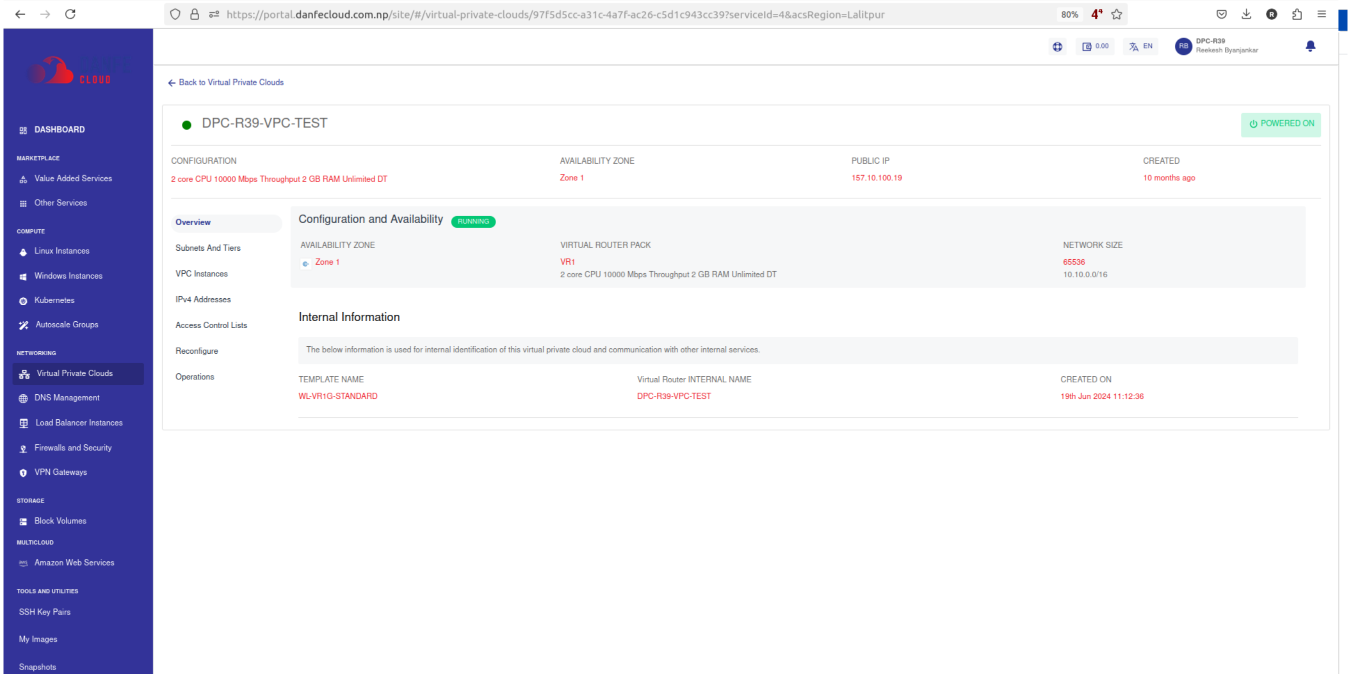
1. About Virtual Private Clouds

Details about Virtual Private Cloud operations and actions can be found in their respective sections.



DPC-R39-VPC-TEST

CONFIGURATION	AVAILABILITY ZONE	PUBLIC IP	CREATED
2 core CPU 10000 Mbps Throughput 2 GB RAM Unlimited DT	Zone 1	157.10.100.19	10 months ago

Configuration and Availability

AVAILABILITY ZONE	VIRTUAL ROUTER PACK	NETWORK SIZE
Zone 1	VR1 2 core CPU 10000 Mbps Throughput 2 GB RAM Unlimited DT	65536 10.10.0.0/16

Internal Information

The below information is used for internal identification of this virtual private cloud and communication with other internal services.

TEMPLATE NAME	Virtual Router INTERNAL NAME	CREATED ON
WL-VR1G-STANDARD	DPC-R39-VPC-TEST	19th Jun 2024 11:12:36

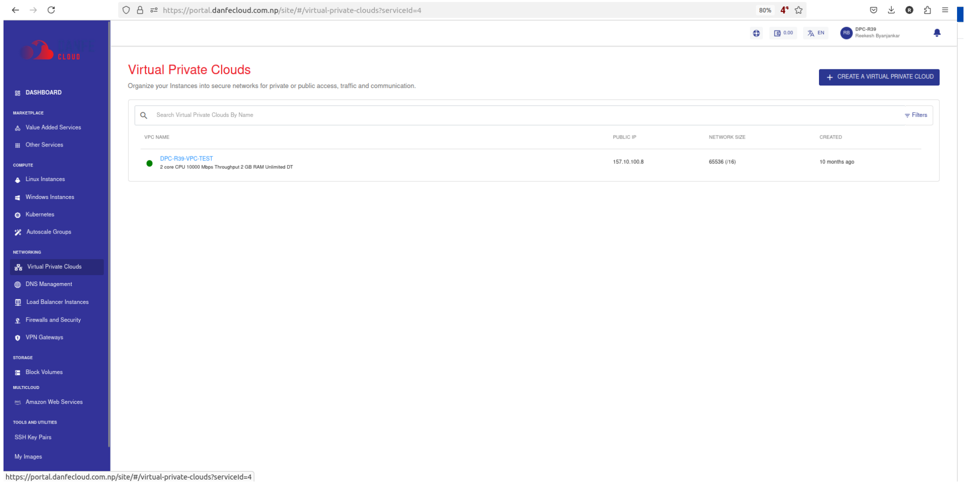
- Create, List and View VPCs
- Overview
- Creating subnets and tiers
- Managing VPC Instances
- Working with IPv4 addresses
- Access control on a VPC
- Reconfiguring the VPC
- VPC operations

2. Create, List and View VPCs

Creating a VPC

To create a VPC, follow the below steps:

1. Navigate to **Networking > Virtual Private Clouds**

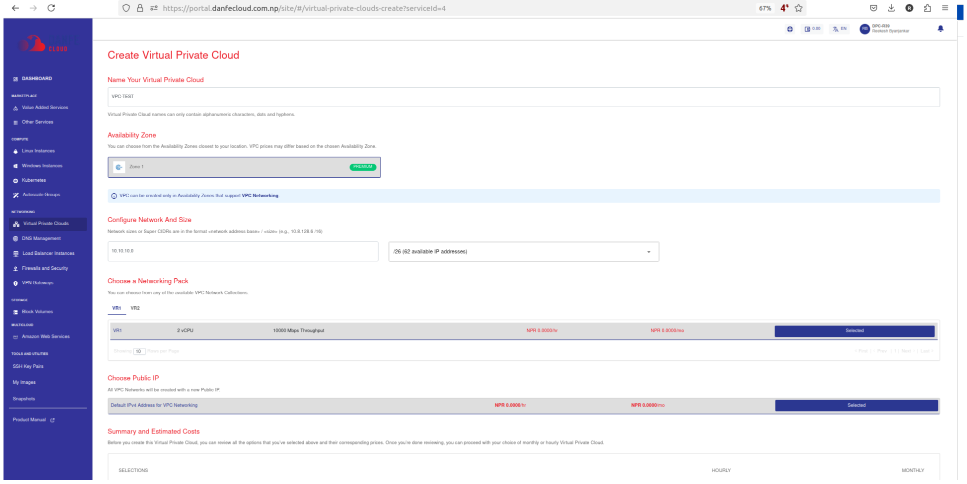


Virtual Private Clouds

Organize your Instances into secure networks for private or public access, traffic and communication.

VPC NAME	PUBLIC IP	NETWORK SIZE	CREATED
● DPC-R39-VPC-TEST 2 core CPU 10000 Mbps Throughput 2 GB RAM Unlimited DT	157.10.100.8	65536 (/16)	10 months ago

2. Click the **NEW VIRTUAL PRIVATE CLOUD** button.
3. Choose an Availability Zone, which is the geographical region where your VPC will be configured.
4. Specify network address base size and select size i.e. The **super CIDR** for the internal IP allocation in an x.x.x.x/x format.
5. Choose a Networking pack from the available network collections.
6. Select the default IPv4 address for VPC Networking to create the VPC network with a new Public IP address.



Create Virtual Private Cloud

Name Your Virtual Private Cloud: VPC-TEST

Virtual Private Cloud names can only contain alphanumeric characters, dots and hyphens.

Availability Zone

You can choose from the Availability Zones closest to your location. VPC prices may differ based on the chosen Availability Zone.

Zone 1

VPC can be created only in Availability Zones that support **VPC Networking**.

Configure Network And Size

Network sizes or Super CIDRs are in the format <network address base> / <size> (e.g., 10.8.128.6 /16)

10.10.10.0 /26 (62 available IP addresses)

Choose a Networking Pack

You can choose from any of the available VPC Network Collections.

VR1	2 vCPU	10000 Mbps Throughput	NPR 0.0000/hr	NPR 0.0000/mo	Selected

Showing 10 Rows per Page

Choose Public IP

All VPC Networks will be created with a new Public IP.

Default IPv4 Address for VPC Networking	NPR 0.0000/hr	NPR 0.0000/mo	Selected

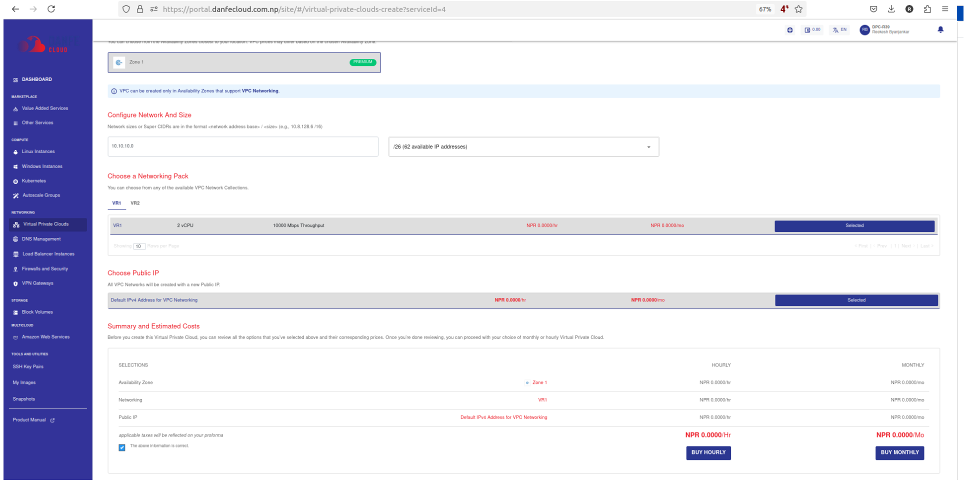
Summary and Estimated Costs

Before you create this Virtual Private Cloud, you can review all the options that you've selected above and their corresponding prices. Once you're done reviewing, you can proceed with your choice of monthly or hourly Virtual Private Cloud.

SELECTIONS	HOURLY	MONTHLY

7. Verify the Estimated Cost of your VPC, based on the options that you have chosen from the Summary and Estimated Costs Section.
8. Select the **I have read and agreed to the End User License Agreement and Privacy Policy** option.
9. Clicking the **BUY HOURLY** or **BUY MONTHLY** button, a confirmation pop-over will open up, and the price summary will be displayed along with the discount codes, if you have any in your account.
    a. You can apply any of the discount codes listed by clicking on the **APPLY** button.
    b. You can also remove the applied discount code by clicking the **REMOVE** button.

c. Clicking on the **CANCEL** button, this action will be canceled.



You can choose from the Availability Zones closest to your location. VPC prices may differ based on the chosen Availability Zone.

Zone 1 PREMIUM

VPC can be created only in Availability Zones that support **VPC Networking**.

Configure Network And Size

Network sizes or Super CIDRs are in the format <network address base> / <size> (e.g., 10.8.128.6 /16)

10.10.10.0

/26 (62 available IP addresses)

Choose a Networking Pack

You can choose from any of the available VPC Network Collections.

VR1 VR2

VR1	2 vCPU	10000 Mbps Throughput	NPR 0.0000/hr	NPR 0.0000/mo	Selected

Showing 10 Rows per Page < First | < Prev | 1 | Next > | Last >

Choose Public IP

All VPC Networks will be created with a new Public IP.

Default IPv4 Address for VPC Networking	NPR 0.0000/hr	NPR 0.0000/mo	Selected

Summary and Estimated Costs

Before you create this Virtual Private Cloud, you can review all the options that you've selected above and their corresponding prices. Once you're done reviewing, you can proceed with your choice of monthly or hourly Virtual Private Cloud.

SELECTIONS		HOURLY	MONTHLY
Availability Zone	Zone 1	NPR 0.0000/hr	NPR 0.0000/mo
Networking	VR1	NPR 0.0000/hr	NPR 0.0000/mo
Public IP	Default IPv4 Address for VPC Networking	NPR 0.0000/hr	NPR 0.0000/mo
applicable taxes will be reflected on your proforma		NPR 0.0000/Hr	NPR 0.0000/Mo

☑ The above information is correct.

BUY HOURLY BUY MONTHLY

10. Click on the **CONFIRM** to create the VPC.

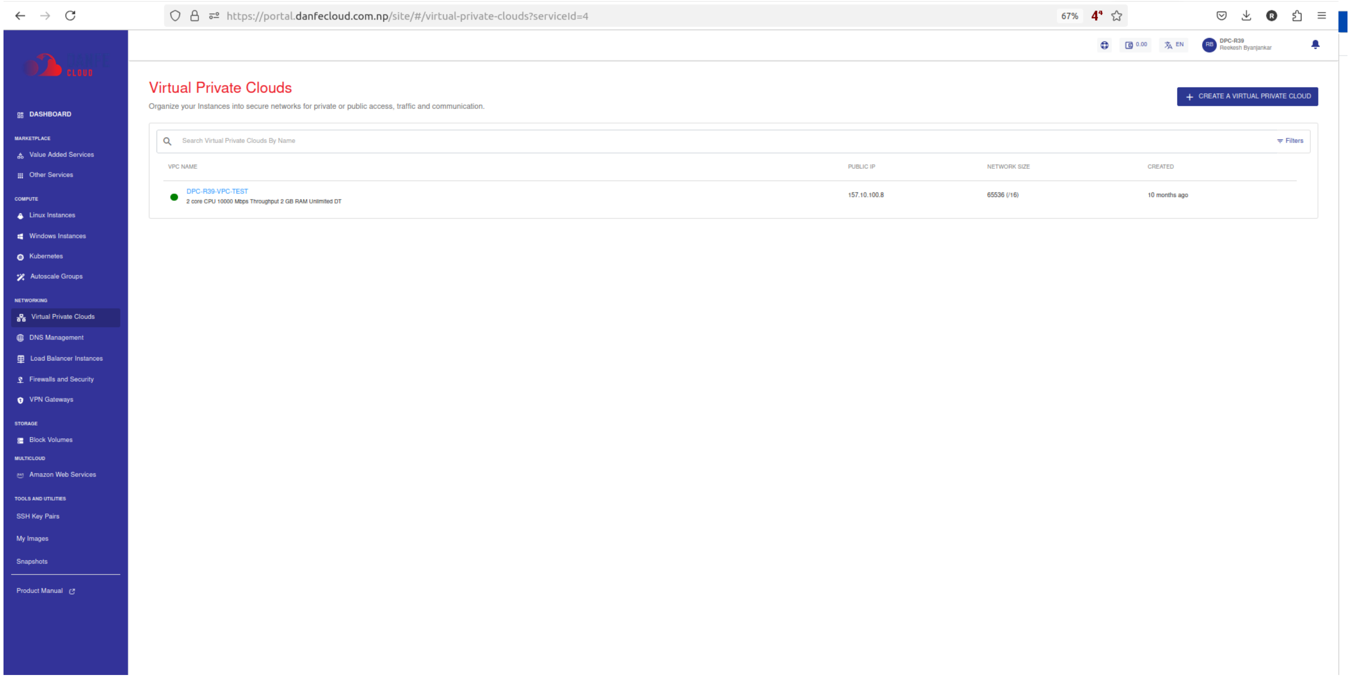
Once ready, you'll be notified of this purchase on your email address on record.

NOTE: This might take up to 5-8 minutes. You may use the Cloud Console during this time, but it is advised that you do not refresh the browser window.

Viewing Available VPC

All VPC created in a user account can be accessed from **Networking > Virtual Private Clouds** on the main navigation panel. The listing will have the following details.

- VPC Name
- Public IP
- Network Size
- Created



Virtual Private Clouds

Organize your Instances into secure networks for private or public access, traffic and communication.

Search Virtual Private Clouds By Name

VPC NAME	PUBLIC IP	NETWORK SIZE	CREATED
● DPC-R39-VPC-TEST 2 core CPU 10000 Mbps Throughput 2 GB RAM Unlimited DT	157.10.100.8	65536 (/16)	10 months ago

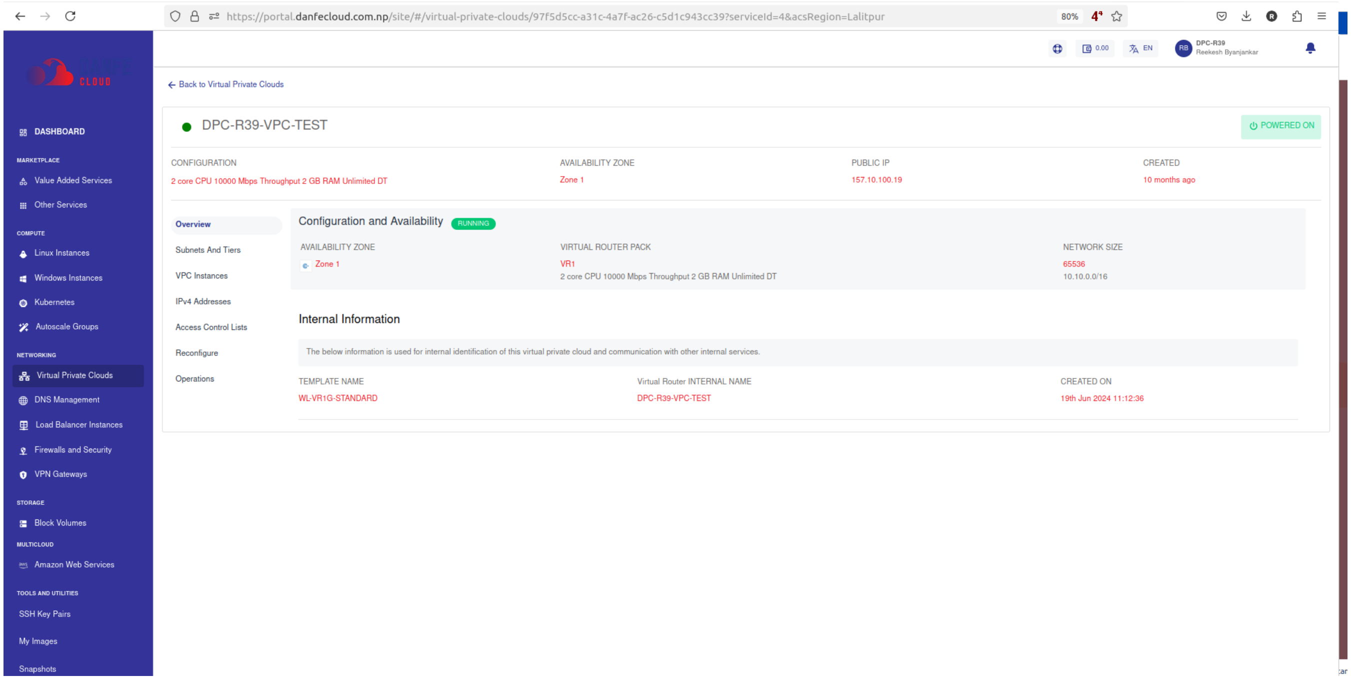
3. Overview

To view a list of sections and the various operations or actions you can perform by going inside the particular section, click on the VPC name. Below the VPC name is an informational view where you can find the details below.

- Configuration
- Availability Zone
- Public IP
- Created

Along with the summary, the following information is readily available under the **Overview** tab:

- **Configuration and Availability**-
  - The instance's status, **RUNNING**, is displayed in **green**, whereas **STOPPED** is displayed in grey.
  - Information about the Virtual Router Pack.
  - Information about the Network Size.
- **Internal Information**-
  This displays the information that is used for internal identification of this VPC router and communication with other internal services.
  - Template Name
  - Virtual Router Internal Name
  - Created On



DPC-R39-VPC-TEST

CONFIGURATION	AVAILABILITY ZONE	PUBLIC IP	CREATED
2 core CPU 10000 Mbps Throughput 2 GB RAM Unlimited DT	Zone 1	157.10.100.19	10 months ago

Configuration and Availability

AVAILABILITY ZONE	VIRTUAL ROUTER PACK	NETWORK SIZE
Zone 1	VR1 2 core CPU 10000 Mbps Throughput 2 GB RAM Unlimited DT	65536 10.10.0.0/16

Internal Information

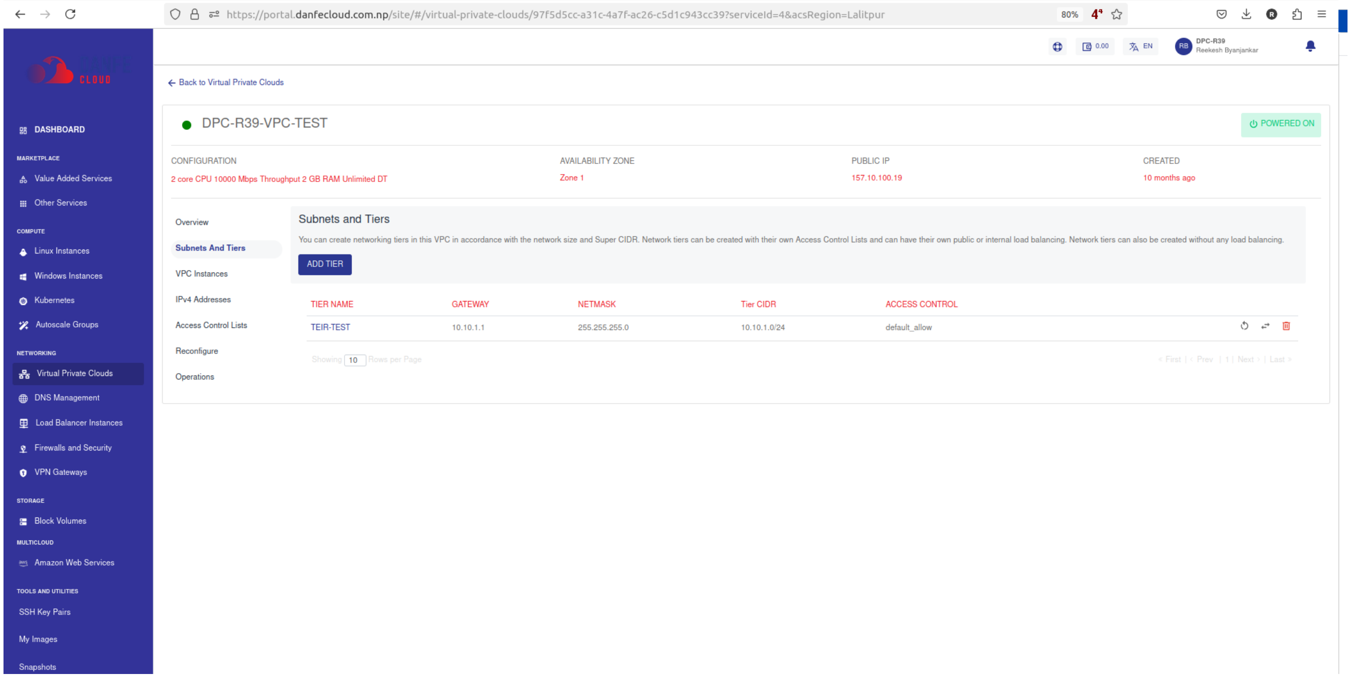
The below information is used for internal identification of this virtual private cloud and communication with other internal services.

TEMPLATE NAME	Virtual Router INTERNAL NAME	CREATED ON
WL-VR1G-STANDARD	DPC-R39-VPC-TEST	19th Jun 2024 11:12:36

From here on, VPC operations, configurations and other available functions can be managed by navigating to the respective tabs/sections.

4. Creating VPC Subnets and Tiers

VPCs follow the convention of 3-tiered architectures, with web, app, and DB tiers forming the norm. You can, however, configure these tiers to suit your application architecture or just follow the common convention.



https://portal.danfecloud.com.np/site/#/virtual-private-clouds/97f5d5cc-a31c-4a7f-ac26-c5d1c943cc39?serviceId=4&acsRegion=Lalitpur

DPC-R39-VPC-TEST

CONFIGURATION	AVAILABILITY ZONE	PUBLIC IP	CREATED
2 core CPU 10000 Mbps Throughput 2 GB RAM Unlimited DT	Zone 1	157.10.100.19	10 months ago

Subnets and Tiers

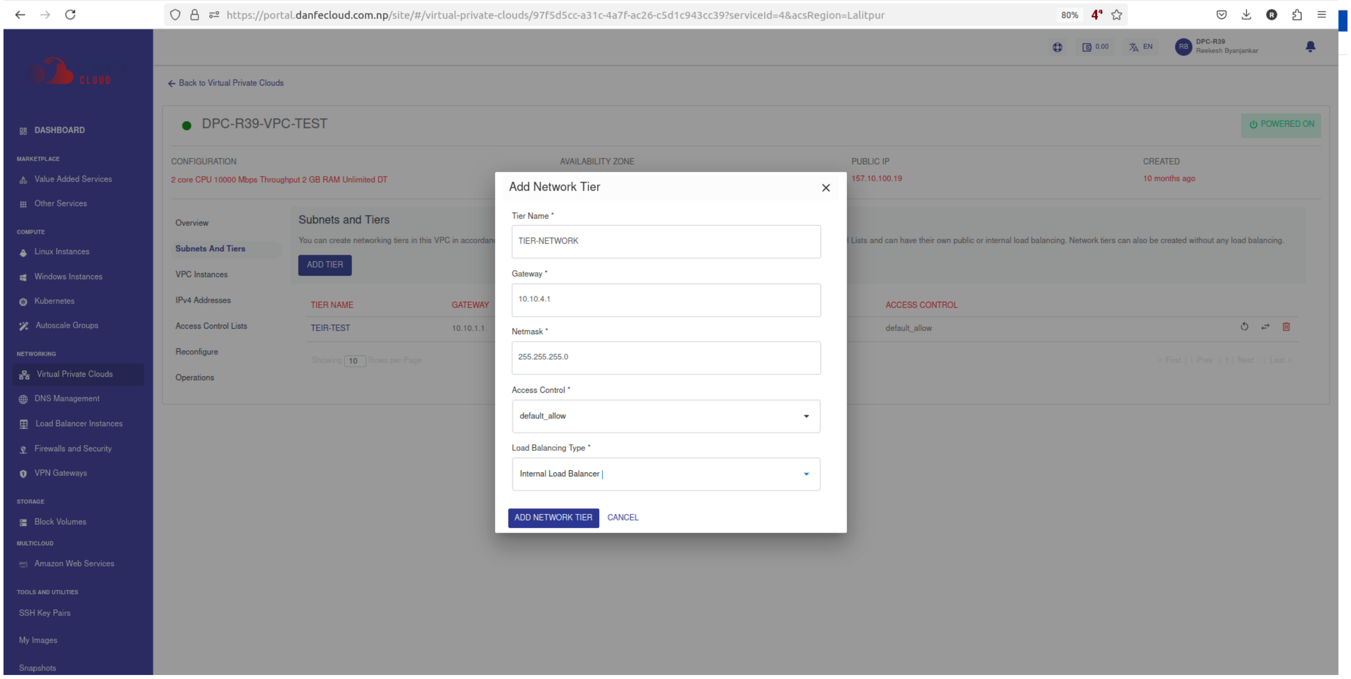
You can create networking tiers in this VPC in accordance with the network size and Super CIDR. Network tiers can be created with their own Access Control Lists and can have their own public or internal load balancing. Network tiers can also be created without any load balancing.

TIER NAME	GATEWAY	NETMASK	Tier CIDR	ACCESS CONTROL
TEIR-TEST	10.10.1.1	255.255.255.0	10.10.1.0/24	default_allow

To add a tier to your VPC, navigate to the VPC you wish to add the tier to, and click the **ADD TIER** option present inside the **SUBNETS AND TIERS** section of the VPC. This will open up a dialog box asking you to provide the following information:

- **Name** of the tier.
- **Gateway** for the subnet.
- **Netmask** for the tier/subnet.
  NOTE:The gateway should be consistent with the subnet mask.

- Default **access control** policy for this tier.
- **Load balancing type** required on this tier.
  *NOTE: To set up a public load balancer, you need to select **Public LB** on this dropdown. There can only be 1 tier of type Public LB in a network.*



Add Network Tier

Tier Name *: TIER-NETWORK

Gateway *: 10.10.4.1

Netmask *: 255.255.255.0

Access Control *: default_allow

Load Balancing Type *: Internal Load Balancer

ADD NETWORK TIER | CANCEL

To create the tier or subnet to be used as part of the VPC, click on **ADD NETWORK TIER**.

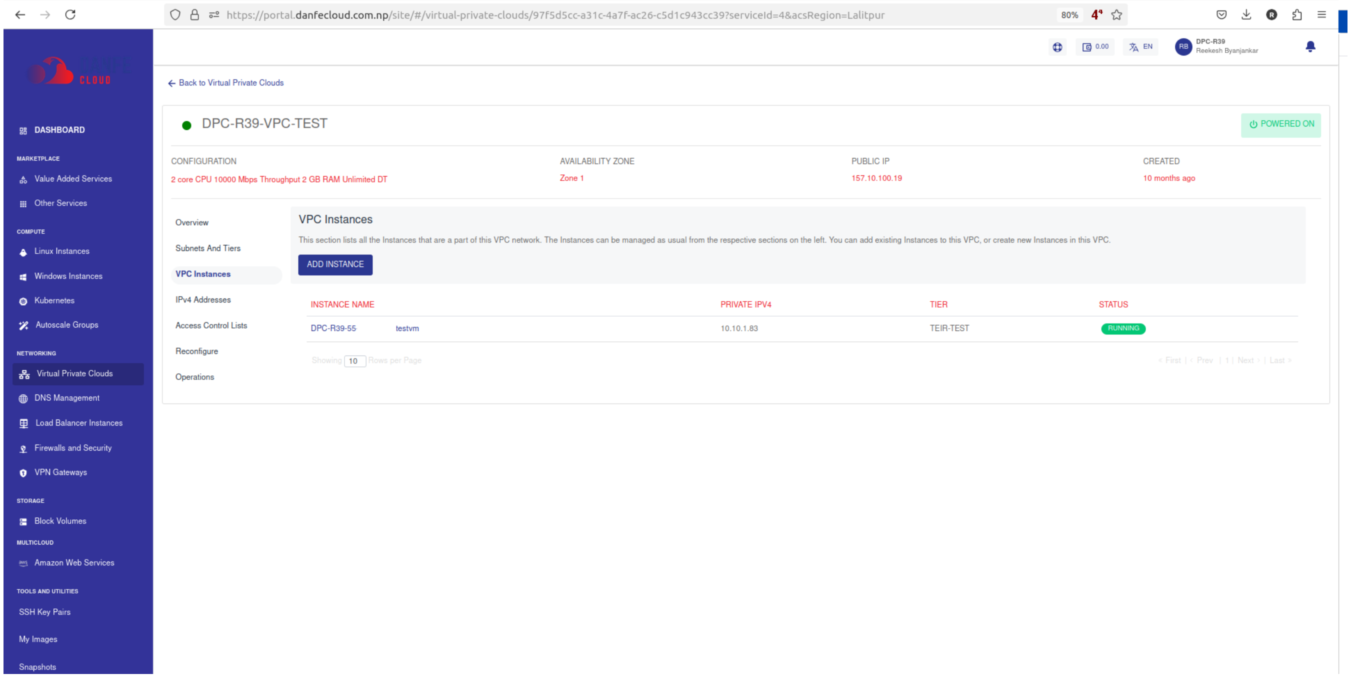
There are three icons available on the right side for quick actions like restarting the network, replacing the access control list, and deleting the tier.

NOTE: Only empty tiers can be deleted, which means that in order to delete a tier, ensure that there are no Instances and no NAT rule(s) associated with it.

5. Managing VPC Instances

Viewing VPC Instances

Apiculus Cloud Console offers a quick means to view Instances that are part of a VPC network, and to associate or dissociate Instances with VPCs by navigating to VPC details and selecting **VPC Instances**.



DPC-R39-VPC-TEST

CONFIGURATION	AVAILABILITY ZONE	PUBLIC IP	CREATED
2 core CPU 10000 Mbps Throughput 2 GB RAM Unlimited DT	Zone 1	157.10.100.19	10 months ago

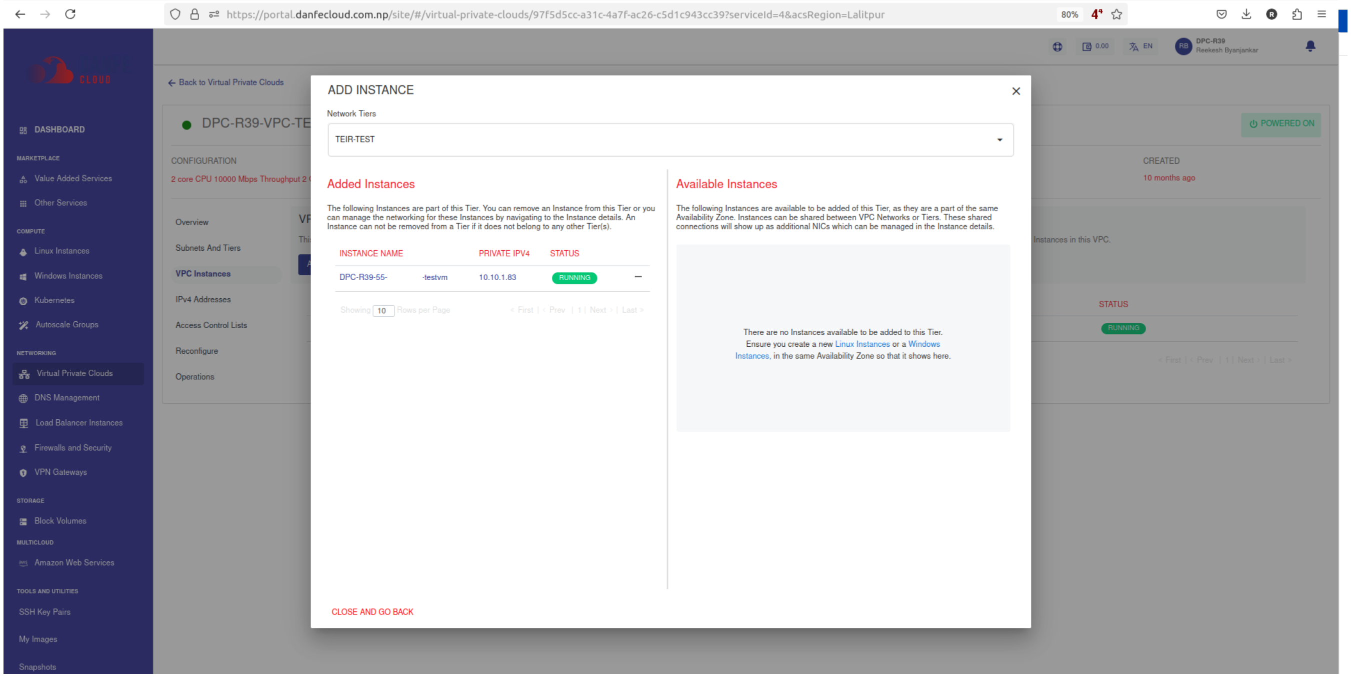
VPC Instances

This section lists all the Instances that are a part of this VPC network. The Instances can be managed as usual from the respective sections on the left. You can add existing Instances to this VPC, or create new Instances in this VPC.

INSTANCE NAME	PRIVATE IPV4	TIER	STATUS
DPC-R39-55 testvm	10.10.1.83	TEIR-TEST	RUNNING

Adding (or Removing) Instances to VPC

To view all Instances that are available to be added to this VPC, click the **ADD INSTANCE** button. Since VPC allows adding multiple NICs to instances, instances can be shared between VPC networks (and across tiers within the same VPC), as long as the VPC networks are within the same Availability Zone.


https://portal.danfecloud.com.np/site/#/virtual-private-clouds/97f5d5cc-a31c-4a7f-ac26-c5d1c943cc39?serviceId=4&acsRegion=Lalitpur
80%
CLOUD
DASHBOARD
Back to Virtual Private Clouds
POWERED ON
ADD INSTANCE
×
Showing 10 Rows per Page
« First | ‹ Prev | 1 | Next › | Last »
CLOSE AND GO BACK

ADD INSTANCE

Network Tiers: TEIR-TEST

Added Instances

The following Instances are part of this Tier. You can remove an Instance from this Tier or you can manage the networking for these Instances by navigating to the Instance details. An Instance can not be removed from a Tier if it does not belong to any other Tier(s).

INSTANCE NAME	PRIVATE IPV4	STATUS	
DPC-R39-55- -testvm	10.10.1.83	RUNNING	−

Available Instances

The following Instances are available to be added of this Tier, as they are a part of the same Availability Zone. Instances can be shared between VPC Networks or Tiers. These shared connections will show up as additional NICs which can be managed in the Instance details.

There are no Instances available to be added to this Tier. Ensure you create a new Linux Instances or a Windows Instances, in the same Availability Zone so that it shows here.

NOTE: An Instance created in any VPC/advanced Availability Zone must be attached to at least one subnet.

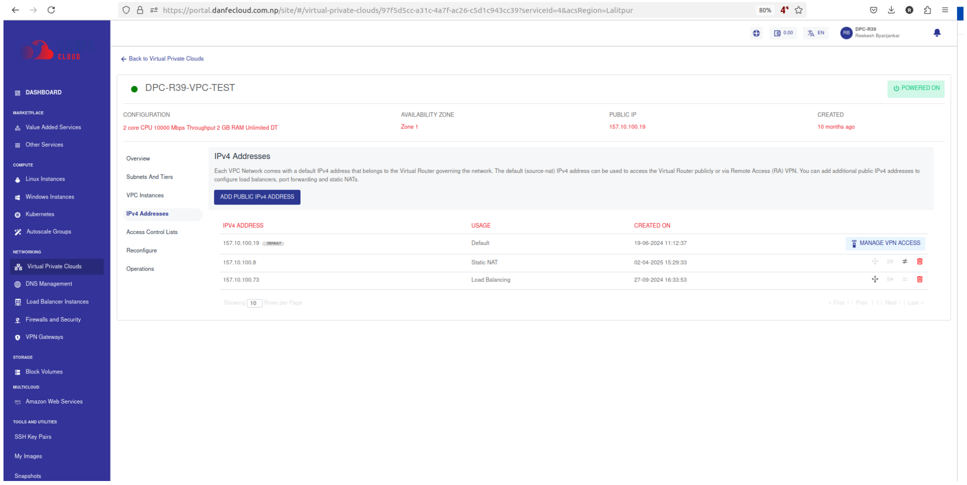
6. IPv4 Addresses and VPC

IPv4 Addresses are an integral part of using VPC networking, and need to be used to access various components of the VPC. By default, a public IPv4 Address is assigned to the VR which can communicate through the internet to transmit traffic to/from the VR. This IPv4 can also be used for configuring remote access (L2TP) and site-to-site (IPSec) VPN connections.

Using Additional IPv4

Primarily, IPv4 Addresses can be used for configuring access and NAT-ing via:

- Load balancing
- Port Forwarding
- Static NAT



DPC-R39-VPC-TEST

CONFIGURATION	AVAILABILITY ZONE	PUBLIC IP	CREATED
2 core CPU 10000 Mbps Throughput 2 GB RAM Unlimited DT	Zone 1	157.10.100.19	10 months ago

IPv4 Addresses

Each VPC Network comes with a default IPv4 address that belongs to the Virtual Router governing the network. The default (source-nat) IPv4 address can be used to access the Virtual Router publicly or via Remote Access (RA) VPN. You can add additional public IPv4 addresses to configure load balancers, port forwarding and static NATs.

IPV4 ADDRESS	USAGE	CREATED ON
157.10.100.19 DEFAULT	Default	19-06-2024 11:12:37
157.10.100.8	Static NAT	02-04-2025 15:29:33
157.10.100.73	Load Balancing	27-09-2024 16:33:53

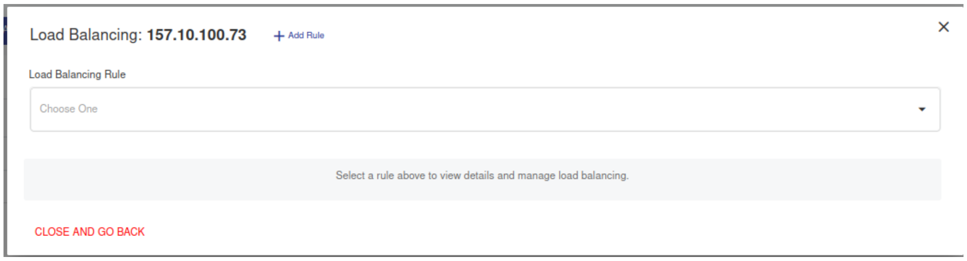
As a first step, a new IPv4 Address needs to be added to the VPC, which can be done using the **ADD PUBLIC IPv4 ADDRESS** button.

note: Public IPv4 addresses may carry a price which may vary depending on availability of IPv4 addresses in the country of operation, and/or how the service provider has priced them.

Configuring Load Balancing

To configure the Load Balancing Rule, follow these steps:

1. To create Load Balancing Rule, click the icon.

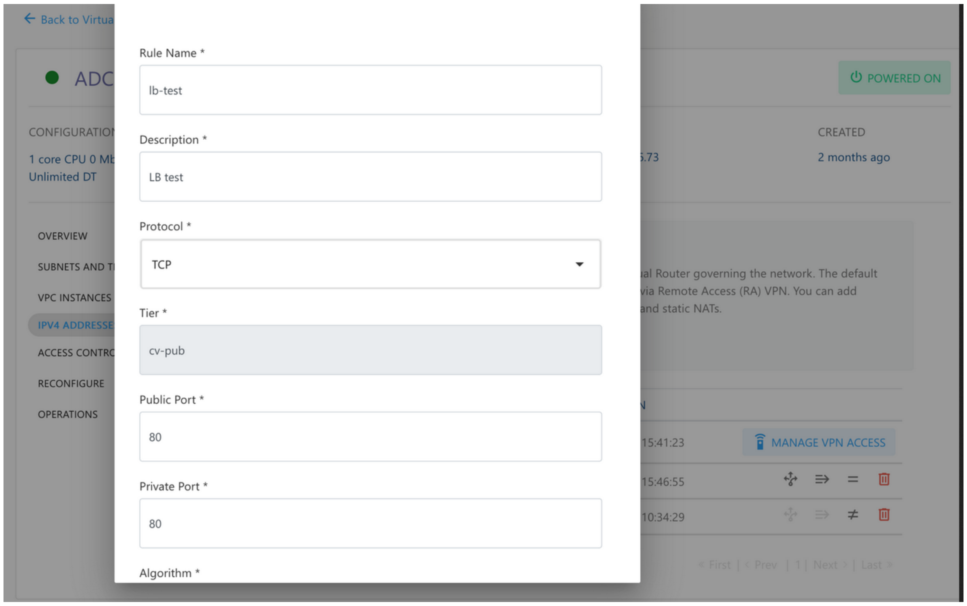


Load Balancing: **157.10.100.73**

Load Balancing Rule: Choose One

Select a rule above to view details and manage load balancing.

2. The following window appears:
3. Click **Add Rule**. The following window appears:



Rule Name * lb-test

Description * LB test

Protocol * TCP

Tier * cv-pub

Public Port * 80

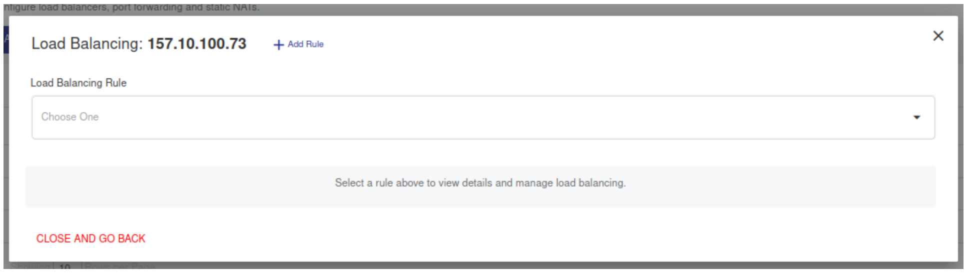
Private Port * 80

Algorithm *

4. Specify the following details in the window:
   - A **name** and **description** for the load balancer rule.
   - **Protocol** to use for the load balancer.
   - Select the **Tier**.
   - The **load balancing algorithm** to use.
   - **Public** and **private** port mapping.
5. Click the **ADD LOAD BALANCING RULE** button.

Once the load balancer rule has been created, you can navigate to load balancer and add (or remove) Instances to this rule. To do this, follow these steps:

1. Click the **Load Balancer Rule** icon.

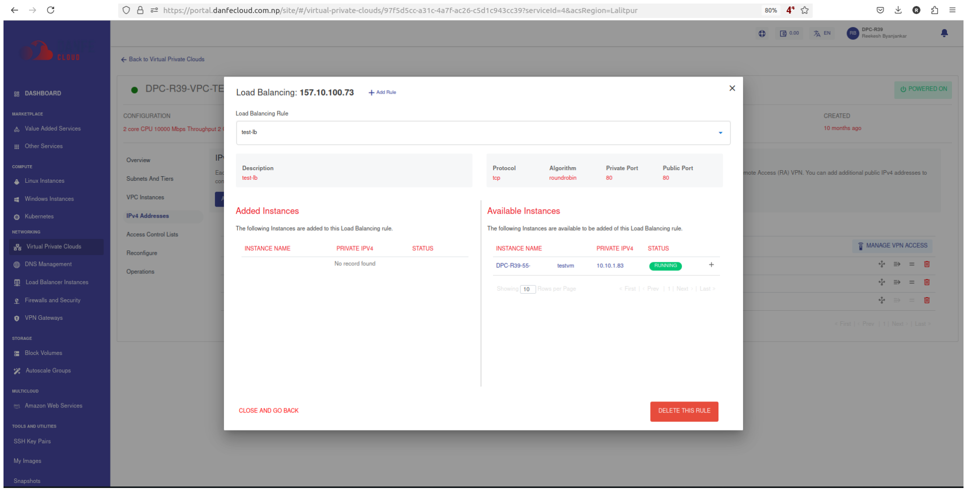


Load Balancing: **157.10.100.73**

Load Balancing Rule: Choose One

Select a rule above to view details and manage load balancing.

2. Select the **Load Balancing Rule**.
3. The following window appears:



Load Balancing: **157.10.100.73** + Add Rule

Load Balancing Rule: test-lb

Description
test-lb

Protocol	Algorithm	Private Port	Public Port
tcp	roundrobin	80	80

Added Instances

The following Instances are added to this Load Balancing rule.

INSTANCE NAME	PRIVATE IPV4	STATUS
No record found		

Available Instances

The following Instances are available to be added of this Load Balancing rule.

INSTANCE NAME		PRIVATE IPV4	STATUS	
DPC-R39-55-	testvm	10.10.1.83	RUNNING	+

4. This window shows Instances that are part of this load balancer, and those available to be added.
5. Click the **+** icon to add an instance and the **X** icon to remove an instance.

*note: To delete this Load Balancing Rule, click **DELETE THIS RULE**.*

To verify the load balancer configuration, log into each virtual machine behind it, create an **index.html** file with different content on each, and access the public IP address from your browser. If configured correctly, each browser page refresh should take turns in loading the two index.html pages.

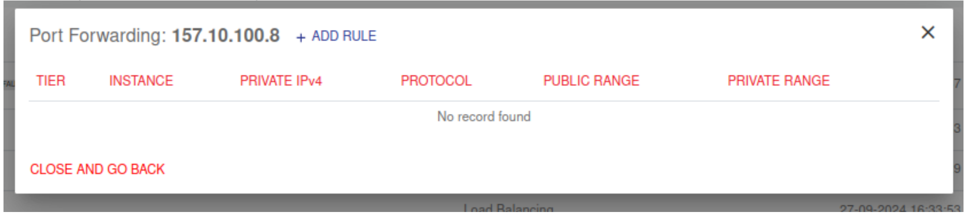
*note: A load balancer IP rule can only be configured if the tier/subnet type is set to **Public IP**.*

Configuring Port Forwarding

A Port Forwarding rule is required for accessing the virtual machines contained in a VPC. Since virtual machines in a VPC only have a private IP address, a public IP address is required for each virtual machine that you want to access from your terminal.

To configure port forwarding, follow these steps:

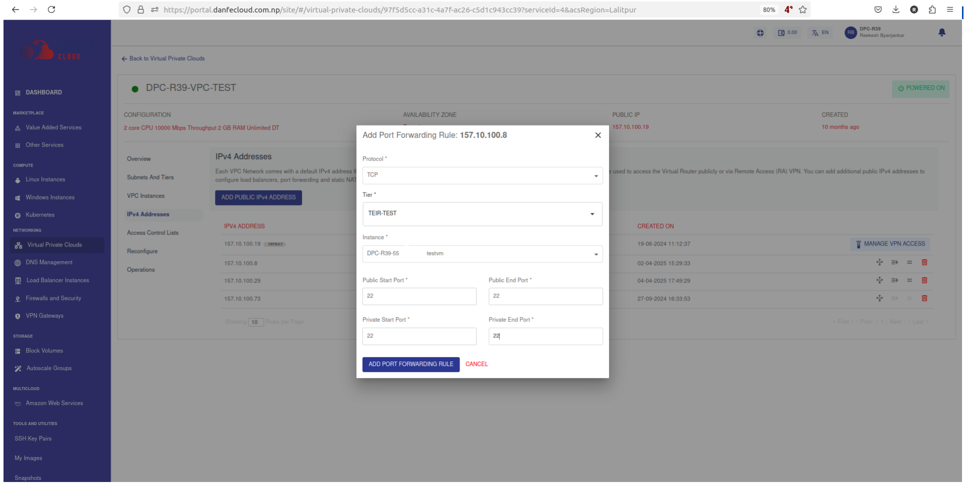
1. To configure Port Forwarding Rule, click the icon.



Port Forwarding: **157.10.100.8** + ADD RULE

TIER	INSTANCE	PRIVATE IPv4	PROTOCOL	PUBLIC RANGE	PRIVATE RANGE
No record found					

2. The following window appears:
3. Click **ADD RULE**. The following window appears:



Add Port Forwarding Rule: **157.10.100.8**

Protocol *: TCP

Tier *: TEIR-TEST

Instance *: DPC-R39-55 testvm

Public Start Port *: 22

Public End Port *: 22

Private Start Port *: 22

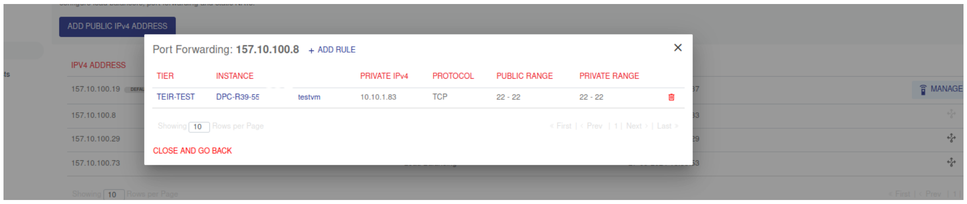
Private End Port *: 22

4. Specify the following details in the window:
    - **Protocol** for port-forwarding.
    - The **tier** and the Instance to port-forward to.
    - Set the**Public** and **private port** range.
5. Click **ADD PORT FORWARDING RULE**.

    - *note: The end ports should be equal to or greater than the start ports.*

Once the Port-Forwarding rule is created, you can view its details by following these steps:

1. Click the **Port Forwarding Rule** icon.



Port Forwarding: **157.10.100.8**

TIER	INSTANCE		PRIVATE IPv4	PROTOCOL	PUBLIC RANGE	PRIVATE RANGE
TEIR-TEST	DPC-R39-55	testvm	10.10.1.83	TCP	22 - 22	22 - 22

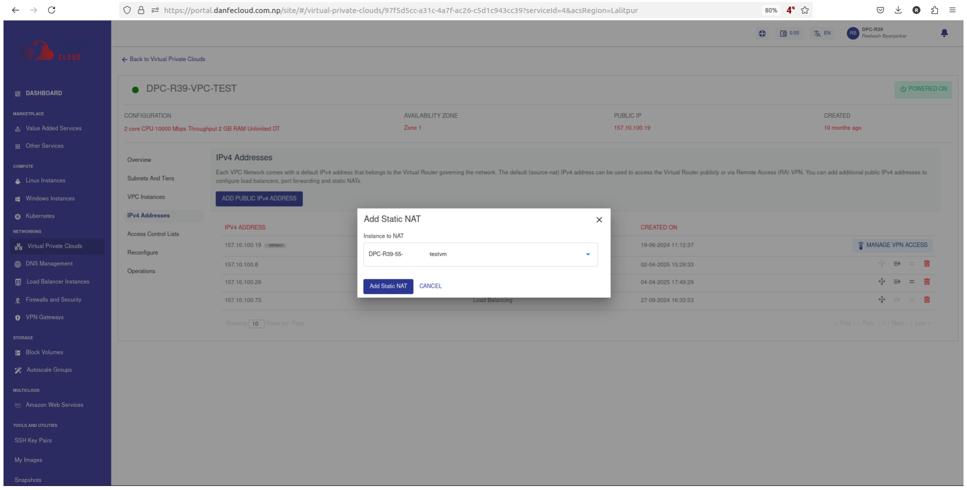
2. The following window appears:
3. In this window, you can view the Instance where this rule is configured, along with the private and public port range mappings.

To test if port-forwarding is configured correctly, use the public IP to SSH into the virtual machine the IP forwards to.

note: A Port-Forwarding IP address can be used to configure multiple Port-Forwarding access rules but with one virtual machine. To port-forward into a different virtual machine, you'll need to purchase an additional public IP address.

Configuring Static NAT

1. To use the public IP as a static translation, click the icon.
2. The following window appears:



Add Static NAT

Instance to NAT: DPC-R39-55- -testvm

3. Select the Instance you want to assign the public IP to, then click **Add Static NAT**.

To test whether static NAT has been configured correctly, you can use the public IP to SSH into the virtual machine that the IP is NAT-ing to.

7. Managing Access Control on VPC Subnets

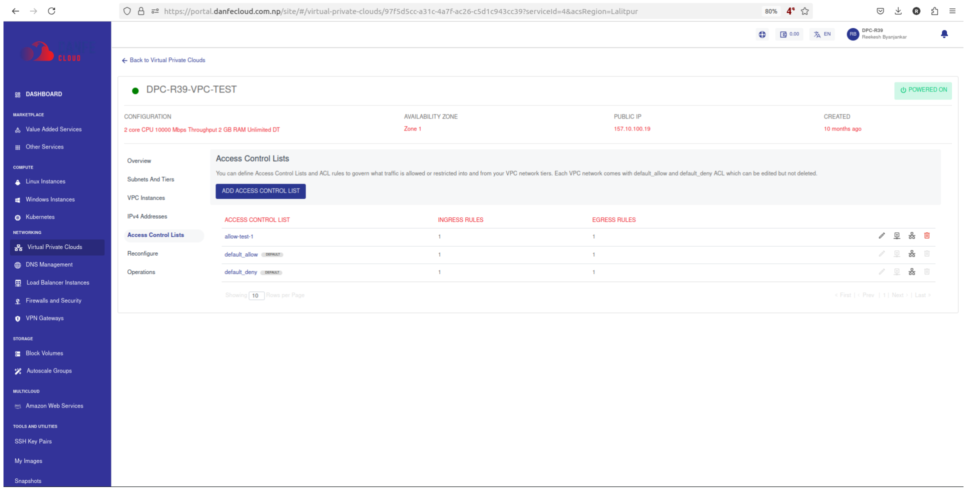
Access control policies can be created using Access Control Lists (ACL) and configuring rules within these ACL (called ACL Rules). An ACL can then be applied to any tier within the VPC. These policies govern what traffic is allowed or restricted into and from your VPC network tiers.

note

Each VPC comes with **default_allow** and **default_deny** ACL, which can be edited but not deleted.

To access the ACL navigate to **VPC details** and select the **Access Control Lists** tab. You can perform the following actions on any available ACL:

- Edit the ACL name
- Add an ACL rule
- Assign the ACL to a tier
- Delete the ACL



DPC-R39-VPC-TEST

CONFIGURATION	AVAILABILITY ZONE	PUBLIC IP	CREATED
2 core CPU 10000 Mbps Throughput 2 GB RAM Unlimited DT	Zone 1	157.10.100.19	10 months ago

Access Control Lists

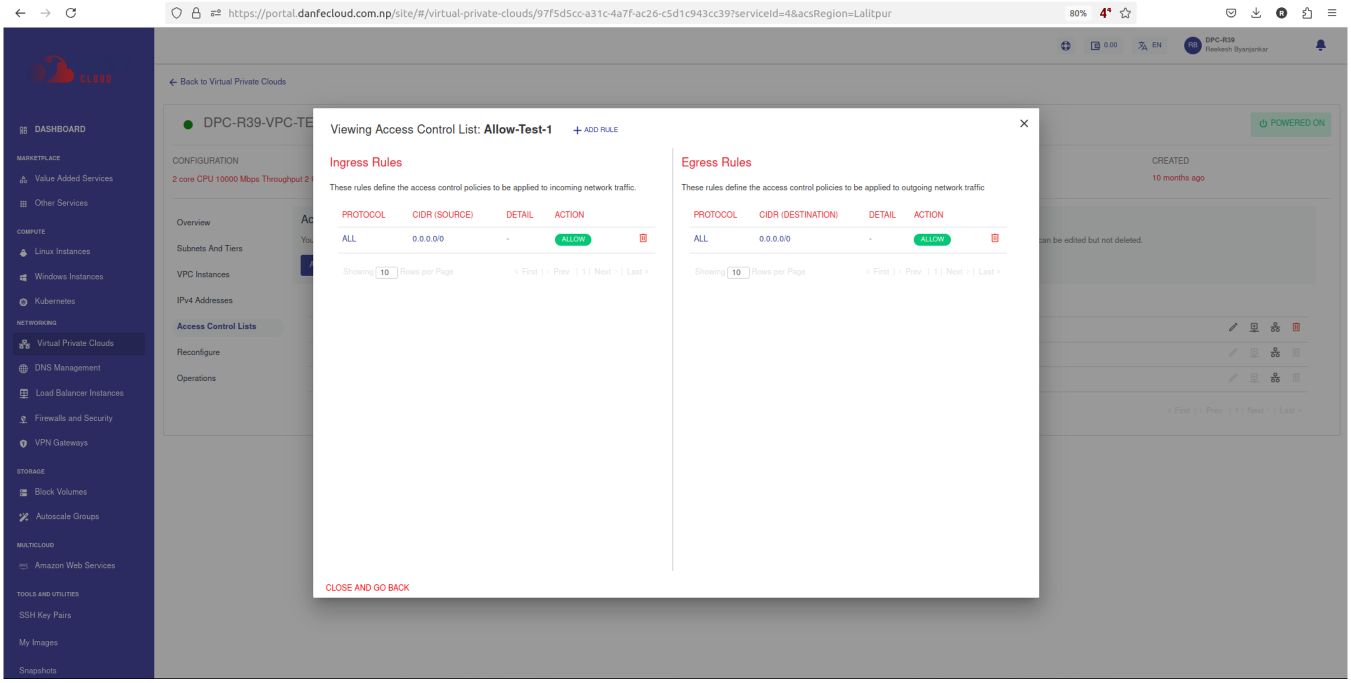
You can define Access Control Lists and ACL rules to govern what traffic is allowed or restricted into and from your VPC network tiers. Each VPC network comes with default_allow and default_deny ACL which can be edited but not deleted.

ACCESS CONTROL LIST	INGRESS RULES	EGRESS RULES
allow-test-1	1	1
default_allow DEFAULT	1	1
default_deny DEFAULT	1	1

Creating Custom ACL and Adding Rules

You can create a custom ACL by clicking the **ADD ACCESS CONTROL LIST** button and assigning a name to the ACL. An ACL is a collection of individual traffic control rules that must be configured after the ACL is created.

Any available ACL (existing or new) can be viewed in detail by clicking its name in the list. This displays a list of rules that govern ingress (incoming) and egress (outgoing) traffic for the subnet. From this section, you can create new rules or delete existing ones.



Viewing Access Control List: **Allow-Test-1**

Ingress Rules

These rules define the access control policies to be applied to incoming network traffic.

PROTOCOL	CIDR (SOURCE)	DETAIL	ACTION
ALL	0.0.0.0/0	-	ALLOW

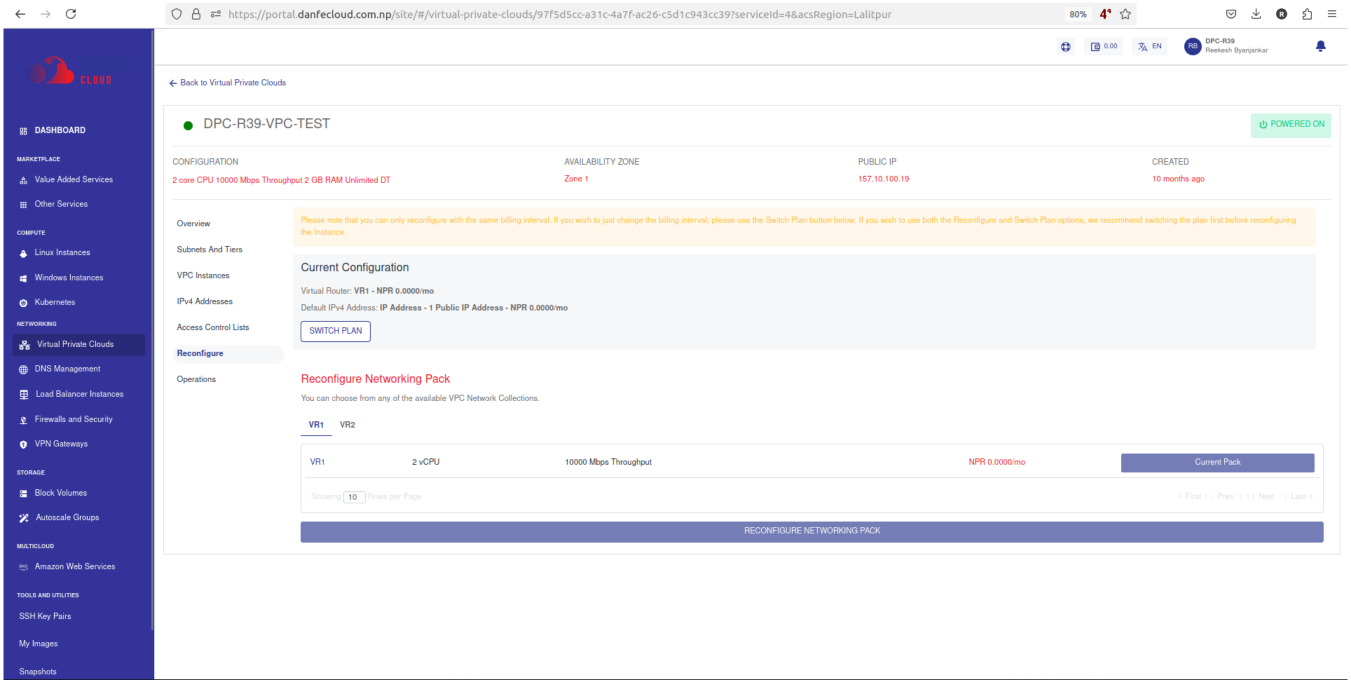
Egress Rules

These rules define the access control policies to be applied to outgoing network traffic

PROTOCOL	CIDR (DESTINATION)	DETAIL	ACTION
ALL	0.0.0.0/0	-	ALLOW

8. Reconfiguring a VPC

The Reconfigure section/tab lists your current subscription details and allows you to reconfigure the networking pack or switch between **hourly** and **monthly** pricing.



DPC-R39-VPC-TEST

CONFIGURATION	AVAILABILITY ZONE	PUBLIC IP	CREATED
2 core CPU 10000 Mbps Throughput 2 GB RAM Unlimited DT	Zone 1	157.10.100.19	10 months ago

Please note that you can only reconfigure with the same billing interval. If you wish to just change the billing interval, please use the Switch Plan button below. If you wish to use both the Reconfigure and Switch Plan options, we recommend switching the plan first before reconfiguring the Instance.

Current Configuration

Virtual Router: **VR1 - NPR 0.0000/mo**

Default IPv4 Address: **IP Address - 1 Public IP Address - NPR 0.0000/mo**

Reconfigure Networking Pack

You can choose from any of the available VPC Network Collections.

VR1	2 vCPU	10000 Mbps Throughput	NPR 0.0000/mo	Current Pack

note: You can only reconfigure with the same billing interval. To change the billing interval, use the Switch Plan button. We recommend switching the plan first before reconfiguring the instance if you wish to use both the Reconfigure and Switch Plan options. In either case, you will be charged based on the reconfiguration, not the existing plan.

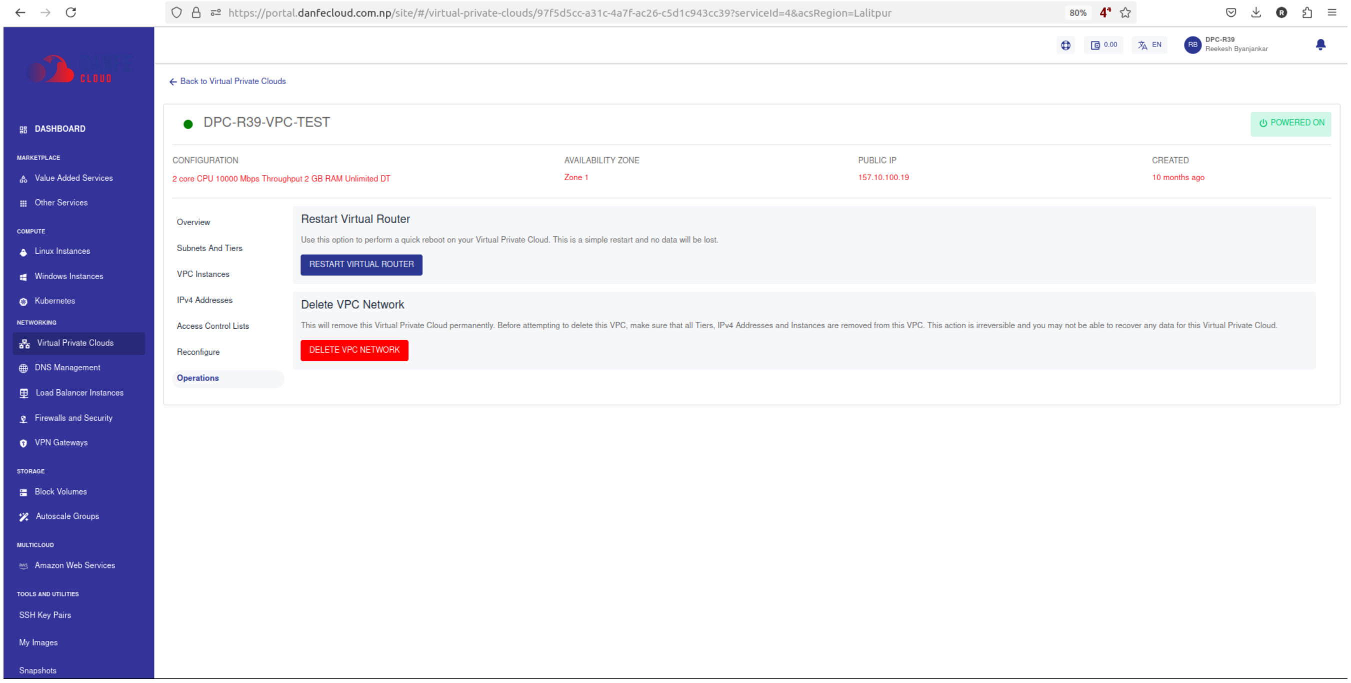
9. VPC Management and Basic Operations

VPC management offers the following operations. These are basic VPC management actions and don't have any impact on the actual network configurations.

Powering ON/OFF the Virtual Router

Switching the VPC power state is possible using the **power status** button on top. This is usually **green** if the VPC is powered ON, and greyed out if powered OFF.

To restart the VPC, navigate to the **Operations** tab and click the **RESTART VIRTUAL ROUTER** option. This performs quick reboot and no data is lost.



https://portal.danfecloud.com.np/site/#/virtual-private-clouds/97f5d5cc-a31c-4a7f-ac26-c5d1c943cc39?serviceId=4&acsRegion=Lalitpur

DPC-R39-VPC-TEST

CONFIGURATION	AVAILABILITY ZONE	PUBLIC IP	CREATED
2 core CPU 10000 Mbps Throughput 2 GB RAM Unlimited DT	Zone 1	157.10.100.19	10 months ago

Restart Virtual Router

Use this option to perform a quick reboot on your Virtual Private Cloud. This is a simple restart and no data will be lost.

Delete VPC Network

This will remove this Virtual Private Cloud permanently. Before attempting to delete this VPC, make sure that all Tiers, IPv4 Addresses and Instances are removed from this VPC. This action is irreversible and you may not be able to recover any data for this Virtual Private Cloud.

Deleting a VPC

To delete a VPC, navigate to the **Operations** Section and click the **DELETE VPC NETWORK** button. Deleting a VPC removes it permanently.

note: Before attempting to delete this VPC, ensure that all Tiers, IPv4 Addresses, and Instances are removed from this VPC. This action is irreversible, and you may not be able to recover any data for this VPC.