

# 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.

The first screenshot shows the Google Cloud Platform console's 'Load balancing' page. The left sidebar lists 'Network services' with 'Load balancing' selected. The main content area shows a table of load balancers. The second screenshot shows the 'Load balancer details' page for 'bhdemo-backend-service'. The 'Frontend' section shows a TCP listener on port 10.0.1.31. The 'Backend' section shows a managed instance group 'bhdemo-managed-instance-group' in the 'us-west2' zone, which is 'Healthy' (1/1 instances) and configured with autoscaling.

**Google Cloud Platform** Search products and resources

**Network services**

- Load balancing
- Cloud DNS
- Cloud CDN
- Cloud NAT
- Traffic Director
- Service Directory
- Cloud Domains
- Private Service Connect

**Load balancing** CREATE LOAD BALANCER REFRESH DELETE

Load balancers Backends Frontends

Filter by name or protocol

| Name                   | Protocol       | Region   | Backends                                      |
|------------------------|----------------|----------|-----------------------------------------------|
| lbmirr1                | TCP (Internal) | us-west1 | 1 regional backend service (1 instance group) |
| bhdemo-backend-service | TCP (Internal) | us-west2 | 1 regional backend service (1 instance group) |

To edit load balancing resources like forwarding rules and target proxies, go to the [advanced menu](#).

**Google Cloud Platform** Search products and resources

**Network services**

- Load balancing
- Cloud DNS
- Cloud CDN
- Cloud NAT
- Traffic Director
- Service Directory
- Cloud Domains
- Private Service Connect

**Load balancer details** EDIT DELETE

bhdemo-backend-service

Frontend

| Protocol | Scope               | Subnetwork            | IP:Ports      | DNS name |
|----------|---------------------|-----------------------|---------------|----------|
| TCP      | Regional (us-west2) | private (10.0.1.0/24) | 10.0.1.31:all |          |

Backend

Region: us-west2 Network: dev1 Endpoint protocol: TCP Session affinity: None Health check: bhdemo-health-check-loadbalancer

[Advanced configurations](#)

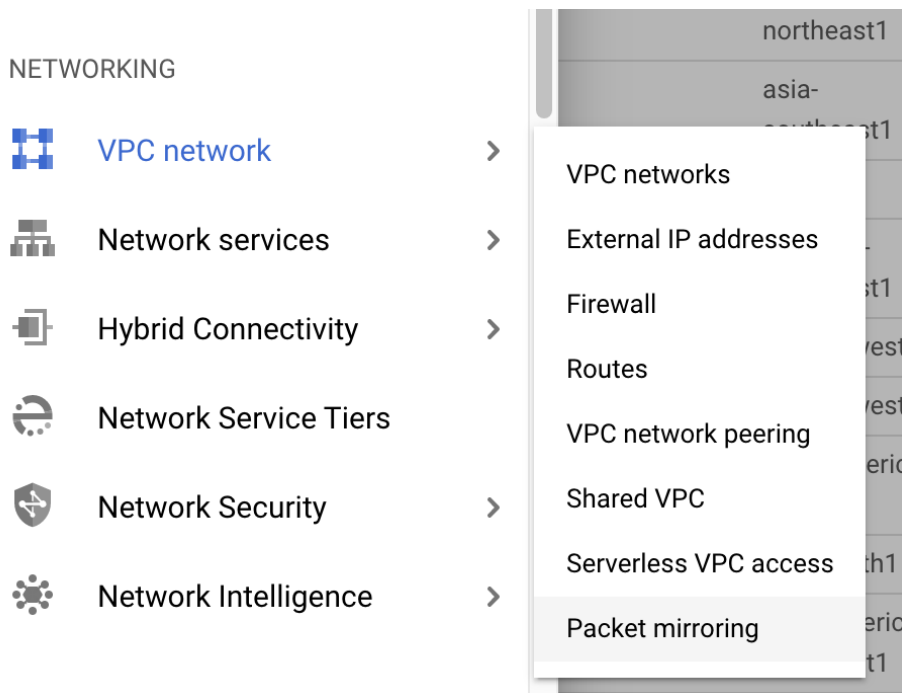
| Instance group                | Zone     | Healthy | Autoscaling                                    | Use as failover group |
|-------------------------------|----------|---------|------------------------------------------------|-----------------------|
| bhdemo-managed-instance-group | us-west2 | 1 / 1   | On: Target received_bytes_count 7500000000/min | No                    |

# Packet Mirroring Configuration

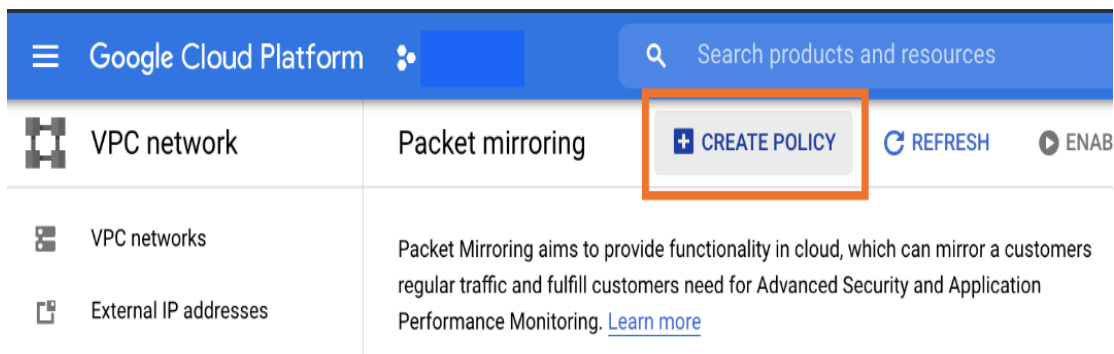
The following steps describe how to configure GCP Packet Mirroring to direct traffic from your source workloads to Qualys for inspection. For more details and troubleshooting, refer to the GCP Packet Mirroring [documentation](#).

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.

Google Cloud Platform

VPC network

Create policy

1 Define policy overview — 2 Select VPC network — 3 Select mirrored source —  
4 Select collector destination — 5 Select mirrored traffic

Policy name \*  
bluehexagon

Region \*  
us-west2

Policy priority  
1000

Policy enforcement  
☒ Enabled  
☐ Disabled

CONTINUE CANCEL

- 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.

Google Cloud Platform

VPC network

Create policy

1 Define policy overview — 2 Select VPC network — 3 Select mirrored source —  
4 Select collector destination — 5 Select mirrored traffic

Select the VPC network or networks where your mirrored and collector instances are located. You can only select networks that you have permissions to use.

If the mirrored and collector instances are in the same network, select **Mirrored source and collector destination are in the same VPC network**. If they are in different networks that are peered, select **Mirrored source and collector destination are in separate, peered VPC networks**. [Learn more](#)

☒ Mirrored source and collector destination are in the same VPC network

Network \*  
dev1

☐ Mirrored source and collector destination are in separate, peered VPC networks

CONTINUE CANCEL

- 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).

Google Cloud Platform

Search products and resources

VPC network

VPC networks

External IP addresses

Firewall

Routes

VPC network peering

Shared VPC

Serverless VPC access

Packet mirroring

Create policy

1 Define policy overview

2 Select VPC network

3 Select mirrored source

4 Select collector destination

5 Select mirrored traffic

Specify the source that will be mirrored. Packet mirroring captures all the ingress and egress traffic of mirrored instances.

Mirrored source

☒ Select one or more subnetworks

Instances in these subnetworks are mirrored

private

☐ Select with network tag

Instances with matching tags are mirrored

☐ Select individual instances

Selected instances are mirrored

CONTINUE

CANCEL

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

Google Cloud Platform

VPC network

Create policy

Define policy overview — Select VPC network — Select mirrored source —

4 Select collector destination — 5 Select mirrored traffic

Select an L4 internal load balancer that balances traffic across your collector instances (the backend instances), which collect all the mirrored traffic. The load balancer must have a forwarding rule specifically for packet mirroring. [Learn more](#)

Collector destination \*

bhdemo-internal-forwarding-rule

You can also [create new L4 internal load balancer](#)

CONTINUE CANCEL

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

Google Cloud Platform

VPC network

Create policy

Define policy overview — Select VPC network — Select mirrored source —

4 Select mirrored traffic

Specify the traffic to mirror. By default, all ingress and egress is mirrored. If you want to reduce the amount of mirrored traffic, add filters to mirror only certain traffic. [Learn more](#)

☐ Mirror all traffic (default)

☒ Mirror filtered traffic

Protocol filters

☒ Allow all protocols

☐ Allow specific protocols

IP range filters

☒ Allow all IP ranges

☐ Allow specific IP ranges

Traffic direction

☒ Allow both ingress and egress traffic

☐ Allow ingress traffic only

☐ Allow egress traffic only

SUBMIT CANCEL



## 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.

Google Cloud Platform

Search products and resources

VPC network

← Create policy

Define policy overview — Select VPC network — Select mirrored source —

Select collector destination — **Select mirrored traffic**

Specify the traffic to mirror. By default, all ingress and egress is mirrored. If you want to reduce the amount of mirrored traffic, add filters to mirror only certain traffic. [Learn more](#)

☐ Mirror all traffic (default)

☒ Mirror filtered traffic

Protocol filters

☒ Allow all protocols

☐ Allow specific protocols

IP range filters

☐ Allow all IP ranges

☒ Allow specific IP ranges

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

Traffic direction

☒ Allow both ingress and egress traffic

☐ Allow ingress traffic only

☐ Allow egress traffic only

SUBMIT CANCEL

## 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

| <input type="checkbox"/> | Name ↑        | Your VPC network | Peered VPC network | Peered project ID | Status   | Exchange custom routes |
|--------------------------|---------------|------------------|--------------------|-------------------|----------|------------------------|
| <input type="checkbox"/> | peerdevtoprod | dev1             | prod1              | diesel-air-197303 | ✓ Active | None                   |
| <input type="checkbox"/> | 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.

The screenshot shows the Qualys Discover portal interface. On the left is a sidebar with navigation icons and a list of file analytics categories. The main panel is titled 'Discover: Connection Outliers' and displays a table of network connection data. The table has columns for Timestamp, Appliance, Originator IP, Responder IP, Count, Responder Country, Duration, and Port List. The data shows various connections from the 'azure\_flow\_logs' appliance to different responder IPs, mostly from the United States, with one connection to Ireland. Each row includes a 'View Info' link.

| Discover: Connection Outliers |                 |                  |                 |          |                      |             |              |
|-------------------------------|-----------------|------------------|-----------------|----------|----------------------|-------------|--------------|
| 4942444 Results               |                 |                  |                 |          |                      |             |              |
| Timestamp ↑↓                  | Appliance ↑↓    | Originator IP ↑↓ | Responder IP ↑↓ | Count ↑↓ | Responder Country ↑↓ | Duration ↑↓ | Port List ↑↓ |
| 2023-03-03 15:57:43           | azure_flow_logs | 10.2.0.4         | 52.123.130.2    | 1        | United States        | 0.000s      | 53/udp       |
| 2023-03-03 15:57:42           | azure_flow_logs | 10.2.0.4         | 205.251.192.9   | 1        | United States        | 0.000s      | 53/udp       |
| 2023-03-03 15:57:08           | azure_flow_logs | 10.0.3.5         | 142.250.128.95  | 1        | United States        | 0.000s      | 443/udp      |
| 2023-03-03 15:57:00           | azure_flow_logs | 10.2.0.4         | 13.107.128.2    | 1        | United States        | 0.000s      | 53/udp       |
| 2023-03-03 15:56:51           | azure_flow_logs | 10.2.0.4         | 108.162.193.135 | 1        | United States        | 0.000s      | 53/udp       |
| 2023-03-03 15:56:48           | azure_flow_logs | 10.2.0.4         | 209.234.234.43  | 1        | United States        | 0.000s      | 53/udp       |
| 2023-03-03 15:56:48           | azure_flow_logs | 10.2.0.4         | 209.234.234.43  | 1        | United States        | 0.000s      | 53/udp       |
| 2023-03-03 15:56:48           | azure_flow_logs | 10.2.0.4         | 209.234.230.6   | 1        | United States        | 0.000s      | 53/udp       |
| 2023-03-03 15:56:48           | azure_flow_logs | 10.2.0.4         | 209.234.230.6   | 1        | United States        | 0.000s      | 53/udp       |
| 2023-03-03 15:56:42           | azure_flow_logs | 10.0.3.4         | 13.69.239.73    | 1        | Ireland              | 0.000s      | 443/tcp      |