Secure Global AI Testing Platform Deployment on GCP

Page 1: Executive Summary

Objective

Design and implement a secure, scalable, and globally available network infrastructure on Google Cloud Platform (GCP) to support an AI certification and testing environment. The system enables authenticated users at thin client sites in USA, Brazil, Japan, Italy, and Thailand/Philippines to connect securely to a central headquarters-based web server for programming and certifying artificial intelligence systems.

Key Business Goals

- Maintain military-grade security across all remote sites.
- Ensure low-latency access to the central test environment.
- Build a future-proof and scalable global mesh network.
- Comply with industry security best practices and cloud-native resilience.

Solution Overview

I deployed a Network Connectivity Center (NCC)-based architecture using HA VPN and dynamic BGP routing to link all global testing centers securely to a central GCP hub region.

Each edge location (regional test center) includes:

- VPN tunnel pairs for redundancy (HA VPN)
- A Cloud Router configured with BGP to enable dynamic route discovery
- A Router Appliance spoke linked to the NCC hub to allow secure, full-mesh communication

The headquarters web server is hosted in a private subnet, exposed only via HTTPS load balancer with Cloud Armor, identity-aware access controls, and encrypted transport (TLS + IPsec).

Secure Global AI Testing Platform Deployment on GCP

Page 2: Technical Implementation & Security Highlights

1. Global NCC Architecture

- NCC Hub Region: us-central1 (Primary)
- Spoke Regions:
  - Brazil: southamerica-east1
  - Japan: asia-northeast1
  - Italy: europe-west8
  - Thailand/Philippines: asia-southeast1 or asia-east2
  - USA: us-east1

Each region contains a router appliance spoke, which securely terminates a BGP HA VPN tunnel from a local edge device or VM instance acting as a gateway.

2. Terraform Infrastructure-as-Code (IaC)

- Built reusable, modular Terraform components for:
  - NCC Hub provisioning
  - HA VPN gateways
  - Cloud Router and BGP configurations
  - Spoke registration
  - Security policies and firewall rules
- Used google provider and followed GCP best practices for naming, IAM roles, and modular reusability.

3. Security & Compliance Features

- Encryption: All inter-site traffic is secured via IPsec (VPN), and all web traffic is encrypted via HTTPS with TLS 1.3.
- Authentication: Used Google Cloud IAP and Identity Federation to restrict access to test systems.
- Firewall: Default deny-all policy with allow rules only for ICMP, SSH (limited ranges), and HTTPS.

Secure Global AI Testing Platform Deployment on GCP

- Monitoring & Audit: Enabled Cloud Logging, VPC Flow Logs, and Cloud Monitoring to provide full observability and compliance visibility.

4. Results & Business Value

- Delivered a fully secure, cloud-native global testing infrastructure in under [X] weeks.
- Built a modular system that can scale to additional sites with minimal changes.
- Reduced complexity through dynamic route exchange (BGP) and Terraform automation.
- Positioned the company for secure global AI development and certification at scale.

Promotion Justification

This project required advanced skills in cloud networking, security engineering, Terraform infrastructure design, and global architecture planning. The result is a hardened, scalable, and business-critical infrastructure directly supporting our AI certification revenue streams.

Based on the impact, technical leadership, and critical nature of this deployment, I respectfully request consideration for a $50,000 salary adjustment.