<Document Title>

Runbook v1.0

Seller Restrictions

The data contained in this document shall not be disclosed and shall not be duplicated, used, or disclosed in whole or in part for any purpose. If a contract is awarded to chosen parties as a result of or in connection with the submission of this data, the client or prospective client shall have the right to duplicate, use, or disclose this data to the extent provided in the contract. This restriction does not limit the client's or prospective client's right to use the information contained in the data if it is obtained from another source without restriction. The data subject to this restriction is contained in all marked sheets.

Version Control

All information given under this version over rides all and any kind of offers, assumptions, deliverables and contracts, given under any previous version. All previous versions of the subject Proposal stand null and void **.**

Document Responsibilities

Role	Name
Author	QUEST DIAGNOSTICS -Security Runbook

Document History

Version No.	Date	Author/Reviewer	Change Description
		Ravi Shanker Upadhayay	Initial Draft

Document Distribution

SL No.	Name	Company	Date	Version No.

Glossary

Abbreviation	Description
OP	Organization policy
CMEK	Customer-managed encryption keys

Contents

1. Introduction

1.1. Document Objective

QUEST DIAGNOSTICS Security run book provides operational information required to manage day-to-day tasks for the Security track. The run book provides details of service levels, scope of service, Security infrastructure and operating procedures.

This document explains the Organization policy at QUEST DIAGNOSTICS. After reading this document, the reader should be able to understand configuration at QUEST DIAGNOSTICS business unit.

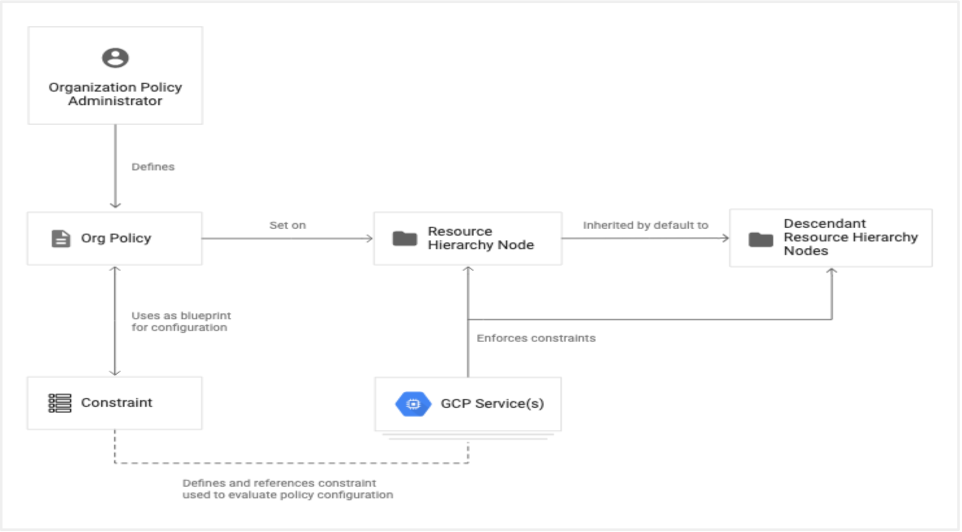
1.2. Scope of this document

The following are the Security technologies/product/tools used for QUEST DIAGNOSTICS project.

No	Technology	GCP
1	Organization Policies	GCP Native
2	Cloud Armor & Advanced network DDoS protection	GCP Native
3	CMEK	GCP Native
4	Firewall rules	GCP Native

2. Organization Policy

2.1. Architecture


Organization Policy Administrator
Defines
Org Policy
Set on
Resource Hierarchy Node
Inherited by default to
Descendant Resource Hierarchy Nodes
Uses as blueprint for configuration
Enforces constraints
Constraint
GCP Service(s)
Defines and references constraint used to evaluate policy configuration

An organization policy acts as a guardrail to enforce security, compliance, and governance best practices across entire gcp cloud environment. It's essentially a set of rules or constraints that you define and apply to control how resources are used within your organization. These rules can be quite granular, allowing you to target specific resource types, configurations, or behaviors.

2.2. Organization Policies

Note that policies are **not** retroactive, meaning existing resources, even if they violate the new policies, will continue to run and function and manual intervention will be required.
If a new organization policy sets a restriction on an action or state that a service is already in, the policy is considered to be in violation**, but the service will not stop its original behavior**.

Enforced Recommended Policies

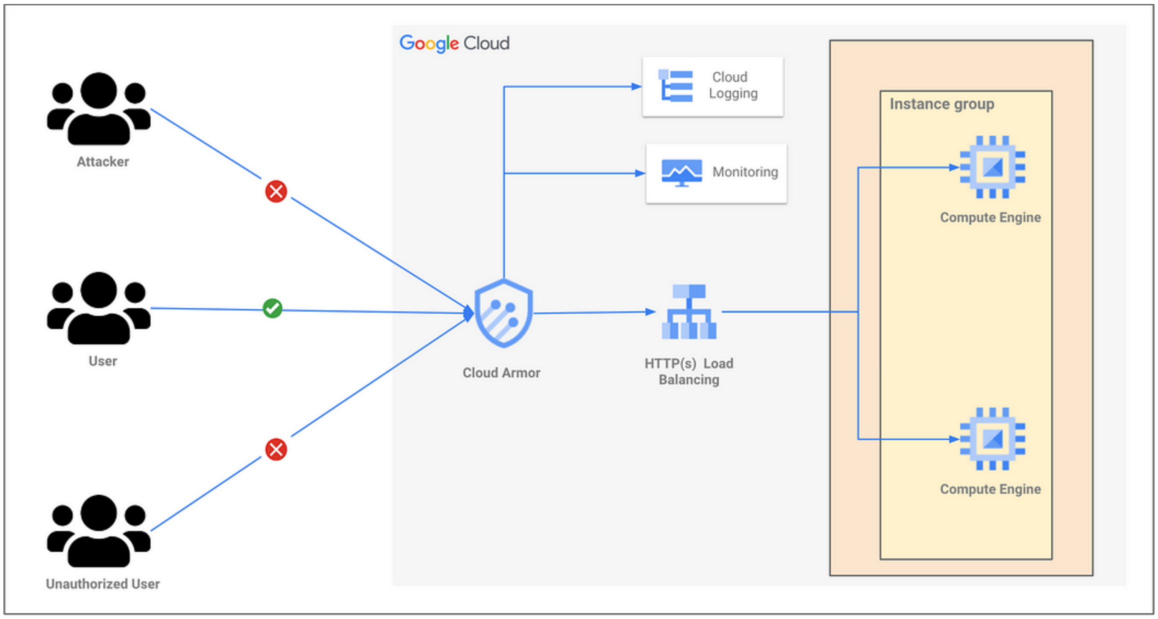
Enforcement state	Name	ID	Constraint type	Value
Active	Google Cloud Platform - Resource Location Restriction	gcp.resourceLocations	List	us-east4,us-west1
Active	Define allowed external IPs for VM instances	compute.vmExternalIpAccess	List	Denied All
Active	Define trusted image projects	compute.trustedImageProjects	List	projects/prj-ospacker-useast-dev-23295
Active	Disable Create Default Service Account (Cloud Build)	cloudbuild.disableCreateDefaultServiceAccount	Boolean	Enforcement on
Active	Disable Project Security Contacts	essentialcontacts.disableProjectSecurityContacts	Boolean	Enforcement on
Active	Disable service account key creation	iam.disableServiceAccountKeyCreation	Boolean (Legacy)	Enforcement on
Active	Disable Service Account Key Upload	iam.disableServiceAccountKeyUpload	Boolean (Legacy)	Enforcement on
Active	Disable VM serial port access	compute.disableSerialPortAccess	Boolean	Enforcement on
Active	Domain restricted contacts	essentialcontacts.allowedContactDomains	List (Legacy)	questdiagnostics.com

Active	Domain restricted sharing	iam.allowedPolicyMemberDomains	List	C038su8z3
Active	Allowed VLAN Attachment encryption settings	compute.allowedVlanAttachmentEncryption	List	IPSEC
Active	Restrict Dedicated Interconnect usage	compute.restrictDedicatedInterconnectUsage	List	projects/prj-shrd-ntwk-3/global/networks/vpc-hub-external
Active	Restrict Shared VPC Host Projects	compute.restrictSharedVpcHostProjects	List	projects/prj-shrd-ntwk-3
Active	Restrict shared VPC project lien removal	compute.restrictXpnProjectLienRemoval	Boolean	Enforcement on
Active	Restrict which projects may supply KMS CryptoKeys for CMEK	gcp.restrictCmekCryptoKeyProjects	List	projects/prj-shrd-secu-5 projects/prj-key-mgt-dev-20334
Active	Restrict which services may create resources without CMEK	gcp.restrictNonCmekServices	List	compute.googleapis.com
Active	Service account key expiry duration in hours	iam.serviceAccountKeyExpiryHours	List	2160h
Active	Restrict Public IP access on Cloud SQL instances	sql.restrictPublicIp	Boolean	Denied All
Active	Skip default network creation	compute.skipDefaultNetworkCreation	Boolean	Enforcement on
Active	RequireLabelsInstance	custom.RequireLabelsInstance	Custom	resource.labels["appserviceid"] == "" || resource.labels["appservicename"] == "" || resource.labels["timestamp"] == "" || resource.labels["iac"] == "" || resource.labels["datatype"] == "" || resource.labels["costcenter"] == "" || resource.labels["tierid"] == ""
Active	Enforce uniform bucket-level access	storage.uniformBucketLevelAccess	Boolean	Enforcement on

Organization Policy IaC repo [QDXEnterpriseOrg/dso-gcpfoundation-iac-org: Repository for gcpfoundation-iac]

3. Cloud Armor & Advanced network DDoS protection

An organization policy acts as a guardrail to enforce security, compliance, and governance best practices across entire gcp cloud environment. It's essentially a set of rules or constraints that you define and apply to control how resources are used within your organization. These rules can be quite granular, allowing you to target specific resource types, configurations, or behaviors.



Advanced network DDoS protection

Always-on attack detection and mitigation to defend against volumetric network and protocol DDoS attacks to workloads using external network load balancers, protocol forwarding, and VMs with Public IP addresses. Advanced network DDoS protection enabled in external network load balancer from gcp console.

3.1. Cloud Armor policies

Preconfigured WAF rule sets to mitigate against the OWASP Top 10 web application security vulnerabilities

Policy Name	Scope	Target name	Target endpoints	Target type
owasp-policies-ue4	us-east4	**gcp-ue4-non-prod-fgt-ilb1-be** **gcp-ue4-prd-fgt-alb-be**	lb-ue4-galb-np-1 lb-ue4-galb-prd-1	Backend service (external application load balancer)
owasp-policies-uw1	us-west1	**gcp-uw1-non-prod-fgt-alb-be** **gcp-uw1-prd-fgt-alb-be**	lb-uw1-galb-np-1 lb-uw1-galb-prd-1	Backend service (external application load balancer)
advanced-network-ddos-protection-for-us-east4	us-east4	**new-network-edge-security-service**	lb-ue4-elb-np-1 lb-uw1-elb-prd-1	Network edge security service
advanced-network-ddos-protection-for-us-west1	us-west1	**new-network-edge-security-service**	lb-uw1-elb-np-1 lb-uw1-elb-prd-1	Network edge security service

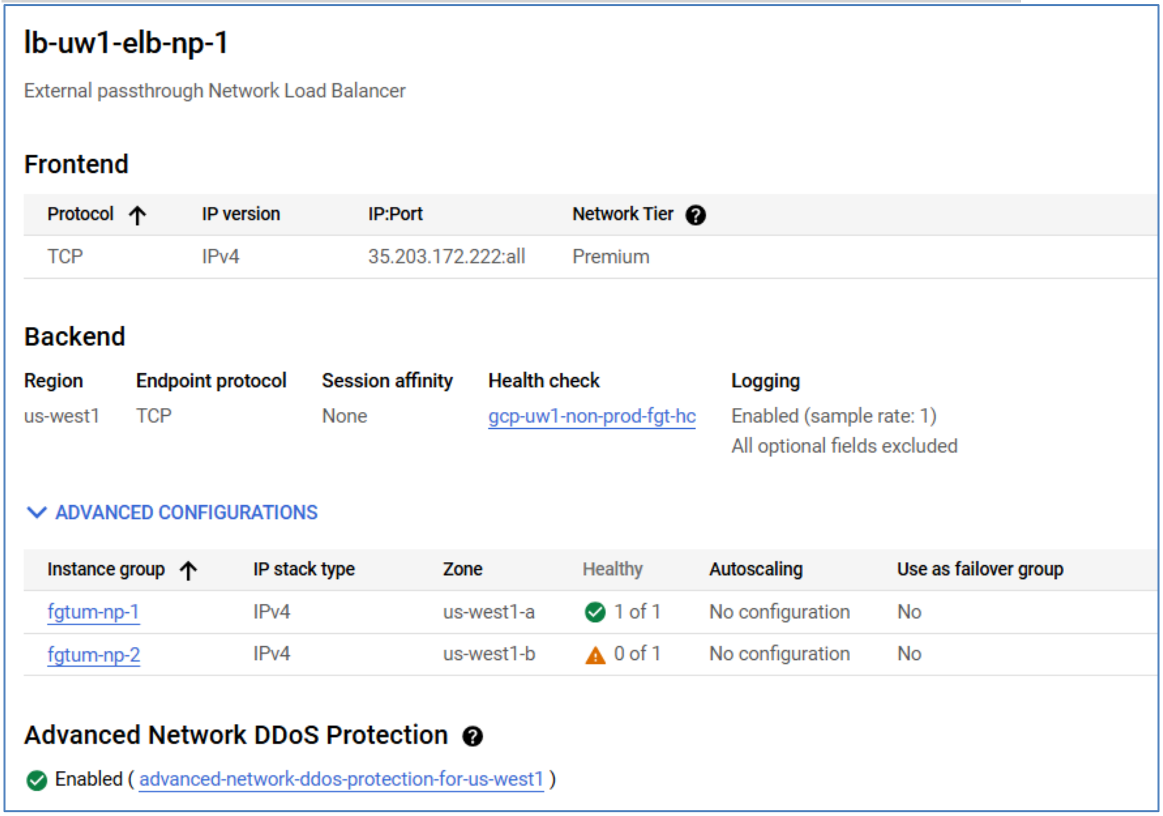
Cloud Armor preconfigured WAF rules configured vi IaC terraform

Cloud Armor IaC Repo Armor Repo

Action	Match	Description	Priority
Deny (403): preview only	evaluatePreconfiguredWaf('sqli-v33-stable', {'sensitivity': 1})	sqli-v33-stable	1
Deny (403): preview only	evaluatePreconfiguredWaf('xss-v33-stable', {'sensitivity': 1})	Cross-site-scripting	2
Deny (403): preview only	evaluatePreconfiguredWaf('lfi-v33-stable', {'sensitivity': 1})	lfi-v33-stable	3
Deny (403): preview only	evaluatePreconfiguredWaf('rfi-v33-stable', {'sensitivity': 1})	rfi-v33-stable	4
Deny (403): preview only	evaluatePreconfiguredWaf('rce-v33-stable', {'sensitivity': 1})	rce-v33-stable	5
Deny (403): preview only	evaluatePreconfiguredWaf('methodenforcement-v33-stable', {'sensitivity': 1})	methodenforcement-v33-stable	6
Deny (403): preview only	evaluatePreconfiguredWaf('scannerdetection-v33-stable', {'sensitivity': 1})	scannerdetection-v33-stable	7
Deny (403): preview only	evaluatePreconfiguredWaf('protocolattack-v33-stable', {'sensitivity': 1})	protocolattack-v33-stable	8
Deny (403): preview only	evaluatePreconfiguredWaf('php-v33-stable', {'sensitivity': 1})	php-v33-stable	9

Deny (403): preview only	evaluatePreconfiguredWaf('sessionfixation-v33-stable', {'sensitivity': 1})	sessionfixation-v33-stable	10
Deny (403): preview only	evaluatePreconfiguredWaf('java-v33-stable', {'sensitivity': 1})	java-v33-stable	11
Deny (403): preview only	evaluatePreconfiguredWaf('nodejs-v33-stable', {'sensitivity': 1})	nodejs-v33-stable	12
Allow	* (All IP addresses)	Default rule, higher priority overrides it	2,147,483,647

External network non-prod Load balancer with Advanced network DDoS protection



lb-uw1-elb-np-1

External passthrough Network Load Balancer

Frontend

Protocol ↑	IP version	IP:Port	Network Tier ?
TCP	IPv4	35.203.172.222:all	Premium

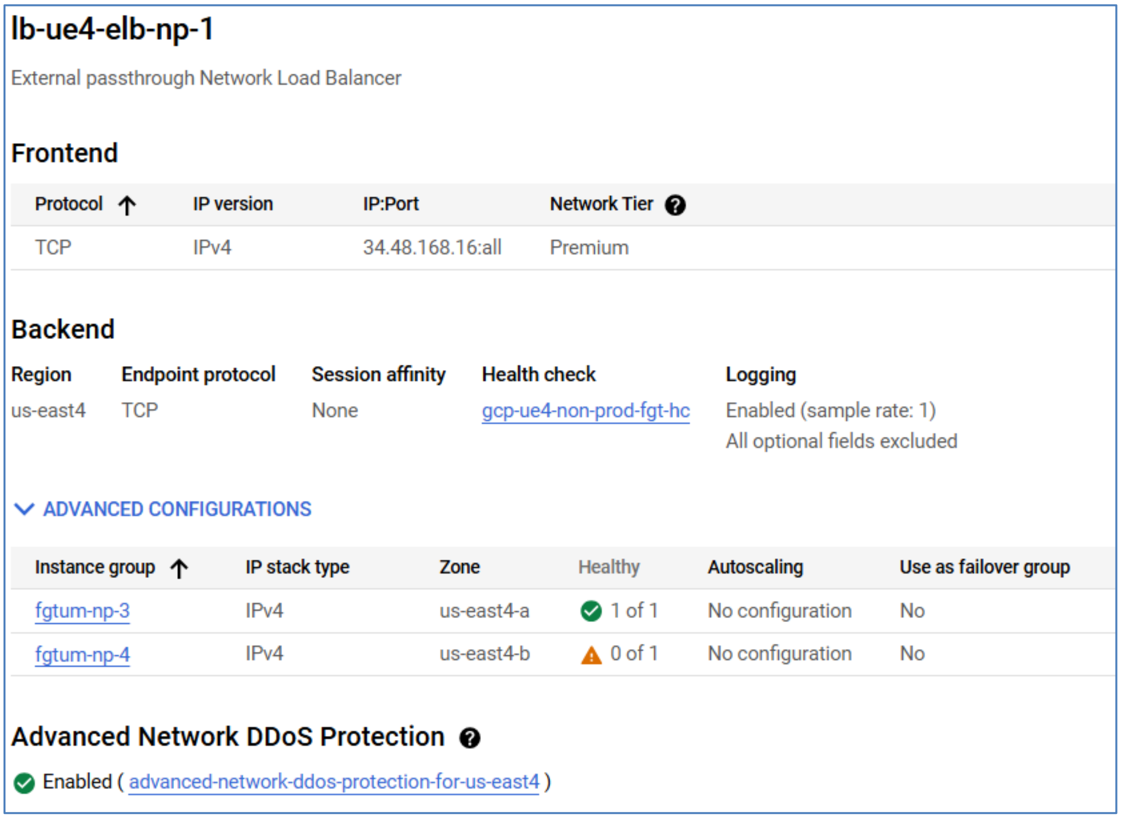
Backend

Region	Endpoint protocol	Session affinity	Health check	Logging
us-west1	TCP	None	gcp-uw1-non-prod-fgt-hc	Enabled (sample rate: 1) All optional fields excluded

Instance group ↑	IP stack type	Zone	Healthy	Autoscaling	Use as failover group
fgtum-np-1	IPv4	us-west1-a	✓ 1 of 1	No configuration	No
fgtum-np-2	IPv4	us-west1-b	⚠ 0 of 1	No configuration	No

Advanced Network DDoS Protection ?

✓ Enabled (advanced-network-ddos-protection-for-us-west1)



lb-ue4-elb-np-1

External passthrough Network Load Balancer

Frontend

Protocol ↑	IP version	IP:Port	Network Tier ?
TCP	IPv4	34.48.168.16:all	Premium

Backend

Region	Endpoint protocol	Session affinity	Health check	Logging
us-east4	TCP	None	gcp-ue4-non-prod-fgt-hc	Enabled (sample rate: 1) All optional fields excluded

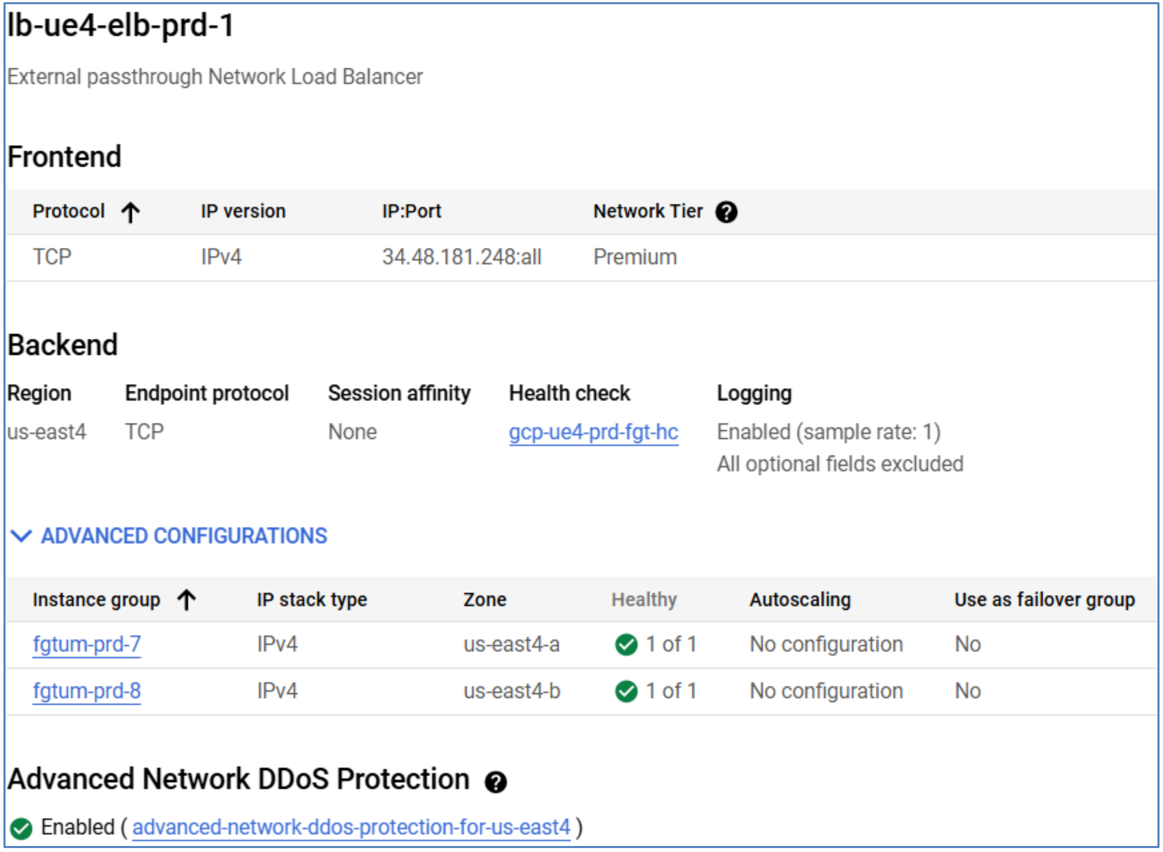
ADVANCED CONFIGURATIONS

Instance group ↑	IP stack type	Zone	Healthy	Autoscaling	Use as failover group
fgtum-np-3	IPv4	us-east4-a	✓ 1 of 1	No configuration	No
fgtum-np-4	IPv4	us-east4-b	⚠ 0 of 1	No configuration	No

Advanced Network DDoS Protection ?

✓ Enabled (advanced-network-ddos-protection-for-us-east4)

External network prod Load balancer with Advanced network DDoS protection



lb-ue4-elb-prd-1

External passthrough Network Load Balancer

Frontend

Protocol ↑	IP version	IP:Port	Network Tier ?
TCP	IPv4	34.48.181.248:all	Premium

Backend

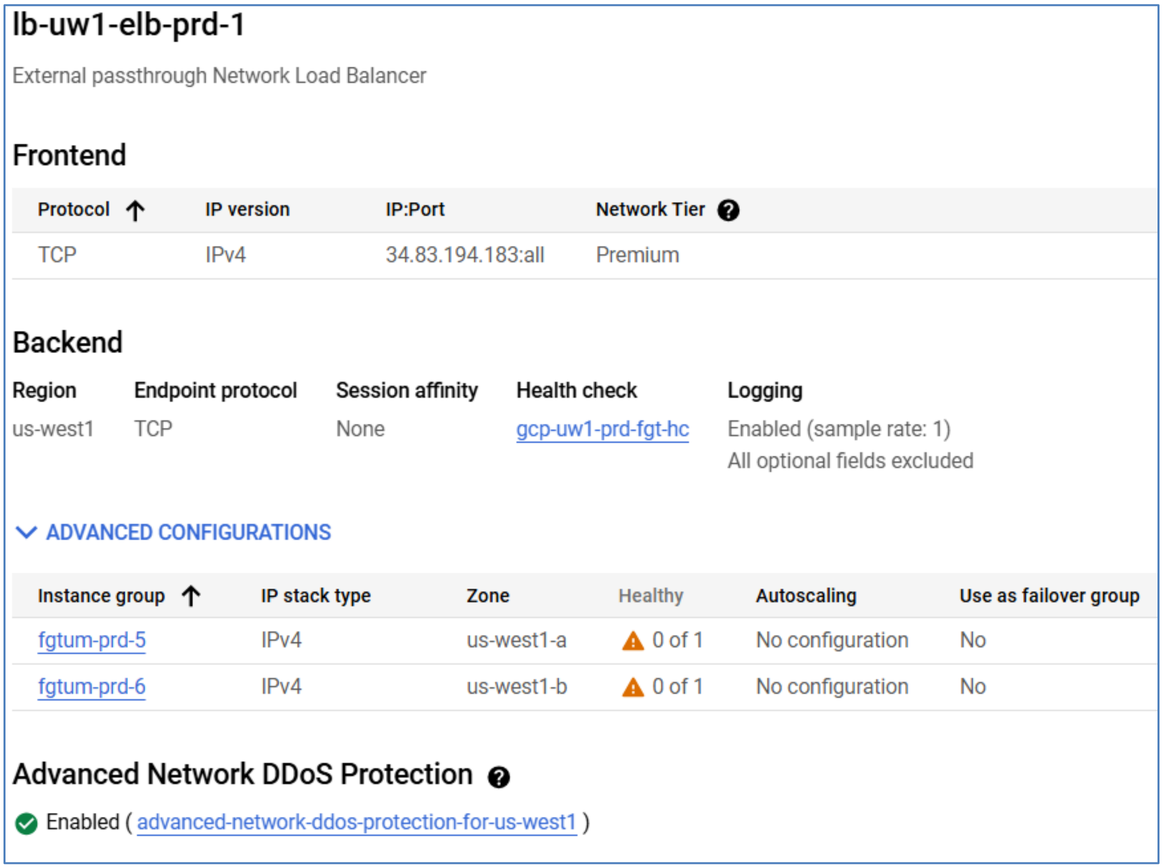
Region	Endpoint protocol	Session affinity	Health check	Logging
us-east4	TCP	None	gcp-ue4-prd-fgt-hc	Enabled (sample rate: 1) All optional fields excluded

ADVANCED CONFIGURATIONS

Instance group ↑	IP stack type	Zone	Healthy	Autoscaling	Use as failover group
fgtum-prd-7	IPv4	us-east4-a	✓ 1 of 1	No configuration	No
fgtum-prd-8	IPv4	us-east4-b	✓ 1 of 1	No configuration	No

Advanced Network DDoS Protection ?

✓ Enabled (advanced-network-ddos-protection-for-us-east4)



lb-uw1-elb-prd-1

External passthrough Network Load Balancer

Frontend

Protocol ↑	IP version	IP:Port	Network Tier ?
TCP	IPv4	34.83.194.183:all	Premium

Backend

Region	Endpoint protocol	Session affinity	Health check	Logging
us-west1	TCP	None	gcp-uw1-prd-fgt-hc	Enabled (sample rate: 1) All optional fields excluded

Instance group ↑	IP stack type	Zone	Healthy	Autoscaling	Use as failover group
fgtum-prd-5	IPv4	us-west1-a	⚠ 0 of 1	No configuration	No
fgtum-prd-6	IPv4	us-west1-b	⚠ 0 of 1	No configuration	No

Advanced Network DDoS Protection ?

✓ Enabled (advanced-network-ddos-protection-for-us-west1)

4. GCP Native Firewall Rules

Firewall rules configured to allow communication to and from the interfaces of the Fortinet Firewall appliance.

Rule Name	Type		Target	Source	Destination	Protocols and ports	Action
from-onprem	Ingress firewall rule	1000	Apply to all	IPv4 ranges: 10.0.0.0/8, 156.30.0.0/16, 172.18.0.0/26	IPv4 ranges: 10.141.0.0/16, 10.142.0.0/16, 10.143.0.0/16	All	Allow
fw-allow-ingress-lbprob-hub-external	Ingress firewall rule	900	Apply to all	IPv4 ranges: 209.85.204.0/22, 209.85.152.0/22, 130.211.0.0/22, 35.191.0.0/16	IPv4 ranges: 34.83.194.183, 35.230.104.110, 35.245.13.221, 35.203.172.222, 34.48.168.16, 10.143.0.0/27, 35.221.52.89, 35.230.47.169,	tcp:8008	Allow

					34.48.181.248, 10.143.0.32/27		
to-onprem-ipranges	Egress firewall rule	1000	Apply to all	IPv4 ranges: 10.141.0.0/16, 10.142.0.0/16, 10.143.0.0/16	IPv4 ranges: 10.0.0.0/8, 156.30.0.0/16, 172.18.0.0/26	All	Allow

GCP Firewall rules configured via terraform.

GCP Native Firewalls Repo QDXEnterpriseOrg/dso-gcpfoundation-iac-network: Repository for gcpfoundation-iac

5. Customer-Managed Encryption Keys (CMEK)

5.1. Key Management

Cloud Key Management Service (Cloud KMS) using customer-managed encryption keys (CMEK) for GCP Projects & services. Provides better control over encryption key management by restricting the source of keys.

Projects configured to supply KMS CryptoKeys for CMEK

Org Policy	Description	Publisher Project / Service
restrictCmekCryptoKeyProjects	Ensures that CMEK keys from other projects cannot be used to protect newly created resources	**projects/prj-shrd-secu-5** **projects/prj-key-mgt-dev-20334**
restrictNonCmekServices	Ensure specified services, newly created resources must be protected by a CMEK key.	**compute.googleapis.com**

KMS CMEK Repo KMS

6. Trusted Images

Specify projects' images can be used to create virtual machines (VMs) in Google Cloud environment. Only allows images from trusted projects and maintains a secure and consistent environment with approved images.

Org Policy	Description	Publisher Projects
compute.trustedImageProjects	only images from trusted projects will be allowed as the source for boot disks for new instances	**projects/prj-ospacker-useast-dev-23295**

Note: Exception given to prj-ospacker-useast-dev-23295 project to pull public images. Although Image with basic hardening script further quest team add required hardening steps.

Packer document Reference Packer Pipeline Documentation

Packer Repo gcp-ospacker-Repo

7. Certificate Manager

Certificate Manager API enabled and based on further application requirement; managed certificate can be easily add/used within certificate manager.

8. VPC Service Control

API enabled based on further application-based and sensitive data it can be used.

9. Security Command Center

Security Command Center **Standard** tier activated manually at organization-level for basic security posture management for Google Cloud. Environment is secure by managed vulnerability assessment scanning for Google Cloud that can automatically detect the highest severity vulnerabilities and misconfigurations for Google Cloud assets.

10. IAM

Identity and Access Management (IAM) admins fine-grained access control used in quest gcp , visibility for centrally managing enterprise cloud resources and enhance security and reduce the risk of unauthorized access.

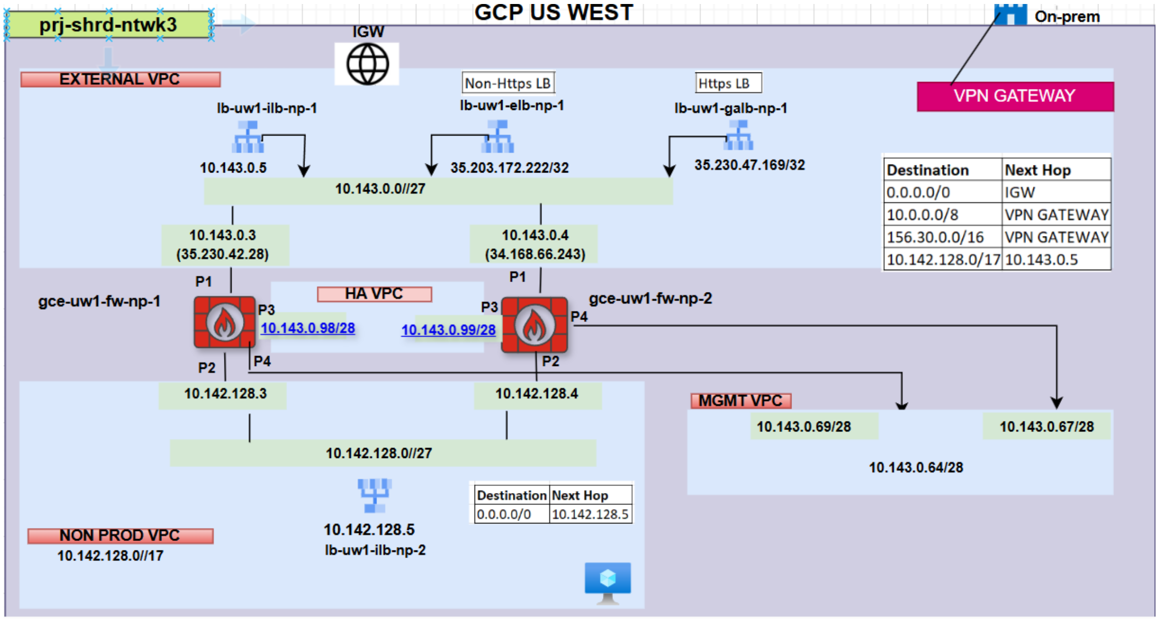
IAM Document IAM document

11. Third Party Tools

11.1. Fortinet Firewall

Fortinet Firewall will be composed of two VMs in an Active-Passive configuration for High Availability. Each VM will be in a different zone of the same region. Internal Network Load Balancers will be used to forward internal traffic to the Active VM. The backends of the NLBs will be two unmanaged instance groups (one for each VM).

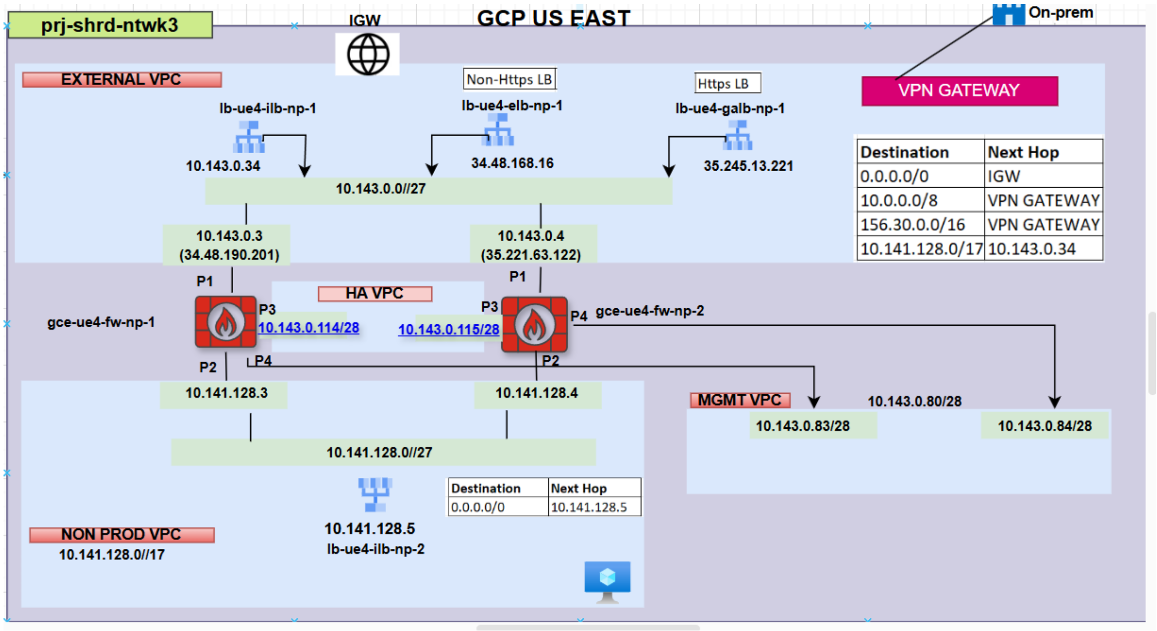
US WEST NP ARCHITECTURE



Destination	Next Hop
0.0.0.0/0	IGW
10.0.0.0/8	VPN GATEWAY
156.30.0.0/16	VPN GATEWAY
10.142.128.0/17	10.143.0.5

Destination	Next Hop
0.0.0.0/0	10.142.128.5

US EAST NP ARCHITECTURE



Destination	Next Hop
0.0.0.0/0	IGW
10.0.0.0/8	VPN GATEWAY
156.30.0.0/16	VPN GATEWAY
10.141.128.0/17	10.143.0.34

Destination	Next Hop
0.0.0.0/0	10.141.128.5

Fortinet document Reference Quest_GCP_FGT_Runbookv1.docx

Fortinet Repo Reference fortigate Repo

11.2. Wiz

Wiz is a cloud security tool used in Quest Google Cloud to secure environments. It can:

- **Assess security**: Scan the entire Google Cloud environment for vulnerabilities and misconfigurations
- **Detect threats**: Identify potential threats in real time
- **Prioritize remediation**: Prioritize remediation efforts based on risk severity
- **Reduce compliance friction**: Perform automated compliance assessments

Wiz.io integration document Reference Wiz.io_integration_Documentation.docx

11.3. Dynatrace

Dynatrace automatically discovers, baselines, and intelligently monitors Google Cloud environments to provide fault domain isolation and infrastructure and end-user visibility in real time.

Dynatrace integration document Reference Dynatrace-GCP integration document

12. IaC Repo Reference

Organization Policy QDXEnterpriseOrg/dso-gcpfoundation-iac-org: Repository for gcpfoundation-iac

GCP Native Firewalls QDXEnterpriseOrg/dso-gcpfoundation-iac-network: Repository for gcpfoundation-iac

GCP OS Packer https://github.com/QDXEnterpriseOrg/dso-gcp-packer

Github selfhost runner dso-gcpfoundation-iac-gha-runner/terraform-google-cloud-ghrunner at gha-config-files · QDXEnterpriseOrg/dso-gcpfoundation-iac-gha-runner

IAM https://github.com/QDXEnterpriseOrg/dso-gcpfoundation-iac-iam

13. Overall Handover documents Reference

HCL to Quest handover Documents