Computacenter

GCP Micro-Segmentation

Google Cloud

THE CHALLENGE

As organisations virtualise their on-premises data centres and adopt cloud environments, their network perimeters vanish and attack surfaces increase. Workloads, automation, and API-based attacks become new threat vectors. Best practice reference architectures for GCP add centralisation of connectivity and management whilst supporting multi-tenancy allowing the flexibility for multiple business lines to deploy workloads within the same resource model.

This results in multiple applications deployed across trust boundaries within an organisation via GCP based network concepts such as regions , zones and virtual private clouds (VPC's) grouped under projects and folders. Whilst these architectures will usually have considered 'north-south' based security patterns to manage ingress/egress traffic from external sources (such as the internet) it is equally critical to enforce security guardrails limiting lateral movement of traffic between these network elements. This is known as east-west based security and prevents security incidents escalating from one compromised VM, service, or container to another.

Gaining this granular control over sensitive workloads and security boundaries in a cloud deployment provides for a **zero-trust** based approach in which an organisation can demonstrate proper security and data separation to simplify audits and regulatory compliance requirements via the strict control of how traffic flows throughout a GCP deployment

OUR APPROACH

At Computacenter we take the approach of providing organisations with the means to deploy micro-segmentation as an integral part of a GCP foundational platform. Micro-segmentation is one of the core functions of a next-generation zero-trust cybersecurity solution creating zones and boundaries in cloud environments to isolate workloads from one another and secure them individually. As a result organisations can feel confident extending their existing datacentre technologies into GCP whilst supporting a common security architecture based on zero-trust.

Our approach supports traffic isolation both north-south and east-west with granular policy control providing a scalable way to create a secure perimeter zone around each workload with consistency across different workload types and environments. This enhances and extends the visibility and control from network or zone-based firewalls. Moving to such an architecture provides an opportunity to simplify the management of firewall policies. Our best practice is to use consolidated firewall policies at the organisation or folder level, rather than performing these functions in different parts of the network, thus enforcing security guardrails across a GCP deployment. Whilst GCP native software based firewalls can be used we also work closely with our partners such as Palo Alto and Cisco to provide best-of-breed firewalling to support and enhance these boundaries with services such as packet inspection, threat detection and anti-virus.

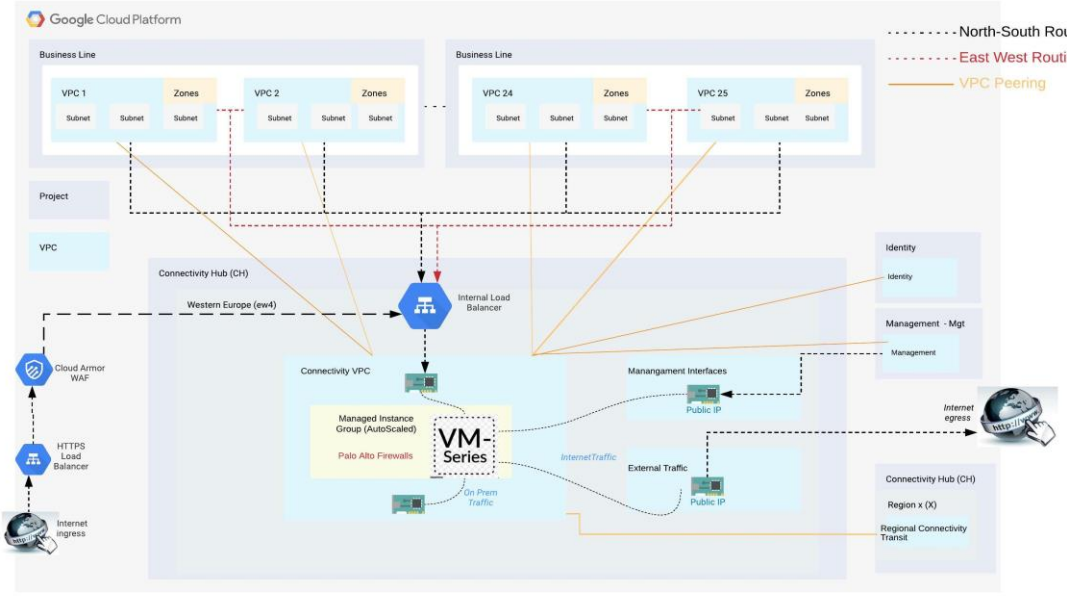
Our skilled, accredited and experienced consultants can work with customers to implement a fully secure and CIS compliant micro-segmentation based approach either as part of one of one our existing GCP services or as a bespoke process to address the challenge. As policy lifecycle management is one of the most challenging parts of implementing such a strategy our security specialists can also help consolidate what may be complex and numerous existing firewall rules that need to be created in to the cloud to support successful and secure workload migration.

HOW TO SECURELY SEGMENT RESOURCES

Micro-Segmentation is a key tenant in our GCP Foundations (Landing Zone) service where we ensure all traffic, both north-south and east-west, traverses a firewall in a centralised connectivity hub. These hubs are regional and can scale as required. We help customers adopt a project factory approach, enabling individual business lines or project based VPC's to be automatically peered to the hub, and traffic routed by default through the firewall. Additionally Computacenter can conduct operations and security reviews that examine the status of an organisations security posture and proposes steps to improve.

- Foundations (Landing Zone) Service
- Cloud Operations Review Service
- Cloud Security Services
- Bespoke Consultancy

We can deploy with both best of breed and GCP native firewall based solutions. Where best of breed is used (such as a Palo Alto VM-Series firewall) these will reside in a high availability GCP managed instance group , with firewalls in separate regional zones behind an internal load balancer , and auto scale as required to manage load and throughput. Using Apache Benchmark we have successfully performance tested that east-west routing between VM's in segregated VPC's could support over 100k requests a minute through a single firewall.



We have further developed a set of best practice set of centralised policy guardrails that can be applied at a hierarchical level within GCP greatly simplifying inter workload or business line communication. This further extends the GCP boundary to both on-premise or hybrid cloud networks with the same level of visibility and granularity.