Secure Web Proxy (SWP) – Full Documentation

1. Introduction

Secure Web Proxy is a Google Cloud-managed service that secures egress HTTP/S traffic from VMs, containers, serverless workloads, and on■prem networks via Cloud VPN or Interconnect.

2. Key Features

- Explicit proxy mode
- Private Service Connect (PSC) attachment mode
- Next-hop routing mode
- Identity-based access control
- Autoscaling Envoy-based proxies
- Default deny-all policy
- URL filtering, TLS inspection
- Logging & monitoring via Cloud Logging

3. Architecture Overview

SWP uses:

- Secure Web Proxy Instance
- Secure Web Proxy Policy & Rules
- URL Lists
- Proxy-only subnets (/23 recommended)
- VPC subnets (purpose=PRIVATE)
- SSL Certificates (optional)

Traffic Flow:

Client → Proxy Instance → Internet

or Client → PSC Endpoint → SWP Instance → Internet

4. Deployment Modes

4.1 Explicit Proxy

Applications explicitly point traffic to SWP hostname (proxy.example.com:443).

4.2 PSC Service Attachment Mode

Centralized deployment for multi-VPC environments using PSC.

4.3 SWP as Next Hop

VPC routes forward tagged traffic to SWP instance.

5. Required APIs

Enable:

- compute.googleapis.com
- networkservices.googleapis.com
- networksecurity.googleapis.com
- certificatemanager.googleapis.com
- privateca.googleapis.com (optional)

6. IAM Roles Required

To provision SWP:

- roles/compute.networkAdmin

Why? Manage networks, routers, addresses.

To upload certificates:

- roles/certificatemanager.editor

Why? Manage TLS certs used by SWP.

For policy management:

- roles/compute.orgSecurityPolicyAdmin

Why? Create/modify gateway security policies.

7. Initial Setup Steps

Step 1 – Enable billing

Step 2 – Enable required APIs

Step 3 – Create VPC subnets (purpose=PRIVATE)

Step 4 – Create Proxy-only subnets (purpose=REGIONAL_MANAGED_PROXY)

Step 5 – Upload TLS certificate (optional)

Step 6 – Deploy SWP instance

Step 7 – Create security policy & rules

Step 8 – Configure routing or explicit proxy

Step 9 – Test connectivity

8. Commands (gcloud)

Enable APIs:

```
gcloud services enable compute.googleapis.com certificatemanager.googleapis.com
networkservices.googleapis.com networksecurity.googleapis.com
```

Create VPC subnet:

```
gcloud compute networks subnets create my-vpc-subnet --purpose=PRIVATE --region=us-central1
--network=myvpc --range=10.10.10.0/24
```

Create Proxy-only subnet:

```
gcloud compute networks subnets create swp-proxy-subnet
--purpose=REGIONAL_MANAGED_PROXY --role=ACTIVE --region=us-central1 --network=myvpc
--range=192.168.0.0/23
```

Upload TLS certificate:

```
gcloud certificate-manager certificates create swpcert --certificate-file=cert.pem
--private-key-file=key.pem --location=us-central1
```

9. Real-World Use Case

Company: Food Delivery App

Problem: Developers accessing 3rd■party APIs (e.g., payment gateways) require strict egress security.

Solution using SWP:

- SWP deployed centrally as PSC service

- All VM traffic routed to SWP

- Policy allows only:

– api.razorpay.com

– googleapis.com

– *.trusted.com

- Block social media, unknown sites
- Logs monitored in Cloud Logging

Result:

- Secure egress
- Full visibility
- No external IPs on VMs

10. Pricing

SWP Pricing Model:

- Charged per GiB processed
- Regional variation applies
- Certificate Manager billing (if using paid CA)
- Standard network egress applies after proxying

11. Logging & Monitoring

SWP integrates with:

- Cloud Logging – logs HTTP/S requests
- Cloud Monitoring – metrics for proxy performance
- Cloud Audit Logs – admin actions

12. Troubleshooting

- 502 errors → certificate mismatch or policy block
- Traffic not using proxy → wrong routing or missing explicit proxy config
- SWP instance creation failure → missing proxy-only subnet
- PSC connectivity errors → incorrect service attachment