**GCP**

1. Reserve IP addresses for the following:
   1. GlobalProtect GW/ELB Frontend
   2. PSC addresses
2. Routes
   1. Create route from each psc to fw in the relevant vpc subnet
3. GCP Firewall ingress rules (applied on external subnet)
   1. Global protect access:
      1. Source – clients public subnet (the subnet for the clients static public ip (ports in the wall))
      2. Destination – Public ip (AKA the GW which you reserved in GCP)
      3. Ports – TCP/443 , UDP/4501
   2. Health check for ELB
      1. Source -
         1. 35.191.0.0/16
         2. 209.85.152.0/22
         3. 209.85.204.15.0/22
      2. Destination – Public ip (AKA the GW which you reserved in GCP)
      3. Port – TCP/443

**ELB details – Requirements**

1. Configured as pass-through – layer 3 , all ports
2. Reserve a public IP in GCP (or other csp if used) for the elb frontend (AKA the GW)
3. Health check:
   1. Destination – the reserved public ip used in frontend
   2. Source -
      1. 35.191.0.0/16
      2. 209.85.152.0/22
      3. 209.85.204.0/22
   3. The port which the health check requires is 443
4. LC algorithm (session affinity) - client ip (2-tuple hashing (Src/dstIP)), ensure both GP portal and GW will go to the same PA-VM

**Host details – Requirements:**

1. Gp version 6.2.6
2. Host FW by intune (workstations team)
3. Allow in host fw the ip addresses for the GW and tunnels
4. GP Root CA needs to be trusted on device (still workstations team)
5. Get a list for all static ip addresses that the client will be using (for the security policies)
6. To allow decryption we need to add this command on the client terminal – gcloud config set core/custom\_ca\_certs\_file [PATH\_TO\_CUSTOM\_CA]

**Global Protect Configuration**

1. Create variable for the public ip pool which the gateway will assign to the client after they connect to it
   1. Create a variable under the proper template. Panoram -> template -> (used template) -> variables -> manage...
2. Create a variable for the tunnel interface the client will automatically connect to after being assigned their ip from the pool.
   1. Create a variable under the proper template. Panoram -> template -> (used template) -> variables -> manage...
3. Create interface mgmt profile, network - > network profile -> interface mgmt, create new interface for load balancer
   1. Htttps enabled
   2. Permitted ip addresses
      1. 35.191.0.0/16
      2. 130.211.0.0/22
      3. 209.85.152.0/22
      4. 209.85.204.0/22
4. Create loopback interface with the public IP (THE GW)
   1. Zone – external
   2. Under loopback interface -> advanced -> mgmt profile, enter the load balancer health check
   3. Ipv4 – public ip (THE GW)
5. Create zone. Network -> zones -> new
   1. (name it) add type layer 3
6. Create tunnel. Network -> interfaces -> tunnel -> new -> ipv4
   1. Add tunnel interface from template variables
   2. Zone GP
7. Add tunnel as interface to GP zone
8. Decryption
   1. Create GP Root CA (Self signed)
   2. Create intermidiate CA (Certificate) signed by Root CA (CN = (GW IP))
9. Create SAML idp (under device)
   1. Download SSO XML from the enterprise application which Workstations team created
   2. Import downloaded XML
   3. **Uncheck validate idp certificate**
10. Create ssl/tls service profile
    1. Add the certificate which you created (uncheck DHE, SHA1,AES-chacha20)
11. Create authentication profile
    1. Type SAML
    2. Idp server profile (the one created in step 9
12. Create GW (network global protect GW)
    1. Interface = loopback created
    2. Ipv4 address = GW
    3. Authentication
       1. Ssl/tls service profile -> use the one created in step 10
       2. Client authentication
          1. Authentication profile the one created in step 11
    4. Agent
       1. Tunnel interface = (tunnel created)
       2. Client setting
          1. Authentication override
             1. Certificate = (certficate (intermididaate ca))
          2. IP Pools
             1. Ip pool = (pool defined in template variables
          3. Split tunnel
             1. Access route

Include PSC IP address (reserved in GCP)

* + - * 1. Domain and application - > include domain = (google service urls)
      1. Network services
         1. Dns server = tunnel interface variable

1. Create portal
   1. Interface = (loopback interface)
   2. Ipv4 address = (GW)
   3. Authentication
      1. SSL/TLS service profile = (the one created in step 10)
      2. Client authentication
         1. Authentication profile the one created in step 11
   4. Agent
      1. Add configs
         1. Authentication override = (certificate created)
         2. External = add the ip address of the GW.
         3. App - > connection method = on demand
      2. Trusted root ca = (root ca in previous steps)
         1. **Check the box for “install in local cert store”**
2. Create DNS proxy
   1. Primary = 8.8.8.8
   2. Interface = (tunnel used)
   3. Static entries
      1. Fqdn = storage.googleapis.com
      2. Address = (psc address)

**Firewall policies**

1. Create address objects for all tunnels, GWS, and IP pools
2. Create tags for GP
3. Security pre rules
   1. Create policy for ELB health check
      1. Source zone = external
      2. Source address = GCP health check address
      3. Destination zone = external
      4. Destination address = GW
      5. Application = SSL
      6. Action = Allow
4. Security post rules
   1. Allow GP connection
      1. Source zone = external
      2. Source address = on prem static ip addresses for the clients
      3. Destination zone = external
      4. Destination address = IPSEC, panos-global-protect
      5. Application = SSL
      6. Action = Allow
   2. Allow gp to bucket
      1. Source zone = GP
      2. Source address = the IP pools the variables
      3. Destination zone = internal zone
      4. Destination address = the PSC
      5. Application = any
      6. Action = Allow
      7. Service = HTTPS
   3. Allow GP to google dns proxy
      1. Source zone = GP
      2. Source address = the IP pools the variables
      3. Destination zone = GP
      4. Destination address = the tunnels
      5. Application = DNS
      6. Action = Allow
   4. GP allow google dns
      1. Source zone = GP
      2. Source address = the tunnels
      3. Destination zone = external
      4. Destination address = 8.8.8.8
      5. Application = DNS
      6. Action = Allow
   5. GCP internal connection to sdk
      1. Source zone = GP
      2. Source address = the IP pools the variables
      3. Destination zone = external zone
      4. Destination address = any
      5. Application = any
      6. Action = Allow
      7. Service = http, https
      8. Url category = google cli sdk urls
5. Nat post rules
   1. GP dns proxy outbound nat
      1. Source zone = GP
      2. Source address = the IP pools the variables
      3. Destination zone = external
      4. Destination address = any
      5. Translated packet
         1. Translation type = dynamic ip and port
         2. Address type = interface address
         3. Interface = ethernet 1/1 (external interface)
         4. Ip type = ip

**Reference:** [DAW Creation Steps.jpg](https://tikshuv.sharepoint.com/:i:/r/sites/defenseSystems/Shared%20Documents/%D7%AA%D7%99%D7%A2%D7%95%D7%93%D7%99%D7%9D/Workstations/DAW/DAW%20Creation%20Steps.jpg?csf=1&web=1&e=f8w1bC)

