Public Cloud – GCP Network – External Ingress Egress

Objective	To provide End Users with Network connectivity to connect Citi's GCP resources from Internet (Ingress/Inbound) and to enable GCP resources/Applications to connect to Internet (Egress/Outbound) in a most secure way. As a developer and user, I need to host and expose production grade applications that are accessible from the internet and the applications should be able to communicate to the internet for business purposes. **Consideration:** ▪ Define GCP folder & project structure and VPC design & sizing for Ingress, Egress, Packet Capture and Inspection ▪ Design Network Connectivity Centre's Ingress and Egress network routing configurations ▪ Design DNS architecture like Zones and resolutions for DMZ ▪ Solution the Ingress Egress Architecture components like LB, WAF, NGFW and Packet Mirroring ▪ Engineer the Network packet Capture to analyse and capture external traffic with Scale and flexibility ▪ Provide Network Security capabilities with GCP's NGFW and its policies ▪ Setup preventative and detective Guardrails and polices to ring fence the DMZ ▪ Provide single plane of glass monitoring capability for metrics and logging. ▪ Build Service engineering environments to test the functionality and scale to provide Signoff and complete ETLC certification ▪ Automate the provisioning of Environments through CNS with infrastructure testing and Network firewall rules with CINS.
Acceptance Criteria	Conditions required to be successful, you can think of any function or non-functional criteria here: ▪ ***Support Zero Trust Architecture*** ▪ ***Conform to NSS standard (IDS, IPS, DPI, WAF, etc)*** ▪ ***Ability to route the Ingress Egress traffic to and from On-premises and Internal VPCs through Inspection Firewall*** ▪ ***Ability to traffic engineering inbound traffic through load balancing configuration*** ▪ ***Ability to capture the network packets of external traffic*** ▪ ***Secured DMZ with Firewalls, Guardrails and Constraints.*** ▪ ***Ability to monitor Network metrics and logs*** ▪ ***Ability to automate and orchestrate the provisioning of Ingress Egress components*** ▪ ***SASE and CCR Integration***
Stakeholders	EUC, SOC, Infrastructure Defence and CTI Network
Resourcing	CTI Cloud Network Infrastructure – 3E x 9 months CTI Cloud Network CNS – 2E x 4 months CTI Cloud Network CINS - 2E x 4 months CISO – Network Security – 2E x 5 months CISO – IAM – 2E x 3 months
Milestones	Design of Ingress Egress Networks, DNS and Network Connectivity Center Network Security Architecture and Rules definition IAM policies & permissions and Preventative & Detective Controls
Submitter	Manokaran Karuppusamy

Please reach out to Haripriya Jagannathan/Siddhi Revandkar/Dolapo Kukoyi once the document is ready for review and post it in **GCP Public Cloud Enablement-CTI-NAM** >> **Foundations** channel >> **EPICs + User Stories** File by Oct 3rd

For Reviewers Use Only

Feedback	Feedback will be provided by reviewers here. Reviewers should record feedback as follow. Date – Reviewer Name – Feedback e.g. 2 Oct, 2024 – Mo Alslaoom – consider deletion of requested accounts to be added to success criteria.
Status	Review | Approved

Partner Connectivity – CSP Hosted

Objective	As a service hosted in GCP, need the ability to connect to other services hosted within the same CSP and across different CSPs
Acceptance Criteria	▪ *Private connectivity options for CSP Native services owned by Citi.* ▪ *Inline inspection and network security controls for partner and 3rd party services hosted within the same CSP or across other CSPs that are Citi connected.* ▪ *Conform to NSS standard (IDS, IPS, DPI, WAF, etc)* ▪ *Continue packet capture??* ▪ *Automated network security enforcement.* ▪ *Citi Connectivity Register (CCR) integration.* ▪ *Ability to traffic engineering inbound traffic through load balancing configuration.* ▪ *DDOS and DNS protection* ▪ *DNS protection.* ▪ *Cross region failover*
Stakeholders	EUC, SOC, Infrastructure Defence and CTI Network
Resourcing	CTI Cloud Network Infrastructure – 2E x 6 months CTI Cloud Network CNS – 2E x 3 months CTI Cloud Network CINS - 2E x 3 months CISO – Network Security – 1E x 3 months
Milestones	Design of Network pattern and Architecture Network Security Architecture and Rules definition
Submitter	Manokaran Karuppusamy

For Reviewers Use Only

Feedback	
Status	