zadara

Zadara Cloud Services - Networking User Guide

Release 24.03

Zadara

Feb 24, 2025

SYSTEM REQUIREMENTS

CHAPTER

ONE

NETWORKING PORTS USED BY ZADARA CLOUD SERVICES

Direction	Usage	Ports	Comments
External	Maestro	80/443	Call home data / support data, tunnel (internet)
	v2v	80/443	Pulling packages from Linux repositories (internet)
	NTP	123	Clock sync (int ernet/internal NTP)
Internal (between Zadara nodes)	API access	80/443	
	Docker	5000	Pull image requests between nodes
	Openstack API	1060, 10100-10105	
	VNC	6080	

CHAPTER

TWO

DISTRIBUTED VIRTUAL SWITCH (DVS)

2.1 DVS Introduction

Distributed Virtual Switch (DVS), is a zCompute networking model which provides layer 2, VLAN-based networking functionality for VMs running on zCompute.

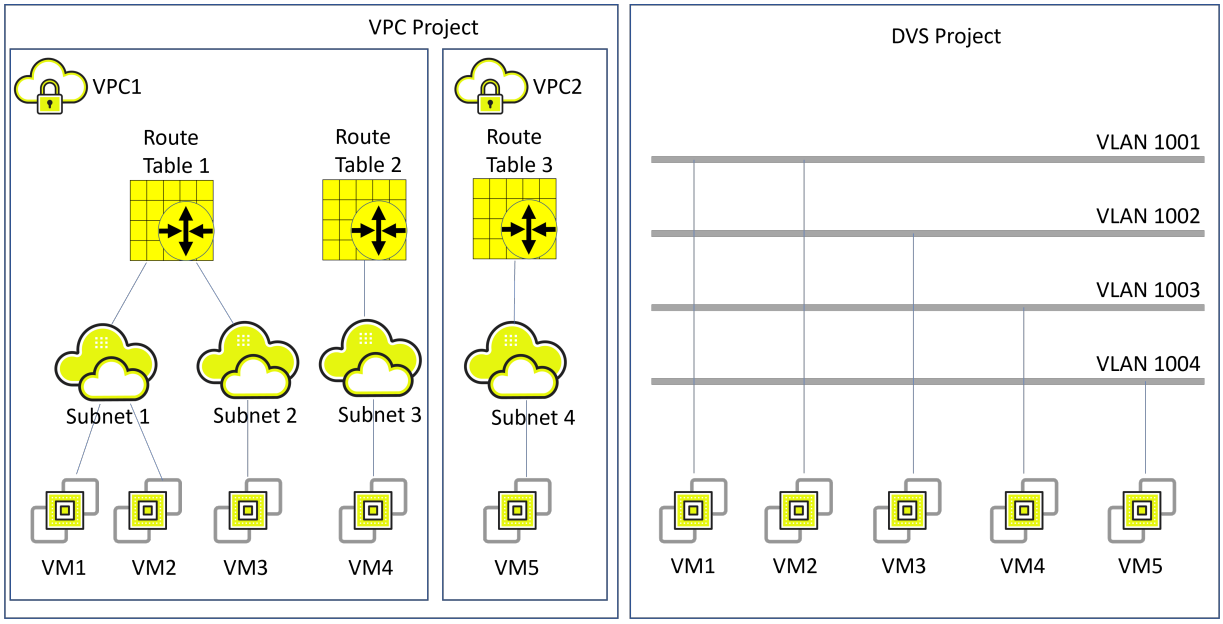
The idea behind DVS is to provide customers who are more familiar with legacy virtualization platforms (for example, VMware, Hyper-V, Nutanix, etc.) with a networking environment similar to the simplified networking model found in such legacy environments.

DVS provides simple OSI layer 2 VLAN-based switched networking functionality for VMs. DVS networks can be used to interconnect VMs attached to them, as well as for connecting these VMs with other network entities that reside in the hosting data center (servers, routers, storage devices, etc.).

The DVS model provides physical switching L2, VLAN-based connectivity, whereas VPC provides a rich IP networking platform (route-tables, subnets, security groups, Internet gateways, DNS, Elastic IPs, etc.) alongside other cloud-native services that are independent of physical switching configuration, such as auto-scaling groups, load-balancers, etc.

Zadara zCompute supports both VPC and DVS networking modes in coexistence: A single zCompute account (tenant), can have multiple VPC-based projects alongside DVS-based projects.

Comparison of VPC and DVS type projects:



✔ **Note:** A zCompute project can be either a VPC project or a DVS project.

2.2 DVS VLANs Management

(zCompute v23.08 and later)

To use DVS-mode networking, a cloud administrator first allocates VLANs or VLAN ranges for use on the zCompute cloud. The cloud administrator then assigns some of these VLANs to various accounts on that zCompute cloud.

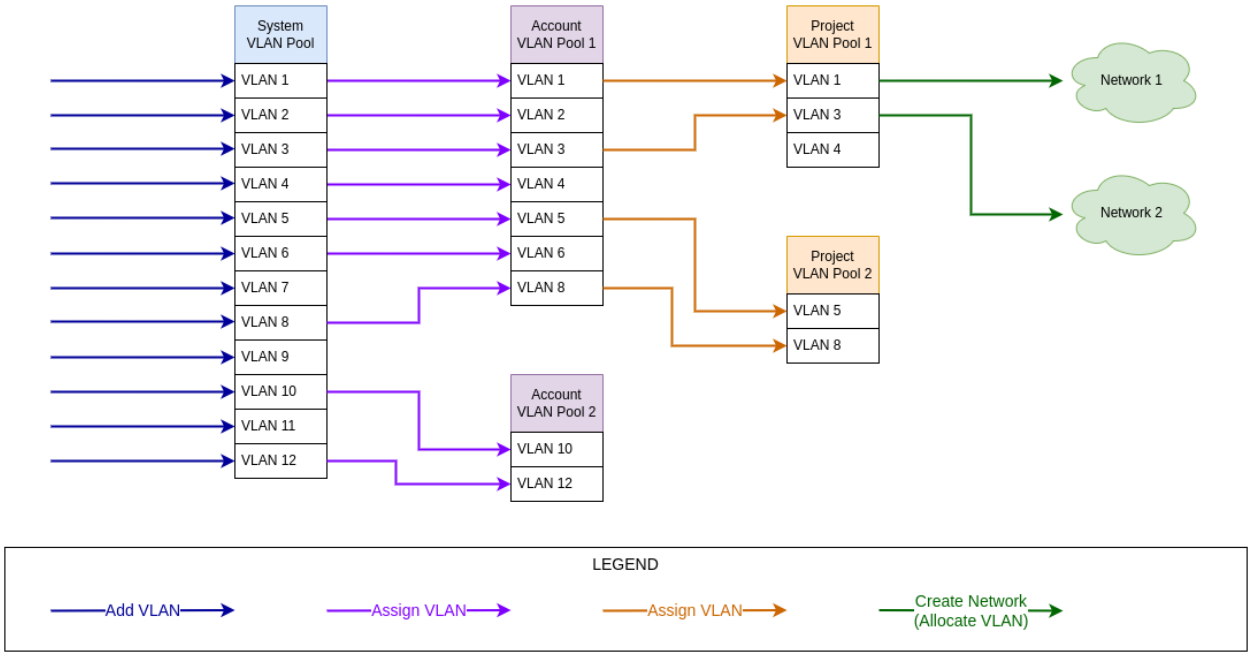
✔ **Note:** A VLAN can be assigned to one account, and cannot be shared between accounts.

An account administrator (or a cloud administrator on behalf of the account) creates one or more DVS projects in an account. The account administrator then assigns VLANs (assigned to the account by a cloud administrator) to the DVS projects on that account.

Once assigned to a project, member users can create DVS networks using these VLANs, and attach VMs to those DVS networks using the zCompute UI, the Symp CLI or APIs.

VLANs assignment is dynamic in the sense that VLANs can be assigned or released from projects, accounts or even the cloud, and re-assigned as needed, governed by the user's role and permissions.

2.2.1 VLAN creation and allocation flow



1. Zadara Operations creates the system VLAN pool, and adds or removes VLANs in the pool.
2. MSPs or Zadara Operations allocate VLANs from the system VLAN pool to an account's VLAN pool.

✔ **Note:**

- An account's VLAN pool is automatically created when the account is created.
- An account can have only one VLAN pool.
- When an account is deleted, its VLAN pool is automatically deleted.
- When an account's VLAN pool is deleted:
  - All of the account's projects' VLAN pools are automatically deleted.
  - All of the account's VLANs are automatically deleted.
- A VLAN in a project's VLAN pool that is released from an account's VLAN pool is first automatically released from the project's VLAN pool.

3. The account administrator (MSP or tenant) assigns VLANs from the account's VLAN pool to a project's VLAN pool.

✔ **Note:**

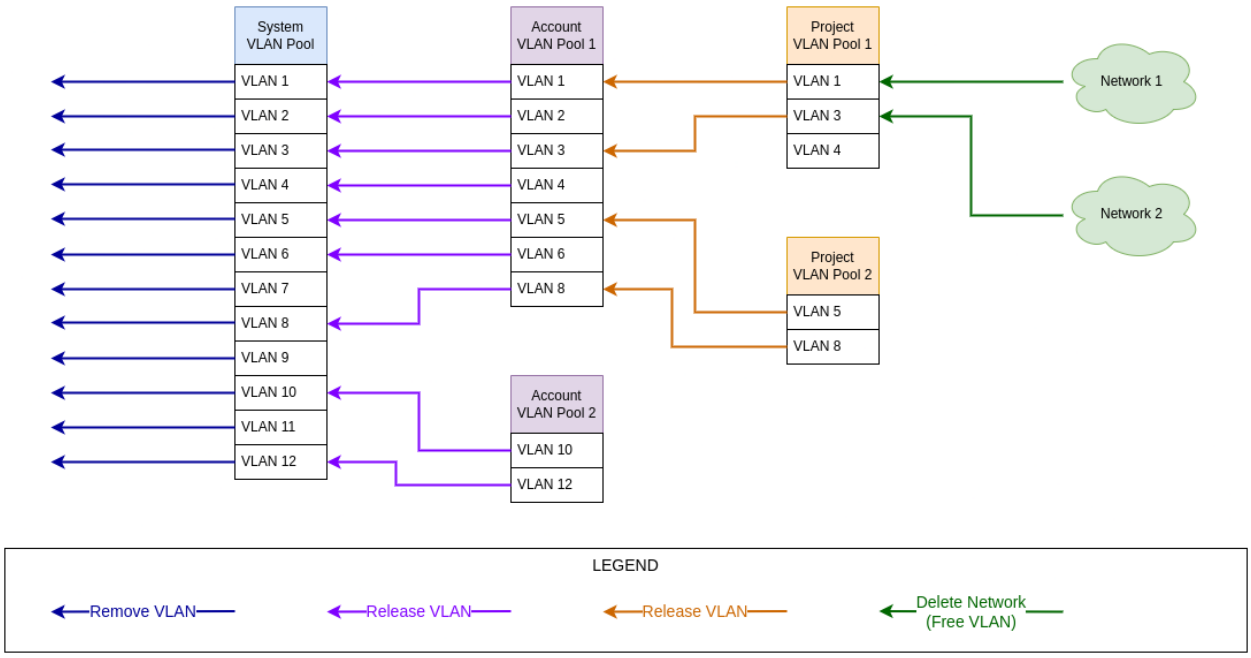
- A project's VLAN pool is automatically created when the project is created.
- A project can have only one VLAN pool.
- When a project's VLAN pool is deleted, all of its VLANs are automatically released.
- When a project is deleted, its VLAN pool is automatically deleted.

4. The account administrator can create a DVS network by allocating a VLAN to a DVS project, and associating a VM instance with the project's network.

✔ **Note:**

- A VLAN in a project's VLAN pool cannot be released if the VLAN is allocated to a network.

2.2.2 VLAN release and deletion flow



1. The account administrator (MSP or tenant) can release a VLAN that is allocated to a network, back to the project's VLAN pool, by deleting its network.
2. The account administrator can release VLANs that are not allocated to a network, from a project's VLAN pool back into the account's VLAN pool.

✔ **Note:**

- A VLAN in a project's VLAN pool cannot be released if the VLAN is allocated to a network.
- When a project's VLAN pool is deleted, all of its VLANs are automatically released.
- When a project is deleted, its VLAN pool is automatically deleted.

---

3. Zadara Operations can release VLANs that are not allocated to a network, from an account's VLAN pool back into the system VLAN pool.

✔ **Note:**

- When an account is deleted, its VLAN pool is automatically deleted.
- When an account's VLAN pool is deleted:
  - All of the account's projects' VLAN pools are automatically deleted.
  - All of the account's VLANs are automatically deleted.
- A VLAN in a project's VLAN pool that is released from an account's VLAN pool is first automatically released from the project's VLAN pool.

---

4. Zadara Operations can remove a VLAN from the system pool.

2.3 DVS - MSP account admin perspective

(zCompute v23.08 and later)

zCompute introduces some powerful VLANs management tools, that provide the ability for account admininstrators to centrally manage multiple VLANs at the zCompute cloud level, alongside the ability to assign multiple VLANs to accounts and delegate control to these accounts for managing these resources in a self-service fashion.

zCompute still allows MSP account administrators to create DVS networks for these accounts as they see fit, in the event that their managed services models and practices require it.

Such DVS VLANs can span beyond the zCompute cloud, into the MSP's physical network switches, over the Zadara switches' uplink trunks.

In order to use VLANs, the Zadara cloud's physical switches need to be configured. The creation and assignment of VLANs to the zCompute cloud requires opening a change-request ticket with Zadara Operations (via Zadara Support's email address: support@zadara.com).

Account administrators can can also release and reassign VLANs to other projects, accounts or even remove VLANs from the cloud.

Since initial configuration of VLANs requires Zadara operations intervention and coordination, it it highly recommended for MSPs to plan ahead and designate a range, or multiple ranges, of VLANs for the zCompute cloud, to make the physical switches a one-off, well-planned activity.

MSPs don't have to configure their upstream switches interfaces to use these VLANs immediately (though it's recommended), but can do so later at a time that suits them.

While MSP administrators can delegate VLAN management to accounts, it is not mandatory. They can still manage VLANs and DVS networks on behalf of other accounts.

2.4 Creating a DVS network (UI and CLI)

(zCompute v23.08 and later)

2.4.1 Prerequisites for creating a DVS network

- An existing DVS project on the tenant's account.
- An existing, unused VLAN defined in zCompute, assigned to the DVS project (implying that it's already assigned to the tenant account).

Creating a DVS project

Create a DVS project using either the zCompute UI or the CLI:

- **zCompute UI**
  1. In the zCompute UI, go to **Identity & Access > Accounts > <account>**.
  2. In the **Projects** tab, click **Create Project**. In the dialog that opens, enter:
     - **Project Name**.
     - **Project Description** (optional).
     - **Project Type**: Select **DVS**.

3. Click **OK**. The new project appears in the projects list, as a project of type **DVS**.

- **Symp CLI**

1. Create a DVS project using the `project create` command with a meaningful project name and description.

   For example:

```
project create --description 'My DVS project' mydvsproj

+-------------+----------------------------------+
| id          | 4d12575ce21c4982a29e6c10077e5af4 |
| name        | mydvsproj                        |
| description | My DVS project                   |
| domain_id   | msp                              |
| domain_name | cloud_msp                        |
| enabled     | true                             |
| is_domain   | false                            |
| is_vpc      | false                            |
| parent_id   | ops                              |
+-------------+----------------------------------+
```

   By default, the project will be `enabled` and will be of type legacy (`is_vpc=false`).

2. Use the `dvs project provision <project-id>` command to complete the DVS project creation.

   For example:

```
dvs project provision 4d12575ce21c4982a29e6c10077e5af4

+-------------------------+--------------------------------------+
| account_id              | b9e1928e69dc48baa504edadd5b72880     |
| created_at              | 2023-08-30T16:22:46Z                 |
| default_edge_network    | none                                 |
| default_edge_subnet     | none                                 |
| default_edgenet_ip_pool | none                                 |
| flowlogs_enabled        | false                                |
| project_id              | 4d12575ce21c4982a29e6c10077e5af4     |
| project_type            | dvs_project                          |
| project_vlan_pool_id    | cc79d8db-da11-46f5-ab4e-2dbfbf91ee72 |
| updated_at              | 2023-08-30T16:22:46Z                 |
| user_id                 | 976f7c47a73244c98505703bfa4c7ace     |
+-------------------------+--------------------------------------+
```

   The project type is set to DVS (`project_type=dvs_project`).

3. The `project list` command, filtered with a search for the project name (or part of it) returns the project attributes, similar to the `project create` command above.

   For example:

```
project list -m grep-i=mydvs
```

Checking available VLANs

- **zCompute UI**

  1. In the zCompute UI, go to **Account Networking > VLANs Management**.

     The account's VLANs are listed.

  2. Check for an available VLAN that is not assigned to a project.

     (A VLAN that does not have a value in the **Project** column.)

- **Symp CLI**

  1. List the VLANs assigned to the account using `vlan-pool vlan list`.

     For example:

```
vlan-pool vlan list -c id -c guest_network_pool_id -c project_vlan_pool_id -c vlan_tag_id

+--------------------------------------+--------------------------------------+----------------
↪----------------------+-------------+
| id                                   | guest_network_pool_id                | project_vlan_
↪pool_id                 | vlan_tag_id |
+======================================+======================================+================================
| 1c654186-8d7f-4bcb-bf71-d7bd61fad225 | f8022add-81b5-42d6-be2c-05d0d082a5b1 | none          
↪                      | 1015        |
| 26813030-5572-4fae-8cc8-43d3173124b6 | f8022add-81b5-42d6-be2c-05d0d082a5b1 | none          
↪                      | 1018        |
| 39b9d144-bbb0-405f-8877-50b85251496e | f8022add-81b5-42d6-be2c-05d0d082a5b1 | none          
↪                      | 1016        |
| fa32bc3f-886e-4b83-8d66-417192527aeb | f8022add-81b5-42d6-be2c-05d0d082a5b1 | 7ce52679-6b31-
↪4a6c-bf55-2bbc371831b0 | 1017        |
+--------------------------------------+--------------------------------------+----------------
↪----------------------+-------------+
```

  2. Locate the the `vlan_tag_id` to use for the DVS project. Confirm that it has not already been allocated to a project (`project_vlan_pool_id=none`).

Assigning a VLAN to an account and DVS project

✔ **Note:** Only MSP administrators and Zadara Operations team can assign a VLAN to an account.

Tenant administrators can assign a VLAN to a project.

- **zCompute UI**

  1. In the zCompute UI, go to **Account Networking > VLANs Management**.

     The account's VLANs are listed.

  2. Check for an available VLAN that is not assigned to a project.

     (A VLAN that does not have a value in the **Project** column.)

  3. If there is an available VLAN, click its row to select it.

     1. From the menu bar, click **Assign**.

2. In the **Assign VLANs** dialog, select the DVS project in the

   Project dropdown.

3. Click **Ok**.

4. If there aren't any available VLANs, and it's necessary to add a new

   available VLAN (or VLAN range) to the account (MSP or Zadara Operations team):

   1. Click **+** to add VLANs.
   2. In the **Add VLANs** dialog, enter:
      - **Node network**: Select the network from the dropdown.
      - **Account**: Select the account from the dropdown.
      - **Project**: Select the DVS project from the dropdown.
      - **VLAN Range**:

        For a single VLAN, enter the VLAN number in both **From** and **To**.

        For a range of consecutive VLAN numbers, enter the range in **Start** and **To**.

        For an additional range, click **Add**, and enter the range.

      - Click **Ok**.

- **Symp CLI**

  1. If necessary, add a new available VLAN to the account. Specify the `guest_network_pool_id` returned from the `vlan-pool vlan list` command above.

     For example:

```
vlan-pool vlan add '[{"vlan": "1020", "guest_network_pool_id": "f8022add-81b5-42d6-be2c-
↪05d0d082a5b1"}]'

-----+-------------------------------------------------------------------------------------------
↪-----------------------------------------------------
value|id                                  |name|account_vl|created_at|guest_netw              ▯
↪           |network_id|project_vl|updated_at|vlan_tag_i
     |                                    |    |an_pool_id|          |ork_pool_i              ▯
↪           |          |an_pool_id|          |d
     |                                    |    |          |          |d                       ▯
↪           |          |          |          |
    ▯
↪|====================================+====+==========+==========+==================================+=========
     |9214c238-15f0-497b-b6c0-fedaa084b4ec|none|none      |2023-08-30|f8022add-81b5-42d6-be2c-
↪05d0d082a5b1|none      |none      |2023-08-30|1020
     |                                    |    |          |T16:23:26Z|                        ▯
↪           |          |          |T16:23:26Z|
-----+-------------------------------------------------------------------------------------------
↪-----------------------------------------------------
```

  2. Assign a VLAN to the account (MSP or Zadara Operations team) and to the DVS project, using:

     - The VLAN's `id` returned from the `vlan-pool vlan add` command or from the `vlan-pool vlan list` command.
     - The `account_vlan_pool_id` and `project_vlan_pool_id` returned from the `vlan-pool vlan list` command above.

1. Assign a VLAN to an **account** (MSP or Zadara Operations team):

   `vlan-pool account-pool assign-vlans <account_vlan_pool_id> <vlan id>`

   For example:

```
vlan-pool account-pool assign-vlans 6fe0b862-c13e-4d85-97a0-d81673814f88 9214c238-15f0-
↪497b-b6c0-fedaa084b4ec

+-------+---------+
| value | Success |
+-------+---------+
```

2. Assign a VLAN to a **project**:

   `vlan-pool project-pool assign-vlans <project_vlan_pool_id> <vlan id>`

   For example:

```
vlan-pool project-pool assign-vlans 7ce52679-6b31-4a6c-bf55-2bbc371831b0 9214c238-15f0-
↪497b-b6c0-fedaa084b4ec

+-------+---------+
| value | Success |
+-------+---------+
```

2.4.2 Creating a DVS network

- **zCompute UI**

  1. In the zCompute UI, go to **DVS Networking > Networks**.

     The account's DVS networks are listed.

  2. Click **+** to add a new DVS network and associate it with a DVS project and VLAN.

     In the **Create DVS Network** dialog, enter:

     1. **Name**: A meaningful name for the DVS network.
     2. **Description**: Enter a description (optional).
     3. **MTU**: Maximum Transmission Unit.
     4. **Project**: Select the DVS project from the dropdown.
     5. **VLAN**: Select a VLAN from the dropdown. If there is only one VLAN configured for the DVS project, it automatically appears in the dropdown as the only valid value.
     6. Click **Finish**.

- **Symp CLI**

  1. Create the DVS network for the selected VLAN ID using `dvs network create`.

     For example:

```
dvs network create --project-id 4fcd1cf44ad14704ae0f7f2c9722152b  --name 'vlan1020-net' --
↪description 'VLAN 1020 DVS network' --mtu 8950 1c654186-8d7f-4bcb-bf71-d7bd61fad225

+-----------------+--------------------------------------+
| id              | 19b2225b-98fd-482f-8666-dc7e68588095 |
```

(continues on next page)

(continued from previous page)

```
| name            | vlan1020-net                           |
| state           | pending                                |
| account_id      | 4fcd1cf44ad14704ae0f7f2c9722152b       |
| created_at      | 2023-08-30T16:25:25Z                   |
| description     | VLAN 1020 DVS network                  |
| dhcp_options_id | 2e00be4a-3cf9-4aca-a3ec-15c85dfafe3c   |
| is_default      | false                                  |
| mtu             | 8950                                   |
| network_type    | dvs_network                            |
| project_id      | 4fcd1cf44ad14704ae0f7f2c9722152b       |
| subnet_infos    | []                                     |
| tags            | []                                     |
| updated_at      | 2023-08-30T16:25:25Z                   |
| vlan            | 1020                                   |
| vlan_uuid       | 1c654186-8d7f-4bcb-bf71-d7bd61fad225   |
| vn_group_id     | b4ca2ba9-5a7d-41ff-8bcd-60c0716adf32   |
+-----------------+----------------------------------------+
```

2.5 DVS project and VLAN management operations

✔ **Note:** MSPs, Zadara Operations and account administrators (tenant administrators) each fulfill their own roles in VLAN management, depending on the phases in an account's, project's and VLAN's lifecycle.

2.5.1 Project operations

Refer to Projects in the zCompute Identity and Access guide for details on the following project actions:

- Creating a project
- Enabling or disabling a project
- Renaming a project
- Deleting a project
- Assigning a user to a project

2.5.2 VLAN operations

Refer to the Creating a DVS network (UI and CLI) section above, for details on the following DVS project and network operations:

- Viewing available VLANs
- Assigning (allocating) a VLAN to an account and to a DVS project
- Creating a DVS network

Modify DVS network

✔ **Note:** To change a DVS network's **Project** or **VLAN assignments**, first delete the DVS network, and then create a new one.

To apply changes to an existing DVS network's **Name**, **Description** or **MTU** configurations:

1. In the zCompute UI, go to **DVS Networking > Networks**. The list of DVS networks is displayed.
2. Select the DVS network to modify.
3. In the top toolbar, click **Modify**.
4. In the **Modify DVS Network** dialog, update the values of:
   - **Name**
   - **Description**
   - **MTU**
5. Click **Finish**.

Set default DVS network

Multiple DVS networks can be configured for the same project.

To configure a DVS network as the default DVS network for the project:

1. In the zCompute UI, go to **DVS Networking > Networks**.

   The list of DVS networks is displayed.
2. Select the DVS network to set as the project's default DVS network.
3. In the top toolbar, click **Set Default**.
4. In the **Set Default Network** confirmation dialog, click **Set Default**.

   In the DVS networks list, the selected network's **Default** icon is marked.

Releasing (freeing) a VLAN

A VLAN can be assigned to only one account, and to one project in that account, and to only one DVS network in that project.

To assign a VLAN to a different DVS network, the DVS network to which it is assigned must first be deleted, to permit creation of a new network with the VLAN assigned to it.

To assign a VLAN to a different project in the same account, the VLAN must be first released from its associated DVS network, by deleting the DVS network. Then, it must be released from its current project, to permit assignment to another project.

To assign a VLAN to a project in a different account, the VLAN must be first released from its associated DVS network and current project. Then, the **MSPs or Zadara Operations** team can remove the VLAN from its current project, and finally from its current account.

- **Releasing (freeing) a VLAN (deleting a DVS network)**
  1. In the zCompute UI, go to **DVS Networking > Networks**. The list of DVS networks is displayed.

2. Select the DVS network to delete.
3. In the top toolbar, click **Delete**.
4. In the **Delete DVS Network** confirmation dialog, click **Delete**.

- **Releasing a VLAN from a project**
  1. In the zCompute UI, go to **Account Networking > VLANs Management**. The list of VLANs is displayed.
  2. Select the VLAN to release from the project.
  3. In the top toolbar, click **Release From Project**.
  4. In the **Release VLAN from Project** confirmation dialog, click **OK**.
- **Releasing a VLAN from an account (MSPs and Zadara Operations only)**
  1. In the zCompute UI, go to **Account Networking > VLANs Management**. The list of VLANs is displayed.
  2. Select the VLAN to release from the project.
  3. (Optional) In the top toolbar, click **Release From Project**.

     In the **Release VLAN from Project** confirmation dialog, click **OK**.
  4. In the top toolbar, click **Remove**.

2.6 Migrating a VM to a DVS project

VMware VMs that are migrated to zCompute using the V2Z utility in the Migrating VMware VMs to zCompute process result in VMs in a rich VPC networking type project rather than in the simpler DVS networking alternative.

This section details the requirements and procedure to migrate a VM instance from a VPC type project to a DVS type project. The same procedure is applicable to any VPC VM, irrespective of whether they are VMs that were migrated from VMware, or VMs created from scratch in VPC projects.

2.6.1 Prerequisites

- DVS project
- DVS network

See:

- Prerequisites for creating a DVS network
- Creating a DVS project
- Creating a DVS network

2.6.2 VPC to DVS VM migration

1. Make sure that the VM is shut down.

   In **Compute > Instances**, locate the VM in the list of instances.

   If the **Status** display is not **Shutoff**:

   1. Select the instance, and on either the right-click menu or the top menu bar, select **Stop**.
   2. Wait for the **Status** display to change to **Shutoff**.

2. In **Compute > Instances** select the VM, and on either the right-click menu select **Create Image** or the top menu bar, select **More > Create Image**.

   In the **Create Image from <source image>** dialog, enter a **Name** that identifies the new DVS type image.

   The **Operating System** is derived from the source image, and cannot be modified.

   Optional: Enter a **Description**, **Tags**, and select whether new VM instances of this image must **Reboot** (recommended to avoid corruption).

   Click **Ok**.

3. To deploy the new VM image to a DVS project:

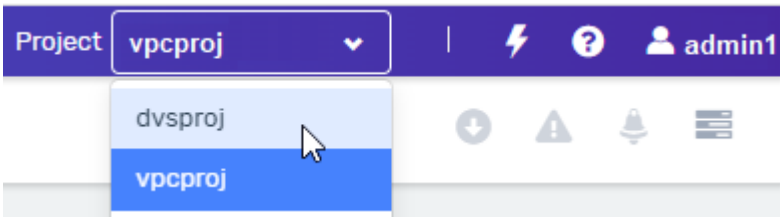
   1. In **Machine Images > Images** wait intil the new image's **Status** displays **Ready**.
   2. To enable creating instances of the image in a DVS project, modify the image's scope so that it is available to all projects in the account:

      Select the image, and on either the right-click menu or the top menu bar, select **Modify**.

      In the **Modify Image** dialog, make sure that **Scope** is set to **Account**.

      Click **Ok**.

   3. If permitted, in the **Project** dropdown at the top right, select the DVS target project for the VM instance, or log out and sign on as a user in the DVS target project.

   4. In **Machine Images > Images** select the image, and on either the right-click menu or the top menu bar, select **Launch**.
   5. In the **Create Instance** dialog:

      In the **Compute** tab:

      1. Enter a **Name** that identifies the new DVS VM instance, and Select the **Instance Type** from the dropdown.
      2. Optionally, apply **Tags** and enable or disable any of the other options.
      3. Click **Next**.

      In the **Storage** tab:

      1. Select the **Boot Volume**'s **Volume Type** from the dropdown.
      2. Optionally, **Add**, create and allocate data volumes.

3. Click **Next**.

In the **Networking** tab:

1. Select a DVS network from the **Network** dropdown.
2. Optionally, **Add**, create and assign additional networks.
3. Click **Finish**.

6. In **Compute > Instances** the new DVS instance's status initially displays **Spawning** while it powers up.

   Wait until the status displays **Active** before connecting to it.

CHAPTER

THREE

VPC

3.1 VPC Introduction

The Virtual Private Cloud (VPC) is a networking resource with a logical router at its core. Within Zadara Cloud Services, it was designed to provide a user experience that is identical to the AWS VPC. The virtual private cloud provides a routed L3 environment into which the user can deploy instances and managed services.

When you create a VPC you specify a CIDR block. All subnets that you will create in the VPC will be carved out from this CIDR block (without overlap). The router will ensure IP connectivity between all these subnets.

You can create a VPC with the UI either using a wizard which helps select the required networking depending on the VPC type, or with a basic **Create** command. The following VPC types are supported:

- **VPC with Single Private Subnet** - the VPC runs in an isolated section of the cloud, without access to the Internet.
- **VPC with Single Public Subnet** - the VPC runs in an isolated section of the cloud with direct access to the Internet. Security groups can be used to control inbound and outbound network traffic.
- **VPC with Public and Private Subnets** - VM instances within the private subnet in the VPC can establish outbound connections to the Internet via the public subnet using Network Address Translation (NAT).

3.2 Default VPC

Every VPC-provisioned project has a Default VPC that is automatically created by Zadara Cloud Services.

1. The Default VPC has 172.31.0.0/16 set as its CIDR block.
2. It also contains a single subnet with 172.31.0.0/20 as its CIDR.
3. The VPC has an Internet Gateway that connects it to the external network that was selected by the project.
4. The route table of the subnet has a local route for the CIDR block of the VPC and a default route to the Internet gateway.
5. A default security group is created that allows inbound traffic from all the virtual interfaces to which it is applied and allows outbound traffic to any destination.
6. A DHCP-options set is also defined with the the domain-name option set to DHCP local.
7. In a regular VPC subnet, the subnet's IP gateway is always the first valid IP address in the subnet CIDR. For example, 172.31.0.1 is the IP gateway of the default subnet in the Default VPC.
8. In a VPC direct subnet, the subnet's external IP gateway must be provided by the user, and is excluded from the subnet's allocation pool.

   The VPC internal router IP is the subnet gateway which attaches it to the VPC route table. This IP address must also be provided by the user, and is also excluded from the subnet's allocation pool.

The standard setup is to set the VPC internal router IP to the first IP address in the subnet CIDR, for example, 10.10.10.1. The subnet's allocation pool starts with the second IP address, for example, 10.10.10.2.

9. DHCP server addresses are always allocated as the two lowest IP addresses in the subnet's allocation pool, excluding the subnet's IP gateway. For example, 172.31.0.1 is the IP gateway of the default subnet in the Default VPC, and 172.31.0.2 and 172.31.0.3 are the DHCP server addresses.

3.3 How VPC passes DNS Servers via DHCP

When VPC DNS is **enabled**, the VPC DHCP service provides VMs with a pair of internal IPs as DNS servers. The VPC DNS service will look up any local zone records internally, and it will forward queries to the DNS servers provided in the DHCP Option Set for all external domains.

When VPC DNS is **disabled**, the VPC DHCP service provides VMs with the exact IPs of the DNS servers configured in the DHCP Option Set. In this case, DNS requests will go directly from VMs to the external DNS nameservers.

3.4 Creating a VPC

- Creating a VPC with the UI Wizard: A simplified lead-through that creates a VPC and all the resources that the VPC needs, as a ready-to-use network.
- Creating a VPC with the UI VPC Create option: An interface for advanced users to create a VPC.

See the video demonstrating the basics of creating and configuring zCompute VPCs:

zCompute provides two options in the UI for creating a VPC:

3.4.1 Creating a VPC with the UI Wizard

To create a VPC using the wizard:

1. Navigate to the **Networking > VPC** view.
2. From the top toolbar, click **Wizard**.
3. In the **VPC Wizard** dialog's **Configuration** tab, select one of the following VPC types. Subsequent UI options will depend on this selection.
   - **VPC with Single Private Subnet**
   - **VPC with Single Public Subnet**
   - **VPC with Public and Private Subnets**
4. Click **Next**.
5. For **VPC with Single Private Subnet**, proceed as follows:
   1. In the **VPC** tab, enter the following:
      - **VPC Name**
      - **VPC Description**
      - **CIDR**
   2. Click **Next**.
   3. In the **Private Subnet** tab, enter the following:

- **Private Subnet Name**
- **Private Subnet Description**
- **CIDR** - This CIDR must be within the CIDR defined for VPC.

4. Click **Finish**.

6. For **VPC with Single Public Subnet**, proceed as follows:
    1. In the **VPC** tab, enter the following:
        - **VPC Name**
        - **VPC Description**
        - **CIDR**
        - **Internet Gateway Name**
    2. Click **Next**.
    3. In the **Public Subnet** tab, enter the following:
        - **Public Subnet Name**
        - **Public Subnet Description**
        - **CIDR** - This CIDR must be within the CIDR defined for VPC.
    4. Click **Finish**.
7. For **VPC with Public and Private Subnets**, proceed as follows:
    1. In the **VPC** tab, enter the following:
        - **VPC Name**
        - **VPC Description**
        - **CIDR**
        - **Internet Gateway Name**
    2. Click **Next**.
    3. In the **Private Subnet** tab, enter the following:
        - **Private Subnet Name**
        - **Private Subnet Description**
        - **CIDR** - This CIDR must be within the CIDR defined for VPC.
    4. Click **Next**.
    5. In the **Public Subnet** tab, enter the following:
        - **Public Subnet Name**
        - **Public Subnet Description**
        - **CIDR** - This CIDR must be within the CIDR defined for VPC, but different than that defined for private subnet.
    6. Click **Next**.
    7. In the **NAT Gateway** tab, enter the following:
        - **NAT Gateway Name**

- **NAT Gateway Description**
- **Elastic IP**

8. Click **Finish**.

3.4.2 Creating a VPC with the UI VPC Create option

To create a VPC using the UI VPC Create option:

1. Navigate to the **Networking > VPC** view.
2. From the top toolbar, click **Create**.
3. In the **Create VPC** dialog, enter the following:
   - **Name** - name of the VPC.
   - **Description** - description of the VPC.
   - **CIDR** - subnet associated with the VPC.
   - **Internet Gateway** - internet gateway associated with VPC.

   ✔ **Note:** An existing internet gateway will only be available from the pull-down list for association with a VPC if it is not already associated with another VPC. In this case, a new internet gateway should be defined by clicking **+**.

4. Other constructs such as additional subnets, NAT Gateway, or Elastic IP's can be associated with the VPC separately with the appropriate networking UI option.

3.5 VPC Operations

After creation of a VPC, it will be displayed in the vpc list in the **Networking > VPC** view. The following operations can be performed by selecting a VPC from the list, and clicking the appropriate icon.

3.5.1 Top Toolbar Operations

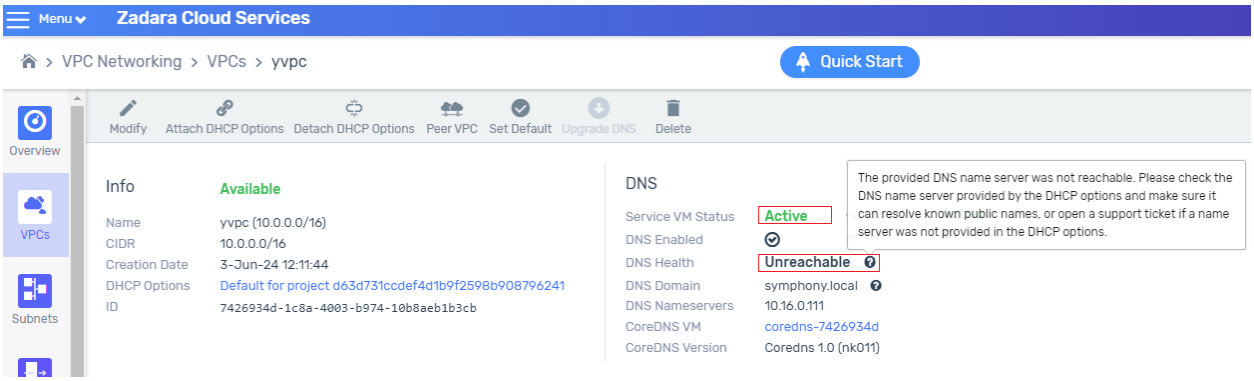
- **Modify** - the following settings can be updated:
  - **Name** - name of the VPC.
  - **Description** - description of the VPC.
  - **DNS enabled** - checkbox to enable or disable the DNS.
  - **Service VM Subnet** - dropdown list of available subnets, or the option to create and assign a new subnet.
- **Attach DHCP Options**
- **Detach DHCP Options**
- **Peer VPC** - Create a Peering Connection to the VPC.
- **Set Default** - set the VPC as the default for given project.
- **Upgrade DNS** - DNS is a system level service. When upgraded to a new version, all related VM instances must be restarted. This requires user confirmation using this option.
- **Delete** - delete the VPC and its configurations.

3.5.2 Lower Toolbar Operations

- **Events** - view configuration events (info) or alarms for the VPC.
- **Peers** - view peering information for the VPC.
- **Subnets** - view subnet information for the VPC.
- **Security Groups** - view security group information for the VPC.
- **Route Tables** - view route table information for the VPC.
- **Internet Gateways** - view internet gateway information for the VPC.
- **DNS Records** - view DNS information for the VPC.
- **VMs** - view VM instance information for the VPC.

3.6 View VPC DNS Status

When DNS is enabled, in the **VPC Networking > VPC >** <VPC name> view, the DNS VM Status and DNS Health information are displayed in the DNS section.



When the DNS service is degraded, a context-sensitive tooltip appears to the right of DNS Health.

Note: The DNS VM Status is checked once per minute returning the DNS Health, except during DNS service actions, when the DNS VM Status check is skipped.

The DNS VM Status can be one of the following:

DNS VM Status	DNS Health
Active	Possible values: • Healthy • No Resolution • Unreachable • Unknown • Error
Pending	Unknown
Processing	Unknown
Deleting	Unknown
Error	Error

When the DNS Health check detects a degraded service, it indicates the possible cause and resolution. The cause and resolution can be viewed in context, by clicking the tooltip icon to the right of DNS Health.

DNS Health	Description	Resolution / actions
Healthy	The DNS service is functioning successfully.	
No Resolution	The provided DNS was not able to resolve a test query.	Check the name server provided by the DHCP options and make sure it can resolve known public names, or open a support ticket if a name server was not provided in the DHCP options.
Unreachable	The provided DNS name server was not reachable.	Check the DNS name server provided by the DHCP options and make sure it can resolve known public names, or open a support ticket if a name server was not provided in the DHCP options.
Unknown	The DNS service state is unknown.	Probably the service is starting up. If the problem persists after 5 minutes, open a support ticket.
Error	An error has been detected.	Try to disable DNS in the VPC settings, save, wait for the changes to apply, and re-enable. If the problem persists after 5 minutes, open a support ticket.

CHAPTER

FOUR

AWS-VPC

The table below describes the AWS-VPC APIs which are supported for the VPC scope management operations.

AWS API Reference	Ignored Param	Optional Parameters
AcceptVpcPeeringConnection	[]	VpcPeeringConnectionId
AssignPrivateIpAddresses	[]	PrivateIpAddress
AssociateDhcpOptions	[]	[]
AssociateRouteTable	[]	[]
AttachInternetGateway	[]	[]
AttachNetworkInterface	[]	[]
AuthorizeSecurityGroupEgress	[]	IpPermissions
CreateDhcpOptions	[]	[]
CreateInternetGateway	[]	[]
CreateNatGateway	[]	[]
CreateNetworkInterface	[]	Description PrivateIpAddress PrivateIpAddresses SecondaryPrivateIp
CreateRoute	[]	GatewayId NatGatewayId NetworkInterfaceId InstanceId VpcPeering
CreateRouteTable	[]	[]
CreateSubnet	[]	AvailabilityZone
CreateVpc	[]	[]
CreateVpcPeeringConnection	[]	VpcId PeerVpcId
DeleteDhcpOptions	[]	[]
DeleteInternetGateway	[]	[]
DeleteNatGateway	[]	[]
DeleteNetworkInterface	[]	[]
DeleteRoute	[]	DestinationCidrBlock
DeleteRouteTable	[]	[]
DeleteSubnet	[]	[]
DeleteVpc	[]	[]
DeleteVpcPeeringConnection	[]	VpcPeeringConnectionId
DescribeDhcpOptions	[]	DhcpOptionsId
DescribeInternetGateways	[]	InternetGatewayId Filter
DescribeNatGateways	[]	NatGatewayId Filter
DescribeNetworkInterfaces	[]	NetworkInterfaceId Filter
DescribeRouteTables	[]	RouteTableId Filter
DescribeSubnets	[]	SubnetId Filter
DescribeVpcAttribute	[]	[]
DescribeVpcClassicLink	[]	VpcId
DescribeVpcClassicLinkDnsSupport	[]	VpcId
DescribeVpcPeeringConnections	[]	VpcPeeringConnectionId Filter

Table 1 – continued from previous pa

AWS API Reference	Ignored Param	Optional Parameters
DescribeVpcs	[]	VpcId Filter
DetachInternetGateway	[]	[]
DetachNetworkInterface	[]	Force
DisassociateRouteTable	[]	[]
ModifyNetworkInterfaceAttribute	[]	SecurityGroupId SourceDestCheck Description Attachment
ModifyVpcAttribute	[]	EnableDnsHostnames EnableDnsSupport
RejectVpcPeeringConnection	[]	VpcPeeringConnectionId
ReplaceRouteTableAssociation	[]	[]
RevokeSecurityGroupEgress	[]	IpPermissions
RevokeSecurityGroupIngress	[]	GroupId GroupName IpPermissions CidrIp FromPort IpProtocol ToPort
UpdateSecurityGroupRuleDescriptionsEgress	[]	GroupId GroupName
UpdateSecurityGroupRuleDescriptionsIngress	[]	GroupId GroupName

CHAPTER

FIVE

SUBNETS

5.1 Subnet Introduction

In the **VPC Networking > Subnets** view, an IP subnet can be defined in a standard CIDR format, and assigned a name for easy reference throughout the UI. It is used primarily for association with a VPC as described in VPC Introduction. VPC subnets are defined by the following constraints:

1. The first four IP addresses and the last IP address in each subnet CIDR block are not available for users, and cannot be assigned to an instance.
2. The second address of the subnet is reserved for the router.
3. The CIDR block of a subnet may be either identical to the VPC's CIDR block, which is the case when there is a single subnet, or a subset of the VPC's CIDR block, when there are multiple subnets. In the latter case, the CIDR blocks of the subnets cannot overlap. The permitted block size ranges from a /28 netmask to a /16 netmask.
4. Every subnet that is created is automatically associated with the main route table of the VPC. You can change the association. A subnet can be associated with only one route table at a time.

5.2 Creating a Subnet

See the video introducing the basics of creating and configuring zCompute VPC Subnets:

To create a subnet:

1. Navigate to the **VPC Networking > Subnets** view.
2. From the top toolbar, click **Create**.
3. In the **Create Subnet** dialog, enter the following:
    - **Name** - name of the subnet.
    - **Description** - optional description of the subnet.
    - **VPC** - VPC which is associated with this subnet.
    - **CIDR** - subnet in CIDR format based on IP/mask.
    - **Tags** - optionally add tags by selecting them from the dropdown, or creating them in this field.

5.3 Subnet Operations

After creating a subnet, it is displayed in the subnet list in the **VPC Networking > Subnets** view. The following operations can be performed by selecting a subnet from the list, and clicking the appropriate icon.

From top toolbar:

- **Modify** - change the name of the subnet.
- **Set Default - set the subnet as the default for a VPC, to be used for** provisioning new entities within the VPC. For example, if a new VM instance is associated with a VPC, it will be configured with an IP from the default subnet.
- **Delete**
- **Test connectivity** - use ping or arping to test connectivity to a specific IP within the selected subnet. For more information on subnet testing, see Testing Subnet Connectivity.
- **Soft Reset** - rebind all DHCP ports on the network.
- **Hard Reset** - recreate DHCP servers on the network.

From lower toolbar:

- **VMs** - view information on VMs associated with the selected subnet.
- **Events** - view configuration events (info) or alarms for the subnet.

In the displayed subnet list, there is an indication of Direct Subnet.

5.3.1 Direct Subnet

In zCompute, a Direct Subnet provides the ability to share the same layer 2 network (VLAN) between the hosting data center's network and a VPC subnet.

This allows end users who require it, to achieve L2 connectivity over a given VLAN ID to resources external to the zCompute cluster, or direct access to zStorage resources available at the data center.

For example, a direct subnet allows the establishment of external and dedicated VPSA Storage Arrays and Object Storages while bypassing unnecessary internet routers. This is extremely common and useful where a dedicated and high-speed NAS/Object Storage solution is required.

Important:

- Due to physical network resource allocation, Direct Subnets are managed by the MSP or Zadara Operations team.

  Typically, the Direct Subnet's CIDR is provided by the MSP partner that manages the data center's routing and IP allocations.
- The Direct Subnet's CIDR and the VPC's CIDR must be foreign to each other and must not overlap.
- DHCP must not be used on this VLAN or subnet, otherwise unexpected DHCP VM configurations might occur.
- The VMs' default GW of VMs attached to the Direct Subnet is always set to the VPC's internal GW, i.e. the internal vRouter and not the external GW of the Direct Subnet.
- The VPC Internal Router IP and all IPs in a Direct Subnet's Allocation Pool must be managed by zCompute. None of these IPs can be used by external systems on the Direct Subnet VLAN.

See the video introducing the basics of connecting local networks into your VPC with Direct Subnets:

Creating a Direct Subnet

To create a direct subnet (MSP or Zadara Operations team only):

1. Navigate to **Account Networking > Direct Subnets** and click **+ Create**.
2. In the **Create Direct Subnet** window, enter:
    - **Name**: The name of the direct subnet.
    - **Description**: Optional description for the direct subnet.
    - **Project**: From the dropdown, select the project to which this direct subnet will be associated.

      ✔ **Note:** A project can have only one Direct Subnet.

    - **VPC**: Optionally, from the dropdown, select the VPC for this direct subnet.
    - **Node Network**: Select the network from the dropdown.
    - **VLAN ID**: The VLAN ID of the physical switches that the direct subnet will use. This VLAN ID should also be configured on Zadara switches by Zadara Operations, for all the switch ports attached to zCompute nodes as well as the switches' uplinks to the partner's upstream switches, and the partner's switches' links to Zadara's switches.
    - **Subnet (CIDR)**: The direct subnet's CIDR block. Typically, this CIDR is provided by the partner, to make it routable from the partner's data center.
    - **VPC Internal Router IP**: The first IP address of the CIDR block. The subnet's virtual router is created by zCompute, and used by payloads created within zCompute to route traffic from the subnet.

      ✔ **Note:** This is not an external gateway, but a virtual router created by zCompute.

      The Direct Subnet cannot overlap the VPC network prefix.

      Similar to other subnets, two IPs are consumed by internal services, so nothing smaller than a /29 can be used.

    - **External Router IP**: Optional IP address for the VPC's external router.
    - **Allocation Pools**:

      One or more ranges of IP addresses allocated for zCompute payloads of this subnet.

      Enter the start and end IP addresses of the range of addresses comprising the pool of addresses, from which subnets can be allocated.

      To configure an additional pool of IP addresses, click **Add** and enter the pool's start and end IP addresses.

      ✔ **Note:** IPs in the allocation pool are managed by zCompute and should not be used by anything on the customer's side of the network.

      The purpose of this configuration is to avoid any potential IP collisions with other IP addresses external to zCompute that might be in use on this subnet, for example, physical L3 switch gateway, physical firewall appliance gateway, and physical servers.

      The Internal Router IP address, and the first and last IP addresses of the CIDR block are not permitted in the allocation pool.

3. Click **Finish**.

   The subnet is immediately available on the specified VPC.

✔ **Note:** The direct subnet is not displayed in the **Account Networking > VLANs Management** screen.

However, the direct subnet's `network_id` can be viewed using the symp `vlan-pool vlan get <id>` command. For example:

```
vlan-pool vlan get 1a8cd9e6-0d7d-4ada-ac5b-0bad3fdd291e

+----------------------+--------------------------------------+
| id                   | 1a8cd9e6-0d7d-4ada-ac5b-0bad3fdd291e |
| name                 | none                                 |
| account_vlan_pool_id | 93cb6144-7f28-44c3-9492-0b46d13da88d |
| created_at           | 2024-11-18T11:47:50Z                 |
| guest_network_pool_id | 684703f5-d641-4ddb-be82-62b81a024509 |
| network_id           | cecc1054-538a-467e-a615-83e750ce04b4 |
| project_vlan_pool_id | adb0d5ba-7927-4813-aea7-d0f0d568d808 |
| updated_at           | 2024-11-18T11:47:51Z                 |
| vlan_tag_id          | 40                                   |
+----------------------+--------------------------------------+
```

Control over VPC Subnet MTU

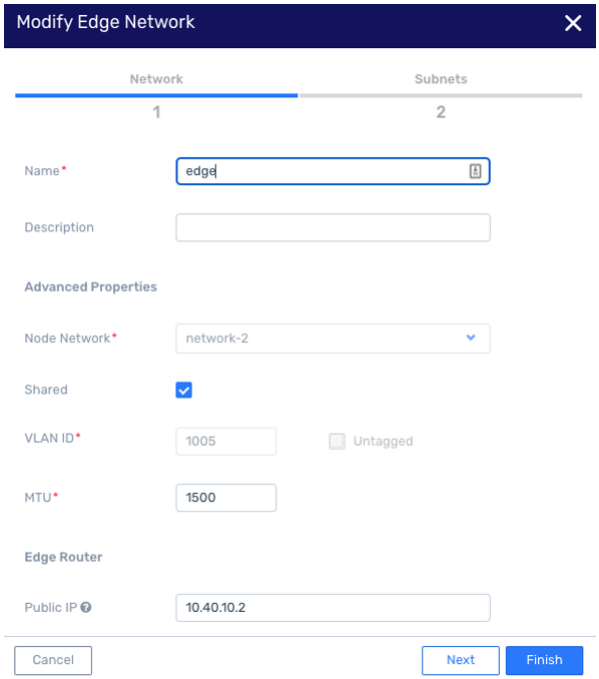
Users can view and change MTU values per virtual network.

✔ **Note:** It is not possible to create a direct subnet in the GUI with desired the MTU. However, the MTU can be updated post-creation.

- **The relevant networks are:**
  - Edge networks (for MSP administrators only)
  - Direct networks (subnets)
  - VPC subnets
- The **minimum** allowed MTU value is 1450 for standard VPC subnets or 1500 for direct subnets or edge networks.
- The **maximum** allowed MTU value depends on the global MTU configured in the cluster (e.g. 9000 or 1500). If the global MTU configured in the cluster is 9000, the maximum allowed MTU value for all virtual networks will be limited to 8950.
- If a VM experiences MTU-related connectivity issues and it resides on a public network (connected via a route-table to an internet-gateway), then it is recommended to set that network MTU to no more than 1500.

Modify Edge Network MTU

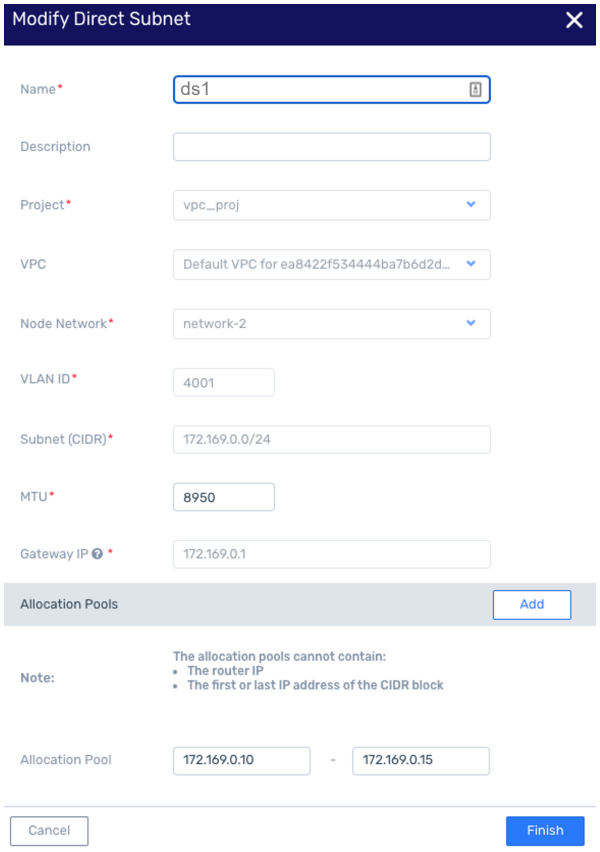
1. Navigate to **Region Networking > Edge Networks**
2. In the Edge Networks list, select the Edge Network to modify.
3. In the selected Edge Network's detail view, on the top menu click **Edit**.
4. In the **Modify Edge Network** dialog, update the **MTU** value.



Click **Finish** to save the updated MTU value.

Modify Direct Subnet MTU

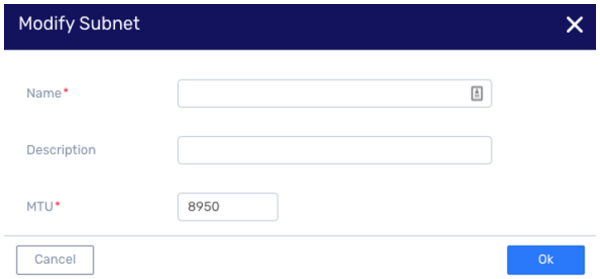
1. Navigate to **Account Networking > Direct Subnets**
2. In the Direct Subnets list, select the Direct Subnet to modify.
3. In the selected Direct Subnet's detail view, on the top menu click **Edit**.
4. In the **Modify Direct Subnet** dialog, update the **MTU** value.



Click **Finish** to save the updated MTU value.

Modify VPC Subnet MTU

1. Navigate to **VPC Networking > Subnets**
2. In the Subnets list, select the Subnet to modify.
3. In the selected Subnet's detail view, on the top menu click **Modify**.
4. In the **Modify Subnet** dialog, update the **MTU** value.



Click **Ok** to save the updated MTU value.

Note:

This feature only changes the MTU as reported to the user VMs via DHCP.
It does not change the actual MTU of the virtual network.

VMs that use the MTU value from DHCP will be updated only after the DHCP lease is renewed.

Routing traffic through an external router

If you want to route traffic from the VPC through an external router connected to the Direct Subnet, the VPC route table associated with the Direct Subnet should be modified.

This can be configured with end user's tenant permissions.

1. If an **External Router IP** was defined in Creating a Direct Subnet, skip to the next step to update the Route Table.

   Otherwise, create an Elastic Network Interface:

   1. Navigate to **VPC Networking > Network Interfaces** and click **+ Create**.
   2. In the **Create Elastic Network Interface** dialog, enter:
      - **Name**: The interface name.
      - **Description**: Optional description text.
      - **VPC**: The VPC for which the external router is being added.
      - **Subnet**: From the dropdown, select the Direct Subnet.
      - **Private IP**: The external router's IP address.
      - **Security Groups**: From the dropdown, select the security groups to apply to the network interface.
   3. Click **Finish**.
2. Navigate to **VPC Networking > Route Tables** and click the name of the Route Table to update.
   1. In the selected Route Table's lower pane, click **+ Create**.
      - **Destination CIDR**: The destination network or networks.
      - **Target Type**: Select **Network Interface** from the dropdown, to display the Network Interface input prompt.
      - **Network Interface**: From the dropdown, select the network interface created in the previous step.
   2. Click **OK**.

5.4 Testing Subnet Connectivity

Connectivity between a VPC Subnet and a specific IP address can be tested by ping, using either the GUI or CLI.

Using the GUI

1. Navigate to the **VPC Networking** > **Subnets** view.
2. Select a subnet from the displayed list and click **Test Connectivity** in top toolbar.
3. In the **Test Connectivity** window, enter a Destination IP address.
4. Select **ping** or **arping**.

✔ **Note:**

- **ping** checks layer 3 connectivity, and is blocked by Security Group filtering if traffic is not allowed from any IP in the Subnet.

- **arping** checks layer 2 connectivity, and bypasses Security Group filtering.

5. Click **OK**.
6. Click **OK**. A message is displayed that the connectivity test is taking place.
7. A few seconds later, the test results will be displayed indicting success or failure as well as other relevant details. This status report is also available in the right-hand sidebar.

Using the CLI

1. The 'guestnet-admin-tool ping-ip create' command with which you can test a subnet's connectivity requires the ID of the given subnet (see 'entity_id' below). Note: '–command-type' is either 'ping' (default) or 'arping'

```
guestnet-admin-tool ping-ip create [-h]
                                   [-f {adaptive_table,json,shell,table,value,yaml}]
                                   [-c COLUMN] [--max-width <integer>]
                                   [--noindent] [--prefix PREFIX]
                                   [-m [NAME=VALUE [NAME=VALUE ...]]]
                                   [--command-type COMMAND_TYPE]
                                   [--name NAME]
                                   entity_id dest_ip
```

2. Run the 'vpc network list' command to locate the ID of Subnet-1.

```
vpc network list -c id -c name
```

3. This returns a list of subnets and their IDs.

```
+--------------------------------------+-----------------------------------------------------------+
| id                                   | name                                                      |
+======================================+===========================================================+
| ceff2b60-fb75-44d0-8b1a-ac4034b260dc | Subnet-1                                                  |
+--------------------------------------+-----------------------------------------------------------+
```

4. Test the connectivity of Subnet-1 to the destination IP address 8.8.8.8.

```
guestnet-admin-tool ping-ip create ceff2b60-fb75-44d0-8b1a-ac4034b260dc 8.8.8.8
```

5. This returns a temporary, pending status of the subnet's connectivity.

```
+--------------+--------------------------------------+
| id           | 2ce18cc5-b1a8-401c-ae98-99e484f99b3e |
| name         | none                                 |
| status       | pending                              |
| command_type | ping                                 |
| created_at   | 2019-05-12T13:39:56.650560           |
| dest_ip      | 8.8.8.8                              |
| entity_id    | ceff2b60-fb75-44d0-8b1a-ac4034b260dc |
| output       | -                                    |
| project_id   | 07650a05e9dd47c8a3b874a2132e178c     |
| updated_at   | 2019-05-12T13:39:56.650581           |
| user_id      | admin                                |
+--------------+--------------------------------------+
```

6. Wait a few seconds and then request the final status of Router-1's connectivity test by using the 'guestnet-admin-tool ping-ip get ping_ip_id', as follows:

```
guestnet-admin-tool ping-ip get 2ce18cc5-b1a8-401c-ae98-99e484f99b3e
```

7. This returns the final, succeeded/failed status of Router-1's connectivity test with relevant output details.

```
+--------------+------------------------------------------------------------------+
| id           | 2ce18cc5-b1a8-401c-ae98-99e484f99b3e                             |
| name         | none                                                             |
| status       | succeeded                                                        |
| command_type | ping                                                             |
| created_at   | 2019-05-12T13:39:56                                              |
| dest_ip      | 8.8.8.8                                                          |
| entity_id    | ceff2b60-fb75-44d0-8b1a-ac4034b260dc                             |
|              +------------------------------------------------------------------+
| output       | PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.                     |
|              | 64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=55.1 ms           |
|              | 64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=53.3 ms           |
|              |                                                                  |
|              | --- 8.8.8.8 ping statistics ---                                  |
|              | 2 packets transmitted, 2 received, 0% packet loss, time 1001ms   |
|              | rtt min/avg/max/mdev = 53.335/54.219/55.104/0.914 ms             |
|              |                                                                  |
|              +------------------------------------------------------------------+
| project_id   | 07650a05e9dd47c8a3b874a2132e178c                                 |
| updated_at   | 2019-05-12T13:39:59                                              |
| user_id      | admin                                                            |
+--------------+------------------------------------------------------------------+
```

✔ **Note:** This information is automatically deleted after approximately one hour.

5.5 Additional options for Subnet (VPC) Connectivity Testing

1. Delete a specific subnet connectivity test

```
guestnet-admin-tool ping-ip delete ping_ip_id
```

2. List all ping_ip requests

```
guestnet-admin-tool ping-ip list
```

CHAPTER

SIX

NETWORK INTERFACES

6.1 Introduction

Zadara Cloud Services UI supports network configurations for VM instances based on the following common network concepts:

- **Subnets** - Standard IP subnet based on IP address and mask.
- **Network Interfaces** - A network interface is simply a specific IP address assigned to a VM instance. To help maintain network consistency, a network interface can be defined as an IP on a specific subnet. The UI will ensure that the selected IP is within the selected subnet.

Important: Zadara recommends configuring only one network interface on a VM

A VM connected to more than one Subnet, one of which has an Elastic IP (EIP) attached to its Elastic Network Interface (ENI), might suffer from an unpredictable Internet connectivity problem.

The reason is that the two ENIs receive a DHCP configuration which includes a default GW (i.e. a default route).

For example:

A VM has all of the following configured:

- A Network Interface on a Direct Subnet
- A Network Interface on the VPC Public Subnet
- An Elastic IP associated with the Network Interface on the VPC Public Subnet
- Security Groups to allow desired Internet traffic to reach the VM via the Elastic IP, for example port 22

As a result, the following symptoms could be expected:

- There are two listings for default route/0.0.0.0 in the guest VM O/S:
  - One points to the GW on the Direct Subnet
  - One points to the GW on the VPC Public subnet
- Outbound requests work correctly, such as ping to Internet sites and requests from the VM to external websites.
- Replies to inbound requests do not work. The VM has two bound network interfaces, but it cannot accept and reply to connections from the Internet via the Elastic IP.
- If the admin manually deletes the default route/0.0.0.0 in the guest VM pointing to the GW on the Direct Subnet, the inbound Internet connections on the Elastic IP start working. But DHCP refreshes all the time, and it repopulates the entry for the default route/0.0.0.0 to the GW on the Direct Subnet soon after it is manually deleted, effectively reinstating prevention of replies to connections from the Internet via the Elastic IP.

6.2 Creating Network Interfaces

To define a network interface:

1. Navigate to the **Networking > Network Interfaces** view.
2. From the top toolbar, click **Create**.
3. In the **Create Elastic Network Interface** dialog, enter the following:
   - **Name** - name of the network interface.
   - **Description** - optional description of the network interface.
   - **VPC** - VPC on which the network interface should be assigned.
   - **Subnet** - select from an existing subnet configured for the VPC or define a new subnet to be added to the VPC.
   - **Private IP** - select private IP within the subnet defined above.
   - **Security Groups** - select security group to control the traffic on the network interface.

   ✔ **Note:** For more information on security groups, see Security Groups Introduction.

6.3 Network Interface Operations

After creation of a network interface, it will be displayed in the network interface list in the **Networking > Network Interface** view. The following operations can be performed by selecting a network interface from the list, and clicking the appropriate icon.

From top toolbar:

- **Modify** - to change the name of the network interface.
- **Security Group** - to change the security group associated with the network interface.
- **Delete**
- **Detach Subnet** - to detach a specific network interface from a VM instance.
- **Soft Reset** - rebind all VM ports.
- **Hard Reset** - unbind and then rebind all relevant ports.

From lower toolbar:

- **Overview** - to see general information related to VM instance associated with the network interface, select **Overview** tab.
- **Events** - to view configuration events (info) or alarms for the network interface, select the **Events** tab in lower portion of view.

CHAPTER

SEVEN

ROUTE TABLES

7.1 Introduction

Route tables control the IP forwarding of all traffic in the subnets with which they are associated. They have the following attributes:

1. A VPC comes with a single built-in, modifiable, main route table.
2. You can create additional custom route tables for your VPC.
3. You cannot delete the main route table, but you can replace the main route table with a custom table that you've created. This table becomes the default table with which each new subnet is associated.
4. Each route in a table specifies a destination CIDR and a target (local/IGW).
5. Every route table contains a local route for communication within the VPC over IPv4. You cannot modify or delete this route.

See the video introducing the basics of configuring Route Tables:

7.2 Creating a Route Table

To create a route table:

1. Navigate to the **Networking > Route Tables** view.
2. From the top toolbar, click **Create**.
3. In the **Create Route Table** dialog, enter the following:
    - **Name** - name of the route table.
    - **Description** - optional description of the route table.
    - **VPC** - VPC which is associated with this route table.
4. Click OK. A route table is created with a single entry for a local route for communication within the VPC.

7.3 Route Table Operations

After creating a route table, it is displayed in the route table list in the **Networking > Route Tables** view. The following operations can be performed by selecting a route table from the list, and clicking the appropriate icon.

From top toolbar:

- **Modify** - change the name of the route table.
- **Set main** - set the route table as the main table for a VPC, replacing the previous default table.
- **Delete**
- **Test connectivity** - use ping or arping to test connectivity to a specific IP covered by routes defined in the route table. For more information on route table testing, see Testing Route Table Connectivity.
- **Soft Reset** - rebind all the ports of the route table.
- **Hard Reset** - restart the route table.

From lower toolbar:

- **Add route** - to add route to table, select **Routes** tab in lower portion of view and click **Create**.
- **Assocate subnets** - to associate a subnet with the route table, select **Subnet Associations** tab in lower portion of view and click **Associate**. Subnet association allows the user to bind an existing subnet to a route table, when the subnet is not explictly listed in the table.
- **Events** - to view configuration events (info) or alarms for the route table, select the **Events** tab in lower portion of view.

7.4 Testing Route Table Connectivity

Connectivity between a VPC Route Table and a specific IP address can be tested by ping using either the GUI or CLI.

Using the GUI

1. Navigate to the **Networking** > **Route Tables** view.
2. Select a Route Table from the displayed list and click **Test Connectivity** in top toolbar.
3. In the **Test Connectivity** window, enter a Destination IP address.
4. Select **ping** or **arping**.

   ✔ **Note:** Ping checks layer 3 connectivity and is blocked by security-group filtering, if traffic is not allowed from any IP in the subnet. Arping check layer 2 connectivity and bypasses security-group filtering.

5. Click **OK**.
6. Click **OK**. A message is displayed that the connectivity test is taking place.
7. A few seconds later, the test results will be displayed indicting success or failure as well as other relevant details. This status report is also available in the right-hand sidebar.

Using the CLI

1. The 'guestnet-admin-tool ping-ip create' command with which you can test a route table's connectivity requires the ID of the given route table (see 'entity_id' below).

   Note: '–command-type' is either 'ping' (default) or 'arping'

```
guestnet-admin-tool ping-ip create [-h]
                                   [-f {adaptive_table,json,shell,table,value,yaml}]
                                   [-c COLUMN] [--max-width <integer>]
                                   [--noindent] [--prefix PREFIX]
                                   [-m [NAME=VALUE [NAME=VALUE ...]]]
                                   [--command-type COMMAND_TYPE]
                                   [--name NAME]
                                   entity_id dest_ip
```

2. Run the 'vpc route-table list' command to locate the ID of Route Table-1.

```
vpc route-table list -c id -c name
```

3. This returns a list of route tables and their IDs.

```
+--------------------------------------+-------------------------------------------------------+
| id                                   | name                                                  |
+======================================+=======================================================+
| 2fd55d1e-60b3-4887-b376-204b63ce2fa8 | Route Table-1                                         |
+--------------------------------------+-------------------------------------------------------+
```

4. Test the connectivity of Route Table-1 to the destination IP address 8.8.8.8.

```
guestnet-admin-tool ping-ip create 2fd55d1e-60b3-4887-b376-204b63ce2fa 8 8.8.8.8
```

5. This returns a temporary, pending status of the route table's connectivity, together with the id of the ping_ip.

```
+--------------+--------------------------------------+
| id           | ab1e76df-4531-42db-a455-02a402e70ae5 |
| name         | none                                 |
| status       | pending                              |
| command_type | ping                                 |
| created_at   | 2019-05-12T14:15:11.379402           |
| dest_ip      | 8.8.8.8                              |
| entity_id    | 2fd55d1e-60b3-4887-b376-204b63ce2fa8 |
| output       | -                                    |
| project_id   | 07650a05e9dd47c8a3b874a2132e178c     |
| updated_at   | 2019-05-12T14:15:11.379416           |
| user_id      | admin                                |
+--------------+--------------------------------------+
```

6. Wait a few seconds and then request the final status of Route Table-1's connectivity test by using the 'guestnet-admin-tool ping-ip get ping_ip_id'.

```
guestnet-admin-tool ping-ip get ab1e76df-4531-42db-a455-02a402e70ae5
```

7. This returns the final, succeeded/failed status of Route Table-1's connectivity test with relevant output details.

```
+--------------+-----------------------------------------+
| id           | ab1e76df-4531-42db-a455-02a402e70ae5    |
| name         | none                                    |
| status       | failed                                  |
| command_type | ping                                    |
| created_at   | 2019-05-12T14:15:11                     |
| dest_ip      | 8.8.8.8                                 |
| entity_id    | 2fd55d1e-60b3-4887-b376-204b63ce2fa8    |
|              +-----------------------------------------+
```

(continues on next page)

(continued from previous page)

```
| output       |  ; error=connect: Network is unreachable |
|              |  ; status=2                              |
|              +------------------------------------------+
| project_id   | 07650a05e9dd47c8a3b874a2132e178c         |
| updated_at   | 2019-05-12T14:15:12                      |
| user_id      | admin                                    |
+--------------+------------------------------------------+
```

This information is automatically deleted after approximately one hour.

7.5 Additional Commands for Route Table (VPC) Connectivity Testing

1. Delete a specific route table connectivity test

```
guestnet-admin-tool ping-ip delete ping_ip_id
```

2. List all ping_ip requests

```
guestnet-admin-tool ping-ip list
```

CHAPTER

EIGHT

INTERNET GATEWAYS

8.1 Introduction

An internet gateway is a logical entity that connects the VPC router to an external network. It is associated with a VPC which has a public subnet. It is used as a target in the VPC route tables for Internet-routable traffic.

See the video introducing Internet Gateways and NAT Gateways:

8.2 Creating an Internet Gateway

To create a internet gateway:

1. Navigate to the **Networking > Internet Gateways** view.
2. From the top toolbar, click **Create**.
3. In the **Create Internet Gateway** dialog, enter the following:
    - **Name** - name of the internet gateway.
    - **Description** - optional description of the internet gateway.
    - **VPC** - VPC which is associated with this internet gateway.

8.3 Internet Gateway Operations

After creation of an internet gateway, it will be displayed in the internet gateway list in the **Networking > Internet Gateways** view. The following operations can be performed by selecting an internet gateway from the list, and clicking the appropriate icon from the top toolbar.

- **Modify** - change name of the internet gateway.
- **Detach** - detach internet gateway from VPC.
- **Delete** - delete internet gateway.

CHAPTER

NINE

DHCP OPTION SETS

9.1 Introduction

A DHCP options set is a set of network configurations that will be delivered to your VM instance when its interface acquires an IP address using the DHCP protocol.

1. DHCP options sets are associated with a project so that you can use them across all of your virtual private clouds (VPC).
2. The supported options for a DHCP options set are as follows:
    1. **Domain-name-servers** - The IP addresses of up to four domain name servers, or ZadaraIaaSProvidedDNS. The default DHCP option set specifies ZadaraIaaSProvidedDNS. Although the custom DNS server is used, the DHCP-supplied DNS server to the VM instances will always be ZadaraIaaSProvidedDNS and the custom DNS will be queried indirectly by ZadaraIaaSProvidedDNS.
    2. **Domain-name** - This value is used to complete unqualified DNS hostnames. This is set by default to 'symphony.local'.
    3. **NTP-servers** - The IP addresses of up to four Network Time Protocol (NTP) servers.
    4. **Netbios-name-servers** - The IP addresses of up to four NetBIOS name servers.
    5. **Netbios-node-type** - The NetBIOS node type (1, 2, 4, or 8).

9.1.1 How VPC passes DNS Servers via DHCP

When VPC DNS is **enabled**, the VPC DHCP service provides VMs with a pair of internal IPs as DNS servers. The VPC DNS service will look up any local zone records internally, and it will forward queries to the DNS servers provided in the DHCP Option Set for all external domains.

When VPC DNS is **disabled**, the VPC DHCP service provides VMs with the exact IPs of the DNS servers configured in the DHCP Option Set. In this case, DNS requests will go directly from VMs to the external DNS nameservers.

9.2 Creating a DHCP Option Set

To create a DHCP Option Set:

1. Navigate to the **Networking > DHCP Option Sets** view.
2. From the top toolbar, click **Create**.
3. In the **Create DHCP Options** dialog, enter the following in the appropriate tab.
   - **Details** tab:
     - **Name** - name of the DHCP Options Set.
     - **Description** - optional description of the DHCP Options Set.
     - **DNS Domain** - valid DNS domain name (e.g. xxx.com)
   - **Servers** tab:
     - **DNS Servers** - IP of DNS Server associated with DHCP Options set being defined. Definition of DNS Server is optional.
     - **NTP Servers** - IP of NTP Server associated with DHCP Options set being defined. Definition of NTP Server is optional.
   - **Netbios** tab:
     - **Netbios Node Type** - The following types may be selected:
       - **Type 1** - B-Node
       - **Type 2** - P-Node
       - **Type 4** - M-Node
       - **Type 8** - H-Node
4. Click **Finish**.

9.3 DHCP Options Set Operations

After creation of a DHCP Options Set, it will be displayed in the list in the **Networking > DHCP Options Set** view. The following operations can be performed by selecting a DHCP Options Set from the list, and clicking the appropriate icon from the top toolbar:

- **Modify** - change name of the DHCP options set.
- **Attach VPC** - attach DHCP options set to VPC.
- **Detach VPC** - detach DHCP options set to VPC.
- **Delete** - delete DHCP options set.

CHAPTER

TEN

SECURITY GROUPS

10.1 Security Groups Introduction

Security groups are firewall (whitelist) rules applied to the virtual network interfaces to control the inbound and outbound traffic. Traffic that does not match any rule in the security group will be discarded. Security group rules are realized using stateful session tracking. This means that you must specify a rule only for the direction in which the session is initiated, with the other direction being implied.

1. A VPC automatically includes a default security group. Each instance that you launch in your VPC is automatically associated with the default security group unless you specified a different security group when you launched the instance.
2. When you create a security group, you must provide it with a name and a description. The following rules apply:
    1. Names and descriptions can be up to 255 characters in length.
    2. For AWS compatibility, names and descriptions are limited to the following characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*.
    3. A security group name cannot start with sg-.
    4. A security group name must be unique within the VPC.
3. For each security group, you include one set of rules that controls the inbound traffic to the instances, and a separate set of rules that controls the outbound traffic from the instances.
4. The following are the basic components of a security group rule in a VPC:
    1. For inbound rules only - The source of the traffic and the destination port or port range. The source can be another security group, an IPv4 or IPv6 CIDR block, or a single IPv4 or IPv6 address.
    2. For outbound rules only - The destination for the traffic and the destination port or port range. The destination can be another security group, an IPv4 or IPv6 CIDR block, or a single IPv4 or IPv6 address.
    3. Any protocol that has a standard protocol number (click here for a complete list of Protocol Numbers). If you specify ICMP as the protocol, you can specify any or all of the ICMP types and codes.

10.2 Creating Security Groups

See the video demonstrating the basics of creating and configuring zCompute Security Groups and Source/Destination checks:

To create a security group:

1. Navigate to **Networking** > **Security Groups**. From top toolbar, click **Create**.
2. In the **Create Security Group** dialog, enter the following information:
    - **Name** – name of the security group.
    - **Description** (optional) - description of the security group.
    - **VPC** - select a VPC with which the security group should be associated.
3. Near **Rules**, click **Add**. For each rule, enter the following:
    - **Internet Protocol Version** - select IPV4 or IPV6.
    - **Direction** - Select EGRESS for defining a rule for outbound traffic. Select INGRESS for defining a rule for inbound traffic
    - **Protocol** - Specify the protocol for which the rule will apply - 'TCP', 'UDP' or 'ICMP'. Permit traffic from any protocol by selecting 'Any'.
    - **Start port and end port**
        - If Protocol = 'Any', then leave blank.
        - If Protocol = 'TCP' or 'UDP', then enter the port range for the rule.
        - If Protocol = 'ICMP', then enter the ICMP Message Type in the first field and ICMP Code in the second field.
    - **Source or Destination** - Based on the rule's **Direction**, select one of the following options to restrict or allow traffic from specified sources (INGRESS), or to specified destinations (EGRESS).
        - **Any**: No restrictions.
        - **Group**: Restrict to a specific group.
        - **Subnet**: Restrict to a specific CIDR or IP address.
4. Click **OK** to create the security group. The new security group appears in the **Networking** > **Security Groups** view.
5. To add another rule, click **Add** again.

10.3 Security Group Operations

After creation of a Security Group, it will be displayed in the list in the **Networking > Security Group** view. The following operations can be performed by selecting a security group from the list, and clicking the appropriate icon.

From top toolbar:

- **Modify** - add or delete rules to the selected security group.
- **Detach** - detach the security group from all associated network interfaces.
- **Delete** - delete the selected security group.

From lower toolbar:

- **Rules** - view rules associated with the selected security group.

- **VMs** - view VM instances associated with the selected security group.
- **Events** - view configuration events (info) or alarms for the route table.

CHAPTER

ELEVEN

ELASTIC IPS

11.1 Introduction

Elastic IPs (EIPs) are used to expose instances and managed services outside of Zadara Cloud Services. An EIP will be used in the network address operation (NAT) of all traffic to/from the virtual network interface with which it is associated.

1. You first allocate an Elastic IP address for use in a VPC, and then associate it with an elastic network interface (ENI) in your VPC. An EIP can be associated with only one ENI at a time.
2. An EIP may be attached only to an ENI that is in a VPC with an internet gateway.

For more information on EIPs, see: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-eips.html .

11.2 Allocating an Elastic IP with the UI

1. Navigate to **Networking > Elastic IPs**.
2. From the top toolbar, click **Allocate**.
3. In the **Allocate Elastic IP** dialog, click **OK**.
4. The new Elastic IP will appear in the displayed list with the following information:
    - **Elastic IP**
    - **Private IP** - once the EIP is associated with a VPC which includes a NAT Gateway, it will be associated with a private IP within the private subnet range for the VPC
    - **Instance** - VPC NAT gateway instance with which the EIP is associated.
    - **VPC** - VPC with which EIP is associated.
    - **Public DNS**

11.3 Elastic IP Operations

After creation of an EIP, it will be displayed in the EIP list in the **Networking > Elastic IP** view. The following operations can be performed by selecting an EIP from the list, and clicking the appropriate icon from the top toolbar.

- **Detach** - detach EIP from NAT gateway instance.
- **Delete** - delete EIP.

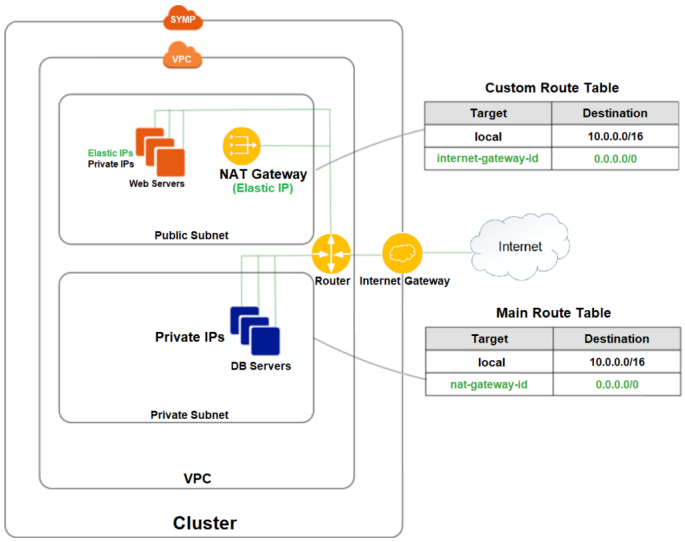
CHAPTER

TWELVE

NAT GATEWAYS

12.1 Introduction

A network address translation (NAT) gateway enables instances in a private subnet to connect to the internet via an elastic IP address, as shown in the diagram below:



See the video introducing Internet Gateways and NAT Gateways:

12.2 Creating a NAT Gateway

To create a NAT Gateway:

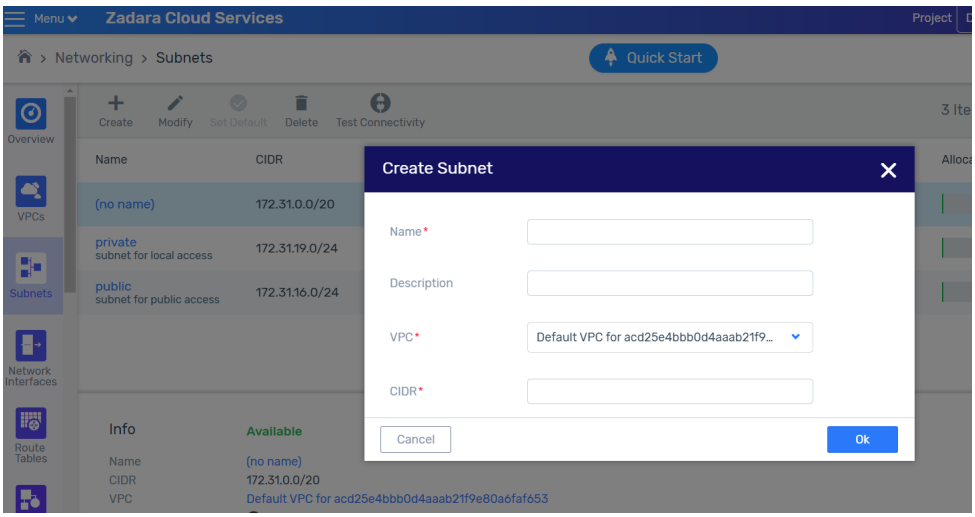
1. Navigate to the **Networking > NAT Gateways** view.
2. From the top toolbar, click **Create**.
3. In the **Create NAT Gateway** dialog, enter the following:
    - **Name** - name of the NAT gateway.
    - **Description** - optional description of the NAT gateway.
    - **VPC** - VPC which is associated with this route table.
    - **Subnet** - select subnet in which the NAT gateway will reside.
    - **Elastic IP** - select elastic IP for NAT gateway.

4. Click **OK**.
5. After creation of the NAT gateway, update the route table associated with at least one of your private subnets such that Internet-bound traffic is directed towards the NAT gateway.
6. The instances in your private subnets will now be able to communicate with the internet.

12.3 Sample NAT Gateway Configuration Flow

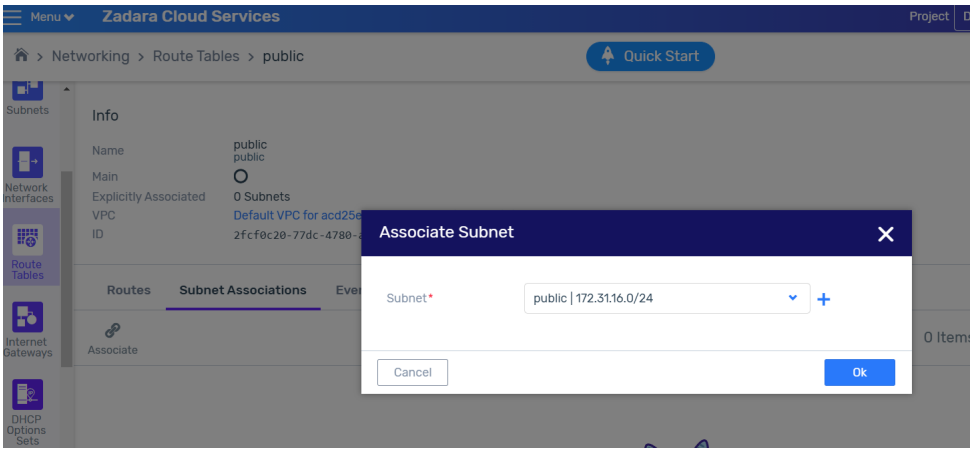
The following procedure provides a complete end-to-end configuration example including VPC and route table configurations related to NAT gateways.

1. To create a VPC with a NAT Gateway, navigate to the **Networking** > **VPCs** view, and click **Create**.
2. In the **Create VPC** window, select an existing Internet Gateway from the pull-down list or create a new one by clicking **+**.
3. Create two subnets in the VPC, one called Public and the other called Private.
    1. Navigate to the **Networking** > **Subnets** view and click **Create**.
    2. In the **Create Subnet** window, create a subnet called 'public'.
    3. Click **OK**.
    4. Click **Create** again.

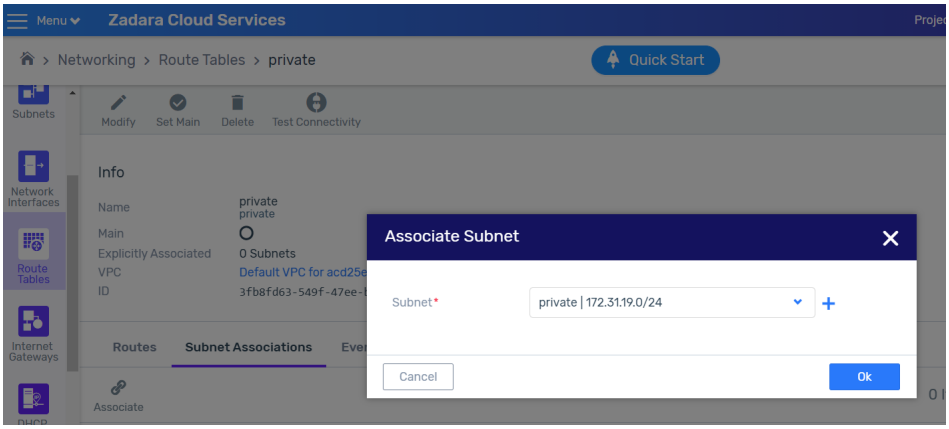


    5. In the **Create Subnet** window, create a subnet called 'private'.
    6. Click **OK**.
4. Create two route tables in the VPC, one called public and the other called private.
    1. Navigate to the **Networking** > **Route Tables** view and click **Create**.
    2. In the **Create Route Table** window, create a Route Table called 'public'.
    3. Click **OK**.
    4. Click **Create** again.
    5. In the **Create Route Table** window, create a Route Table called 'private'.
    6. Click **OK**.

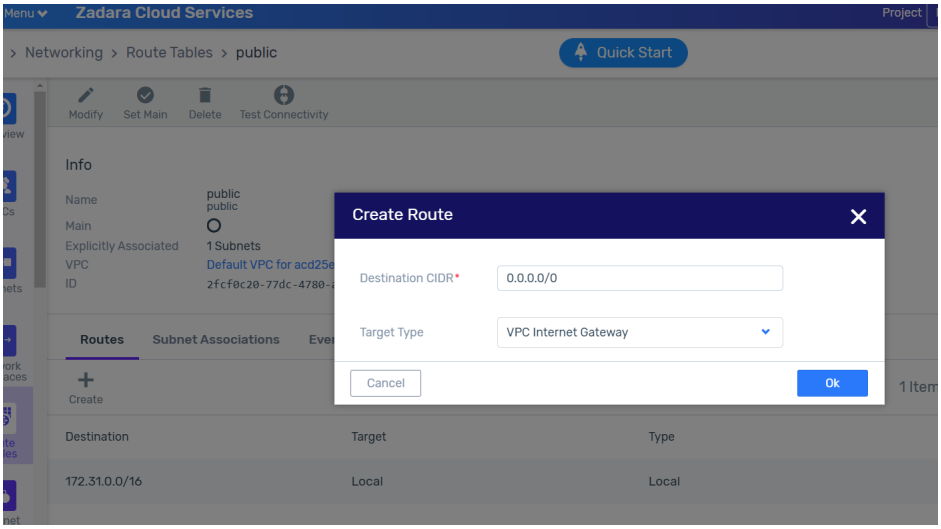
5. Associate the public subnet to the public route table, and the private subnet to the private route table.
    1. Navigate to the **Networking** > **Route Tables** view and click on the **public** route table.
    2. In the bottom of the display showing the Route Table details, select the **Subnet Associations** tab.
    3. Click **Associate**.



    4. In the Associate Subnet window, associate the **public** subnet to the **public** route table.
    5. Click **OK**.
    6. Navigate to the **Networking** > **Route Tables** view and click on the **private** route table.
    7. In the bottom of the display showing the Route Table details, select the **Subnet Associations** tab.
    8. Click **Associate**.

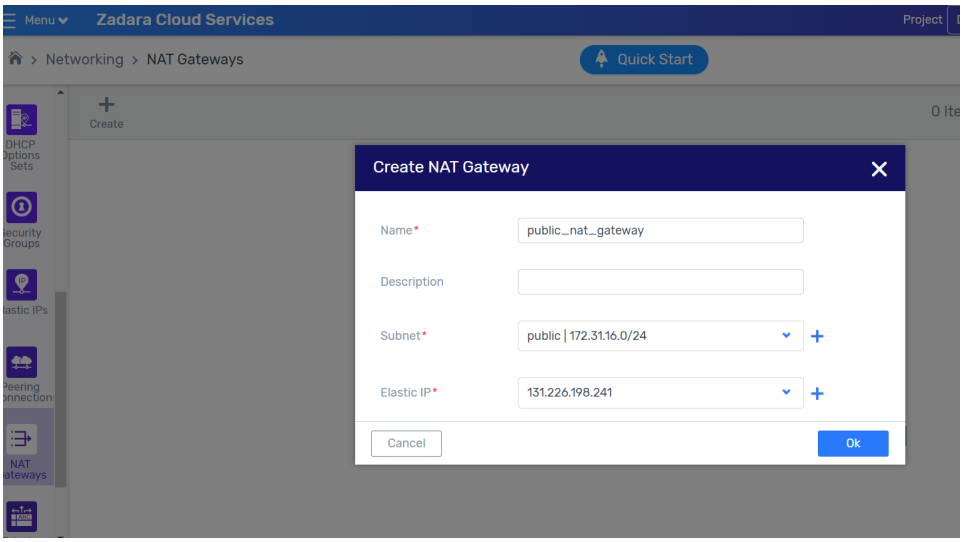


    9. In the Associate Subnet window, associate the **private** subnet to the **private** route table.
    10. Click **OK**.
6. In the **public** route table create a default route with the VPC Internet Gateway as the target.
    1. Navigate to the **Networking** > **Route Tables** view and click on the **public** route table.
    2. In the bottom of the display showing the Route Table details, select the **Routes** tab.
    3. Click **Create**.
    4. In the **Create Route** window, create a default route (0.0.0.0/0) with the VPC Internet Gateway as the target.
    5. Click **OK**.



7. Create a NAT gateway on the public subnet and allocate an elastic IP to it. Wait for the NAT GW state to move from pending to available.

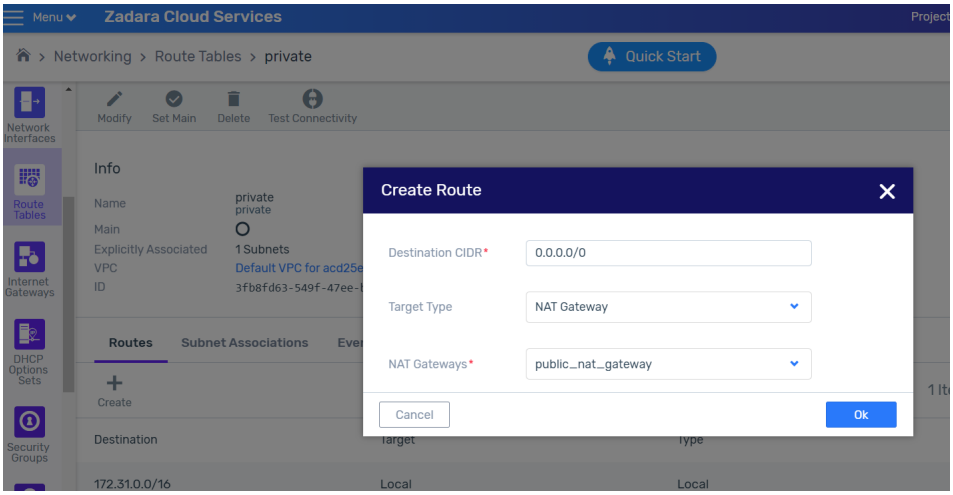
    1. Navigate to the **Networking** > **NAT Gateways** view and click **Create**.
    2. In the **Create NAT Gateway dialog** window, select an existing elastic IP from the drop down list or click **+** to create a new one.



    3. Click **OK**.

8. In the **private** route table create a default route with the created NAT Gateway as the target.

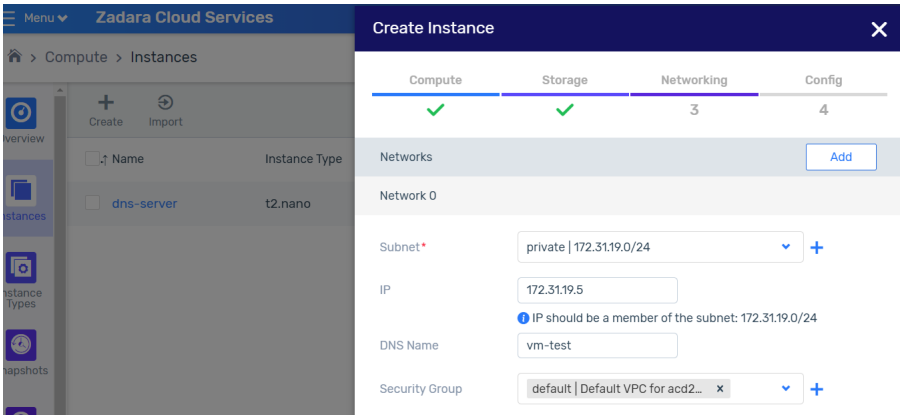
    1. Navigate to the **Networking** > **Route Tables** view and click on the **private** route table.
    2. In the bottom of the display showing the Route Table details, select the **Routes** tab.
    3. Click **Create**.
    4. In the **Create Route** window, create a default route (0.0.0.0/0) with the created NAT Gateway as the target.



5. Click **OK**.

9. Create a VM on the private subnet

    1. Navigate to the **Compute** > **Instances** and click **Create**.

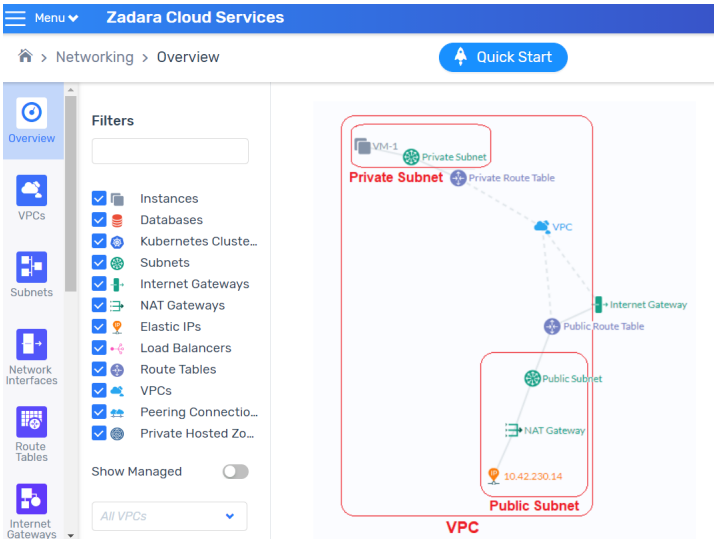


    2. In the **Create VM wizard**, associate the VM with the private subnet created.

10. You can now connect the VM to the internet via the NAT Gateway Elastic IP.

11. View the Network Topology diagram of the NAT Gateway in a VPC.

    1. In the **Networking** > **Overview** screen see the VPC view of the Network Topology.



Note: The red Subnet and VPC frames and labels shown in the diagram are illustrative only and not part of the Zadara Cloud Services Network Topology UI display.

CHAPTER

THIRTEEN

PRIVATE HOSTED ZONES

13.1 Introduction

A private hosted zone is a collection of DNS domain records which can be associated with one or more VPCs.

13.2 Creating a Private Hosted Zone

To create a private hosted zone:

✔ **Note:** This can be performed by Admin, Tenant Admin or Member users.

1. Navigate to the **Networking > Private Hosted Zones** view.
2. From the top toolbar, click **Create**.
3. In the **Create Private Hosted Zone** dialog, enter the following:
    1. **Name**
    2. **Description**
    3. **Domain**
    4. **VPC Associations** - VPC's to be associated with the Private Hosted Zone.

        ✔ **Note:** A Member user can select only those VPC's owned by the member's project. An Admin user can select from all of the projects in the cluster.

    5. Click **OK**. A private hosted zone is created.

13.3 Private Hosted Zone Operations

After creation of a private hosted zone, it will be displayed in the private hosted zone list in the **Networking > Private Hosted Zone** view. The following operations can be performed by selecting a private hosted zone from the list, and clicking the appropriate icon or tab.

From top toolbar:

- **Modify** - change name, description, or domain associated with the private hosted zone.
- **Delete** - delete the private hosted zone.

From lower toolbar:

- **Record Sets** - select this tab to display, create, delete, or modify DNS records sets associated with the private hosted zone.
- **VPC Associations** - select this tab to associate or disassociate a VPC with the private hosted zone.

CHAPTER

FOURTEEN

DNS SERVICES

14.1 Introduction

Zadara Cloud Services supports DNS services on the following levels:

1. **VPC** - DNS at this level allows the definition of DNS names that are resolvable within the context of a single VPC. VPC-level DNS services support the A (IPv4 address) DNS record type only. Once the CoreDNS engine is enabled by an admin user, any member user can enable or disable DNS services from any VPCs to which they have access.
2. **Private Hosted Zone** - DNS at this level allows the definition of DNS names that are resolvable within the context of one or more VPCs associated to a hosted zone. Hosted Zone-level DNS services support all Route 53 DNS record types. Hosted zones are created and managed by admin or member users. Once the CoreDNS engine is enabled by an admin user, any member user can enable or disable DNS services from any VPCs to which he has access.

14.2 VPC DNS Support

Zadara Cloud Services supports VPC level DNS. VM instances can resolve all DNS addresses in the context of a single VPC. After the Core-DNS engine has been enabled and the VPC-DNS engine has been disabled, you must individually enable or disable each VPC.

Any newly created VPC is by default DNS-enabled, with an A record type for the domain's IP address.

14.2.1 How VPC passes DNS Servers via DHCP

When VPC DNS is **enabled**, the VPC DHCP service provides VMs with a pair of internal IPs as DNS servers. The VPC DNS service will look up any local zone records internally, and it will forward queries to the DNS servers provided in the DHCP Option Set for all external domains.

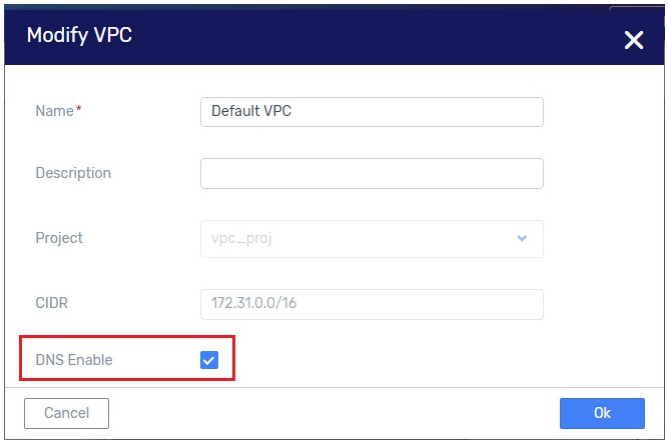
When VPC DNS is **disabled**, the VPC DHCP service provides VMs with the exact IPs of the DNS servers configured in the DHCP Option Set. In this case, DNS requests will go directly from VMs to the external DNS nameservers.

14.2.2 Enable or Disable VPC-DNS

Enable or disable VPC-DNS via UI

To enable or disable VPC-DNS via the UI:

1. Navigate to the **Networking > VPCs** view.
2. Select the VPC from the displayed list and click **Modify** from the top toolbar.
3. In the **Modify VPC** window which opens, check or uncheck the **DNS Enabled** box to enable or disable DNS.
4. Click **OK**.



Enable or disable VPC-DNS via CLI

To enable or disable VPC-DNS via the CLI:

1. Use the following command to enable DNS support for a VPC:

```
vpc update --enable-dns-support true vpc_id
```

2. Use the following command to disable DNS support for a VPC:

```
vpc update --enable-dns-support false vpc_id
```

Upgrade

For VPCs which were created before enabling the Coredns engine, but were not DNS-enabled:

1. Navigate to the **Networking > VPCs** view.
2. Select the VPC from the displayed list and click **Modify** from the top toolbar.
3. In the **Modify VPC** window which opens, check the **DNS Enabled** box and click **Modify**.
4. Click **OK**.

For VPCs which were created before enabling the Coredns engine, and are DNS-enabled:

1. Navigate to the **Networking > VPCs** view.
2. Select the VPC from the displayed list and click **Modify** from the top toolbar.
3. In the **Modify VPC** window which opens, uncheck the **DNS Enabled** box and click **Modify**.
4. Click **OK**. This detaches the VPC from the VPC-DNS engine.

5. Re-open the **Modify VPC** dialog, check the DNS Enable field, and click **OK**. This enables the DNS services for this VPC through the Core-DNS engine.

To display DNS engine for each VPC via CLI

Enter the following command from the CLI:

```
vpc list -c id -c name -c service_vms
```

The 'service_vms' field will be empty if there is no DNS service. If there is a DNS service the 'sevice_vms/vm_type' field will display either 'dnsmsq' for the older VPC_DNS engine, or 'coredns' for the new DNS engine.

14.3 Sample Terraform Scenario

The following is an example of how to use VPC-DNS support with Terraform.

1. Enable DNS in the VPC as described in VPC DNS Support.
2. In the Terraform script, set the `enable_dns_support` flag to true, for a specific VPC.

   With DNS support enabled, any VM that you create within this VPC can use the `private_dns_name` returned in the **describeInstances** response to access other VMs in the VPC.

   When DNS support is enabled in a VPC, the system creates a VM with the following host name: `host-a-b-c-d` (where a.b.c.d is the VM IP address in the VPC)

   Any other VM instance in the VPC can access the host with the command: "`ping host-a-b-c-d`" instead of "`ping a.b.c.d`.

   This functionality is useful for applications that require DNS names and do not work with IP addresses.
3. In addition, you can also add DNS A records to external IPs so they will be resolved within this VPC.

   For example, you can add an A record to resolve "service.<vpc-domain>" to any IP (usually external to the VPC). This allows you to define a globally named service resolution that resides external to the VPC.

   This DNS A record feature is useful for the same reason mentioned above- some applications require DNS names and do not work with IP addresses.

CHAPTER

FIFTEEN

VPC PEERING CONNECTION (SAME CLOUD)

Note:

- For VPC Peering between zCompute VPCs in the same Zadara Edge Cloud, use zCompute's built-in VPC Peering Connection (same cloud) solution.
- For VPC Peering between zCompute VPCs in different Zadara Edge Clouds, or zCompute VPC to customer on-premises peering, use the VPC Peering for multiple Zadara Edge Clouds solution that leverages open-source pfSense software.

15.1 Introduction

VPC peering lets users create direct IP connectivity between any two VPCs. Direct connectivity between VPCs means that servers in a VPC can be reached from the other VPC without the need for elastic IPs or traffic flowing through the edge network.

- VPC peering is simply L3 connectivity realized using routing tables and IP connectivity.
- VPC peering can only be achieved between VPCs that do not have an address overlap (as the connectivity is based solely on routing).
- VPC peering is between exactly two VPCs in one Zadara region.
- VPC peering is subject to the Zadara Cloud Services permission scheme. This means that to create a peering connection, a user must have permissions in both VPCs.
- Unlike VPC peering in AWS, the Zadara Cloud Services implementation does not require the two ends of the peering connection to consent.
- A peer VPC can be referenced in a security group only by the peer's CIDR.
- The VPC peering functionality can be used in a star topology with one central VPC and 3 peered VPCs.

15.2 VPC peering implementation in zCompute

VPC peering is an additional router that lies between the peer VPCs.

This peering router is populated with the two VPCs' addresses (CIDRs).

Important: VPC peering does not support transitive routing from one VPC through another VPC to another network, whether it's the Internet (for IGW sharing) or routing to an on-prem network through a direct subnet etc.

15.3 Creating a Peering Connection

To create a peering connection:

1. Navigate to **Networking** > **Peering Connections**.
2. From the top toolbar, click **Peer VPC** and enter the following fields:
    - **Name** - name of peering connection.
    - **Description** - description of peering connection.
    - **Requester** - select requester VPC from pull down list.
    - **Accepter** - select accepter VPC from pull down list or by entering VPC ID shown in detailed VPC view in **Networking** > **VPCs**.
3. Click **OK**. The peering connection will appear in the list with status **Pending-Acceptance**.
4. To accept the peering request, click the status **Pending-Acceptance** and select **Accept** from top toolbar. The status should change to **Active**.

To allow traffic to flow, you must create routes in the relevant route tables. A route can be to the entire VPC or to specific subnets. The target of the route is the peering connection.

To create a route:

1. Navigate to **Networking** > **Route Tables**.
2. From top toolbar, select **Create** and enter the following fields:
    - **Name** - name of route table.
    - **Description** - description of route table.
    - **VPC** - VPC for one of the requester VPC.
3. Click **OK**. The route table is created.
4. Select the new route table from the displayed list, and from the lower toolbar, select the **Routes** tab and click **Create**.
5. In the **Create Route** dialog, select **Target Type** = **Peering Connections** and then select CIDR in the accepter VPC.
6. Click **OK**.

To confirm that a VPC peering connection is working, ping between two VM instances in two different VPCs that have a VPC peering connection.

CHAPTER

SIXTEEN

VPC PEERING FOR MULTIPLE ZADARA EDGE CLOUDS

Note:

- For VPC Peering between zCompute VPCs in the same Zadara Edge Cloud, use zCompute's built-in VPC Peering Connection (same cloud) solution.
- For VPC Peering between zCompute VPCs in different Zadara Edge Clouds, or zCompute VPC to customer on-premises peering, use the VPC Peering for multiple Zadara Edge Clouds solution that leverages open-source pfSense software.

VPC Peering for Zadara Edge Clouds enables routing network traffic between two VPCs, using private IPv4 addresses.

This implementation uses IPSec technology for securing private connections between instances communicating with each other in a Zadara Edge Cloud.

16.1 Introduction

16.1.1 Virtual Private Cloud (VPC)

A virtual private cloud (VPC) is a virtual network dedicated to your Zadara Edge Cloud account. It is logically isolated from other virtual networks. You can launch virtual machines running computing workloads into your VPC.

The VPC model allows a user in a multi-tenant environment to make use of advanced networking capabilities and services for microsegmentation, isolation and routing.

16.1.2 zCompute VPC Peering

A VPC Peering connection is a networking connection between two VPCs that enables routing network traffic between them using private IPv4 addresses. Instances in either VPC can communicate with each other as if they are within the same network. Zadara Edge Cloud uses the existing infrastructure of a VPC to create a VPC Peering connection.

A VPC Peering connection helps you to facilitate the transfer of data. When you establish peering relationships between VPCs across different Zadara Edge Clouds, resources in the VPCs in the different edge clouds can communicate with each other using private IP addresses, without using a gateway, VPN connection, or network appliance. The traffic remains in the private IP space. All inter-cloud traffic is encrypted by IPSec.

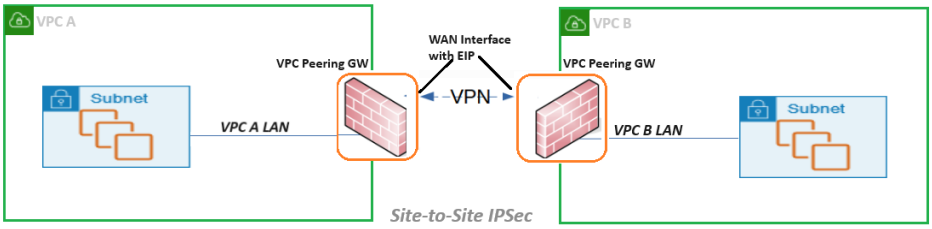
Leveraging zCompute capabilities, Zadara offers self-managed VPC Peering, based on the open-source pfSense software.

zCompute VPC Peering supports the following use cases:

- VPC to VPC

- VPC to on-premises

VPC to VPC



For the **VPC to VPC** use case implementation, the VPC Peering Gateway (GW) image in zCompute's Marketplace should be deployed on instances allocated on a VPC that need peering connectivity. The VPC Peering GW implements Firewall (FW) functions between the internal VPC subnet and the external public WAN. The VPC Peering GW is attached to the internal VPC subnet and external WAN subnet. It has capabilities for managing access and pass-through rules over FW. The WAN interface of the VPC Peering GW associated with an Elastic IP (EIP) and used for Site-to Site IPSec VPN, provides highly secured private connectivity between VPCs. The same architecture is used for multi-point VPC Peering supporting full mesh topologies between multiple VPCs.

VPC to on-premises

The **VPC to on-premises** use case implementation enables secure connectivity from a VPC to a customer's on-premises data center and internal network. The deployment of **VPC to on-premises** peering is achieved by an IPSec tunnel between the VPC Peering GW on a Zadara Edge Cloud and the FW installed on a customer network GW.

16.2 VPC Peering GW Deployment

The deployment workflow for VPC Peering is based on pfSense software.

16.2.1 Deployment Requirements

- X86-64 Instance
- 1 vCPU
- 2GB RAM
- 8 GB disk drive
- 2 NICs (WAN and LAN)
- EIP on WAN interface
- There is no overlapping CIDR between peered VPCs.

- A zCompute VPC configured with Public and Private Subnets.

  See Creating a VPC with the UI Wizard.

16.2.2 Deployment Workflow

✔ **Note:** The initial deployment flow is identical for both VPC Peering for multiple Zadara Edge Clouds and for VPN Service for Zadara Edge Clouds.

The following workflow must be run on a VPC GW instance that is configured with:

- Public and Private Subnets
- A Security Group preconfigured for this deployment. See the section on Security Hardening at the end of this page.

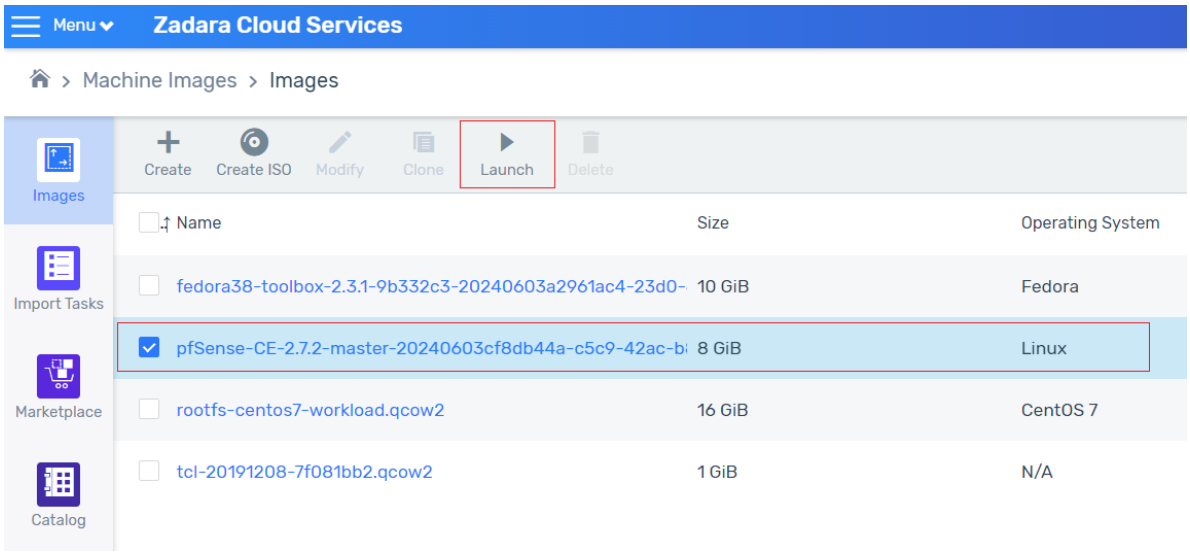
A preloaded image is available in the zCompute Marketplace, and provides an easy to use pfSense OpenVPN deployment option.

Download the pfSense image from Marketplace

1. In the zCompute UI, go to **Machine Images > Marketplace** and select the **pfSense-CE** (VPC Peering GW) image.
2. Set the **Scope** to **Project** or **Account**, and download the image.

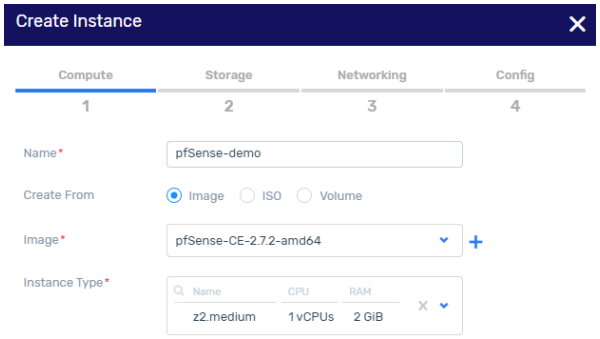
Create an instance based on the pfSense image

1. In **Machine Images > Images**, select the VPC Peering GW (pfSense-CE) image.



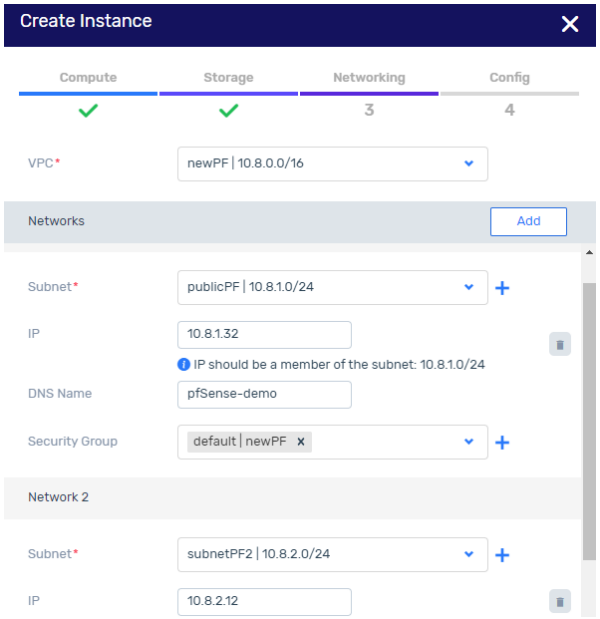
2. Click **Launch** to create an instance with 2 subnets.

   One subnet is for the internal VPC LAN. The other subnet will be used for the public-facing WAN interface.



3. In the **Storage** tab, accept the default settings. Click **Next**.
4. In the **Networking** tab, configure the public subnet.

   On completion of the public subnet configuration, click **Add** to configure the private subnet.



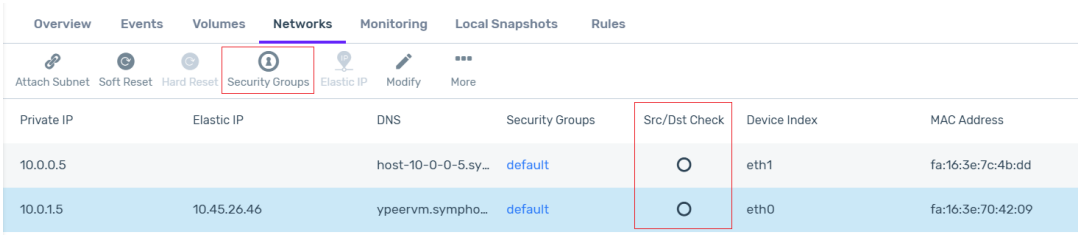
✔ **Note:** The significance of first configuring the public subnet followed by the private subnet is so that the public subnet should be associated with eth0, and the private subnet associated with eth1.

Networking configuration for the pfSense instance

1. Go to **Compute > Instances** and select the instance.
   1. In the instance's lower pane, click the **Networks** tab.
   2. Attach an Elastic IP to the public subnet:
      1. Click the row of the public subnet.
      2. In the lower menu, select **More > Attach Elastic IP**. Attach an Elastic IP to the NIC attached to the WAN/public subnet, for example eth0.

         The Elastic IP will be used for the WAN interface on the VPC GW.
   3. For each of the **eth0** and **eth1** interfaces (both the public and private subnets), disable the **Src/Dst Check**:

1. In the instance's **Networks** tab in the lower pane, click the network interface row.
2. Click **Security Groups**. In the **Security Groups** modal that opens, uncheck the **Source/Destination** check-box, and save the configuration.



Networking setup on the pfSense VM

1. Connect to the VM VNC to set up the networking configuration.

   Go to **Compute > Instances > [VM instance name] > Connect**.

   The VNC window opens, and the pfSense menu displays:

```
FreeBSD/amd64 (Temp.home.arpa) (ttyv0)

KVM Guest - Netgate Device ID: 33b55fc3e002f2456b4b

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on Temp ***

 WAN (wan)       -> vtnet0     -> v4: 10.8.1.61/24
 LAN (lan)       -> vtnet1     -> v4/DHCP4: 10.0.0.101/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 1
```

2. From the menu, select option **1: Assign interfaces**:

> ✔ **Note:** There is no need to set up VLANs.

```
Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(vtnet0 vtnet1 or a): vtnet0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vtnet1 a or nothing if finished): vtnet1

The interfaces will be assigned as follows:

WAN  -> vtnet0
LAN  -> vtnet1

Do you want to proceed [y|n]? y
```

1. Set up **vtnet0** for **WAN** (mapped to **eth0** on the VM instance).
2. Set up **vtnet1** for **LAN** (mapped to **eth1** on the VM instance).

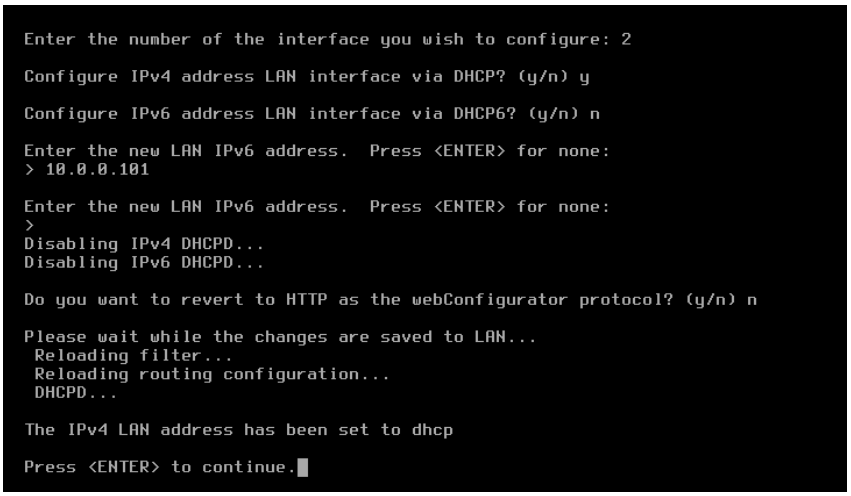
After assignment of the network interfaces, the pfSense menu reappears.

3. From the menu, select option **2: Set interface(s) IP address**.
    1. Setup the WAN to static IPv4.

       For example:

    2. Set up the LAN interface with IPv4 DHCP.

       For example:



On completion of the IP setup, the updated WAN and LAN IP assignments display, followed by the pfSense menu.

✔ **Note:** The deployment flow up to this step is identical for both VPC Peering for multiple Zadara Edge Clouds and for VPN Service for Zadara Edge Clouds.

Sign on to the pfSense web client to continue the specific deployment implementation.

---

4. In a browser window, launch the pfSense web client using the Elastic IP assigned earlier to the public subnet. For example, `https://10.41.31.5`.

   The pfSense web client's default credentials:

   - username: `admin`
   - password: `pfsense`

✔ **Note:** The recommended best practice is to change the pfSense admin password at the first sign-on to the pfSense web client.

IPSec VPN setup

Important: This procedure involves configuration on 2 sites.

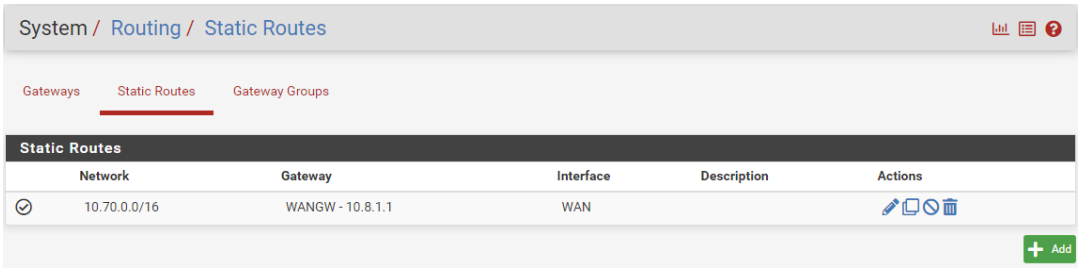
Ensure that you complete the setups and bring up pfSense instances on both VPCs.

---

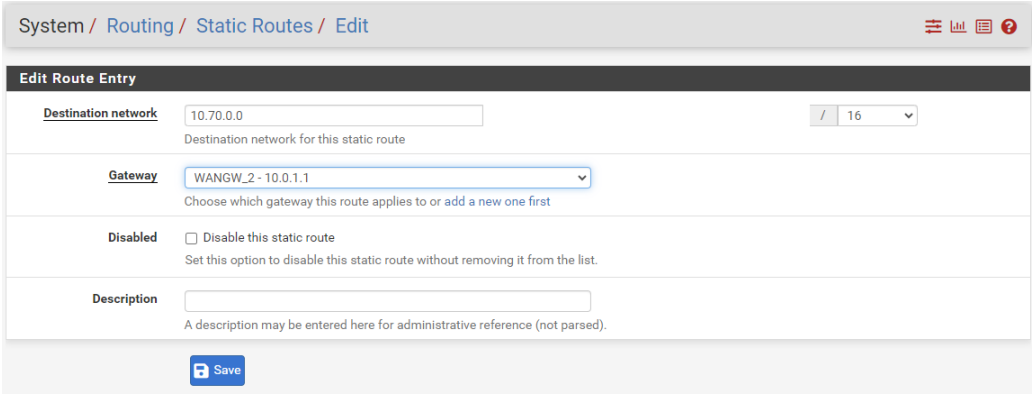
1. Set up a site-to-site IPsec tunnel according to the comprehensive step by step IPsec Site-to-Site VPN Example in the pfSense user guide.
2. Routing configuration:

   On both sides of the IPsec tunnel, there is the need to define static routes to the remote VPC:

   1. To define a static route over IPSec tunnel on the pfSense FW:
      1. In the **pfSense** web client, navigate to **System > Routing > Static Routes**.

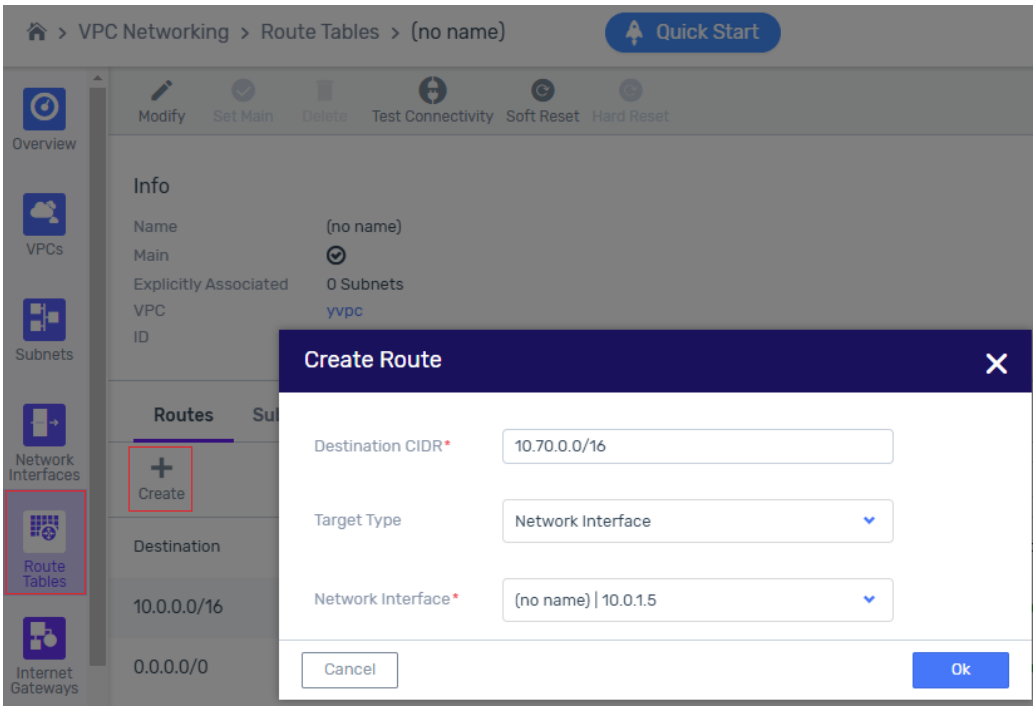


1. Click **Add** below the **Static Routes** table.
2. In the **Edit Route Entry** form, enter:



   - **Destination network**: CIDR of the destination VPC.
   - **Gateway**: Select the WAN GW of the pfSense instance.
3. Click **Save**.
4. In the **Static Routes** screen, click **Apply Changes**.

2. In **zCompute**, add the route to the remote VPC CIDR with the GW Network Interface allocated for the WAN port on the pfSense instance:
   1. Navigate to **VPC Networking > Route Tables**, and click the route table associated with the VPC.
   2. In the VPC's lower menu **Route** tab, click **+ Create**.
   3. In the **Create Route** dialog, enter:



- **Destination CIDR**: CIDR of the destination VPC.
- **Target Type**: Select **Network Interface** from the dropdown, to display the **Network Interface** input prompt.
- In the **Network Interface** prompt, select the GW Network Interface allocated for the WAN port on the pfSense instance.

4. Click **Ok** to save.

Important: In the destination's pfSense web client and zCompute VPC Route Tables screen, repeat this procedure for the reverse direction.

16.2.3 Security hardening configuration

1. Change default passwords to non-default ones.
2. Update the VPC Security Group to block non-essential ports.

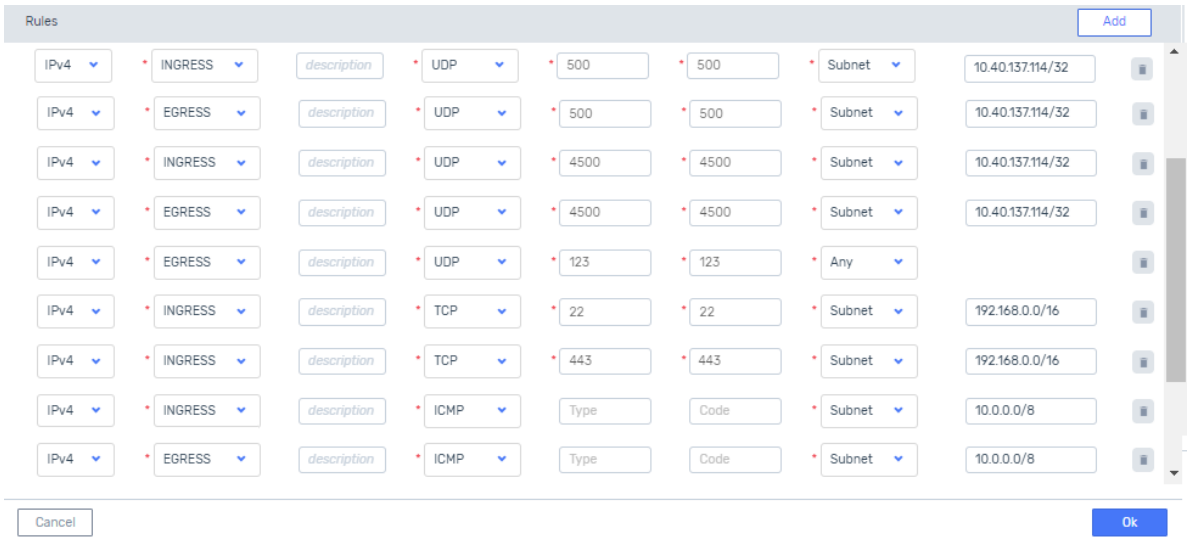
   The VPC Peering GW requires the following ports for normal operations:

   - UDP ports 500 and 4500 for IPSec

     The Subnet Remote Value on these ports must be set to the EIP of the destination VPC's Peering GW.
   - UDP port 123 for NTP
   - TCP ports 22 (SSH) and 443 (HTTPS) for managing the pfSense virtual appliance

     These ports can be blocked when the configuration is complete.
   - ICMP for troubleshooting

     This configuration can be blocked when troubleshooting is complete.



Additional ports might be needed for applications running on VPC VM instances.

Important: In the destination zCompute VPC's Security Group screen, repeat this configuration for the reverse direction.

CHAPTER

SEVENTEEN

VPN SERVICE FOR ZADARA EDGE CLOUDS

The VPN Service for Zadara Edge Clouds enables remote access to a VPC.

The implementation uses OpenVPN technology for securing private connections between remote clients and Zadara Edge Cloud resources.

17.1 Introduction

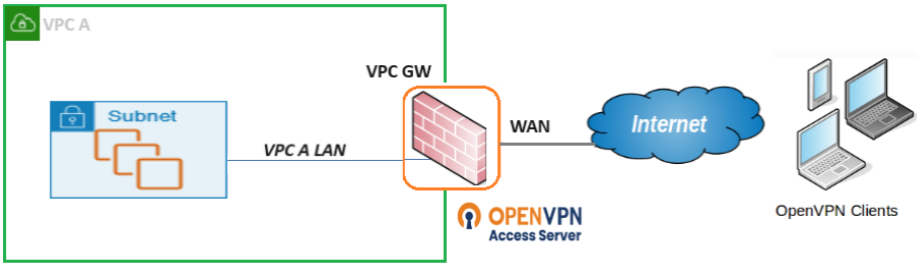
17.1.1 Virtual Private Cloud (VPC)

A virtual private cloud (VPC) is a virtual network dedicated to your Zadara Edge Cloud account. It is logically isolated from other virtual networks. You can launch virtual machines running computing workloads into your VPC.

17.1.2 zCompute VPN Service for VPC

A VPN service for VPC enables secure access from remote clients to resources running on a VPC associated with Zadara Edge accounts. Zadara Edge Cloud uses the existing infrastructure of a VPC to create a VPC access GW, providing authentication and authorization services based on OpenVPN technology.

Leveraging zCompute capabilities, Zadara offers a self-managed VPN Service for VPC, based on the open-source pf-Sense software.



The VPN Service is based on the VPC GW image available in zCompute's Marketplace, for deployment on instances allocated in the VPC. The VPC GW implements Firewall (FW) functions between the internal VPC subnet and the external public WAN. The VPC GW is attached to the internal VPC subnet and external WAN subnet. It has capabilities for managing access and pass-through rules over FW. The WAN interface of the VPC GW is associated with an Elastic IP (EIP) and used for OpenVPN deployment, and provides highly secured private access from clients to VPC resources.

The VPC GW image comes with a built-in easy installation for clients, to be applied on remote machines supporting various OSes.

17.2 VPC GW Deployment

The deployment workflow for the VPN Service is based on pfSense software.

17.2.1 Deployment Requirements

- X86-64 Instance
- 1 vCPU
- 2GB RAM
- 8 GB disk drive
- 2 NICs (WAN and LAN)
- EIP on WAN interface
- A zCompute VPC configured with Public and Private Subnets.

  See Creating a VPC with the UI Wizard.

17.2.2 Deployment Workflow

✔ **Note:** The initial deployment flow is identical for both VPC Peering for multiple Zadara Edge Clouds and for VPN Service for Zadara Edge Clouds.

The following workflow must be run on a VPC GW instance that is configured with:

- Public and Private Subnets
- A Security Group preconfigured for this deployment. See the section on Security Hardening at the end of this page.

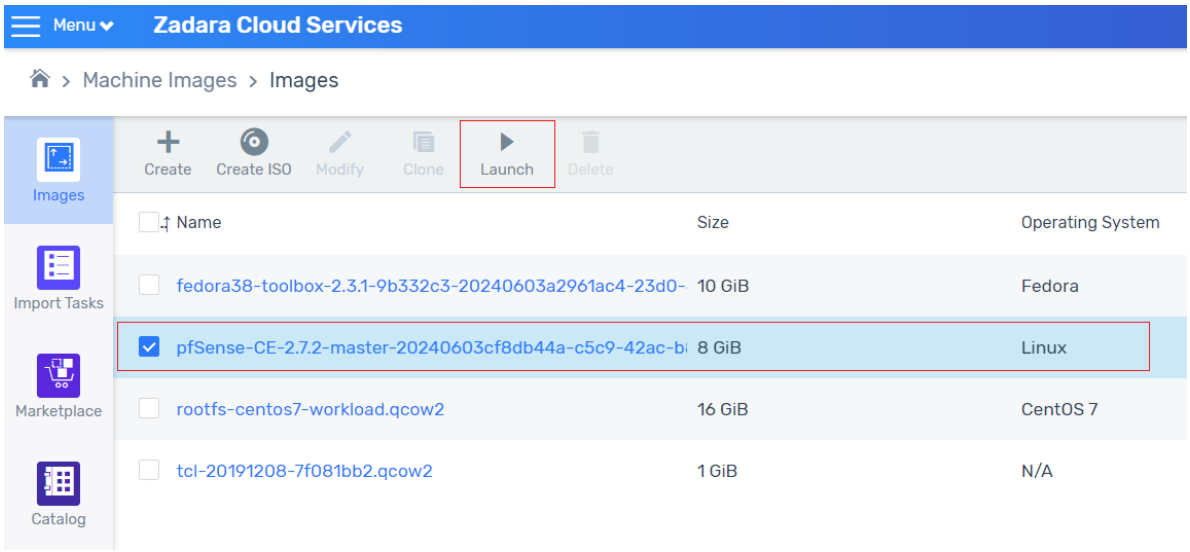
A preloaded image is available in the zCompute Marketplace, and provides an easy to use pfSense OpenVPN deployment option.

Download the pfSense image from Marketplace

1. In the zCompute UI, go to **Machine Images > Marketplace** and select the **pfSense-CE** (VPC Peering GW) image.
2. Set the **Scope** to **Project** or **Account**, and download the image.

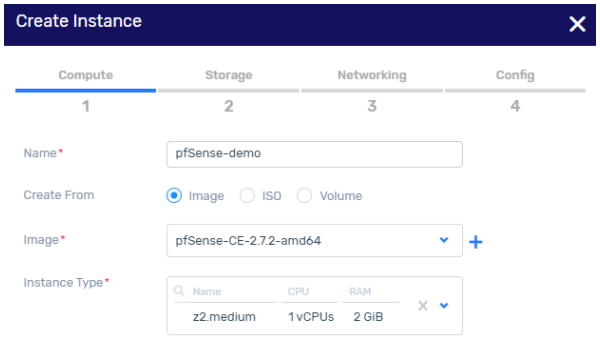
Create an instance based on the pfSense image

1. In **Machine Images > Images**, select the VPC Peering GW (pfSense-CE) image.



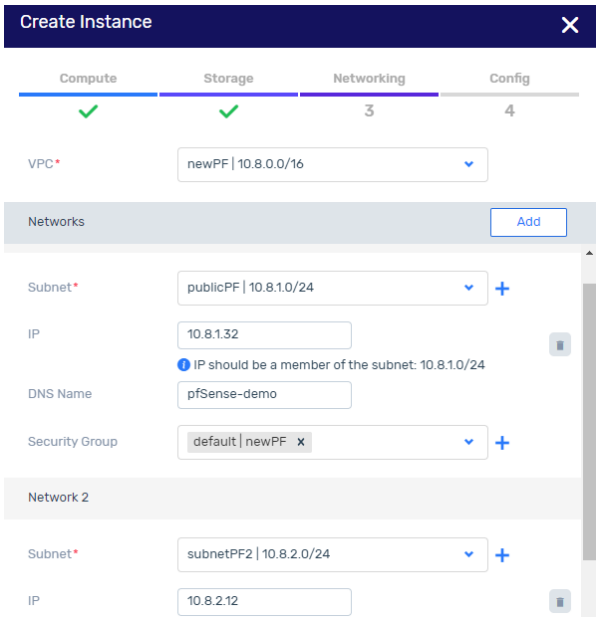
2. Click **Launch** to create an instance with 2 subnets.

   One subnet is for the internal VPC LAN. The other subnet will be used for the public-facing WAN interface.



3. In the **Storage** tab, accept the default settings. Click **Next**.
4. In the **Networking** tab, configure the public subnet.

   On completion of the public subnet configuration, click **Add** to configure the private subnet.

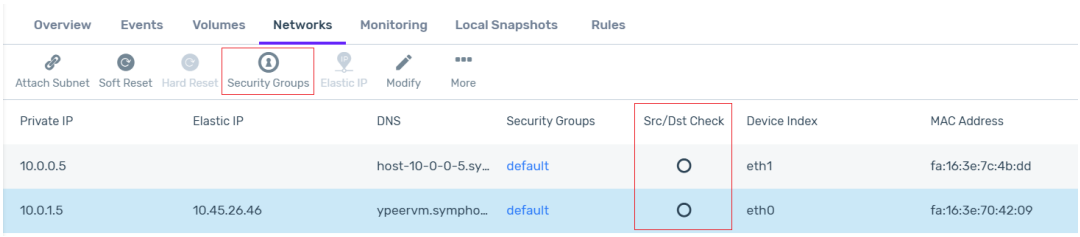


Note: The significance of first configuring the public subnet followed by the private subnet is so that the public subnet should be associated with eth0, and the private subnet associated with eth1.

Networking configuration for the pfSense instance

1. Go to **Compute > Instances** and select the instance.
    1. In the instance's lower pane, click the **Networks** tab.
    2. Attach an Elastic IP to the public subnet:
        1. Click the row of the public subnet.
        2. In the lower menu, select **More > Attach Elastic IP**. Attach an Elastic IP to the NIC attached to the WAN/public subnet, for example eth0.

           The Elastic IP will be used for the WAN interface on the VPC GW.
    3. For each of the **eth0** and **eth1** interfaces (both the public and private subnets), disable the **Src/Dst Check**:
        1. In the instance's **Networks** tab in the lower pane, click the network interface row.
        2. Click **Security Groups**. In the **Security Groups** modal that opens, uncheck the **Source/Destination** check-box, and save the configuration.

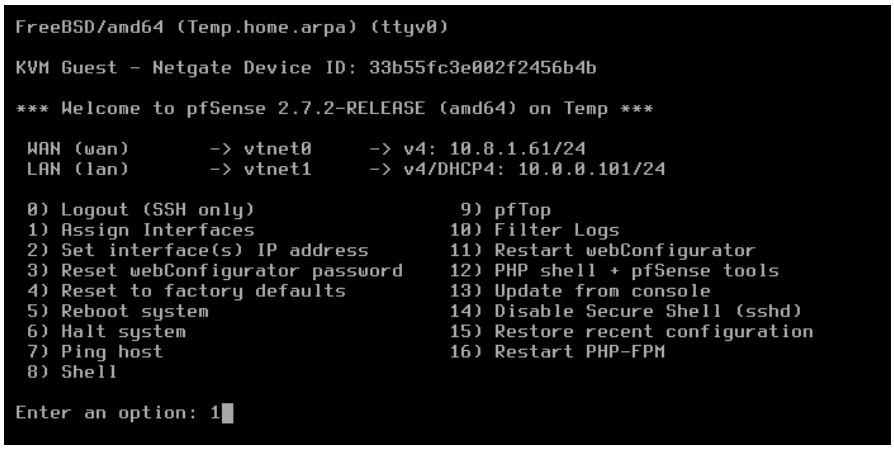


Networking setup on the pfSense VM

1. Connect to the VM VNC to set up the networking configuration.

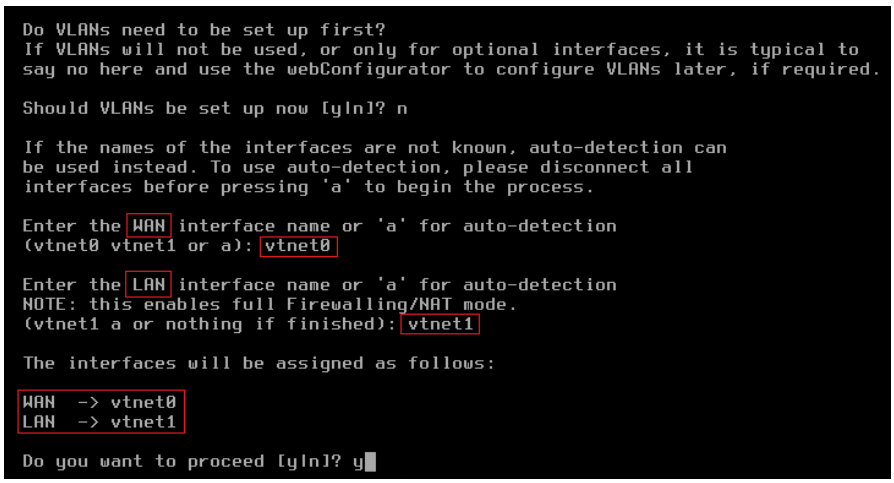
   Go to **Compute > Instances > [VM instance name] > Connect**.

   The VNC window opens, and the pfSense menu displays:



2. From the menu, select option **1: Assign interfaces**:

   ✔ **Note:** There is no need to set up VLANs.



   1. Set up **vtnet0** for **WAN** (mapped to **eth0** on the VM instance).
   2. Set up **vtnet1** for **LAN** (mapped to **eth1** on the VM instance).

   After assignment of the network interfaces, the pfSense menu reappears.

3. From the menu, select option **2: Set interface(s) IP address**.

   1. Setup the WAN to static IPv4.

      For example:

```
Enter an option: 2

Available interfaces:

1 - WAN (vtnet0 - static)
2 - LAN (vtnet1 - dhcp)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 10.0.1.5

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 10.0.1.1

Should this gateway be set as the default gateway? (y/n) y

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on WAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to WAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 WAN address has been set to 10.0.1.5/24

Press <ENTER> to continue.
```

2. Set up the LAN interface with IPv4 DHCP.

   For example:

```
Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) y

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address.  Press <ENTER> for none:
> 10.0.0.101

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to dhcp

Press <ENTER> to continue.
```

On completion of the IP setup, the updated WAN and LAN IP assignments display, followed by the pfSense menu.

✔ **Note:** The deployment flow up to this step is identical for both VPC Peering for multiple Zadara Edge Clouds

and for VPN Service for Zadara Edge Clouds.

Sign on to the pfSense web client to continue the specific deployment implementation.

4. In a browser window, launch the pfSense web client using the Elastic IP assigned earlier to the public subnet. For example, `https://10.41.31.5`.

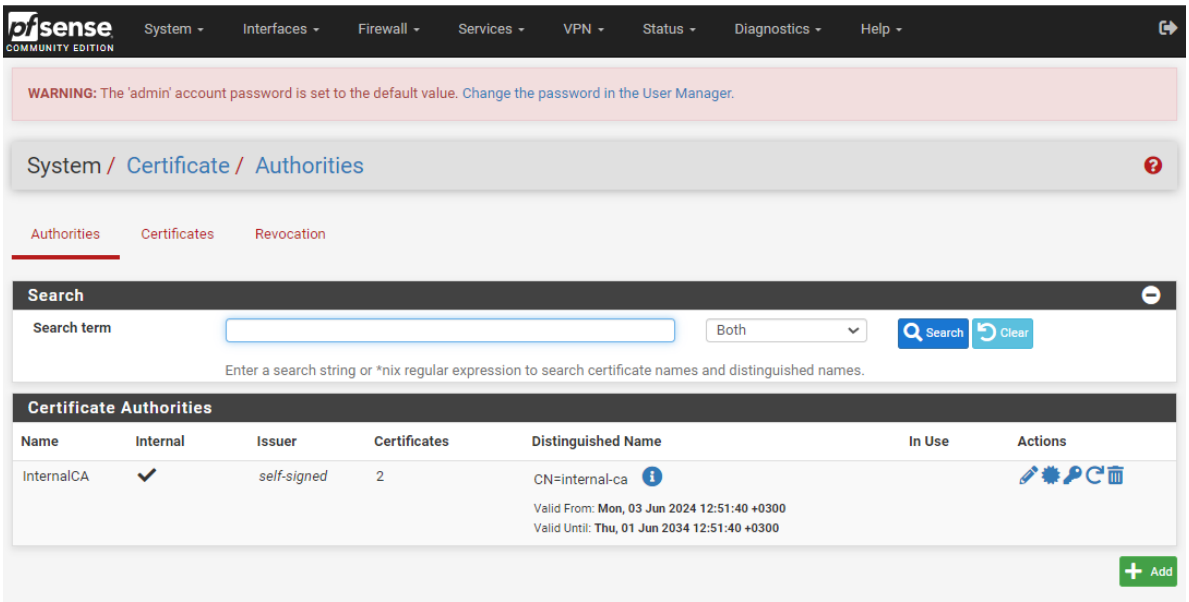
   The pfSense web client's default credentials:

   - username: `admin`
   - password: `pfsense`

   ✔ **Note:** The recommended best practice is to change the pfSense admin password at the first sign-on to the pfSense web client.

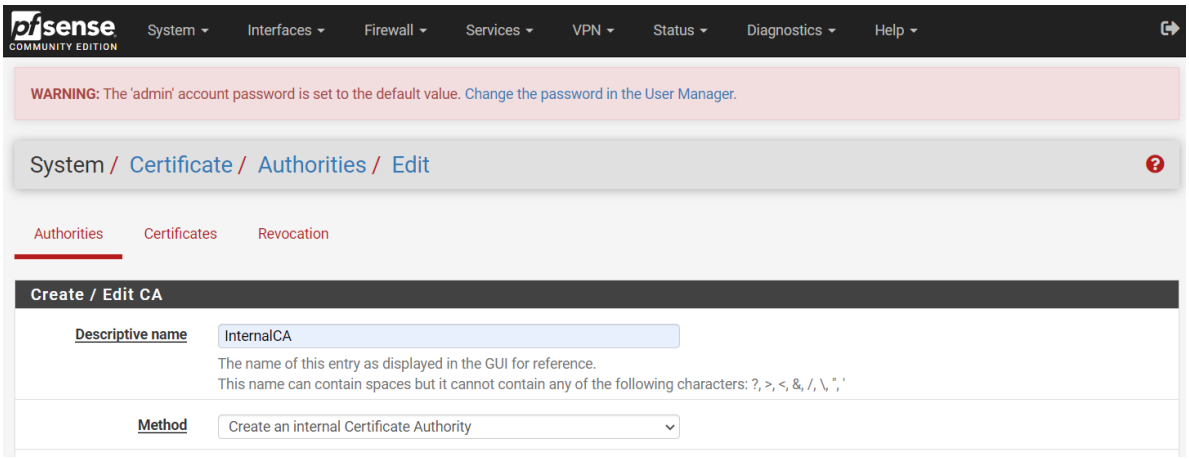
Certificate Authority setup

1. In the pfSense web client, navigate to **System > Certificates**.



2. Under the **Certificate Authorities** list, click **Add**.

   In the Certificate Authorities input form, configure the following:

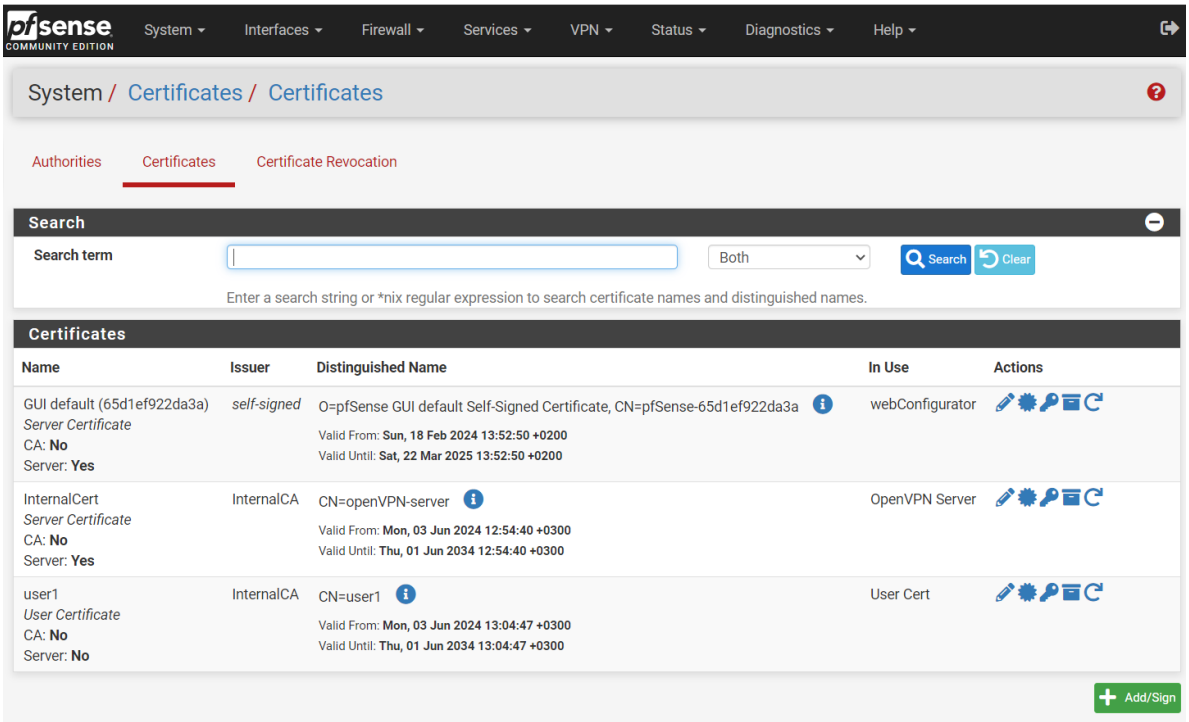


1. **Descriptive name**: Enter a meaningful name for the Certificate Authority.
2. **Method**: Select **Create an internal Cerificate Authority**.
3. Accept the other defaults and click **Save**.

   The new configuration is added to the Certificate Authorities list.

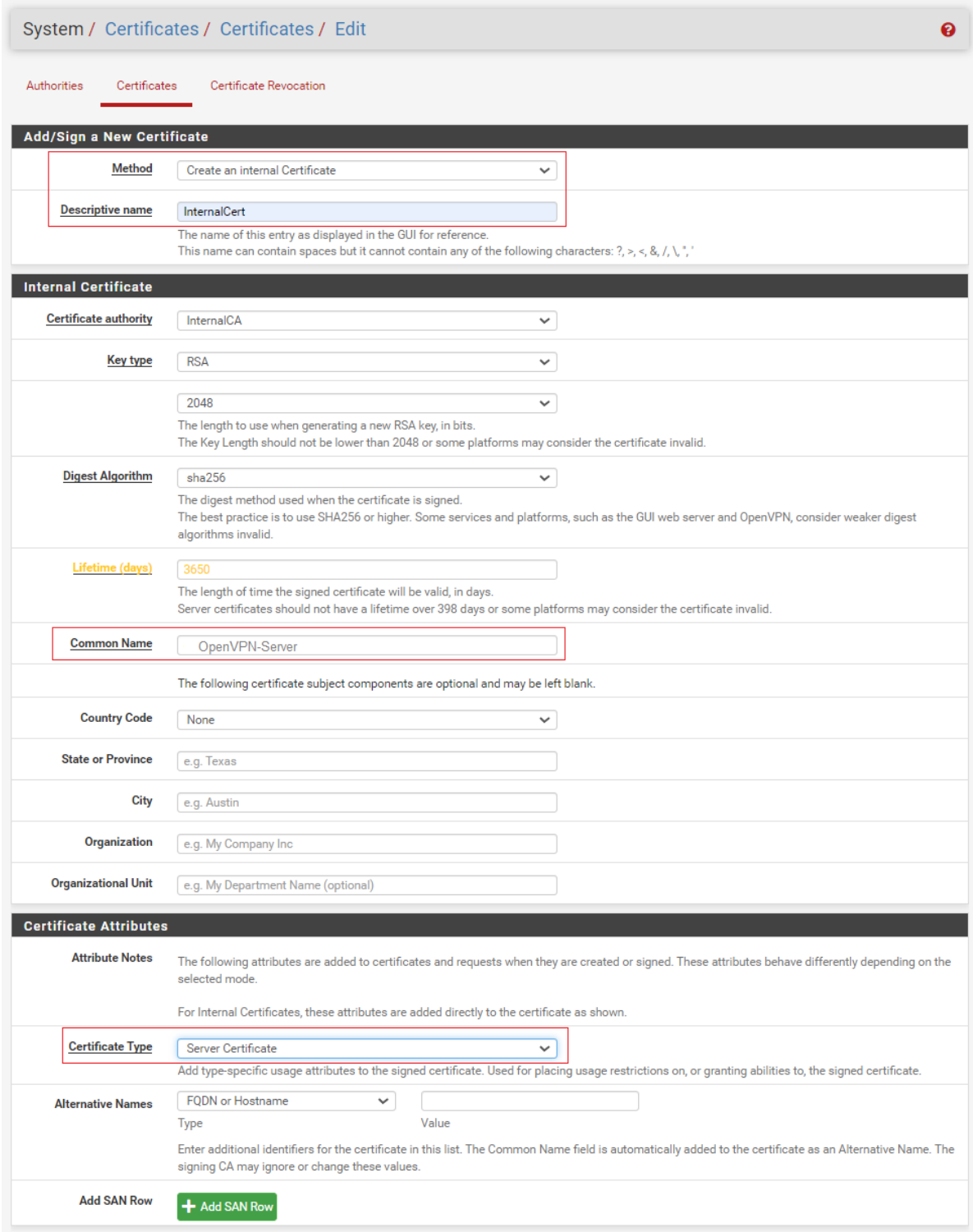
OpenVPN Access Server setup

1. In the pfSense web client, navigate to **System > Certificates**. Click **Certificates tab**.



2. Under the Certificates list, click **Add** to create a server certificate.

   In the Certificate input form, configure the following:



1. **Method**: Select **Create an internal Cerificate**.
2. **Descriptive name**: Enter a meaningful name for the certificate.
3. **Common Name**: Enter a meaningful name, for example, `OpenVPN-Server`.
4. **Certificate Type**: Select **Server Certificate**.

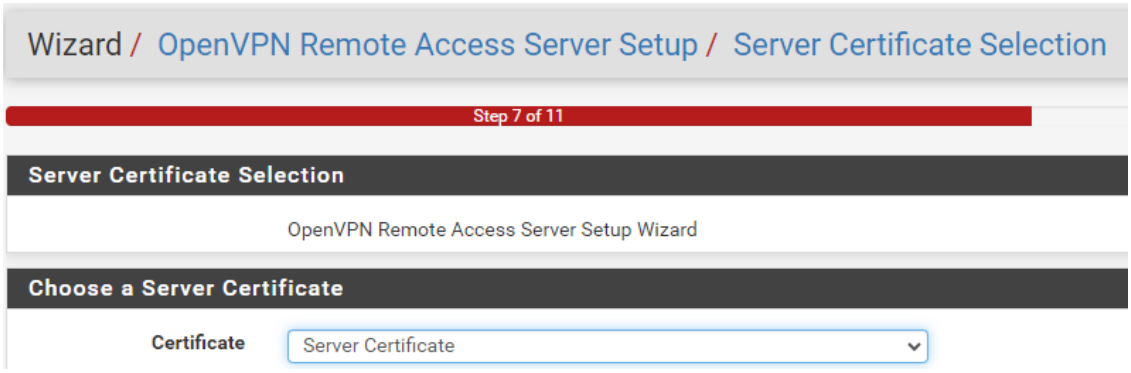
5. Accept the other defaults and click **Save**.

   The new certificate is added to the Certificates list.

3. In the pfSense web client, navigate to **VPN > OpenVPN**, and click the **Wizards** tab.

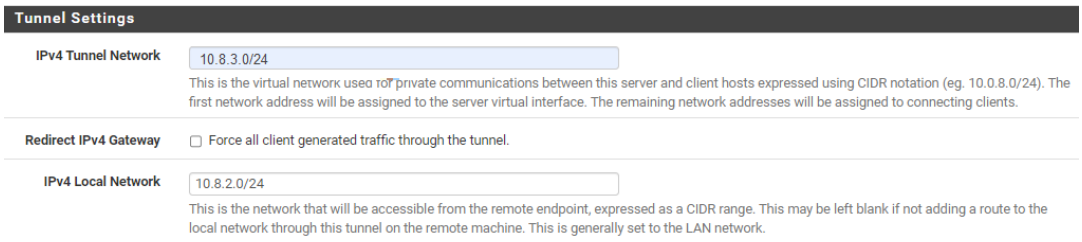
   In the **OpenVPN Remote Access Server Setup** wizard, accept the default settings, with the following exceptions:

   1. In step 7 of the wizard, select the server certificate created previously in Certificate Authority setup.

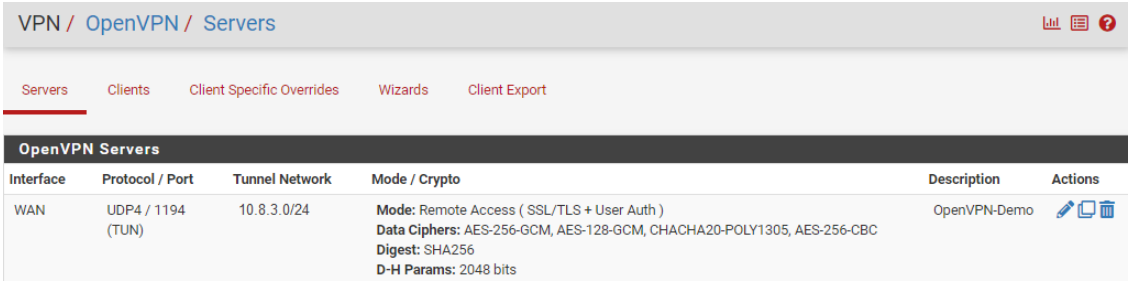


   2. In step 9 of the wizard, in the **Tunnel Settings** section:

      1. **IPv4 Tunnel Network**: Enter a unique CIDR.
      2. **IPv4 Local Network**: Enter the CIDR of the private subnet allocated for the instance.



   The configured OpenVPN server will be added to the list of OpenVPN Servers.

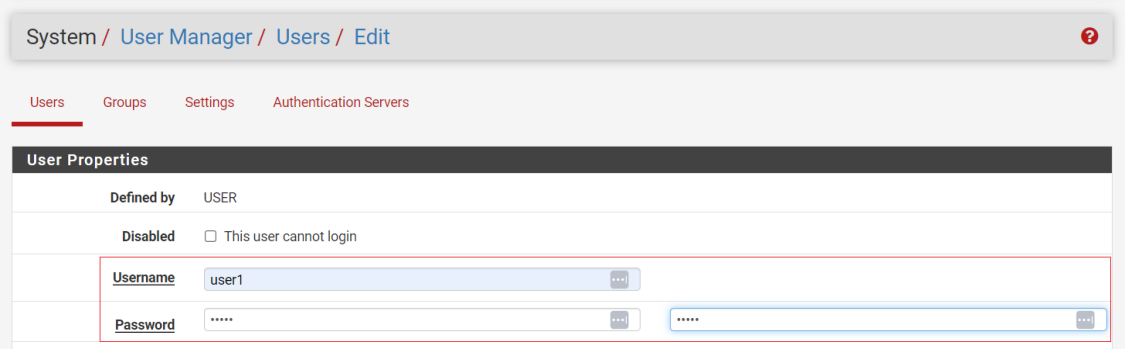


✔ **Note:** For more detailed information, the pfSense user guide provides a comprehensive step by step OpenVPN Remote Access Configuration Example.

OpenVPN Client setup

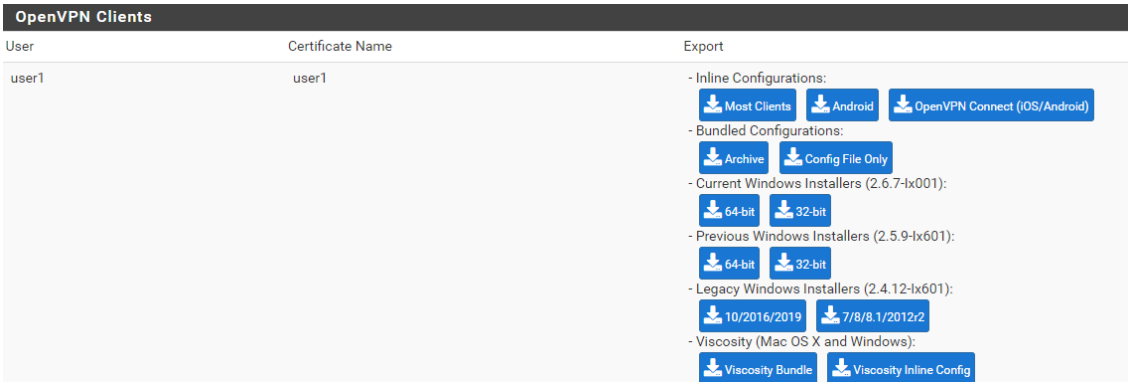
This workflow uses local user authentication. The following steps provide an example for adding a user for accessing the cloud from a remote client machine:

1. In the pfSense web client, navigate to **System > User Manager**.
    1. Add a user for remote access.
    2. Click **Save**, and edit again to generate a user certificate with the certificate authority defined previously in Certificate Authority setup.



    3. In the pfSense web client navigate to **VPN > OpenVPN > Client Export**.

       At the bottom of the Client Export page, select the user, and the OS that will host the OpenVPN client.



       For example, by clicking **Windows 64-bit**, to download its OpenVPN installation package to the local client machine. The installation package includes the configuration and certificate required for the user to connect to the VPN from the specified OS.

Important: To export a user+OS of a new VPN to a client machine that already has an OpenVPN client and configuration for an existing VPN:

- Select the user's **Bundled Configurations > Archive**.

The same procedure applies for configuring a new user who will access an existing VPN on the client machine.

---

2. On the remote client machine:
    1. Install the OpenVPN client:
        - **For a client machine that does not yet have an OpenVPN client installation**:

Install the OpenVPN client on the remote client machine, using the OpenVPN installation package downloaded in the previous step.

- **For a client machine that already has an OpenVPN client and configuration for an existing VPN**:

  On the local client machine, open the zipped package into the OpenVPN configuration folder, for example, `C:\\Program Files\\OpenVPN\\config`.

2. Configure the VPN:

   Edit the user's OpenVPN client configuration file, for example, `C:\\Program Files\\OpenVPN\\config\\<name>-<username>-config`. For example:

```
dev tun
persist-tun
persist-key
data-ciphers AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305:AES-256-CBC
data-ciphers-fallback AES-256-CBC
auth SHA256
tls-client
client
resolv-retry infinite
remote 10.0.1.5 1194 udp4
verify-x509-name "openVPN-server" name
auth-user-pass
pkcs12 Temp-UDP4-1194-user1.p12
tls-auth Temp-UDP4-1194-user1-tls.key 1
remote-cert-tls server
explicit-exit-notify
```

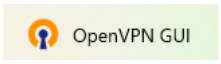
   In the user's OpenVPN client configuration file, in the `remote <private IP address>` line, replace the private IP address with the Elastic IP address.

✔ **Note:** This step applies to all scenarios for the client machine, whether it's a first-time OpenVPN installation, or the addition of a new VPN, or the addition of a new user on an existing VPN configuration. #. Connect to the VPN:

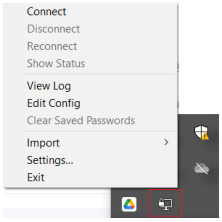
---

3. Connect to the VPN:

   1. On the remote client machine, launch the OpenVPN client GUI.

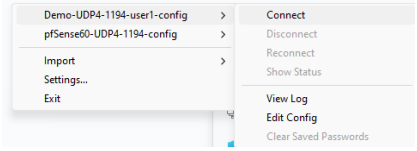
      On the first launch of the OpenVPN client GUI, the OpenVPN icon is added to the system tray:

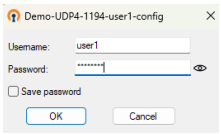
   2. Right-click the **OpenVPN** icon in the system tray.

      The OpenVPN client menu opens.

      - If a single VPN is configured on the client machine, click **Connect**.
      - If there are multiple VPNs configured on the client machine, select the desired VPN and click **Connect**.

3. Sign on using the user credentials that were defined earlier in the pfSense web client's **System > User Manager** configurations.

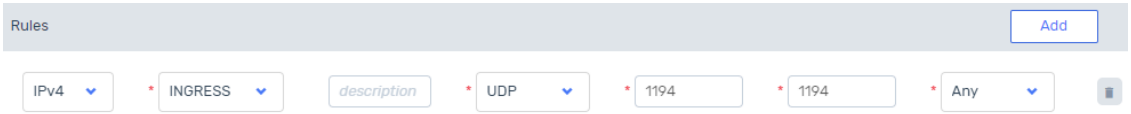


17.2.3 Security hardening configuration

1. Change default passwords to non-default ones.
2. Update the VPC Security Group to block non-essential ports.

   The OpenVPN Service requires the following port for normal operations:

   - UDP port 1194 for OpenVPN access



   Additional ports might be needed for applications running on VPC VM instances.