Qualys CDR for GCP - Terraform

- Qualys Setup
  - Prerequisites
  - Qualys Security Audit Setup
  - Qualys Flow Logs Monitor
- Qualys Network Threat Defense Setup
  - Getting Started
  - Deployment
- Packet Mirroring Configuration
  - Mirror Only Internet Traffic
  - Cross-VPC Packet Mirroring
  - Shared VPC Packet Mirroring
- Verify Setup

To install Qualys Agentless Runtime Cloud Security powered by Deep Learning AI, you must have a valid Qualys CDR license. To install Qualys Security Audit, you must have a valid Qualys SaaS license. Please contact your Qualys TAM to obtain the necessary licenses. You can request a free trial license here.

Qualys Setup

Installation and deployment of Qualys Agentless Runtime Cloud Security powered by Deep Learning AI is done via GCP recommended Terraform templates.

Prerequisites

- Download the Qualys for GCP package here. Your Qualys representative will provide you GCP license key(s) and the password to decrypt the package.
- Terraform (Qualys strongly recommends using GCP Cloud Shell which conveniently provides Terraform and other utilities.)
- Unzip the Qualys for GCP package - enter the password when prompted.
- `$ unzip qualys_gcp.zip`
- `Archive:  qualys_gcp.zip`
- `[bluehexagon_gcp.zip] password:`
- `  inflating: bluehexagon/bh_gcp_registration.py`
- `  inflating: bluehexagon/README.md`
- `  inflating: bluehexagon/main.tf`
- `  inflating: bluehexagon/terraform.tfvars`
  `  inflating: bluehexagon/variables.tf`

- Add the necessary input values in the `terraform.tfvars` file.

Terraform variable description

Key	Type	Description
`bh_license_ndr`	String	Qualys CDR license
`bh_license_saas`	String	Qualys SaaS license
`environment`	String	Environment label
`project_id`	String	GCP Project ID in which you want to deploy Qualys
`region`	String	GCP Region in which you want to deploy Qualys
`zones`	String	GCP Zone(s) in which you want to deploy Qualys
`network`	String	VPC Network in which you want to deploy Qualys
`subnet`	String	VPC Subnetwork in which you want to deploy Qualys
`min_auto_scale_count`	Integer	Minimum count of Qualys Inspection VMs
`max_auto_scale_count`	Integer	Maximum count of Qualys Inspection VMs
`enable_ndr`	Boolean	Enable Qualys Threat Defense
`enable_flow_logs_monitor`	Boolean	Enable Qualys Flow Logs Monitor

- Deploy via Terraform
    - `# Run once`
    - `terraform init`
    -
    - `# Deploy`
    - `terraform apply [--auto-approve]`
    -
    - `# Destroy`
    - `terraform destroy [--auto-approve]`

Qualys Flow Logs Monitor

To enable Qualys Flow Logs Monitor, set `enable_flow_logs_monitor` in the provided `terraform.tfvars` file to `true` (default is `false`).

Qualys Network Threat Defense Setup

These following steps deploy the Qualys for GCP solution with GCP Packet Mirroring. Qualys inspects network traffic generated by GCP Compute Engine and GCP Kubernetes Engine workloads to uncover and respond to threats in real-time.

Your Qualys TAM can assist you to deploy the solution.

Getting Started

Share the email ID of user or service account doing the deployment and share the email ID of the Google APIs Service Agent with your Qualys TAM. Qualys will in turn share a custom Compute Engine image and add the provided email address as an Image User, as described here.

The Google APIs Service Agent is a Google-managed service account used to access the APIs of Google Cloud Platform services. You may find it in `GCP Console -> IAM -> Principals` and will be in this format: `{PROJECT_ID}@cloudservices.gserviceaccount.com`.

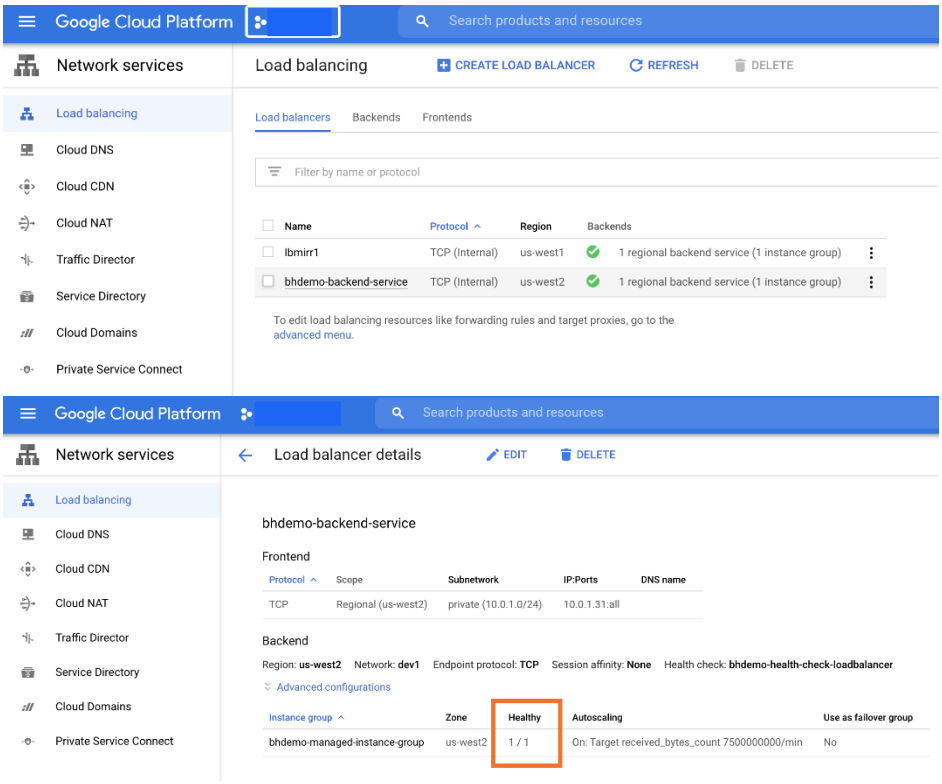
Prerequisites

- You must have a GCP project with a VPC containing at least one private subnet.
- The VPC must be configured for Cloud NAT to allow Qualys virtual appliances deployed in the private subnet to reach out to the Qualys cloud.
- The Qualys Terraform templates create a 0.0.0.0/0 outbound firewall rule to allow outbound communications with the Qualys cloud - do not remove this.

Deployment

Qualys is deployed as an autoscaling managed instance group behind an internal load balancer in a subnet in your VPC.

On success, you can check to see that the internal load balancer has been created along with a healthy backend managed instance group, as shown in the screenshots below.

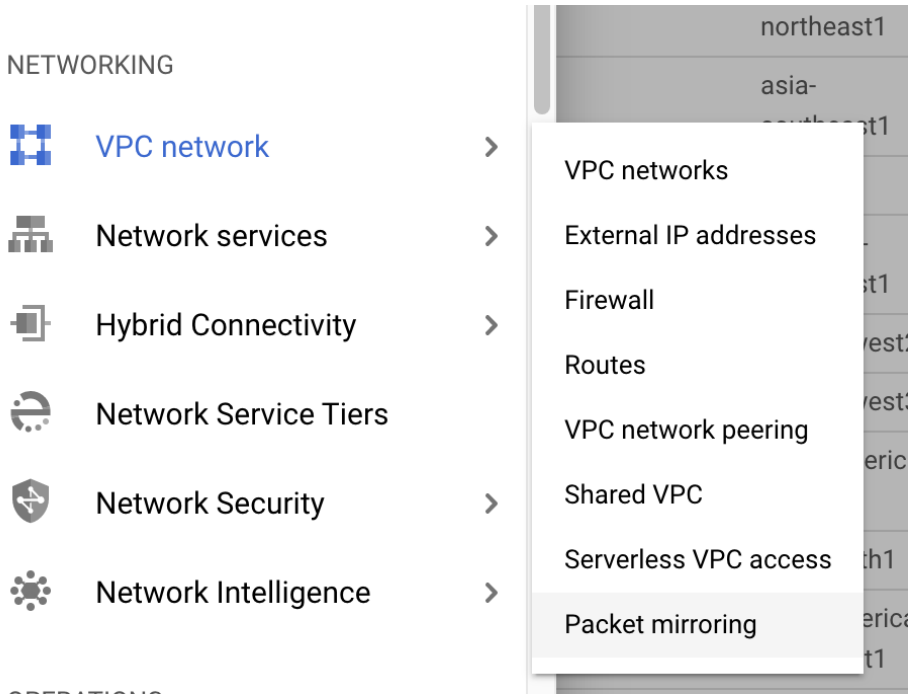


Packet Mirroring Configuration

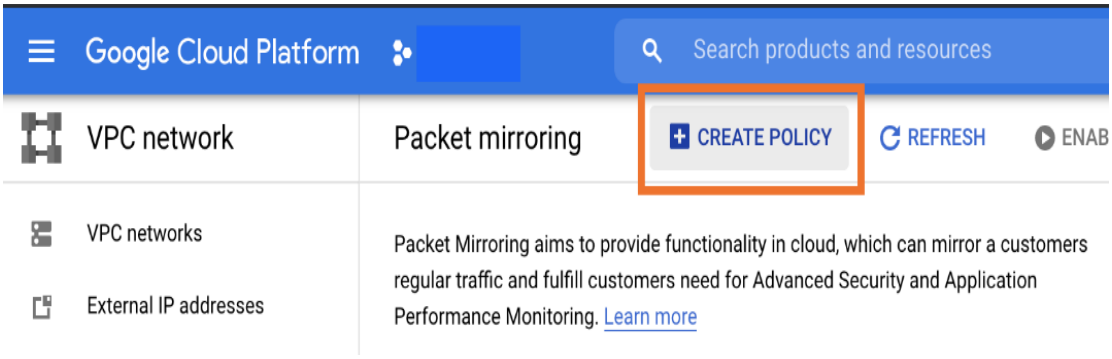
The following steps describe how to configure GCP Packet Mirroring to direct traffic from your source workloads to Qualys for inspection. For more details and troubleshooting, refer to the GCP Packet Mirroring documentation.

Follow the steps below in the GCP console to configure GCP Packet Mirroring to direct traffic from your source workloads in GCP Compute Engine and GCP Kubernetes Engine to Qualys deployed in the previous steps.

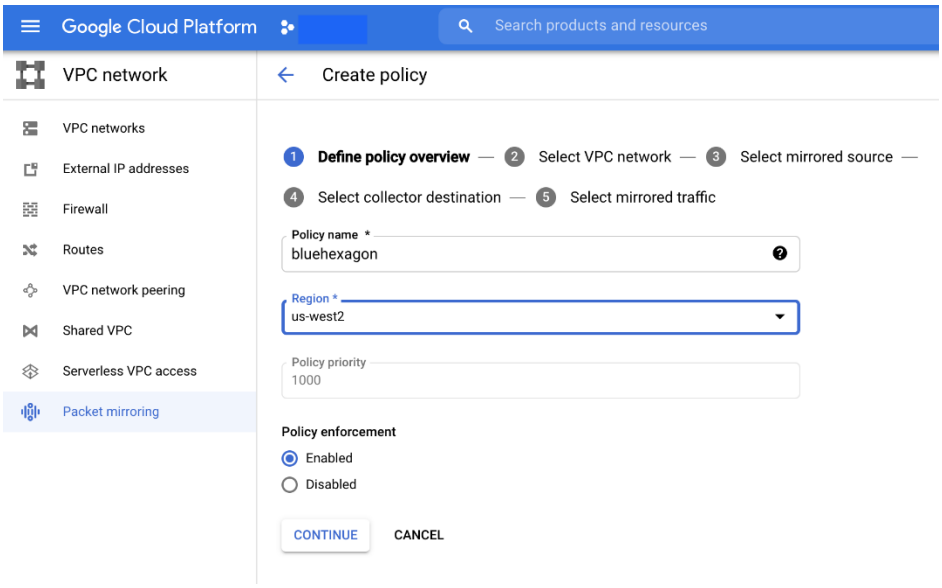
- Go to VPC network > Packet mirroring.



- Create a new Packet Mirroring policy.

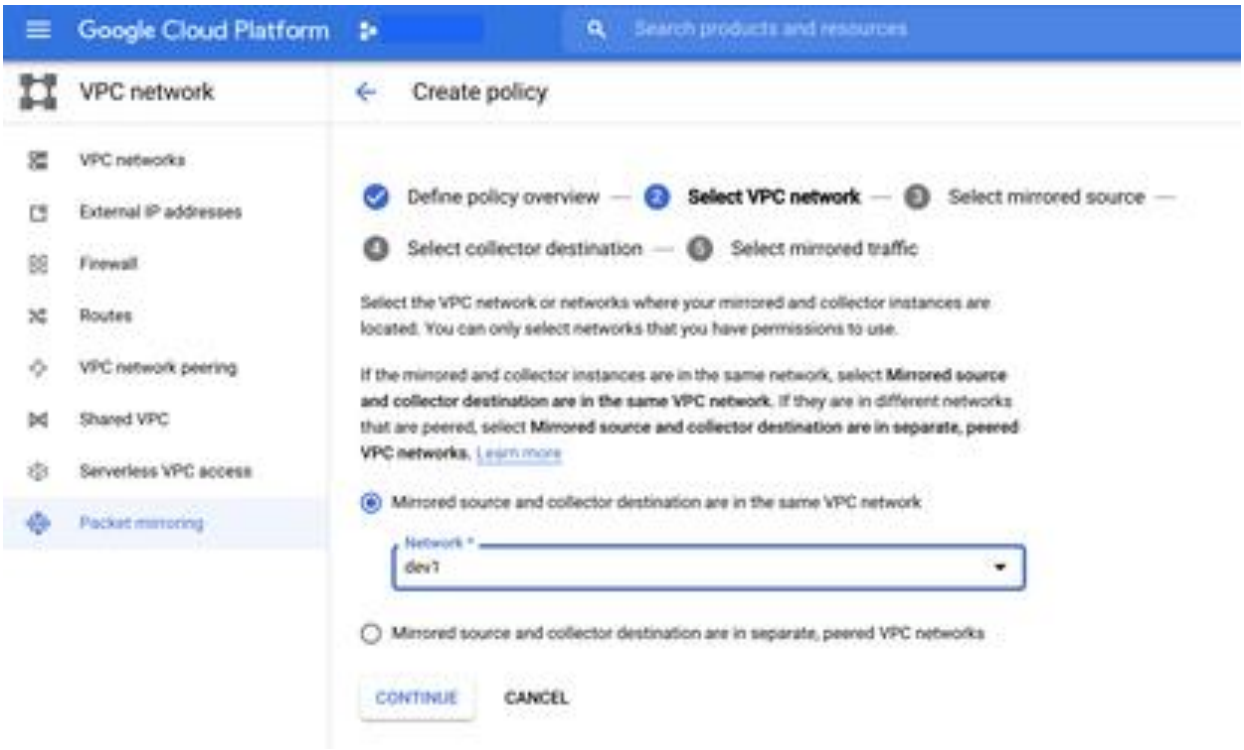


- Define policy overview.

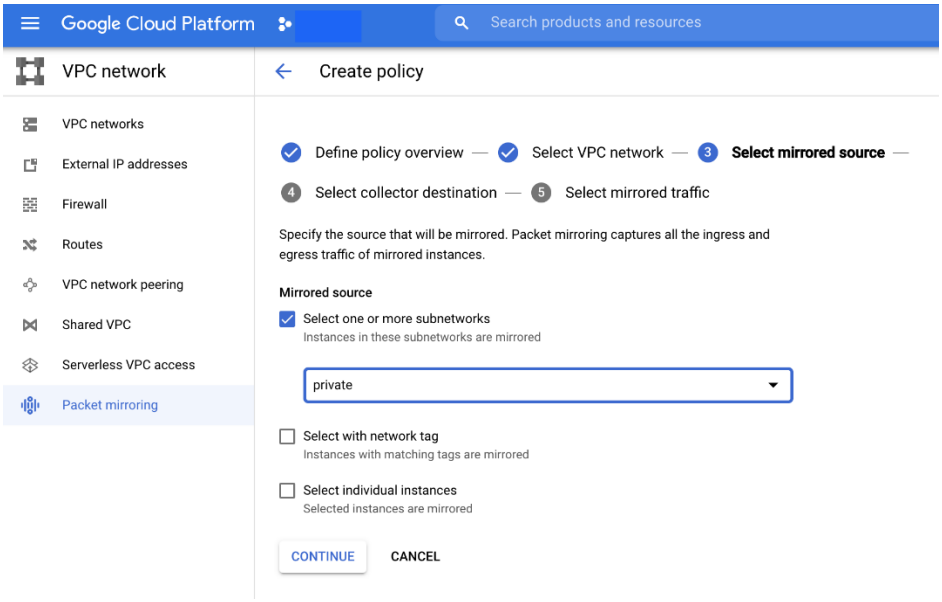


- Select VPC network containing workloads to mirror.

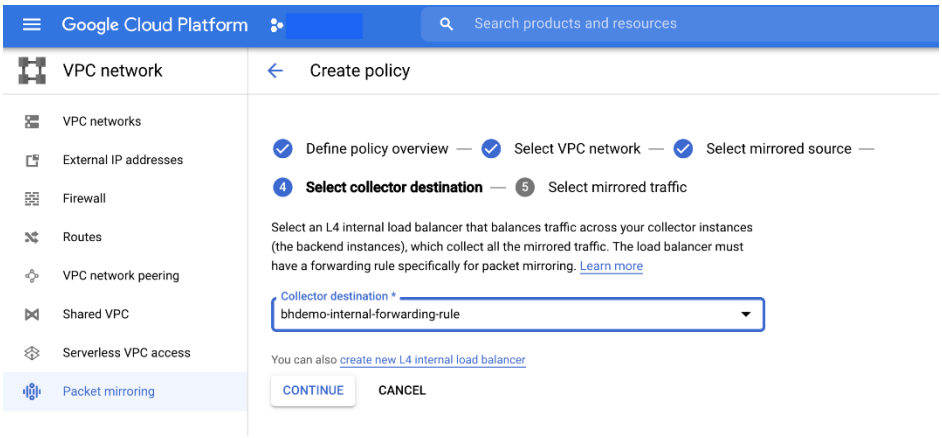
The VPC containing workloads to mirror may be different from the VPC in which the Qualys *collector* is deployed. If so, set up VPC peering between the mirrored source and collector VPCs.



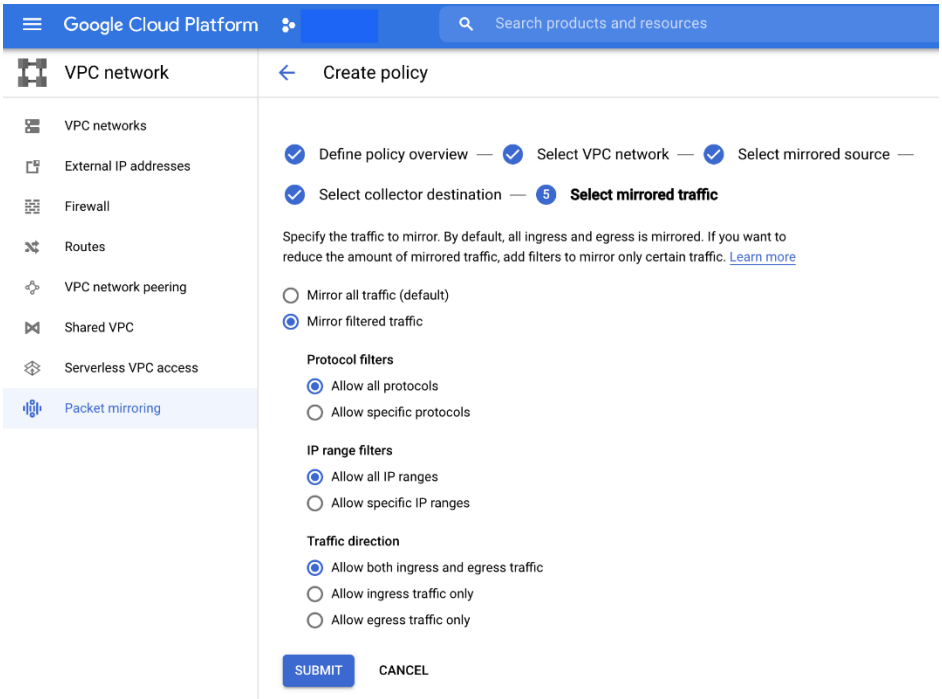
- Specify the traffic source that will be mirrored. You can specify the source by selecting:
  - one or more subnets (as shown in this example),
  - instances with matching tags, or
  - individual instances (VMs).



- Select the newly created internal load balancer (forwarding rule) as the destination of packet mirroring.



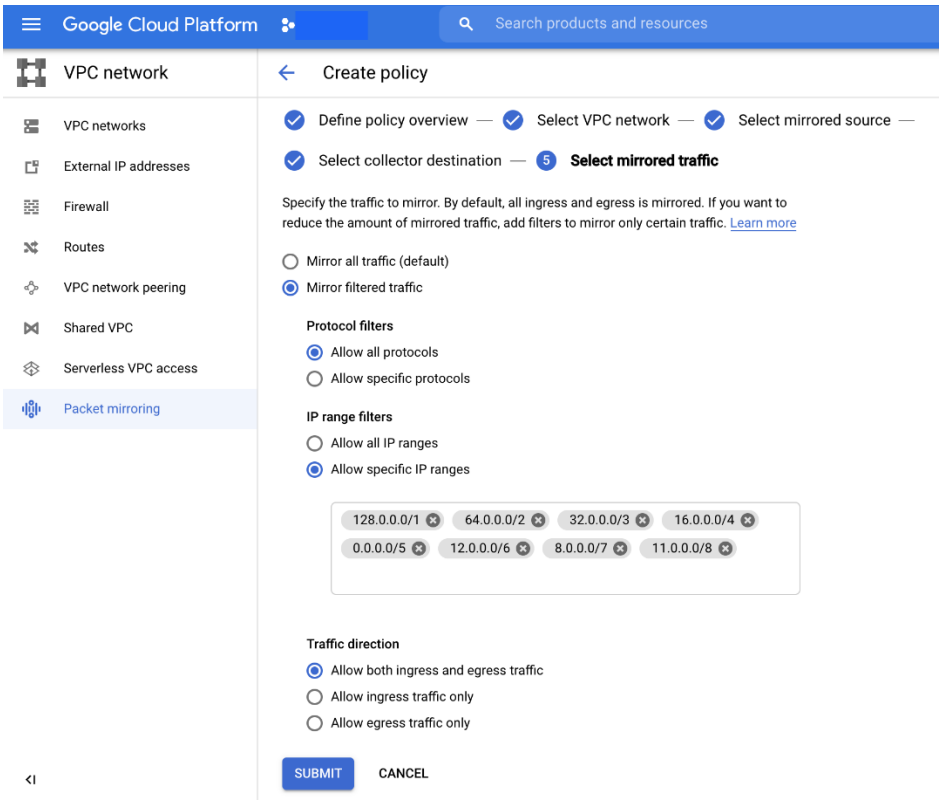
- You can choose to mirror all traffic (default and recommended) or mirror only specific protocols / IP ranges as shown below.



Mirror Only Internet Traffic

GCP Packet Mirroring currently does not support *negative* filters supporting the “not” condition, e.g. not 10.0.0.0/8. To work around this and mirror only internet traffic, specify a filter that includes public CIDR blocks and excludes 10.0.0.0/8 internal traffic. IP ranges to use:
`128.0.0.0/1 64.0.0.0/2 32.0.0.0/3 16.0.0.0/4 0.0.0.0/5 12.0.0.0/6 8.0.0.0/7 11.0.0.0/8`

NOTE: Each CIDR block needs to be added one by one for GCP to recognize it. The whole string above cannot be cut and pasted.



Cross-VPC Packet Mirroring

You can set up cross-VPC (and cross-project) Packet Mirroring by following the steps described in the [GCP Packet Mirroring documentation](#).

Peering needs to be setup both ways from network1 to network2 and vice-versa

Name	Your VPC network	Peered VPC network	Peered project ID	Status	Exchange custom routes
peerdevtoprod	dev1	prod1	diesel-air-197303	Active	None
peerprodtodev	prod1	dev1	diesel-air-197303	Active	None

Shared VPC Packet Mirroring

You can set up packet mirroring in a Shared VPC setting by following the steps described in the [GCP Packet Mirroring documentation](#).

Intranode visibility

You can setup packet mirroring to show intranode visibility (internal to containers)

https://cloud.google.com/kubernetes-engine/docs/how-to/intranode-visibility?hl=en

Verify Setup

If Qualys and Packet Mirroring are setup correctly, you will see observations in the Qualys portal from the `gcp` appliance in the Discover view as shown below.