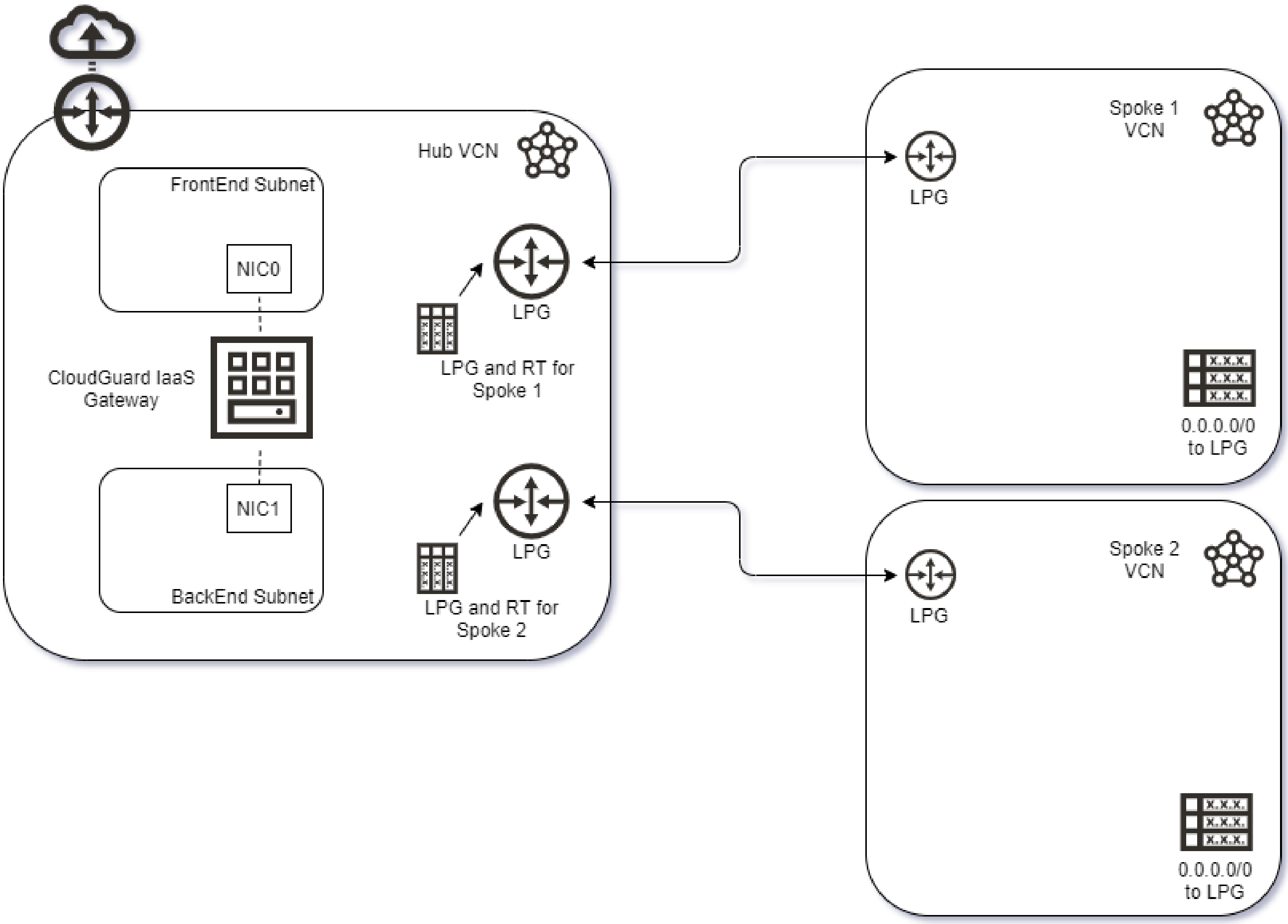
OCI Hub and Spoke CloudGuard

Christian Abraham Castillo Porras
Cloud Security Architect - LATAM
September 2020

The design of a Check Point Gateway to protect the traffic inside OCI deployments was with the use of several NIC, this create a hard to manage and the use of big Instance sizes to overcome the vNIC quantity OCI limitation number.

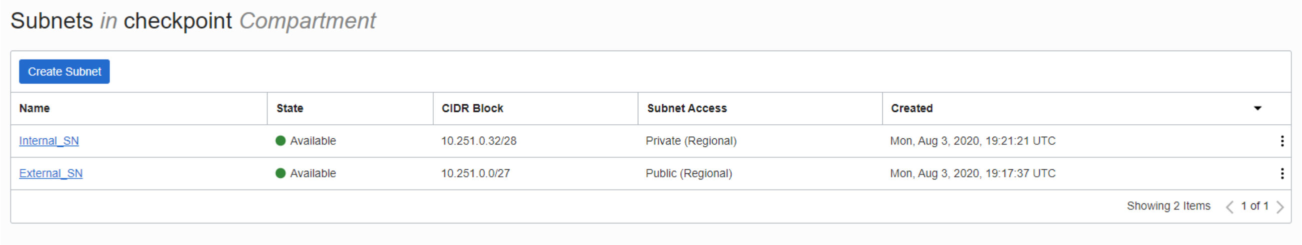
In this admin guide, we will show how to create a 2-vNIC machine in the same VCN, to protect several VCN with the use of LPG and Route Tables, for the use case, we will create a single GW deployment on this guide but it supports Cluster deployment also following the SK142872.



The diagram explain what we want to achieve, the Local Peering Gateways (LPG) located at Hub VCN will have an attached Route Table (RT) that points to the Check Point NIC1 IP address, this will create the flow as when the traffic comes from Spokes the default route will be the LPG at Spoke and when the traffic emanates on the Hub will be directed to the Check Point CloudGuard IaaS.

Traffic to Internet (browsing) and between Spokes (segmentation) will be inspected and firewalled on the IaaS device, creating a Threat Prevention flow.

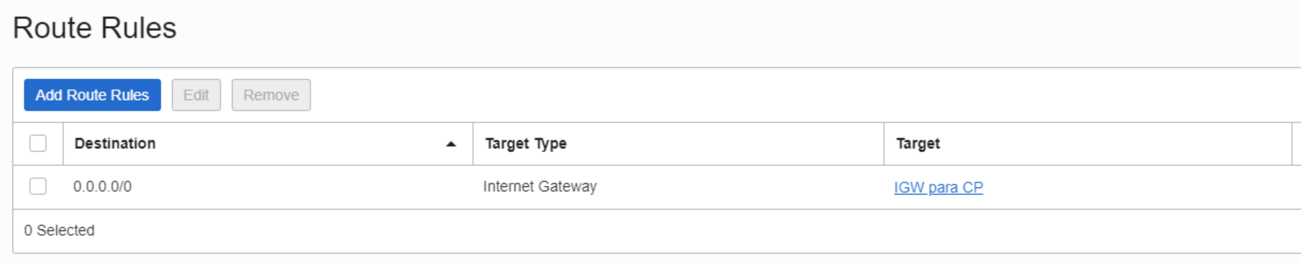
We will start creating the Huv VCN, this will have two subnets; since the Check Point Gateway uses 2 vNIC machines; one should be assigned to internet faced interface (eth0) and the other one to the internal facing interface (eth1) you can create it in Private and Public Subnet access mode.



Subnets *in* checkpoint *Compartment*

Name	State	CIDR Block	Subnet Access	Created
Internal_SN	● Available	10.251.0.32/28	Private (Regional)	Mon, Aug 3, 2020, 19:21:21 UTC
External_SN	● Available	10.251.0.0/27	Public (Regional)	Mon, Aug 3, 2020, 19:17:37 UTC

This VCN also needs to have the Internet Gateway and the next route table attached to the Internet facing subnet.

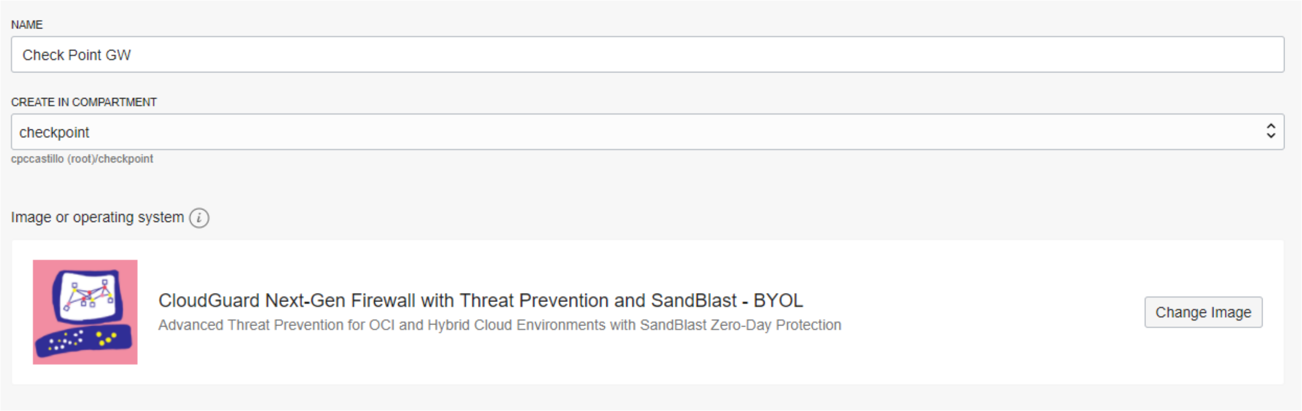


Route Rules

	Destination	Target Type	Target
□	0.0.0.0/0	Internet Gateway	IGW para CP

0 Selected

Create the Check Point VM, you can use the sk168202 for templates.



NAME: Check Point GW

CREATE IN COMPARTMENT: checkpoint

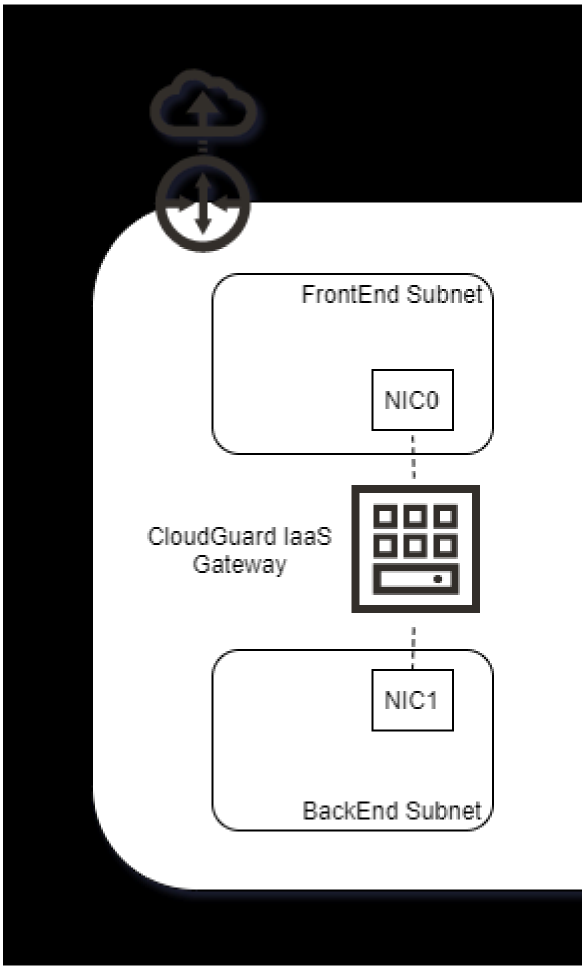
cpccastillo (root)/checkpoint

Image or operating system

CloudGuard Next-Gen Firewall with Threat Prevention and SandBlast - BYOL

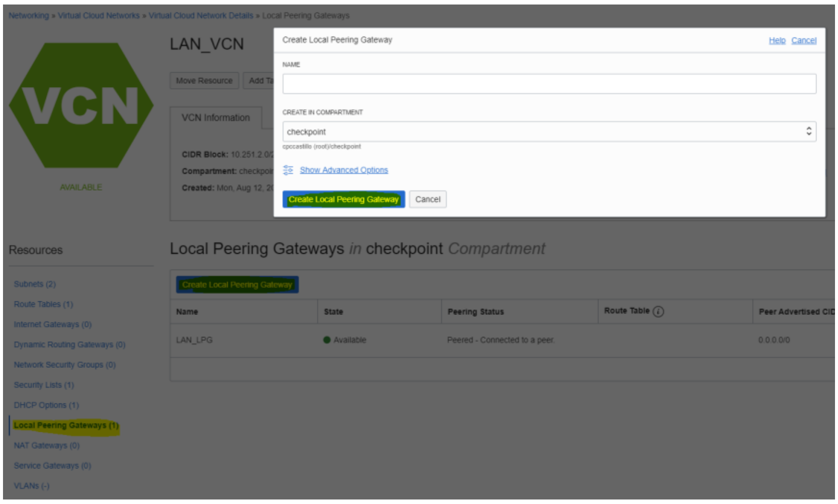
Advanced Threat Prevention for OCI and Hybrid Cloud Environments with SandBlast Zero-Day Protection

At the end, we will have our machine on the Hub VCN with the two-vNIC deployment.



Now is time to connect the other VCN to the new hub and redirect the traffic to the Check Point Gateways, for this OCI have the option to connect several VCN by Local Peering Gateways (LPG), so let us start by connecting the Hub VCN with one Spoke.

In the Spoke we will go to LPG and create a new one


Networking » Virtual Cloud Networks » Virtual Cloud Network Details » Local Peering Gateways

LAN_VCN

CIDR Block: 10.251.2.0/
Compartment: checkpoi
Created: Mon, Aug 12, 2

Create Local Peering Gateway

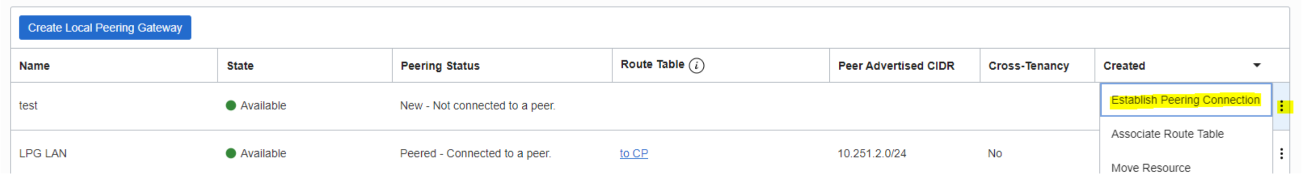
NAME

CREATE IN COMPARTMENT: checkpoint
cpccastillo (root)/checkpoint

Local Peering Gateways *in* checkpoint *Compartment*

Name	State	Peering Status	Route Table	Peer Advertised CID
LAN_LPG	● Available	Peered - Connected to a peer.		0.0.0.0/0

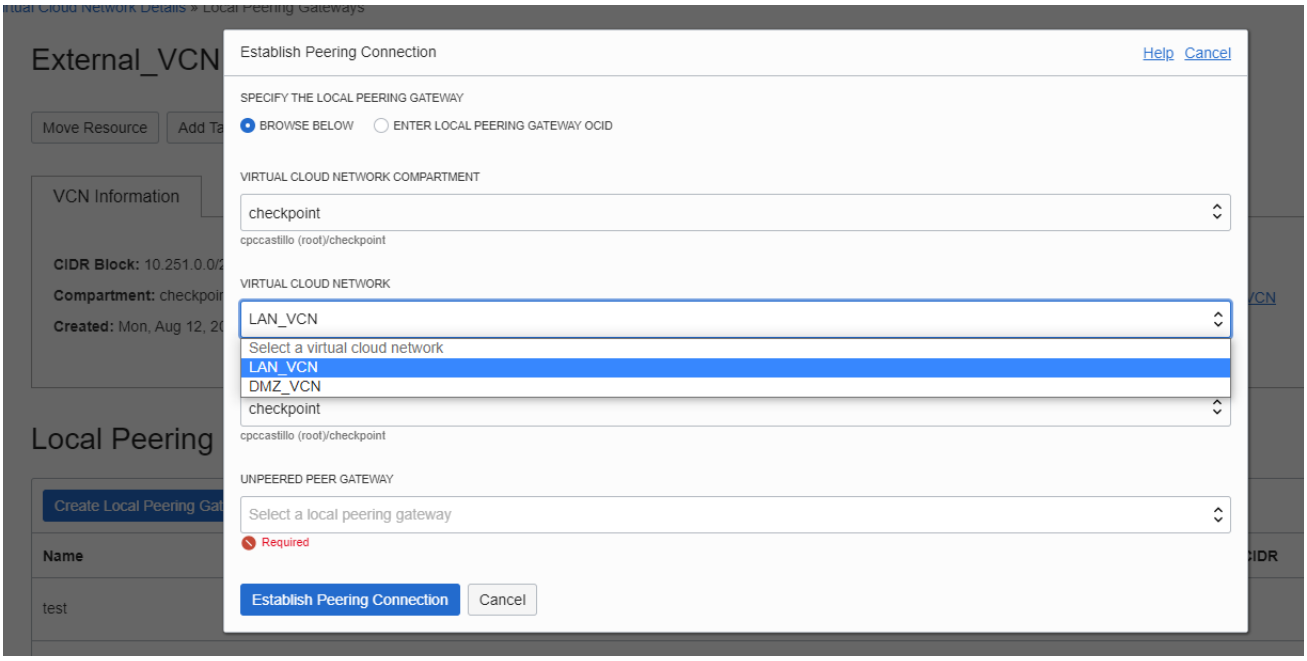
All the newly deployed LPG are disconnected, but ready to be connected; now we need to create a connector on the Hub VCN (another LPG), when both LGP are created we need to stablish a conection, in this case, click on the three buttons of the LGP and “Establish…”



Create Local Peering Gateway

Name	State	Peering Status	Route Table	Peer Advertised CIDR	Cross-Tenancy	Created
test	● Available	New - Not connected to a peer.				
LPG LAN	● Available	Peered - Connected to a peer.	to CP	10.251.2.0/24	No	

In the next window need to look for the previously deployed LPG



Establish Peering Connection

SPECIFY THE LOCAL PEERING GATEWAY

● BROWSE BELOW ○ ENTER LOCAL PEERING GATEWAY OCID

VIRTUAL CLOUD NETWORK COMPARTMENT: checkpoint

cpccastillo (root)/checkpoint

VIRTUAL CLOUD NETWORK: LAN_VCN

Select a virtual cloud network
LAN_VCN
DMZ_VCN

checkpoint

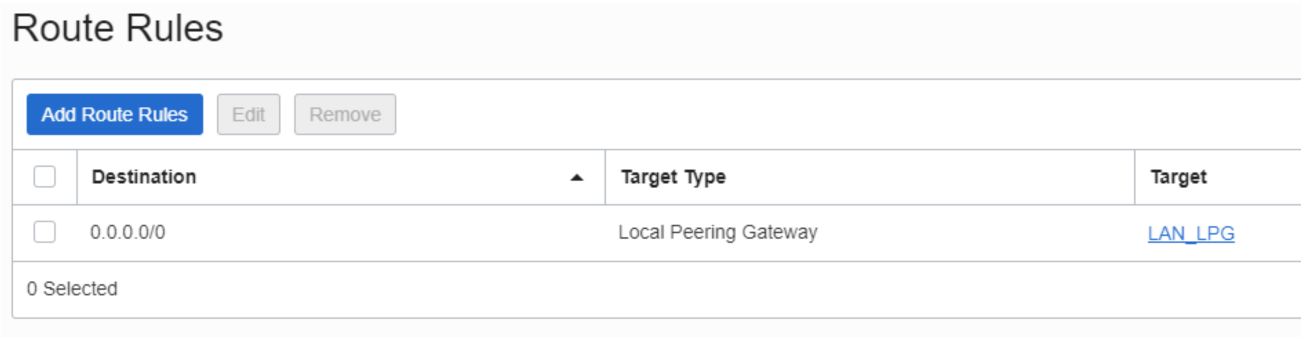
cpccastillo (root)/checkpoint

UNPEERED PEER GATEWAY: Select a local peering gateway

Required

This create the connection, now our two VCN have connectivity.

There is a feature that allow us to create transit (routing traffic from one VCN to a different CIDR block than the Connected hub), on the side of the Spoke we will redirect the desired traffic to be analyzed to the LPG as next hop, for example if we want to send all internet traffic to the hub we create a Route Table with 0.0.0.0/0 to LPG (the local one)



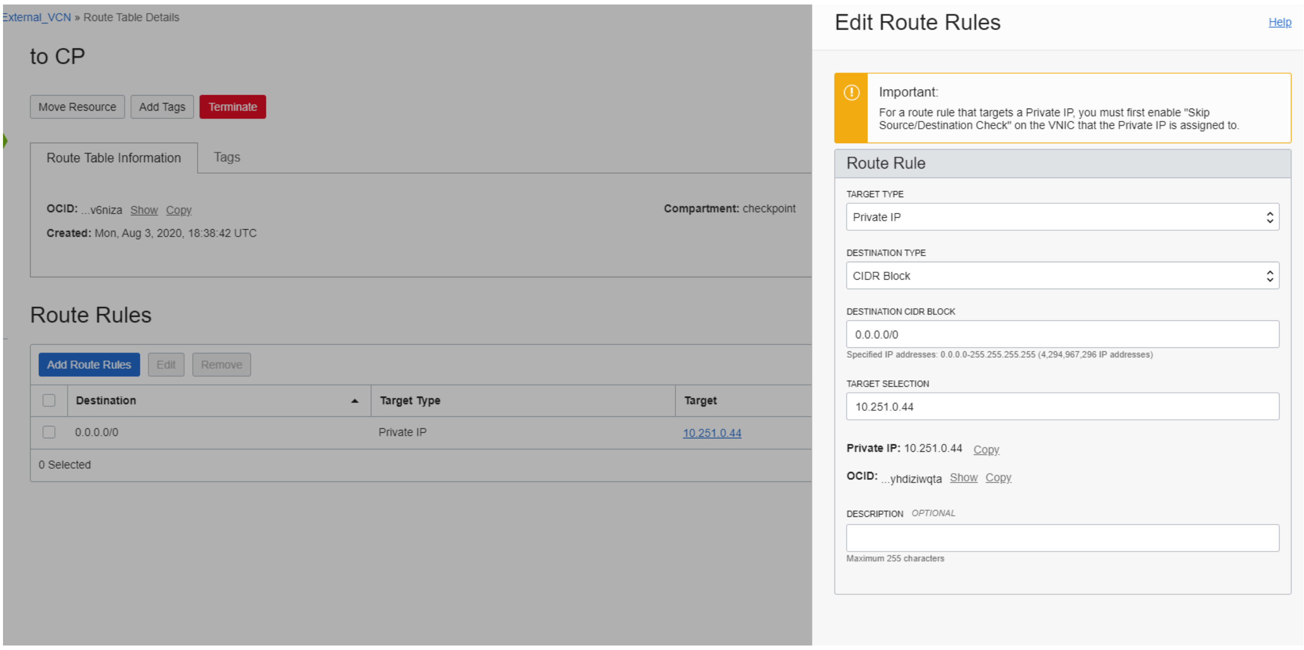
Route Rules

□	Destination	Target Type	Target
□	0.0.0.0/0	Local Peering Gateway	LAN_LPG

0 Selected

With this all the traffic 0.0.0.0/0 will be send to the hub, but now we need to say to the traffic how to go to a device, this is by assigning a RT to the Hub LPG, whit this the feature will say how the emanating traffic from the LPG needs to behave.

The route table needs to be 0.0.0.0/0 to the secondary vNIC of the Check Point VM, so we grab the OCID of that interface and create a route table.



External_VCN » Route Table Details

to CP

OCID: ...v6niza Show Copy

Compartment: checkpoint

Created: Mon, Aug 3, 2020, 18:38:42 UTC

Route Rules

	Destination	Target Type	Target
□	0.0.0.0/0	Private IP	10.251.0.44

0 Selected

Edit Route Rules

Important:
For a route rule that targets a Private IP, you must first enable "Skip Source/Destination Check" on the VNIC that the Private IP is assigned to.

Route Rule

TARGET TYPE: Private IP

DESTINATION TYPE: CIDR Block

DESTINATION CIDR BLOCK: 0.0.0.0/0

Specified IP addresses: 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses)

TARGET SELECTION: 10.251.0.44

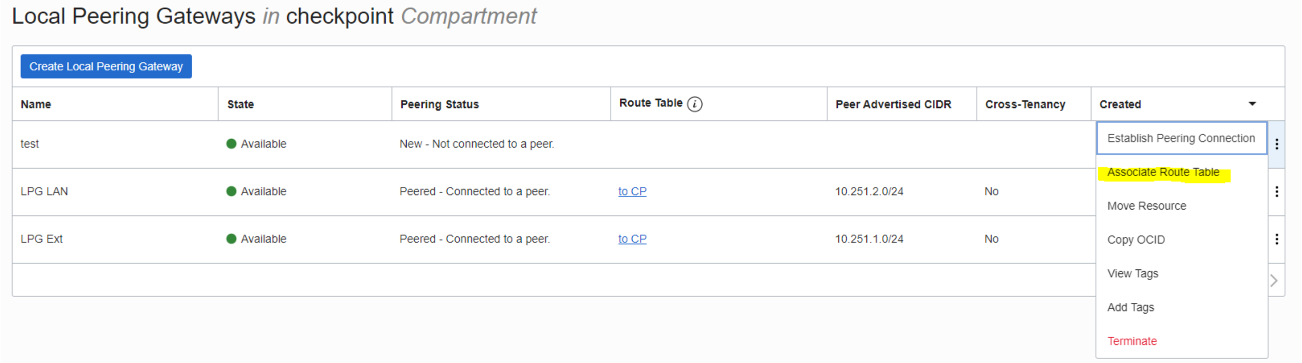
Private IP: 10.251.0.44 Copy

OCID: ...yhdiziwqta Show Copy

DESCRIPTION *OPTIONAL*

Maximum 255 characters

In addition, associate this route table to the LPG from the Hub



Local Peering Gateways *in* checkpoint *Compartment*

Name	State	Peering Status	Route Table	Peer Advertised CIDR	Cross-Tenancy	Created
test	● Available	New - Not connected to a peer.				
LPG LAN	● Available	Peered - Connected to a peer.	to CP	10.251.2.0/24	No	
LPG Ext	● Available	Peered - Connected to a peer.	to CP	10.251.1.0/24	No	

Now to maintain symmetry on the routes need to tweak two things, the RouteTable associated to the internal subnet of the hub to point the CIDR block of the Spokes to the relevant LPG for the reply and also the Gaia OS routes to point all the CIDR block of Spokes (can be supernet) to the first host of the Internal Subnet on HUB.