Google Compute Deployment Guide Eli-v6.5.391

Bridgeworks
Unit 1, Aero Centre, Ampress Lane,
Ampress Park, Lymington,
Hampshire SO41 8QF
Tel: +44 (0) 1590 615 444
Email: support@4bridgeworks.com

Table of Contents

1 Requirements for deployment on GCE

In order to deploy your PORTrockIT you will need access to a shared image provided to you by Bridgeworks and a licence for your unit. In order to obtain your licence you must provide Bridgeworks with Project Id(s) applicable to the GCE instances they will be used on.

The image will be made available to you via a shared image which is located in the Google Compute project *bridgeworks-cloud*.

This guide assumes that the user is acquainted with Google Compute Engine and is comfortable using the Google Cloud Shell terminal interface.

2 Guide layout

This guide is divided into a series of ordered steps that should be followed through in order. If at any point you run into trouble with a step please refer to the Useful Links section at the end of this document.

It is recommended to print this list of steps out and check off each step as you complete them.

- ☐ Step 1. Virtual machine creation
- ☐ Step 2. Routes
- ☐ Step 3. Firewall
- ☐ Step 4. Accessing the GUI

3 Virtual machine creation

The VM for your PORTrockIT must be created from a shared image which is located in the project *bridgeworks-cloud*. Bridgeworks will supply you with details of the specific file that should be used.

Unfortunately due to limitations in the graphical interface, you must use the gcloud command line interface to deploy your new instances.

An example of the basic command is shown below:

```
gcloud compute instances create my-instance-name \
    --image-project=bridgeworks-cloud \
    --image=portrockit-image-name \
    --tags=https-server \
    --network-interface=nic-type=GVNIC
```

In this example it will deploy a new instance called *my-instance-name* using the Bridgeworks source image called *portrockit-image-name*, apply the *https-server* tag to allow https access in the *default* network, and add gVNIC support.

The Google Virtual NIC (gVNIC) provides optimal performance for your device and can be used for higher network bandwidths (50-100 Gbps). For these reasons it is recommended to specify this NIC when deploying instances.

In our example we didn't specify a machine type, so a default will be selected. For real deployments the user should specify a machine type based on the required performance characteristics. Additional information can be found in Performance Considerations.

The recommended minimum RAM for Bridgeworks products is shown below:

PORTrockIT tier	Minimum RAM size
PORTrockIT 100 Series	2 GBytes
PORTrockIT 200 Series	4 GBytes
PORTrockIT 400 Series	12 GBytes

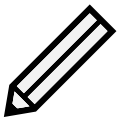
It should be noted that on units with less than the recommended minimum RAM a warning event will be displayed on the PORTrockIT indicating performance may be restricted. Users can if required specify a custom setting using the `--custom-memory=xx` option, where *xx* specifies the RAM size.

Once your VM instance has started you should navigate to *VPC Network -> External IP addresses* and *RESERVE* the external IP address for your instance so that it does not change after a reboot, or use the following gcloud command to promote the ephemeral IP address to static:

```
gcloud compute addresses create ADDRESS_NAME --addresses=IP_ADDRESS \
    [--region=REGION | --global]
```

Further details of using gVNIC can be found in the Google documentation:

https://cloud.google.com/compute/docs/networking/using-gvnic



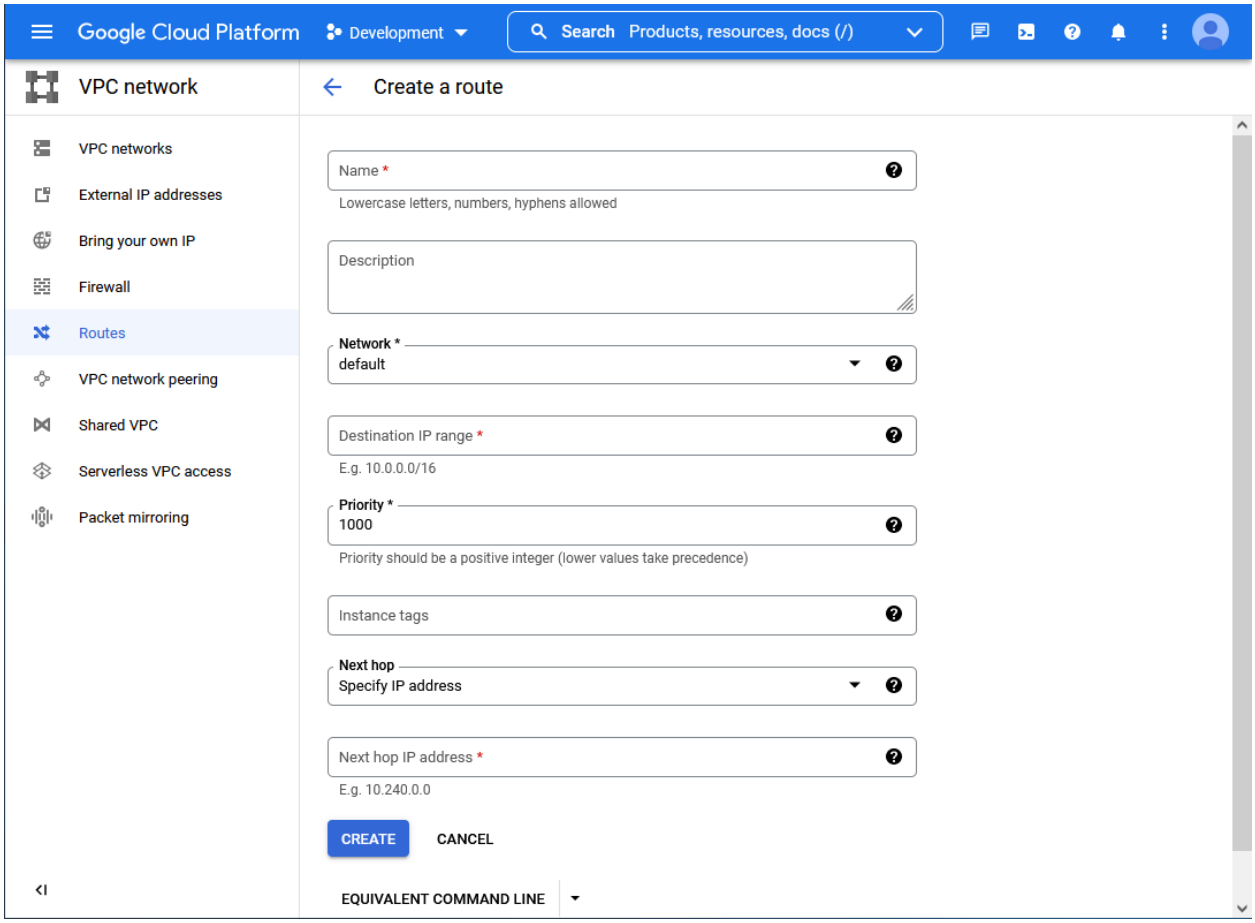
Note: The Bridgeworks software supports both single IP (/32 addresses) and multi IP working on Google Compute. For normal deployments it is perfectly acceptable to use a single interface and IP address. For multi IP working the user should contact Bridgeworks Support for details of using images with the *MULTI_IP_SUBNET* option enabled.

4 Routes

If you are deploying your PORTrockIT Node and require to run in the “Logical-In-Path” mode, then please follow this section to allow traffic to be passed to the PORTrockIT for acceleration. If you are configuring the PORTrockIT to be used in “Out-of-Path” mode then please proceed to Chapter 5: Firewall. For help with deciding on modes of operation please consult the Bridgeworks “PORTrockIT Topology Overview” document.

To add routes in Google Compute the user has the choice of defining routes using the gcloud command line interface or the graphical interface.

The graphical interface is shown below:



The equivalent gcloud command for the above takes the form of:

```
gcloud beta compute routes create NAME \
    --project=PROJECT_NAME \
    --network=default \
    --priority=1000 \
    --destination-range=DESTINATION_RANGE \
    --next-hop-address=NEXT_HOP_ADDRESS
```

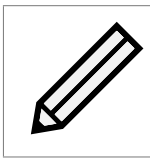
5 Firewall

The Google VPC Network will need firewall rules defining to allow traffic to and from the PORTrockIT. Similar to the *VPC Network Routes* its possible to use both the graphical and gcloud command line interfaces to set up firewall rules. A typical command would take the following general form:

```
gcloud compute --project=PROJECT_NAME firewall-rules create NAME \
    --direction=INGRESS \
    --priority=1000 \
    --network=default \
    --action=ALLOW \
    --rules=PROTOCOL:PORT,...
```

The table below details the ports that must be added to the firewall:

Protocol/Port	Description	Recommended Source
TCP 22	SSH, used for accessing the Command Line Interface (CLI).	”My IP”
TCP 80	HTTP, used for accessing the web interface (unencrypted).	”My IP”
TCP 443	HTTPS, used for accessing the web interface (encrypted).	”My IP”
TCP 16665	PORTrockIT main transfer port.	Public facing IP address of the WAN interface of your partner PORTrockIT Node.
UDP 4500	IPsec, used for encrypting PORTrockIT traffic.	Public facing IP address of the WAN interface of your partner PORTrockIT Node.
UDP 500	IPsec used for encrypting PORTrockIT traffic.	Public facing IP address of the WAN interface of your partner PORTrockIT Node.



Note: Note: For the default network Google will add Ports 80 and 443 automatically if the instance is tagged with *http-server* and *https-server* appropriately.

In addition to these ports, those appropriate to the accelerated protocols will also need to be considered, for example for FTP, TCP port 21 is needed.

6 Accessing the GUI

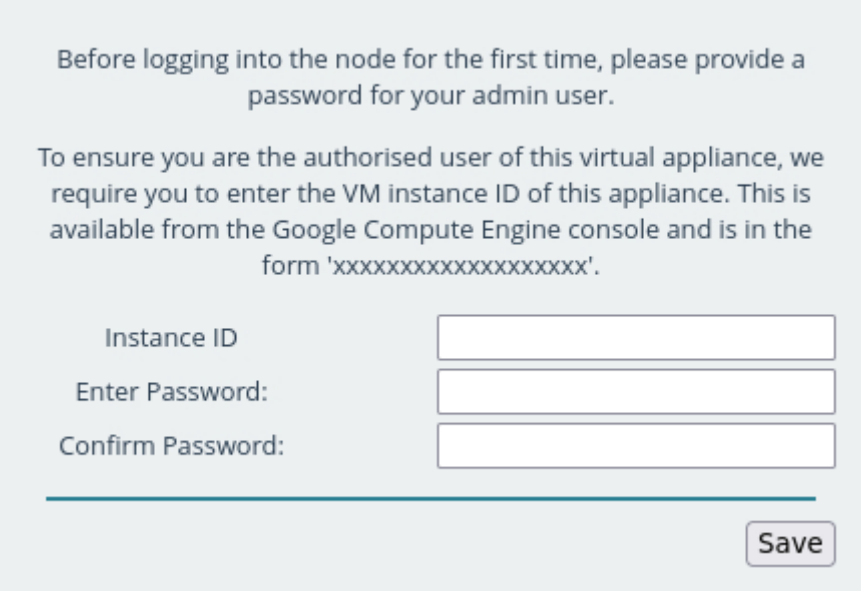
With a PORTrockIT virtual machine running there is now a web GUI available.

To access the GUI you need to know the public IP address for your virtual machine.

Open a new tab in your browser and enter the IP address taken from the Compute Engine VM Instances screen to access your PORTrockIT.

You will now be presented with the password prompt page.

The first time the unit is accessed it is necessary to set up the password for the unit. As a security measure it will prompt you to supply the instance id of the unit. Simply follow the on-screen prompts to set the password and log in.



For further guidance on setting up data acceleration and routing, see the *Policy Routed* guide.

7 Troubleshooting

7.1 Deployment Problems

The Google Compute Engine has no specific issues unique to the environment other than detailed in Performance Considerations

Typically when things don't work at all the issue is most likely in the area of firewalls and/or routing, extra information can be found in Useful Links.

8 Useful Links

Further documentation and support is available through our website: https://support.4bridgeworks.com/

If your question is not answered in our documentation, please submit a ticket: https://support.4bridgeworks.com/contact/

Appendix A: Performance Considerations

There are various performance limitations that need to be taken into account that apply across Google:

- Gbit/s total for all egress flows to external IP addresses.
- Gbit/s per individual egress flow to an external IP address.
- Mpacket/s ingress traffic delivered to an external IP address associated with the VM.
- Gbit/s ingress traffic delivered to an external IP address associated with the VM.

In addition to these limits there is a limit imposed by the machine type. Details of all these different limits can be found in the Google documentation:

https://cloud.google.com/compute/docs/network-bandwidth

As well as the Google limits the Bridgeworks PORTrockIT is performance limited as detailed in the following table:

PORTrockIT tier	Maximum throughput
PORTrockIT 100 Series	1 Gbits/s
PORTrockIT 200 Series	2 Gbits/s
PORTrockIT 400 Series	10 Gbits/s

At the time of writing a PORTrockIT 400 Series running on *N2 series* machine connected to another unit on an external IP address would be limited to 3Gbit/s egress due to the Google cloud egress limit, and 10Gbit/s ingress due to Bridgeworks licence limit for the 400 Series. To achieve this level of performance the *N2* instance must have sufficient CPU's and memory, and of course the infrastucture external to Google must be able to support this level of performance.