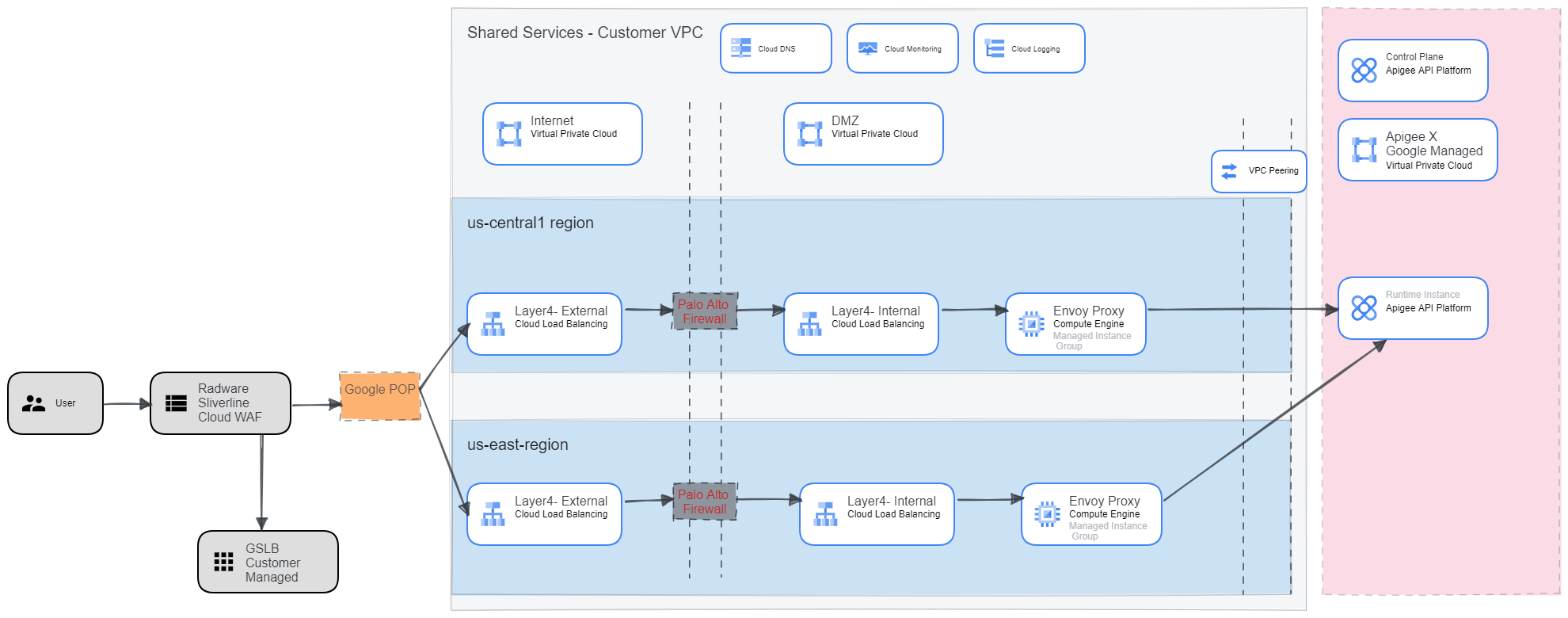
**mTLS with Apigee X**



1. Client Application sends request to connect for mTLS authenticated applications

2. Request is routed to Radware Sliverline Edge protect WAF solutions for security inspection. Radware also provide pass-through mTLS authentication options to configure

3. Customer managed GSLB handles DNS based load balancing to GCP regions

4. Request is routed via External Layer4 Load balancer forwarding rule to the Palo-Alto Firewalls

5. The Palo-Alto firewall translate(NAT) the request to the internal Layer4 load balancer forwarding rule for the Envoy Proxy MIG

6. The Envoy Proxy MIG terminates the SSL connection, provides managed MTLS authentication as required and routes the request to Apigee X Instance managed by Google via the established VPC Network peer

7. Apigee X processes the requests