

1. Introduction

1.1. Purpose of this Document: This document serves as a comprehensive knowledge transfer resource for the Google Cloud Platform (GCP) network services deployed for Quest Diagnostics . Its primary aim is to equip the designated team with the necessary understanding and practical guidance to effectively manage, maintain, and troubleshoot the current GCP network infrastructure. This document consolidates information derived from the original Technical Design Document (TDD) prepared by GCP Architects and includes implementation details, configuration specifics, and validation procedures for all core networking components. Ultimately, this handover document empowers the team to independently operate and evolve the GCP network environment to meet future business requirements. It promotes continuity, reduces reliance on specific individuals, and ensures the long-term stability and security of the cloud infrastructure.

1.2. Scope: The scope of this document encompasses all networking components implemented within the Quest's Google Cloud Platform environment, as documented in the original Technical Design Document (TDD). It specifically covers:

- Network connectivity solutions, including the plan for Dedicated Interconnect to On-Premises, Classic VPN to On-Premises, GCP Classic VPN to AWS , GCP VPN to Azure and cross-cloud interconnect plans for AWS and Azure.
- Virtual Private Cloud (VPC) infrastructure, including Shared VPCs, Standalone VPCs, Subnets, and VPC Flow Logs configuration.
- Private access mechanisms for Google APIs and Google Services, including Private Google Access (PGA), Private Service Connect (PSC), and Private Service Access (PSA).
- IP Addressing Spaces allocated and routing strategy configured for entire network estate .
- Google Cloud Stateful Firewall Rulesets, details with their implementation / purpose

This document will explicitly refer to specific page numbers within the original TDD where more detailed information can be found. This Document excludes compute, IAM and storage setup for network infra related functions.

1.3. Target Audience: This document is primarily intended for the following personnel and teams within Quest:

- **Cloud Operations Team:** Responsible for the day-to-day operations of the GCP environment.

- **Network Engineers:** Responsible for designing, implementing, and troubleshooting network connectivity and security within GCP.
- **Security Engineers:** Responsible for ensuring the security posture of the GCP network infrastructure, including firewall rules and access controls.
- **Infrastructure Architects:** Responsible for planning and designing future GCP infrastructure enhancements and expansions
- **Application development teams :** Support design review or access of external APIs from applications .

The document assumes a working knowledge of cloud computing concepts, network fundamentals (TCP/IP, routing, firewalls), and basic familiarity with the Google Cloud Platform. While comprehensive, some advanced topics might require consultation of the original TDD or official Google Cloud documentation .

1.4. Document Version History: To maintain accuracy and track changes over time, all revisions to this document will be recorded in the table below. This ensures transparency and facilitates the identification of the most current and relevant information. The document would be reviewed by Quest stakeholders.

Version	Date (YYYY-MM-DD)	Author	Changes Description
1.0	2025-02-13	Sonal Sharma	Initial Draft – Based on TDD.

2. Overview of GCP Network Architecture

2.1. High-Level Design (Reference TDD Page 45):

- **Purpose of Networking Design:** The networking design's core purpose is to enable secure and efficient communication between Google Cloud resources, Quest's on-premises data centers, and third-party cloud environments (AWS and Azure). The design emphasizes both connectivity and segregation/protection of resources to align with Quest's security and compliance requirements. As depicted in the TDD on page 45, the architecture is centered around Fortinet Firewall appliances used to inspect and control traffic traversing between the internal & external world with Internet breakout also handled. External Load Balancers is also part of external routing as a design. A hub-and-spoke model with Fortinet inspection at the center is employed for comprehensive traffic control. This design supports the following key requirements outlined in Section 5.1 of the TDD:

- Support for a multi-region GCP footprint (US initially, with future expansion to Europe possible).
- Dedicated, high-capacity, and low-latency connection from Google Cloud to Quest's US data centers.
- High-capacity connections from Google Cloud to Quest's environments in AWS and Azure.
- Secure and encrypted connections for all external communications, with encrypted connection between VPCs wherever its possible & based security concern , review
- Utilization of Fortinet NGFW appliances for:
 - Traffic inspection between On-Premises and Google Cloud.
 - Traffic inspection between other Cloud providers (AWS & Azure) and Google Cloud.
 - Traffic inspection between the Internet and Google Cloud.
 - Traffic inspection between non-production and production Google Cloud environments.
- Possibility of traffic inspection between network segments within Google Cloud (supported but dependent on workload VPC placement).
- Internal DNS naming resolution across all environments, leveraging google manage Cloud DNS system for easy manageability and in real-time & near live performance DNS Resolution.
- Comprehensive logging of all network traffic within Google Cloud.
- Protection of externally exposed applications with a Web Application Firewall (WAF) native solution at each regions deployed in GCP & also enabled logging policies and alerted with integration ,
- Use of CDN solutions to efficiently serve content closer to end-users on high available ,

Two separate environments have created in Fortinet (Production Vs Non - Prod) in dedicated VMs created , to cater individual requirement , from various client groups / tier applications across hosted instances under their subnet ranges.

2.2. Google Cloud Regions (Reference TDD Page 47):

- Quest utilizes two regions within the US to host their Google Cloud resources. Future expansion to regions in Europe is also under consideration. As described on TDD page 47, these two regions were selected based on the following requirements:

- **User Proximity:** Optimal locations to minimize latency for users in both the US East and West.
 - **Data Center Proximity:** Consideration of proximity to Quest’s existing data centers near Philadelphia and Dallas and minimize impact on access tier / traffic redirection, causing latencies due geographic distance across locations and hop counts between the gateways (Cloud).
 - **Resource Availability and Region Health:** Assured availability of necessary resources and overall region stability to avoid capacity constraints & proper function of the services is key across globe .
 - **Feature Release Timing:** Selection of regions that generally receive new Google Cloud features and services early, Google consider priority. Interconnect links with support for MACsec ports.
- Based on these criteria, the following two regions were selected for the initial deployment with consideration of region access , uptime history - us-east4 and us-west1 :

Region	Google Cloud Region	Details
US East	us-east4 (Virginia)	Excellent connectivity to the East Region and good availability of services.
US West	us-west1 (Oregon)	Excellent connectivity to the West Region and suitable for disaster recovery.

3. Connection to Google Cloud

Pre-requisites for Interconnect(Dedicated & Cross-Cloud) Links :

- Project “prj-shrd-intc-9” created under the Shared Infra Network folder.
- Request to whitelist the project to order MACSec 10Gbps links. This was enabled and approved on 17 Dec 2024

3.1. Dedicated Interconnect to On-Premises DC’s (Reference TDD

Page 47)

- Note: While the Dedicated Interconnect is not deployed, documenting the plan helps future reference, and provide business continuity planning if business comes with Dedicated line/ Interconnect line later with GCP). Google PSO has shared “Interconnect Setup” document upload in Quest Sharepoint with specific details

3.1.1.Pre-requisites for Dedicated Interconnect to On-Premises DC's :

- On-Prem IP ranges which would connect to GCP over the Dedicated Interconnect

3.1.2.Steps to follow for setting up Dedicated Interconnect to On-Premises DC's(QDC & TDC)

Order Dedicated Interconnect Links:

1. Order 4 links (2 each for us-east & us-west) according to the Technical Design Document (TiDD) manually in the console.
2. Retrieve LOAs (Letter of Authorization) and share them with the Telco Provider (Lumen & Verizon) .
3. Wait for the link to be up and test the link.

Google Cloud Configuration:

4. In Project :- **prj-shrd-ntwk-3**, Create Cloud Routers in Google Cloud with VPC/Network:- **vpc-hub-external** and Region:- **us-east4**.
5. Create VLAN attachments for **us-east4** in Project :- **prj-shrd-ntwk-3** using steps mentioned in [GCP Document](#) . Using option :- To use connections in another project, select **In another project**, and then enter the Project ID:- **prj-shrd-intc-9** of the project.
6. Configure the on-premises router using steps mentioned in GCP [Document](#).
7. Configure MACsec using steps mentioned in GCP [Document](#).

Repeat the steps 4 to 7 for the second Dedicated Interconnect connection pair for region (us-west1).

When we create the second set of VLAN attachments for the second Dedicated Interconnect connection pair, specify a second region (us-west1) with another Cloud Router.

3.2. Setup Cross-Cloud Interconnect to AWS:

Cross-Cloud Interconnect lets us establish a dedicated physical connection between Google Cloud and Amazon Web Services (AWS) networks. Google provisions this physical connection on our behalf. However, as part of the setup process, we must complete several tasks. Google PSO has shared "Interconnect Setup" document upload in Quest Sharepoint with specific details

3.2.1.Prerequisite for Cross-Cloud Interconnect to AWS :-

AWS VPC ranges which would connect to GCP over the Cross-Cloud Interconnect

3.2.2. Steps to follow for setting up Cross-Cloud Interconnect to AWS:-

1. AWS Cross-Cloud Interconnect Locations :- The Locations have already been finalized and updated in TiDD, here is the same table for reference :-

Google Cloud Region	AWS Region	Metro area	Google Remote Location	AWS Remote Location
us-east4	us-east-1	Washington DC	aws-eqdc2	EqDC2
us-west1	us-west-2	Oregon	aws-ecpo1	ECPO1

2. Order Cross-Cloud Interconnect connections:- We need to Order Cross-Cloud Interconnect links from the console in **Project ID:- prj-shrd-intc-9** according to TiDD.

We need to place an order for two Cross-Cloud Interconnect connections—a primary connection(us-east4 region) and a redundant one (us-west1 region). In response, Google reserves two ports for Quest in the facility specified below & document in TiDD. For each port, Google sends a confirmation email that contains instructions related to the next step: ordering your AWS ports.

Here is link of Google official document for :- <https://cloud.google.com/network-connectivity/docs/interconnect/how-to/ci/aws/order-google-connections>

3. Order AWS ports :- Once google confirms the order then we Order the AWS ports for this cross-cloud interconnect and download the corresponding letter of authorization (LOA). This document confirms our right to use the ports.

Note:- To set up redundancy, order two LAGs by following the LAG ordering process twice

We will send the LOA to Google, following the instructions from the confirmation email that Google sent you. After Google receives the LOA, they begin the process of establishing these connections.

Here is link of Google official document for :- <https://cloud.google.com/network-connectivity/docs/interconnect/how-to/ci/aws/order-aws-ports>

4. Configure your Google Cloud resources:- In **Project prj-shrd-ntwk-3** , we would create 2 cloud routers each for us-east4 and us-west1 region(as per the region for which Order has been placed) in VPC/network (vpc-hub-external).

Cloud Router an ASN of 16550 or any private ASN (64512-65534,4200000000-4294967294) which is not used in AWS.

Here is link of Google official document for :- <https://cloud.google.com/network-connectivity/docs/router/how-to/create-router-vpc-network#create-a-cloud-router>

After links are up in **Project :- prj-shrd-intc-9**, we create two VLAN attachments in **Project prj-shrd-ntwk-3** in our VPC/network (**vpc-hub-external**), one for each of your Cross-Cloud Interconnect connections in **Project :- prj-shrd-intc-9** using steps mentioned in [GCP Document](#).

Each VLAN attachment represents a logical connection between a region in your VPC network and your AWS resources.

Then, for each VLAN attachment, use a Cloud Router to configure a Border Gateway Protocol (BGP) peering session. Configure Border Gateway Protocol (BGP) sessions in **project prj-shrd-ntwk-3**, one for each VLAN attachment using steps mentioned in [GCP Document](#).

5. Configure your AWS resources:- Create Direct Connect Gateway, Virtual Private Interface, and Virtual Private Gateway in AWS using steps mentioned in [GCP Document](#).

6. Verify your connections using steps mentioned in [GCP Document](#).

7. Setup and enable MACsec using steps mentioned in [GCP Document](#).

3.3. Setup Cross-Cloud Interconnect to Azure (Planned but Not Yet Implemented)

Like AWS Cross-Cloud Interconnect, Google provisions this physical connection on our behalf. However, as part of the setup process, we must complete several tasks. While we complete some tasks before Google provisions our connection and some tasks done afterward. Google PSO has shared “Interconnect Setup” document upload in Quest Sharepoint with specific details

3.3.1. Prerequisite for Cross-Cloud Interconnect to Azure

Azure Vnet with subnets which would connect to GCP over the Cross-Cloud Interconnect

3.3.2. Steps to follow for setting up Cross-Cloud Interconnect to Azure

1. Azure Cross-Cloud Interconnect Locations :- The Locations have already been finalized and updated in TiDD, here is the same table for reference :-

Google Cloud Region	Azure Region	Metro area	Google Remote Location	Azure Remote Location
us-east4	US-East-1 -(N. Virginia)	Washington D.C.	azure-equinix-ashburn-dc2	Equinix-Ashburn-DC2
us-west1	US-West2 -(California)	San Francisco	azure-coresite-santa-clara-sv7	CoreSite-Santa-Clara-SV7

2. Order Cross-Cloud Interconnect connections :- we need to Order Cross-Cloud Interconnect links from the console in **Project ID:- prj-shrd-intc-9** according to TiDD.

We need to place an order for two Cross-Cloud Interconnect connections—a primary connection(us-east4 region) and a redundant one (us-west1 region). In response, Google reserves two ports for Quest in the facility specified below & document in TiDD. For each port, google sends a confirmation email that contains instructions related to the next step: ordering your Azure ports.

Here is link of Google official document for :- <https://cloud.google.com/network-connectivity/docs/interconnect/how-to/cci/azure/order-google-connections>

3. Order Azure ports :- Once google confirms the order then we Order the Azure ports for this cross-cloud interconnect and download the corresponding letter of authorization (LOA). This document confirms our right to use the ports. We send the LOA to Google, following the instructions from the confirmation email that Google sent you. After Google receives the LOA, they begin the process of establishing these connections.

Here is link of Google official document for :- <https://cloud.google.com/network-connectivity/docs/interconnect/how-to/cci/azure/order-azure-ports>

4. Configure your Google Cloud resources :- In **Project prj-shrd-ntwk-3** , we would create 2 cloud routers each for us-east4 and us-west1 region(as per the region for which Order has been placed) in VPC/network (vpc-hub-external). Cloud Router should have any ASN of 16550 or any private ASN that doesn't conflict with Azure requirements. (Azure reserves the 65515-65520 range for its internal use, which leaves 64512-65514 and 65521-65534.)

After the links are up , then we would create a redundant set of VLAN attachments in our Virtual Private Cloud (VPC) network (vpc-hub-external) . Each VLAN attachment represents a logical connection between a region in our VPC network (vpc-hub-external) and your Azure resources. Then, for each VLAN attachment, use a Cloud Router to configure a Border Gateway Protocol (BGP) peering session.

Here is link of Google official document for :- <https://cloud.google.com/network-connectivity/docs/interconnect/how-to/cci/azure/configure-google-resources>

5. Configure your Azure resources :- Configure your Azure resources. This step includes creating an ExpressRoute circuit, creating a private peering, and completing other tasks.

Here is link of Google official document for :- <https://cloud.google.com/network-connectivity/docs/interconnect/how-to/cci/azure/configure-azure>

6. Verify your connections :- Follow the recommended steps to verify that your networks are connected.

7. Setup and enable MACsec using steps mentioned in GCP [Document](#).

3.4. Classic VPN to On-Premises (Reference TDD Page 54)

Establish Temporary VPN Connectivity to On-Premises via Classic VPN using Static Routes for the Connection. Since existing On-Prem firewall devices don't support Dynamic BGP router capabilities therefor Classic VPN has been implemented for GCP to On-Prem connectivity ".

For redundancy 2 tunnels were created for Classic VPN's each from both of us-east4 and us-west1 region would be connecting to QDC(Philadelphia). End Point for both this tunnel is same On-Prem Side.

Note:- There is no direct connection to TDC(Dallas).

3.4.1. Prerequisite for Classic VPN to On-Prem

- Remote Peer IP Address - Public IP address of the On-Prem VPN Gateway.
- Remote Network IP Ranges - Static On-Prem IP ranges.

3.4.2. Steps for setting up Classic VPN gateway in GCP to On-Prem

Configure the Classic VPN Gateway

1. Navigate to the VPN Page :

- In the Google Cloud console, go to the VPN page of Project:- prj-shrd-ntwk-3.

2. Create a VPN Connection :

- Select the VPN setup wizard .
- Choose the Classic VPN option.
- Click Continue .

3. Specify Gateway Settings :

- Name : Enter the name of the VPN gateway (cannot be changed later).
- Description : Optionally, add a description.

- Network : Specify an existing VPC network(vpc-hub-external) in which to create the VPN gateway and tunnel.

- Region : us-east4 or us-west1

- IP Address : Create a regional external IP address by Reserving a new static IP address(This would be shared with the Peer{On-Prem, AWS, Azure} Networking Team)

Configure Tunnels

4. Specify Tunnel Settings :

- Name : Enter the name of the VPN tunnel (cannot be changed later).

- Description : Optionally, add a description.

- Remote Peer IP Address : Specify the external IP address of the peer VPN gateway((This is provided by Peer{On-Prem, AWS, Azure or other GCP Organizations} Networking Team).

- IKE Version : Choose the appropriate IKE version supported by the peer VPN gateway. IKEv2 is preferred & has been used for On-Prem & AWS VPN's.

- Click Generate & Copy for a new IKE Pre-Shared Key (This would be shared with the Peer{On-Prem, AWS, Azure} Networking Team)

For Route-Based Tunnels

6. Routing Options :

- Under Routing options , select Route-based .

- Remote Network IP Ranges : Provide a space-separated list of the IP ranges used by the peer network. These ranges are used to create custom static routes whose next hop is this VPN tunnel.

7. Add More Tunnels :

- If needed, click Add tunnel and repeat the previous steps to create more tunnels on the same gateway.

8. Create the VPN Connection :

- Click Create .

Complete the Configuration

9. Set Up the Peer(On-Prem, AWS, Azure or other GCP Organizations) VPN Gateway :

- using the GCP Tunnel External IP and Pre-Shared Key generated after steps 3 & 4 respectively.

- Configure the corresponding tunnel on the peer VPN gateway. Refer to specific configuration guidance for certain peer VPN devices or general configuration parameters.

10. Configure Firewall Rules :

- Set up firewall rules in Google Cloud and your peer network as required.

Filter: 10.0.0.0/8 Enter property name or value											
<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ↑	Logs	Hit count ?	Last hit ?
<input type="checkbox"/>	fw-allow-egress-gcp-onprem	Egress	Apply to all	IP ranges: 156.30.0.0/16, 10.0.0.0/8, 172.18.0.0/26 Local IP ranges: 10.142.0.0/16, 10.141.0.0/16, 10.143.0.0/16	All	Allow	1000	vpc-hub-external	On	50051	2025-02-20 (15:21:00)
<input type="checkbox"/>	fw-allow-ingress-onprem-gcp	Ingress	Apply to all	IP ranges: 156.30.0.0/16, 10.0.0.0/8, 172.18.0.0/26 Local IP ranges: 10.142.0.0/16, 10.141.0.0/16, 10.143.0.0/16	All	Allow	1000	vpc-hub-external	On	9145	2025-02-20 (15:21:00)

11. Check VPN Tunnel Status :

- Verify the status of your VPN tunnel and forwarding rules.

Google Cloud

prj-shrd-ntwk3

vpn

Search

Network Connect...

Network Connectivity Cen...

VPN

Interconnect

Cloud Router

VPN

VPN SETUP WIZARD

REFRESH

RECOMMENDED ALERTS

CLOUD VPN TUNNELS

CLOUD VPN GATEWAYS

PEER VPN GATEWAYS

CREATE VPN TUNNEL

VPN tunnels

DELETE

MANAGE FLOW LOGS

Filter

Peer VPN gateway (IP): 216.203.80.98

Enter property name or value

<input type="checkbox"/>	Name	Cloud VPN gateway (IP)	Peer VPN gateway (IP)	VPN tunnel status	Routing type	VPC network	Region	Type	Description
<input type="checkbox"/>	tun-ext-vpn-ue4-1	vpn-gw-ue4 34.48.201.245	216.203.80.98	Established	Route-based	vpc-hub-external	us-east4	Classic	Tunnel 1 VPN Gateway for US-East4
<input type="checkbox"/>	tun-ext-vpn-uw1-1	vpn-gw-uw1 34.168.101.124	216.203.80.98	Established	Route-based	vpc-hub-external	us-west1	Classic	Tunnel 1 for US-West 1 VPN Gateway

12. View VPN Routes :

- Go to the project routing table and filter for Next hop type: VPN tunnel to view your VPN routes.

tun-ext-vpn-ue4-1-route-1	Static	IPv4	10.0.0.0/8	1000	—	VPN tunnel tun-ext-vpn-ue4-1	vpc-hub-external
tun-ext-vpn-ue4-1-route-2	Static	IPv4	156.30.0.0/16	1000	—	VPN tunnel tun-ext-vpn-ue4-1	vpc-hub-external
tun-ext-vpn-ue4-1-route-3	Static	IPv4	172.18.0.0/26	1000	—	VPN tunnel tun-ext-vpn-ue4-1	vpc-hub-external
tun-ext-vpn-ue4-1-route-4	Static	IPv4	35.199.192.0/19	1000	—	VPN tunnel tun-ext-vpn-ue4-1	vpc-hub-external
tun-ext-vpn-uw1-1-route-1	Static	IPv4	10.0.0.0/8	1000	—	VPN tunnel tun-ext-vpn-uw1-1	vpc-hub-external
tun-ext-vpn-uw1-1-route-2	Static	IPv4	156.30.0.0/16	1000	—	VPN tunnel tun-ext-vpn-uw1-1	vpc-hub-external
tun-ext-vpn-uw1-1-route-3	Static	IPv4	172.18.0.0/26	1000	—	VPN tunnel tun-ext-vpn-uw1-1	vpc-hub-external
tun-ext-vpn-uw1-1-route-4	Static	IPv4	35.199.192.0/19	1000	—	VPN tunnel tun-ext-vpn-uw1-1	vpc-hub-external

Here is link of Google official document for :- <https://cloud.google.com/network-connectivity/docs/interconnect/how-to/cci/azure/configure-google-resources>
<https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns#console>

S. No	Gateway name	Cloud VPN gateway IP address	VPC network	Region	VPN tunnels	Peer VPN gateway (IP)	VPN tunnel status	Routing type	Description
1	vpn-gw-ue4	34.48.201.245	vpc-hub-external	us-east-4	tun-ext-vpn-ue4-1	216.203.80.98	Established	Route-based	GCP to On-Prem VPN gateway for Us-East4
2	vpn-gw-uw1	34.168.101.124	vpc-hub-external	us-west-1	tun-ext-vpn-uw1-1	216.203.80.98	Established	Route-based	GCP to On-Prem VPN gateway for US-West1

3.5. GCP VPN to AWS & Azure

VPNs are temporary solution while the Cross-Cloud Interconnect are setup. Once the Cross-Cloud Interconnect has been setup then we could decommission these VPN's.

3.5.1. Classic VPN to AWS (Reference TDD Page 55)

HA VPN was initially planned as per TiDD but as per Quest AWS Networking setup, deploying Transit gateway or Virtual private gateway was not an option and the Endpoint for GCP Tunnel would be Fortinet Firewall in AWS. Therefore, Classic VPN was setup for connecting GCP to AWS thru VPN.

3.5.1.1. Prerequisite for Classic VPN to On-Prem

- Remote Peer IP Address - Public IP address of the AWS Fortinet Firewall VPN Gateway.
- Remote Network IP Ranges - Static AWS IP ranges.

Using the steps mentioned for “Classic VPN gateway in GCP to On-Prem”, Classic VPN to AWS was setup. Firewall rules and Routing on both sides was setup to allow traffic.

Firewall Rules to allow traffic :-

Filter Filter: 10.0.0.0/8 × Enter property name or value ?											
<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ↑	Logs	Hit count ?	Last hit ?
<input type="checkbox"/>	fw-allow-egress-gcp-onprem	Egress	Apply to all	IP ranges: 156.30.0.0/16, 10.0.0.0/8, 172.18.0.0/26 Local IP ranges: 10.142.0.0/16, 10.141.0.0/16, 10.143.0.0/16	All	Allow	1000	vpc-hub-external	On	50051	2025-02-20 (15:21:00)
<input type="checkbox"/>	fw-allow-ingress-onprem-gcp	Ingress	Apply to all	IP ranges: 156.30.0.0/16, 10.0.0.0/8, 172.18.0.0/26 Local IP ranges: 10.142.0.0/16, 10.141.0.0/16, 10.143.0.0/16	All	Allow	1000	vpc-hub-external	On	9145	2025-02-20 (15:21:00)

Tunnel Status

VPN tunnels DELETE MANAGE FLOW LOGS ▼

Filter aws × Enter property name or value ×									
<input type="checkbox"/>	Name ↑	Cloud VPN gateway (IP)	Peer VPN gateway (IP)	VPN tunnel status	Routing type	VPC network	Region	Type	Description
<input type="checkbox"/>	clv-tun-gcp-ue4-aws-dev	clv-gcp-ue4-aws-dev 35.194.89.203	3.224.235.238	✔ Established	Route-based	vpc-hub-external	us-east4	Classic	Tunnel from GCP US-East4 to AWS Dev FortiGate Firewall
<input type="checkbox"/>	clv-tun-gcp-ue4-aws-ue1	clv-gcp-ue4-aws-ue1 34.48.105.115	52.204.89.228	✔ Established	Route-based	vpc-hub-external	us-east4	Classic	Tunnel from GCP US-East4 to AWS Prod US East1 FortiGate Firewall
<input type="checkbox"/>	clv-tun-gcp-uw1-aws-dev	clv-gcp-uw1-aws-dev 35.233.176.211	3.224.235.238	❌ No incoming packets	Route-based	vpc-hub-external	us-west1	Classic	Tunnel from Classic VPN from GCP US-west1 to AWS Dev FortiGate Firewall
<input type="checkbox"/>	clv-tun-gcp-uw1-aws-ue1	clv-gcp-uw1-aws-ue1 35.185.209.61	52.204.89.228	✔ Established	Route-based	vpc-hub-external	us-west1	Classic	Tunnel from Classic VPN from GCP US-west1 to AWS Prod US East1 FortiGate Firewall

Routes

+ CREATE ROUTE ↻ REFRESH

Filter aws × Enter property name or value							
<input type="checkbox"/>	Name ↑	Type	IP version	Destination IP range	Priority	Next hop	Network
<input type="checkbox"/>	clv-tun-gcp-aws-dev-route-3	Static	IPv4	10.124.0.0/14	1000	VPN tunnel clv-tun-gcp-ue4-aws-dev	vpc-hub-external
<input type="checkbox"/>	clv-tun-gcp-ue4-aws-dev-route-1	Static	IPv4	10.183.0.0/17	1000	VPN tunnel clv-tun-gcp-ue4-aws-dev	vpc-hub-external
<input type="checkbox"/>	clv-tun-gcp-ue4-aws-ue1-route-1	Static	IPv4	10.183.128.0/17	1000	VPN tunnel clv-tun-gcp-ue4-aws-ue1	vpc-hub-external
<input type="checkbox"/>	clv-tun-gcp-uw1-aws-dev-route-1	Static	IPv4	10.183.0.0/17	1000	VPN tunnel clv-tun-gcp-uw1-aws-dev	vpc-hub-external
<input type="checkbox"/>	clv-tun-gcp-uw1-aws-ue1-route-1	Static	IPv4	10.183.128.0/17	1000	VPN tunnel clv-tun-gcp-uw1-aws-ue1	vpc-hub-external

S. No	Gateway name	Cloud VPN gateway IP address	VPC network	Region	VPN tunnels	Peer VPN gateway (IP)	VPN tunnel status	Routing type	Description
1	clv-gcp-ue4-aws-dev	35.194.89.203	vpc-hub-external	us-east4	clv-tun-gcp-ue4-aws-dev	3.224.235.238	Established	Route-based	Classic VPN from GCP US-East4 to AWS Dev Fortinet Firewall
2	clv-gcp-ue4-aws-ue1	34.48.105.115	vpc-hub-external	us-east4	clv-tun-gcp-ue4-aws-ue1	52.204.89.228	Established	Route-based	Classic VPN from GCP US-East4 to AWS Prod US East1 Fortinet Firewall

3	clv-gcp-uw1-aws-dev	35.233.176.211	vpc-hub-external	us-west1	clv-tun-gcp-uw1-aws-dev	3.224.235.238	No incoming packets	Route-based	Classic VPN from GCP US-west1 to AWS dev Fortinet Firewall
4	clv-gcp-uw1-aws-ue1	35.185.209.61	vpc-hub-external	us-west1	clv-tun-gcp-uw1-aws-ue1	52.204.89.228	Established	Route-based	Classic VPN from GCP US-west1 to AWS Prod US East1 Fortinet Firewall

Here is link of Google official document for :- <https://cloud.google.com/network-connectivity/docs/interconnect/how-to/cci/azure/configure-google-resources>
<https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns#console>

3.5.2. VPN to Azure (Reference TDD Page 56)

HA VPN is recommended for VPN connection to Azure. But Quest Networking Team is working on setting up Azure side for GCP VPN . Once the Azure Vnet IP ranges and Remote Peer Public IP's are provided then we could follow the same steps we used for setting up "Classic VPN from GCP to On-Prem"

Here is link of Google official document for :- <https://cloud.google.com/network-connectivity/docs/interconnect/how-to/cci/azure/configure-google-resources>
<https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns#console>

3.5.3. VPN to Liferay GCP Organization

As part of QAW Project, Connectivity to Liferay GCP Organization was setup using the Classic VPN . Liferay Team provided the Remote Peer Public IP and Liferay IP Ranges.

Using these inputs, we created a single tunnel Classic VPN as required by Liferay and then shared our Cloud VPN gateway IP address , IKE2 Pre-Shared Key and Subnet/IP range to which Liferay tunnel would send traffic i.e. subnet :- sn-ue4-cloudsql-psc-dev-1(10.141.132.0/27) .

Firewall Rules allowing traffic:-

Filter: 10.0.0.0/8 Enter property name or value × ?											
<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ↑	Logs	Hit count ?	Last hit ?
<input type="checkbox"/>	fw-allow-egress-gcp-onprem	Egress	Apply to all	IP ranges: 156.30.0.0/16, 10.0.0.0/8, 172.18.0.0/26 Local IP ranges: 10.142.0.0/16, 10.141.0.0/16, 10.143.0.0/16	All	Allow	1000	vpc-hub-external	On	50051	2025-02-20 (15:21:00)
<input type="checkbox"/>	fw-allow-ingress-onprem-gcp	Ingress	Apply to all	IP ranges: 156.30.0.0/16, 10.0.0.0/8, 172.18.0.0/26 Local IP ranges: 10.142.0.0/16, 10.141.0.0/16, 10.143.0.0/16	All	Allow	1000	vpc-hub-external	On	9145	2025-02-20 (15:21:00)

Tunnel Status

VPN tunnelsDELETEMANAGE FLOW LOGS

Filter lif

Enter property name or value

<input type="checkbox"/>	Name ↑	Cloud VPN gateway (IP)	Peer VPN gateway (IP)	VPN tunnel status	Routing type	VPC network	Region	Type	Description
<input type="checkbox"/>	clv-tun-gcp-ue4-lif-uc1	clv-gcp-ue4-lif-uc1 34.145.131.128	35.222.151.148	Established	Route-based	vpc-hub-external	us-east4	Classic	Tunnel from GCP US-East4 to Liferay US-Central1 GCP

Routes

Filter lif

Enter property name or value

<input type="checkbox"/>	Name ↑	Type	IP version	Destination IP range	Priority	Next hop	Network
<input type="checkbox"/>	clv-tun-gcp-ue4-lif-uc1-route-1	Static	IPv4	10.101.0.0/20	1000	VPN tunnel clv-tun-gcp-ue4-lif-uc1	vpc-hub-external
<input type="checkbox"/>	clv-tun-gcp-ue4-lif-uc1-route-2	Static	IPv4	10.108.0.0/20	1000	VPN tunnel clv-tun-gcp-ue4-lif-uc1	vpc-hub-external

S.No	Gateway name	Cloud VPN gateway IP address	VPC network	Region	VPN tunnels	Peer VPN gateway (IP)	VPN tunnel status	Routing type	
1	clv-gcp-ue4-lif-uc1	34.145.131.128	vpc-hub-external	us-east4	clv-tun-gcp-ue4-lif-uc1	35.222.151.148	Established	Route-based	

4. Virtual Private Cloud (VPC) Configuration

4.1. Shared VPC

Shared VPC allows an organization to connect resources from multiple projects to a common Virtual Private Cloud (VPC) network, enabling secure and efficient communication using internal IPs. In this setup, a project is designated as a host project, and one or more service projects are attached to it. The VPC networks in the host project are referred to as Shared VPC networks. Eligible resources from service projects can utilize subnets within the Shared VPC network. Each project involved in a Shared VPC is either a host project or a service project.

To ensure network isolation between non-production and production environments, two Shared VPCs will be created: one for non-prod and one for prod.

The Fortinet VMs are configured with a multi-nic setup, having network interfaces in both the External VPC and the Shared VPCs. For simplicity, the Fortinet management and HA sync interfaces are not depicted in the diagram.

Whenever a new environment is required, a subnet is created in the corresponding Shared VPC. This subnet is linked to a service project (spoke), allowing spoke members to use the subnet to create resources.

This setup ensures that:

- Intra-VPC traffic is not filtered by the Firewall (including inter-region traffic within the VPC).
- Inter-VPC traffic is routed through the firewall.

Each VPC can and should be secured with VPC Firewall rules, which are stateful rules designed to filter VM traffic.

- Shared VPCs Created : vpc-non-prod-shared-host and vpc-prod-shared-host.
- Deployment Method : Infrastructure as Code (IAC).
- Status : Completed.

4.2. Standalone VPCs

When applications require environments with East-West traffic inspection, a Standalone VPC should be created. Standalone VPCs are designed to host workloads that need comprehensive traffic inspection. These VPCs will be connected to the Hub VPCs via Peering or VPN, ensuring secure and efficient communication. According to Google Cloud documentation, Standalone VPCs provide networking functionality for Compute Engine VM instances, Google Kubernetes Engine (GKE) clusters, and serverless workloads.

Ingress and egress traffic from Standalone Spoke VPCs will be inspected by the centralized firewall appliance(Fortinet).

- Purpose : Host workloads requiring East-West traffic inspection.
- VPCs Created : vpc-hub-external, vpc-hub-ha-forti, and vpc-hub-management-forti.
- Deployment Method : Infrastructure as Code (IAC).
- Status : Completed.

Google Cloud prj-shrd-ntwk-3 Search (/) for resources, docs, products, and more

VPC Network / VPC networks

VPC networks CREATE VPC NETWORK REFRESH

NETWORKS IN CURRENT PROJECT SUBNETS IN CURRENT PROJECT

SMTP port 25 allowed in this project. [Learn more](#)

VPC networks

Filter Enter property name or value

Name ↑	Subnets	MTU ?	Mode	IPv6 ULA range	Gateways	Fin
vpc-hub-external	4	1460	Custom			
vpc-hub-ha-forti	2	1460	Custom			
vpc-hub-management-forti	2	1460	Custom			
vpc-non-prod-shared-host	11	1460	Custom			
vpc-prod-shared-host	8	1460	Custom			

4.3. Sandbox VPCs

Quest aims to create Sandbox environments to experiment with new services, run PoCs, and support early development of applications that may later evolve into production. These Sandbox environments might require connectivity to Quest's networks.

Whenever a Sandbox environment is needed, it should be created in a corresponding Sandbox project, following the defined organization hierarchy. If networked resources are required, a completely isolated VPC should be created. This isolated VPC will not be connected to Quest's network, allowing the network team to assign any CIDR range without concerns about overlapping ranges.

If connectivity to Quest's network is necessary, the Sandbox VPC should be treated as a standard connected Non-Production VPC.

- Purpose : Experiment with new services, run PoCs, and early development of applications.
- Configuration : Created in a corresponding Sandbox project. Completely isolated if no connectivity to Quest's network is needed. Treated as a normal connected Non-Production VPC if connectivity is needed.
- Status : No Sandbox VPCs were created as part of this deployment.

4.4. IP Ranges and VPCs

4.4.1. GCP CIDR Ranges :

"10.141.0.0/16", "10.142.0.0/16", "10.143.0.0/16".

4.4.2. Divisions :

- GCP US East: 10.141.0.0/17 (Prod) & 10.141.128.0/17 (non-prod).
- GCP US West: 10.142.0.0/17 (Prod) & 10.142.128.0/17 (non-prod).
- GCP Shared Infra: 10.143.0.0/16.

4.4.3. VPCs :

- 3 Standalone VPCs: vpc-hub-external, vpc-hub-ha-forti, vpc-hub-management-forti.
- 2 Shared VPCs: vpc-prod-shared-host, vpc-non-prod-shared-host.

4.5. Provisioning New Environments

4.5.1. Shared VPC :

- Create a project for application resources.
- Create a subnet in the Shared VPC.
- Configure Google Cloud Firewall rules.
- Tag application components.
- Add Fortinet Firewall policies if needed.

4.5.2. Standalone VPC :

- Create a project for the application.
- Create a VPC and peer it with Hub VPC.
- Configure routes and subnets.
- Configure Google Cloud Firewall rules.
- Tag application components.
- Add Fortinet Firewall policies if needed.

4.5.3. Sandbox VPC :

- Create a project for sandbox applications.
- Create and customize the VPC.
- Configure subnets, regions, CIDR ranges, and routes.

- Configure Google Cloud Firewall rules.

4.6. Subnets

- Initial Subnets : Subnets were created for the two US regions with CIDR ranges defined by Quest for the Google Landing Zone specifically for Fortinet Firewalls.

- o Fortinet Subnets: created for hosting Fortinet Firewalls Management and Routing.
- o Number of Subnets: Specify that 12 subnets were created.
- o Deployment Method: IAC
- o Status: Completed
- o All subnets have Private Google Access and VPC Flow Logs enabled.

- Subnets for Fortinet Firewall :

VPC/Network Name	Subnet Name	Region	IP Range
Vpc-hub-external	External US West	us-west1	10.143.0.0/27
Vpc-hub-external	External US East	us-east4	10.143.0.32/27
Vpc-hub-external	Proxy only West	us-west1	10.143.2.0/24
Vpc-hub-external	Proxy only East	us-east4	10.143.1.0/24
Management	Management US West	us-west1	10.143.0.64/28
Management	Management US East	us-east4	10.143.0.80/28
HA Sync	HA Sync US West	us-west1	10.143.0.96/28
HA Sync	HA Sync US East	us-east4	10.143.0.112/28
Non Prod Hub	Non Prod Hub US West	us-west1	10.142.128.0/28
Non Prod Hub	Non Prod Hub US East	us-east4	10.141.128.0/28
Prod Hub	Prod Hub US West	us-west1	10.142.0.0/28
Prod Hub	Prod Hub US East	us-east4	10.141.0.0/28

Subsequently as the Project progressed & new service deployed. New Subnets got created in different VPC's.

Here is the details list of subnets , Reserved proxy-only subnets for load balancing and IP Ranges Allocated for Private Services Access.

VPC Hub External :-

VPC Name	Subnet Name	Region	Stack Type	Primary IPv4 range	Gateway	Private Google Access	Flow logs
vpc-hub-external	sub-external-ue4	us-east4	IPv4 (single-stack)	10.143.0.32/27	10.143.0.33	On	On
	sub-external-uw1	us-west1	IPv4 (single-stack)	10.143.0.0/27	10.143.0.1	On	On
Reserved proxy-only subnets for load balancing							
VPC Name	Subnet Name	Region	IP address ranges	Gateway	Role	Purpose	
vpc-hub-external	sub-proxy-np-ue4	us-east4	10.143.2.0/24	10.143.2.1	Active	Regional Managed Proxy	
	sub-proxy-np-uw1	us-west1	10.143.1.0/24	10.143.1.1	Active	Regional Managed Proxy	

vpc-hub-ha-forti :-

VPC Name	Subnet Name	Region	Stack Type	Primary IPv4 range	Gateway	Private Google Access	Flow logs
vpc-hub-ha-forti	sub-ha-ue4	us-east4	IPv4 (single-stack)	10.143.0.112/28	10.143.0.113	On	On
	sub-ha-uw1	us-west1	IPv4 (single-stack)	10.143.0.96/28	10.143.0.97	On	On

vpc-hub-management-forti :-

VPC Name	Subnet Name	Region	Stack Type	Primary IPv4 range	Gateway	Private Google Access	Flow logs
vpc-hub-management-forti	sub-management-ue4	us-east4	IPv4 (single-stack)	10.143.0.80/28	10.143.0.81	On	On
	sub-management-uw1	us-west1	IPv4 (single-stack)	10.143.0.64/28	10.143.0.65	On	On

vpc-non-prod-shared-host :-

S.No	Subnet Name/Reserved IP Range Name	Description	Region	CIDR
1	sub-non-prod-hub-ue4	For Fortigate Firewall Us-East4	us-east4	10.141.128.0/28
2	sn-ue4-dyn-dev-1	For Dynatrace Dev	us-east4	10.141.128.32/27
3	sn-ue4-gke-ghrunner-dev-1	For Github Runner Dev	us-east4	10.141.129.0/24
4	sn-ue4-cribl-dev-1	For Cribl Dev	us-east4	10.141.130.0/24
5	sn-ue4-ospac-dev-1	For OS Packer Dev	us-east4	10.141.131.0/27
6	sn-ue4-pscsql-dev-1	For Cloud SQL PSC Dev	us-east4	10.141.132.0/27
7	sn-ue4-cloudsql-psc-stg-1	For Cloud SQL PSC Staging	us-east4	10.141.133.0/24
8	reserved-b42481a6-e07a-45b3-9b26-808bbdb4a0b3	Reserved/Allocated IP Range for Dev DataStream PSA	us-east4	10.141.134.0/29
9	sn-ue4-cloudsql-psc-tst-1	For Cloud SQL PSC Test	us-east4	10.141.135.0/24
10	testpsubnetue4	US-East4 Test Subnet for Firewall Team	us-east4	10.141.254.0/24
11	sub-non-prod-psa-ue4	Reserved/Allocated IP Range for PSA-US-East4	us-east4	10.141.255.0/24
12	sub-non-prod-hub-uw1	For Fortigate Firewall Us-West1	us-west1	10.142.128.0/28
13	Testpsubnet	US-West1 Test Subnet for Firewall Team	us-west1	10.142.254.0/24
14	sub-non-prod-psa-uw1	Reserved/Allocated IP Range for PSA-US-West1	us-west1	10.142.255.0/24

Testpsubnetue4 and Testpsubnet to be deleted

vpc-prod-shared-host :-

S.No	Subnet Name/Reserved IP Range Name	Description	Region	CIDR
1	sub-prod-hub-ue4	For Fortigate Firewall Us-East4	us-east4	10.141.0.0/28
2	sn-ue4-dyn-prd-1	For Dynatrace Prod	us-east4	10.141.1.0/25
3	sn-ue4-gke-ghrunner-prd-1	GitHub HostRunner Prod	us-east4	10.141.2.0/26
4	sn-ue4-cribl-prd-1	Cribl GKE autopilot cluster Prod	us-east4	10.141.3.0/24
5	sn-ue4-cloudsql-psc-prd-1	Cloud SQL PSC - Us-East4- Prod	us-east4	10.141.4.0/24
6	sub-prod-ue4-test	Test Subnet	us-east4	10.141.126.0/24
7	psa-cidr-prod-us-east4	Allocated IP Range for PSA for Us-East4 – Prod	us-east4	10.141.127.0/24
8	sub-prod-hub-uw1	Fortigate Firewall us-west1	us-west1	10.142.0.0/28
9	sub-prod-uw1-test	Test Subnet	us-west1	10.142.126.0/24
10	psa-cidr-prod-us-west1	Allocated IP Range for PSA for us-west1 – Prod	us-west1	10.142.127.0/24

sub-prod-ue4-test and sub-prod-uw1-test to be deleted

4.7. Traffic Logging thru VPC Flow Logs^(Reference TDD Page 63)

VPC Flow Logs are enabled on each subnet. They capture a sample of packets sent and received by VMs, including those used in Google Kubernetes Engine, and packets through VLAN attachments for Cloud Interconnect and Cloud VPN tunnels. These logs are stored for 30 days by default.

- Purpose : The purpose of VPC Flow Logs is for network monitoring, forensics, security analysis, and expense optimization. These logs, aggregated by IP connection (5-tuple), can be viewed and exported via Cloud Logging.
- Deployment Method : IAC (Infrastructure as Code) with each subnet.
- Status : Completed

5. Private Access to Google APIs and Google Services

5.1. Private Google Access ^(Reference TDD Page 64)

- Configuration : Private Google Access is enabled on each subnet. This allows VM instances with only internal IP addresses to reach the external IP addresses of Google APIs and services without using the internet.
- Private DNS Zone : A “dns-glo-goo-apis-new” Private DNS Zone is created in Cloud DNS for PGA. This includes configuring a private DNS zone for the DNS Name “.googleapis.com” with CNAME as “private.googleapis.com” and first A record for private.googleapis.com pointing to the following IP addresses: 199.36.153.8, 199.36.153.9, 199.36.153.10, 199.36.153.11 and second A record for restricted.googleapis.com pointing to the following IP addresses: 199.36.153.4, 199.36.153.5, 199.36.153.6, 199.36.153.7.
- Deployment Method : IAC (Infrastructure as Code) with each subnet.
- Status : Completed

5.2. Private Service Connect (Reference TDD Page 66)

Private Service Connect (PSC) allows you to create private and secure connections from your VPCs to Google services, third-party services, or your own services. PSC uses endpoints and backends to manage traffic, ensuring that it remains within Google Cloud.

Endpoints are deployed using forwarding rules that provide the consumer an IP address mapped to the PSC service or Backends are deployed using network endpoint groups (NEGs) that direct traffic to a load balancer before reaching the PSC service.

As per TiDD there were no tasks defined related to Private Service Connect but as required for Liferay QAW Project PSC was deployed manually thru Google Console or gcloud commands for connecting to Cloud SQL.

5.2.1. Create a Private Service Connect endpoint

1. In the Google Cloud console, go to the Private Service Connect page under Project:- prj-shrd-ntwk-3.
2. Click Create endpoint: Click the Create endpoint button.
3. Target: Select the type of service as **Published service** for our Cloud SQL Use Case.
4. Target service: Enter the service attachment URI for the Cloud SQL Instance with Private Service connect enabled to which we want to connect to. This URI is provided by the service provider.
5. Endpoint name: Enter a name for your endpoint(CloudSqlName-projectno-environmenttype).
6. Network: Select the VPC network(vpc-prod-shared-host or vpc-non-prod-shared-host) where you want to create the endpoint.

7. Subnetwork: Select the subnet (like sn-ue4-pscsql-dev-1 or sn-ue4-cloudsql-psc-stg-1 or sn-ue4-cloudsql-psc-tst-1 or sn-ue4-cloudsql-psc-prd-1, etc.) where you want to create the endpoint.
8. IP address: Choose an internal static IP address for the endpoint from the selected subnet.
9. Select "Enable global access".
10. Click Add Endpoint button to create the endpoint.

Configure DNS

11. Create a DNS zone: Create a private DNS zone for the service you are connecting to. Zone name:- endpointname-ext-prod/nprod-zone , DNS Name:- endpointname.gcp.qdx.com with zone visible to "vpc-hub-external" Network.
12. Create a Record Set under this Private DNS Zone with DNS Name:- endpointname.gcp.qdx.com, Record Type :- A and lastly select the IP address of the Private Service Connect endpoint.
13. Test the connection :- Access the service: Try to access the service from a virtual machine in your VPC network or allowed & connect On-Prem instances. You should be able to access the service using its private IP address or the custom DNS name created to resolve the IP Address.

Steps & Details for setting up Private service connect for Cloud SQL thru gcloud commands & IAC has been covered under Data Handover or Cloud SQL Service Documentation

5.3. Private Service Access (Reference TDD Page 67)

Private Services Access (PSA) allows your VM instances in a VPC network to reach Google services using internal IP addresses. This ensures that traffic remains private and secure within Google Cloud.

5.3.1 Key Points related to PSA

- Configuration : PSA requires allocating an internal IP address range and creating a private connection (peering) to the service producer's VPC network
- IP Range Allocation for PSA : IP ranges were allocated for Private Service Access as follows:
 - VPC Name :- vpc-prod-shared-host for US-East4 : 10.141.127.0/24 and for US-West1 : 10.142.127.0/24
 - VPC Name :- vpc-non-prod-shared-host for US-East4 : 10.141.255.0/24 and for US-West1 : 10.142.255.0/24
- Deployment Method : IAC (Infrastructure as Code)

- Status : Completed

vpc-prod-shared-host

<

SUBNETS

STATIC INTERNAL IP ADDRESSES

FIREWALLS

FIREWALL ENDPOINTS

ROUTES

VPC NETWORK PEERING

PRIVATE SERVICES ACCESS

Use Private Services Access to connect to specific Google and third-party services without assigning external IP addresses to your Google Cloud and Google or third-party resources [Learn more](#)

Private services access requires you to first allocate an internal IPv4 address range and then create a private connection [Learn more](#)

ALLOCATED IP RANGES FOR SERVICES

PRIVATE CONNECTIONS TO SERVICES

Internal IP address ranges that are allocated for services private connection [Learn more](#)

ALLOCATE IP RANGE

RELEASE

<input type="checkbox"/>	Name ↑	Internal IP range	Service producer	Connection name
<input type="checkbox"/>	psa-cidr-prod-us-east4	10.141.127.0/24	-	-
<input type="checkbox"/>	psa-cidr-prod-us-west1	10.142.127.0/24	-	-

vpc-non-prod-shared-host

<

SUBNETS

STATIC INTERNAL IP ADDRESSES

FIREWALLS

FIREWALL ENDPOINTS

ROUTES

VPC NETWORK PEERING

PRIVATE SERVICES ACCESS

Use Private Services Access to connect to specific Google and third-party services without assigning external IP addresses to your Google Cloud and Google or third-party resources [Learn more](#)

Private services access requires you to first allocate an internal IPv4 address range and then create a private connection [Learn more](#)

ALLOCATED IP RANGES FOR SERVICES

PRIVATE CONNECTIONS TO SERVICES

Internal IP address ranges that are allocated for services private connection [Learn more](#)

ALLOCATE IP RANGE

RELEASE

<input type="checkbox"/>	Name ↑	Internal IP range	Service producer	Connection name
<input type="checkbox"/>	psa-cidr-non-prod-us-east4	10.141.255.0/24	-	-
<input type="checkbox"/>	psa-cidr-non-prod-us-west1	10.142.255.0/24	-	-
<input type="checkbox"/>	reserved-b42481a6-e07a-45b3-9b26-808bbdb4a0b3	10.141.134.0/29	-	-

8. IP Addressing Spaces (Reference TDD Page 76)

- Explained in detail under 4.4. IP Ranges and VPCs.

Quest has allowed the following CIDR ranges for their Google Cloud Landing Zone, according to regional needs.

Region	CIDR Range	Environment
GCP US East	10.141.0.0/16	10.141.0.0/17 (Prod)
		10.141.128.0/17 (Non Prod)
GCP US West	10.142.0.0/16	10.142.0.0/17 (Prod)
		10.142.128.0/17 (Non Prod)
GCP Shared Infra	10.143.0.0/16	N/A

9. Routing (Reference TDD Page 77)

In GCP, routes determine how network traffic travels from a virtual machine (VM) instance to other destinations. These destinations can be within the same Virtual Private Cloud (VPC) network, such as another VM, or outside of GCP(On-Prem,AWS,Azure,etc).

A route in a VPC network consists of a single destination prefix in CIDR format and a single next hop. When a VM in the VPC network sends a packet, GCP delivers the packet to the route's next hop if the packet's destination address falls within the route's destination range.

- Routes Created: Indicate that routes have been created.
- Deployment Method: IAC & Manually during VPN Tunnels creation
- Status: Completed

9.1. Production and Non-Production Hub VPCs Routes :

- Static Route : "0.0.0.0/0" with regional tag(us-east4/ue4 or us-west1/uw1) pointing to the internal static IP of the ILB.
- Private Google Access : Static route "199.36.153.8/30" for private Google access.
- Automatic Subnet Routes : Created automatically for each subnet.

To route traffic outside of the VPC via the Fortigate FW, a static route is added with next hop as the regional ILB. This route is applied to regional instances based on a network tag. So all VMs in the VPCs must have a network tag to identify the region.

Network "vpc-prod-shared-host" Route

[+ CREATE ROUTE](#)
[REFRESH](#)

Filter **Network : vpc-prod-shared-host** Enter property name or value

<input type="checkbox"/>	Name ↑	Type	Description	Destination IP range	Scope limits ?	Next hop	Network
<input type="checkbox"/>	route-ue4-prd-to-rinlb	Static	ue4 prod forwarding rule of network LB	0.0.0.0/0	Instance tags: us-east4	Forwarding rule of internal passthrough Network Load Balancer 10.141.0.5	vpc-prod-shared-host
<input type="checkbox"/>	route-us-gcpprod-to-pga	Static		199.36.153.8/30	—	Default internet gateway	vpc-prod-shared-host
<input type="checkbox"/>	route-uw1-prd-to-rinlb	Static	uw1 prod forwarding rule of network LB	0.0.0.0/0	Instance tags: us-west1	Forwarding rule of internal passthrough Network Load Balancer 10.142.0.5	vpc-prod-shared-host

Network “vpc-non-prod-shared-host” Route

[+ CREATE ROUTE](#)
[REFRESH](#)

Filter **Network : vpc-non-prod-shared-host** Enter property name or value

<input type="checkbox"/>	Name ↑	Type	Description	Destination IP range	Scope limits ?	Next hop	Network
<input type="checkbox"/>	route-ue4-nprd-to-rinlb	Static	ue4 non prod forwarding rule of network LB	0.0.0.0/0	Instance tags: us-east4	Forwarding rule of internal passthrough Network Load Balancer 10.141.128.5	vpc-non-prod-shared-host
<input type="checkbox"/>	route-us-gcpnonprod-to-pga	Static		199.36.153.8/30	—	Default internet gateway	vpc-non-prod-shared-host
<input type="checkbox"/>	route-uw1-nprd-to-rinlb	Static	route-uw1-nprd-to-rinlb	0.0.0.0/0	Instance tags: uw1	Forwarding rule of internal passthrough Network Load Balancer gcp-uw1-non-prod-igt-ilb2-frontend	vpc-non-prod-shared-host

9.2. VPC Hub External Routes :

- Static Routes : Routes to on-premises and other cloud providers AWS/AZURE.
- Static Routes : Specific CIDR ranges for different regions and environments.
- Default Route : "0.0.0.0/0" for internet access.

Route from Network “vpc-hub-external” to On-Prem

+

CREATE ROUTE

↺

REFRESH

Filter

Network : vpc-hub-external

tun-ext

Enter property name or value

✕ ?

<input type="checkbox"/>	Name ↓	Type	Description	Destination IP range	Scope limits ?	Next hop	Network
<input type="checkbox"/>	tun-ext-vpn-uw1-1-route-4	Static		35.199.192.0/19	—	VPN tunnel tun-ext-vpn-uw1-1	vpc-hub-external
<input type="checkbox"/>	tun-ext-vpn-uw1-1-route-3	Static		172.18.0.0/26	—	VPN tunnel tun-ext-vpn-uw1-1	vpc-hub-external
<input type="checkbox"/>	tun-ext-vpn-uw1-1-route-2	Static		156.30.0.0/16	—	VPN tunnel tun-ext-vpn-uw1-1	vpc-hub-external
<input type="checkbox"/>	tun-ext-vpn-uw1-1-route-1	Static		10.0.0.0/8	—	VPN tunnel tun-ext-vpn-uw1-1	vpc-hub-external
<input type="checkbox"/>	tun-ext-vpn-ue4-1-route-4	Static		35.199.192.0/19	—	VPN tunnel tun-ext-vpn-ue4-1	vpc-hub-external
<input type="checkbox"/>	tun-ext-vpn-ue4-1-route-3	Static		172.18.0.0/26	—	VPN tunnel tun-ext-vpn-ue4-1	vpc-hub-external
<input type="checkbox"/>	tun-ext-vpn-ue4-1-route-2	Static		156.30.0.0/16	—	VPN tunnel tun-ext-vpn-ue4-1	vpc-hub-external
<input type="checkbox"/>	tun-ext-vpn-ue4-1-route-1	Static		10.0.0.0/8	—	VPN tunnel tun-ext-vpn-ue4-1	vpc-hub-external

Route from Network “vpc-hub-external” to Quest AWS

+

CREATE ROUTE

↺

REFRESH

Filter

Network : vpc-hub-external

aws

Enter property name or value

✕ ?

<input type="checkbox"/>	Name ↑	Type	Description ↑	Destination IP range	Scope limits ?	Next hop	Network
<input type="checkbox"/>	clv-tun-gcp-aws-dev-route-3	Static	AWS Non-Prod (Dev & QA) Super-net Route	10.124.0.0/14	—	VPN tunnel clv-tun-gcp-ue4-aws-dev	vpc-hub-external
<input type="checkbox"/>	clv-tun-gcp-ue4-aws-dev-route-1	Static		10.183.0.0/17	—	VPN tunnel clv-tun-gcp-ue4-aws-dev	vpc-hub-external
<input type="checkbox"/>	clv-tun-gcp-ue4-aws-ue1-route-1	Static		10.183.128.0/17	—	VPN tunnel clv-tun-gcp-ue4-aws-ue1	vpc-hub-external
<input type="checkbox"/>	clv-tun-gcp-uw1-aws-dev-route-1	Static		10.183.0.0/17	—	VPN tunnel clv-tun-gcp-uw1-aws-dev	vpc-hub-external
<input type="checkbox"/>	clv-tun-gcp-uw1-aws-ue1-route-1	Static		10.183.128.0/17	—	VPN tunnel clv-tun-gcp-uw1-aws-ue1	vpc-hub-external

Route from Network “vpc-hub-external” to Internet(0.0.0.0/0)

+

CREATE ROUTE

↺

REFRESH

Filter

Network : vpc-hub-external

0.0.0.0/0

Enter property name or value

✕

<input type="checkbox"/>	Name ↓	Type	Description	Destination IP range	Scope limits ?	Next hop	Network
<input type="checkbox"/>	route-us-ext-to-internet	Static		0.0.0.0/0	—	Default internet gateway	vpc-hub-external

Route from Network “vpc-hub-external” to Liferay’s GCP VPN

+

CREATE ROUTE

↺

REFRESH

Filter

Network : vpc-hub-external

lif

Enter property name or value

✕ ?

<input type="checkbox"/>	Name ↓	Type	Description	Destination IP range	Scope limits ?	Next hop	Network
<input type="checkbox"/>	clv-tun-gcp-ue4-lif-uc1-route-2	Static	Liferay GCP IP range traffic to Liferay GCP VPN	10.108.0.0/20	—	VPN tunnel clv-tun-gcp-ue4-lif-uc1	vpc-hub-external
<input type="checkbox"/>	clv-tun-gcp-ue4-lif-uc1-route-1	Static		10.101.0.0/20	—	VPN tunnel clv-tun-gcp-ue4-lif-uc1	vpc-hub-external

Route from Network “vpc-hub-external” to Network Load Balancer

[+ CREATE ROUTE](#) [REFRESH](#)

Filter **Network : vpc-hub-external** **Next hop type : Forwarding rule of internal passthrough Network Load Balancer** Enter property name or value

<input type="checkbox"/>	Name ↓	Type	Description	Destination IP range	Scope limits	Next hop	Network
<input type="checkbox"/>	route-uw1-ext-to-prd	Static		10.142.0.0/17	—	Forwarding rule of internal passthrough Network Load Balancer 10.143.0.9	vpc-hub-external
<input type="checkbox"/>	route-uw1-ext-to-nprd	Static	uw1 ext forwarding rule of network LB	10.142.128.0/17	—	Forwarding rule of internal passthrough Network Load Balancer 10.143.0.5	vpc-hub-external
<input type="checkbox"/>	route-ue4-ext-to-prd	Static		10.141.0.0/17	—	Forwarding rule of internal passthrough Network Load Balancer 10.143.0.41	vpc-hub-external
<input type="checkbox"/>	route-ue4-ext-to-nprd	Static	ue4 ext forwarding rule of network LB	10.141.128.0/17	—	Forwarding rule of internal passthrough Network Load Balancer 10.143.0.34	vpc-hub-external
<input type="checkbox"/>	from-onpremononprod-uw1	Static		10.142.128.0/17	—	Forwarding rule of internal passthrough Network Load Balancer gcp-uw1-non-prod-fgt-ilb1-frontend	vpc-hub-external
<input type="checkbox"/>	from-onpremononprod-ue1	Static		10.141.128.0/17	—	Forwarding rule of internal passthrough Network Load Balancer lb-ue4-ilb-np-1-fe	vpc-hub-external

9.3. Fortigate Management and HA Sync VPCs Routes :

- Static Route : "0.0.0.0/0" for internet access.
- Automatic Subnet Routes : Created automatically.

[+ CREATE ROUTE](#) [REFRESH](#)

Filter **forti** Enter property name or value

<input type="checkbox"/>	Name ↓	Type	Description	Destination IP range	Scope limits	Next hop	Network
<input type="checkbox"/>	route-us-fwmgmt-to-Internet	Static		0.0.0.0/0	—	Default internet gateway	vpc-hub-management-forti
<input type="checkbox"/>	route-us-fwha-to-Internet	Static		0.0.0.0/0	—	Default internet gateway	vpc-hub-ha-forti

9.4. Standalone Spoke VPCs Routes :(To Be created when required)

- Static Route : "0.0.0.0/0" with regional tag(us-east4/ue4 or us-west1/uw1) pointing to the internal static IP of the ILB from the peered hub.
- Private Google Access : Static route "199.36.153.8/30".

10. Google Cloud Stateful Firewall Rules (Reference TDD Page 79)

Google Cloud Stateful Firewall Rules are L3/L4 stateful rules that allow you to control traffic to and from your Virtual Machines (VMs) based on a specified configuration. These rules are always enforced, ensuring the protection of your instances regardless of their configuration and operating system, even if they haven't started up.

Every Virtual Private Cloud (VPC) network in Google Cloud functions as a distributed cloud firewall. Although the firewall rules are defined at the network level, they are applied on a per-instance basis.

This means that the rules not only exist between your instances and other networks but also between individual instances within the same network. The rules can be matched via IP address, arbitrary tags, or service accounts.

Firewall rules, along with tags in the VMs, are used to ensure isolation between applications or teams within the same Shared VPC. This helps in maintaining security and organization within your cloud environment.

- Deployment Method: IAC
- Status: Completed

Allow traffic between On-Prem & GCP IP ranges

<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ↑	Logs
<input type="checkbox"/>	fw-allow-egress-gcp-onprem	Egress	Apply to all	IP ranges: 156.30.0.0/16, 10.0.0.0/8, 172.18.0.0/26 Local IP ranges: 10.142.0.0/16, 10.141.0.0/16, 10.143.0.0/16	All	Allow	1000	vpc-hub-external	On
<input type="checkbox"/>	fw-allow-ingress-onprem-gcp	Ingress	Apply to all	IP ranges: 156.30.0.0/16, 10.0.0.0/8, 172.18.0.0/26 Local IP ranges: 10.142.0.0/16, 10.141.0.0/16, 10.143.0.0/16	All	Allow	1000	vpc-hub-external	On

Cloud DNS Traffic

Filter 35.199.192.0/19 ✕ Enter property name or value									
<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ↑	Logs
<input type="checkbox"/>	cloud-dns-external-vpc	Ingress	Apply to all	IP ranges: 35.199.192.0/19	tcp:53 udp:53	Allow	1000	vpc-hub-external	On
<input type="checkbox"/>	cloud-dns-non-prod-vpc	Ingress	Apply to all	IP ranges: 35.199.192.0/19	tcp:53 udp:53	Allow	1000	vpc-non-prod-shared-host	On
<input type="checkbox"/>	cloud-dns-prod-vpc	Ingress	Apply to all	IP ranges: 35.199.192.0/19	tcp:53 udp:53	Allow	1000	vpc-prod-shared-host	On

11. DNS (Reference TDD Page 80)

11.1. Resolution of Google Cloud Names from On-Prem

- Configuration: a GCP Domain Private Zone with “gcp.qdx.com” was created, and a DNS Inbound Policy was created for allowing inbound DNS query.

On-Prem DNS Team added forwarding to rule for “gcp.qdx.com”.

- Deployment Method: IAC
- Status: Completed

dns-glo-pri-zon-gcp

DNS name	gcp.qdx.com.
Description	private DNS zone for GCP domain
Type	Private

RECORD SETS

IN USE BY

[+ ADD STANDARD](#)

[+ ADD WITH ROUTING POLICY](#)

[🗑 DELETE RECORD SETS](#)

[🔄 REFRESH](#)

[≡ Filter](#) Filter record sets

<input type="checkbox"/>	DNS name ↑	Type	TTL (seconds)	Record data
<input type="checkbox"/>	gcp.qdx.com.	SOA	21600	ns-gcp-private.googledomains.com. cloud-dns-hostmaster.google.com. 1 21600 3600 259200 300 ^
<input type="checkbox"/>	gcp.qdx.com.	NS	21600	ns-gcp-private.googledomains.com.

dns-inboundpolicy-onprem-gcp

Dns Inboundpolicy Onprem gcp policy

RULES

IN USE BY

Inbound query forwarding ?

On

DNS64 ?

Off

Logs

On

Alternative DNS servers

i Allows to forward all DNS queries for the network to the configured

Server location ↑

Private forwarding

No rows to display

11.2. Resolution of On-Prem Domain from Google Cloud

- Configuration: a Forwarding Zone for the On-Prem Domain was created; DNS Peering was configured for other VPCs and Google APIs Zone.
- Deployment Method: Initially IAC, then manually recreated.
- Status: Completed. Note that it was initially deployed through IAC but recreated manually due to resolution issues. On-Prem DNS is now resolving from all VPCs.

dns-forw-zon-gcp-onprem

DNS name	qdx.com.
Description	Forwarding Private Zone for On-Prem qdx.com Domain
Type	Forwarding

OUTBOUND FORWARDING

IN USE BY

Outbound queries for this DNS zone and its subdomains will be forwarded to alternative DNS server(s)

Destination DNS server location

Server location	Forwarding target type
10.202.0.11	Private
156.30.233.11	Private

dns-peer-zon-ext-prod-nopr-vpc

DNS name	qdx.com.
Description	DNS Peering hub-external for On-Prem qdx.com domain with Prod & NonProd VPC
Type	Peering
DNS peering	Enabled
Peer project ID	prj-shrd-ntwk-3
Peer network	vpc-hub-external

IN USE BY

ADD NETWORKS

REMOVE NETWORKS

<input type="checkbox"/>	Network name ↑	Project	
<input type="checkbox"/>	vpc-non-prod-shared-host	prj-shrd-ntwk-3	⋮
<input type="checkbox"/>	vpc-prod-shared-host	prj-shrd-ntwk-3	⋮

dns-glo-goo-apis-new

DNS name	googleapis.com.
Type	Private

RECORD SETS

IN USE BY






+

ADD STANDARD

+ ADD WITH ROUTING POLICY

 DELETE RECORD SETS REFRESH

 Filter Filter record sets

<input type="checkbox"/>	DNS name 	Type	TTL (seconds)	Record data
<input type="checkbox"/>	*.googleapis.com.	CNAME	300	private.googleapis.com. 
<input type="checkbox"/>	googleapis.com.	NS	21600	ns-gcp-private.googledomains.com. 
<input type="checkbox"/>	googleapis.com.	SOA	21600	ns-gcp-private.googledomains.com. cloud-dns-hostmaster.google.com. 1 21600 3600 
<input type="checkbox"/>	private.googleapis.com.	A	300	199.36.153.8 
<input type="checkbox"/>	restricted.googleapis.com.	A	300	199.36.153.4 