GCP Network Security Architecture

When a wholistic healthcare organization was undertaking a digital transformation that included establishing a new GCP landing zone (LZ), they needed network security experts to establish a secure network fabric. This healthcare customer expressed a need for a more secure and manageable alternative to legacy networking solutions. They were looking for a network architecture to advance their zero trust and use-centric computing objectives.

Edge assembled a team of their GCP security architect and engineers to assist the customer with the needed expertise. The team began engaging the customer gathering the leading security frameworks and secure network design principles most important to the customer. Armed with HIPAA and HiTrust as the customers leading security frameworks and zero trust and defense in-depth security principles, the Edge team presented the customer with several network security designs. One of the designs focused on the network security of the VPC network.

For the GCP LZ, the Edge team, in collaboration with customer security engineers, deployed native GCP firewalls to establish the segmentation boundaries. This included GCP firewalling VPC connections to on-premises computing and API-based services to protect inbound and outbound VPC traffic. This deployment also included the use of Cloud Armor, web application firewall, for DDoS and Geo-location access control for protection of cloud deployed applications.

Within the VPC, the Edge team deployed GCP firewalling to achieve trusted zones where production workloads run, and production data is processed. The defense in-depth firewalling deployment enabled segregation of production environments from development and UAT environments. and data run and micro-segmentation.

The customer was especially appreciative of how the network security integration with ***GCP Security Command Center*** gave them on-going visibility and management of the network security configurations. Cloud computing environments are ever changing, and the telemetry provided by the GCP Security Command Center is vital to maintaining a secured GCP VPC under an ever-evolving cloud computing environment.