PSC Ingress Documentation for GKE (Producer: hsbc-11465671-unyin1-dev, Consumer: hsbc-11465671-unyin2-dev)

1. Overview

This document explains how to expose a private GKE NGINX Ingress as a PSC (Private Service Connect) producer service from project hsbc-11465671-unyin1-dev (region: asia-south1, VPC: hsbc-default-network) and consume it from project hsbc-11465671-unyin2-dev (region: asia-south2, VPC: hsbc-default-network).

PSC allows fully private cross-VPC service consumption without public IPs or routable networks.

2. Producer Setup (Project: hsbc-11465671-unyin1-dev, Region: asia-south1)

2.1 Create PSC NAT subnet

This subnet provides NAT source IPs for ALL PSC consumers.

It MUST be in the same VPC and region as the Ingress ILB.

Command:

```
gcloud compute networks subnets create psc-asia-south1 --project=hsbc-11465671-unyin1-dev
--region=asia-south1 --network=hsbc-default-network --range=10.200.0.0/24
--purpose=PRIVATE_SERVICE_CONNECT
```

Explanation:

This pool is used by Google to NAT inbound PSC traffic before delivering it to the ILB.

2.2 Configure NGINX Ingress ILB Service

Ensure NGINX Ingress uses an internal load balancer with global access enabled.

2.3 Create ServiceAttachment in GKE

This object exposes the ILB as a PSC producer service.

Example YAML:

```
apiVersion: networking.gke.io/v1

kind: ServiceAttachment

metadata:

name: ingress-psc-sa
```

```
namespace: ingress-nginx
spec:
connectionPreference: ACCEPT_AUTOMATIC
natSubnets:
- psc-asia-south1
resourceRef:
kind: Service
name: ingress-nginx-controller
```

After creation, extract the ServiceAttachment URI:

```
kubectl -n ingress-nginx get serviceattachment ingress-psc-sa -o
jsonpath='{.status.serviceAttachment}'
```

3. Consumer Setup (Project: hsbc-11465671-unyin2-dev, Region: asia-south2)

3.1 Allocate Private IP for PSC Endpoint

This IP will be the DNS entry used by workloads.

Command:

```
gcloud compute addresses create psc-endpoint-ip-unyin2 --project=hsbc-11465671-unyin2-dev
--region=asia-south2 --subnet=clients-subnet --addresses=10.60.0.10
```

3.2 Create PSC Endpoint (Forwarding Rule)

This connects the consumer VPC to the PSC producer in prj1.

Command:

```
gcloud compute forwarding-rules create psc-endpoint-fr-unyin2
--project=hsbc-11465671-unyin2-dev --region=asia-south2 --network=hsbc-default-network
--address=psc-endpoint-ip-unyin2 --target-service-attachment=projects/hsbc-11465671-unyin1-dev
/regions/asia-south1/serviceAttachments/ingress-psc-sa --allow-psc-global-access
```

4. DNS Configuration

If you maintain a private DNS zone (example: internal.hsbc), point the service hostname to the PSC endpoint IP allocated in prj2.

Example:

```
A api.backend.internal.hsbc → 10.60.0.10
```

Explanation:

DNS decouples clients from underlying PSC architecture.

5. Verification

5.1 Check PSC connection status

```
gcloud compute forwarding-rules describe psc-endpoint-fr-unyin2
--project=hsbc-11465671-unyin2-dev --region=asia-south2 --format="value(pscConnectionStatus)"
```

Expected: ACCEPTED

5.2 Test connectivity from a Pod in GKE

```
kubectl exec -it pod -- curl -vk https://api.backend.internal.hsbc/
```

6. Summary

- NAT subnet must exist in producer VPC.

- ServiceAttachment exposes ILB securely.

- PSC endpoints in each consumer project give private service entry.

- DNS directs traffic per project/region logic.