by the customer
- Highly Scalable
- Highly Available

Forwarding Zones

- Zone used to forward DNS queries to IP targets.
- Target can be
  - A VM running in the associated VPC
  - An On-prem server connected to the associated VPC via VPN or IC.
  - Public DNS server.
- **Outbound** forwarding only.

Peering Zones

- Peering zone points to a VPC network (Can be in same or different project).
- Follows the name resolution order of another VPC.
- Can be used to resolve the names that are defined in the other VPC network.
- Uses the concept of producer and consumer networks.

DNS Server Policies

- Can be applied at a per VPC level.
- Can either be **Inbound**, **outbound** or **both**.
- Also used to enable logging.

Make sure to...

Enjoy the journey as much as the destination!