Date published: 15.06.2018	Estimated reading time: 20 minutes	Authors: Editorial Team

The bookmarks and navigation in this tutorial are optimized for **Adobe Reader.**

How to set up a Virtual Private Cloud (VPC)

Introduction

As you get started with your Open Telekom Cloud (OTC), setting up one or more Virtual Private Clouds (VPC) is one of the first things you will need to do. OTC VPCs form the basis for most of the further work you will be doing to build and configure your OTC environment and resources.

Who should read this tutorial?
This tutorial was created for new OTC users. It is designed and structured to help new users quickly get acquainted with what OTC VPCs are, how to set them up and how to modify them. Working through and understanding the steps and related settings in this tutorial is foundational for understanding the fundamentals of OTC VPCs.

What will you gain from reading this tutorial?
In this tutorial, you will learn how to create a basic *default* VPC in easy-to-understand steps. You will learn about the individual resources and their default settings that make up a default VPC. You will also learn how to modify a default VPC once it has been created.

Default VPCs are designed to make it easy for you to set up networking for your OTC environment. A default VPC is quick and easy to create and ready for you to use, which means for many user scenarios you often don't have to change any of the default settings. This makes a default VPC suitable for getting started quickly, and it will usually suffice for launching public instances such as a blog or simple website.

At the end of this tutorial, under Further Resources, you can find plenty of additional how-to/help material in the form of video tutorials, user guides and application programming interface (API) reference guides.

Prerequisites

You will need the following in order to set up a VPC:
- Login access to your OTC account.
- In your OTC account, OTC user permissions to access the **Network** service console and create a VPC.

Step 1: Overview

Understanding what a VPC is
A virtual private cloud (VPC) is an isolated, on-demand configurable pool of shared computing resources allocated within a public cloud environment – in this case, your OTC account. The virtual resources that make up a VPC of one OTC account are securely separated (i.e. isolated) from those in other OTC accounts. This is the case regardless of whether the OTC accounts belong to the same customer or different OTC customers. In an OTC environment, this is achieved by reserving a separate IP address range for each individual VPC, which only the user in question can access. This prevents other users of other VPCs from accessing the services stored there – even accidentally.

Setting up a VPC is a basic yet very effective security measure. It means you are setting up your own exclusive cloud datacenter within your OTC environment. With your own VPC, you reserve a private, secure IP address range within the OTC that belongs solely to you.

Understanding what you can do with a VPC
An OTC VPC enables you to deploy your OTC resources into a virtual network that you have configured. With your OTC's VPC service, you can provision logically isolated, configurable, and manageable virtual networks for Elastic Cloud Servers (ECSs). You can create security groups and Virtual Private Networks (VPNs), configure IP address segments, and specify bandwidth sizes in your VPC. With a VPC, you can manage and configure internal networks and change network configurations, simplifying network management. You can also enhance ECS security by customizing access rules within a single, or across multiple security groups.

Specifically, a VPC enables you to:
- Have full control over your virtual networks, for example, creating your own network.
- Create security groups to improve your network security.
- Assign elastic IP addresses (EIPs) for use in a VPC, and bind them to ECSs in your VPC to connect the ECSs to the Internet.
- Connect a VPC to your data center using a VPN for smooth application migration to the cloud.
- Communicate with other VPCs using VPC peering connections.

The figure below illustrates a typical topology of a VPC of several ESCs that access the internet through a VPN. The topology utilizes many of the VPC resources required for configuring the scenarios listed above.
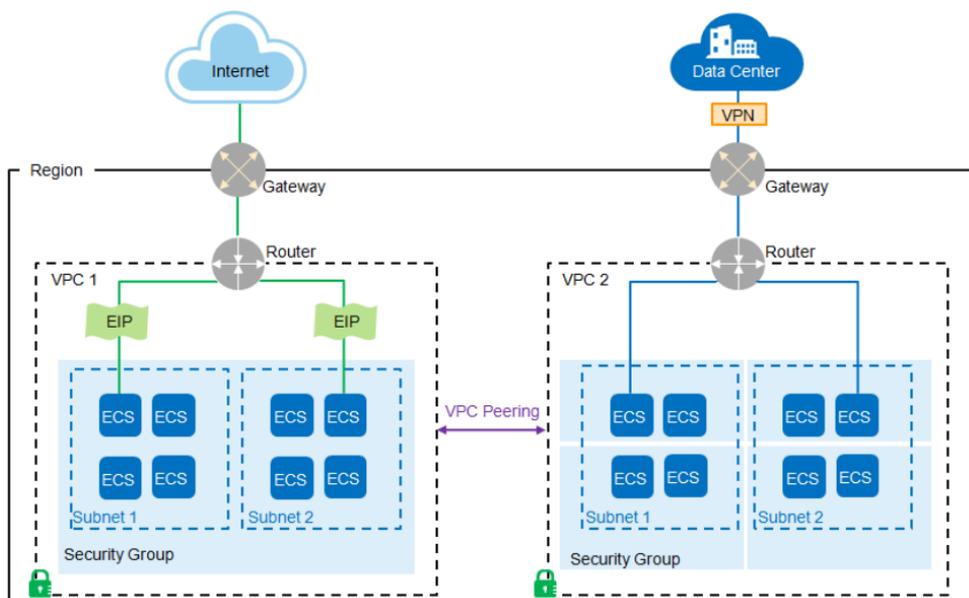
Overview of VPC resources

Step 2: Log into your OTC account

The first thing you need to do is log into your OTC account. After you log in, the first thing you will see is your **Management Console** homepage, which is pictured below.
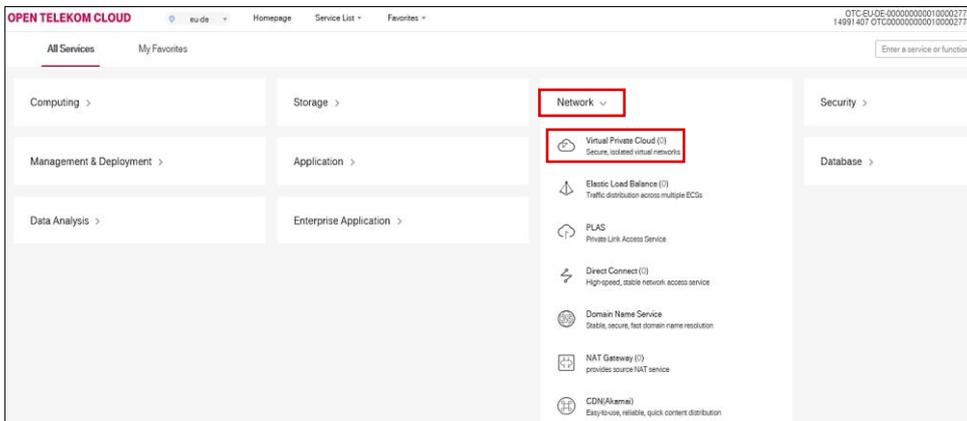
Your OTC account's Management Console homepage

Management Console homepage
The **Console** homepage is the first thing you see when you log into one of your OTC accounts.

Individual Service Consoles
The **Console** homepage provides an over-view of the individual service consoles. Clicking on a service console will expand it to display its specific services.

On the **Console** homepage pictured here, the *Network* service console has been ex-panded to display its services, which in-cludes *Virtual Private Cloud*.

On your **Management Console** homepage, you need to go to your **Network Console** page. To do this, on the homepage, look for the *Network* service console. If it isn't already expanded, as highlighted in red on the **Management Console** homepage pictured above, click on it to expand. Then click on *Virtual Private Cloud*.

Step 3: How to create a default VPC

Clicking on *Virtual Private Cloud* in step 1 will take you to the **Network Console**, pictured below.
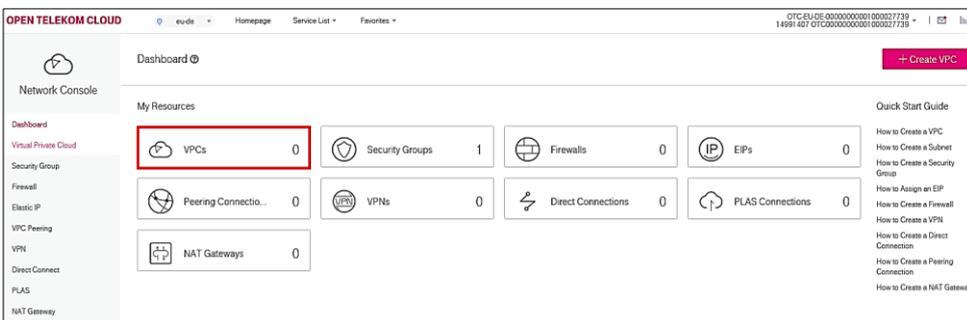
Network Console page

Network Console page
Clicking on *Dashboard* at the top of the navigation pane on the left-hand side of the screen will give you an overview of all the resources that are available in the **Network Console**.

Under *My Resources*, the dashboard over-view will show you the status of each avail-able resource.

On the **Network Console** page pictured here, the status of VPCs, which is highlighted in red, is currently zero. This means that no VPCs have yet been set up. Now follow the steps below to set up a VPC.

a. Click on the magenta *+Create VPC* button in the upper right-hand corner of the Network Console screen.

b. A new *Create VPC* browser window should open displaying the *Basic Information* and *Subnet* settings of the new VPC. Both groups of setting are pictured and explained below in detail. It is important to understand that most of these settings have already been configured by default.

Create VPC page (upper half)
The upper half of the **Create VPC** page (pictured here) shows the **Basic Information settings**. These consist of Region, Name, CIDR Block and Tag.

These settings are briefly explained directly below.

Further below, the bottom half of the **Create VPC** page, which contains the **Subnet** settings, is pictured and the setting are explained.

Create VPC page (upper half): Basic Information settings

The settings in the upper half of the **Create VPC page** pictured below are briefly described below.

- *Region*: Use the region selector to select the desired region. In the example above, the region *eu-de* has been selected by default. A region is a geographical area where you can run your VPC service. Each region comprises one or more availability zones (AZs) and is completely isolated from other regions. AZs in the same region can communicate with one another through an internal network, while those in different regions cannot communicate with one another through an internal network.

- *Name*: This specifies the name for the new VPC. A default name is automatically created. You can leave this as is or select a new name. You can also modify this later on after VPC has been created

- *CIDR Block:* This specifies the Classless Inter-Domain Routing (CIDR) block for the VPC. When you create a VPC, an IP address range for the VPC must be specified. This is done in the form of a CIDR block. **The CIDR block specified here is the primary CIDR block for your VPC**. The following VPC CIDR blocks are supported:

  - 10.0.0.0/8–24
  - 172.16.0.0/12–24
  - 192.168.0.0/16–24

When you click on the magenta *+Create VPC* button to create a new VPC, a default VPC CIDR block is automatically configured. In the Create VPC screen pictured above, the default CIDR block has been set to *192.168.0.0/16*. This corresponds to one of the three supported VPC CIDR blocks listed directly above.

  NOTE: When creating a VPC, you can leave the default VPC CIDR block setting as is or change it. You can also change the setting any time after a VPC has been created. If you change the value, however, you must make sure it is within the range of the supported VPC CIDR blocks listed above. Also, you must ensure that the CIDR settings of all subnets in the VPC are within the range of the new VPC CIDR settings you want to set. Please see below for more about subnet CIDR settings.

- *Tag*: This specifies the VPC tag, which consists of a key and value pair. A tag identifies a cloud resource and facilitates its identification and administration. In this case, a VPC tag identifies the VPC you are now creating.

Tags can be added to VPCs to facilitate VPC identification and administration. You can add a tag to a VPC when creating the VPC. Alternatively, you can add a tag to an existing VPC on the VPC details page (under *My Resources* on the **Network Console** page). You can add a maximum of ten tags to each VPC.

When it comes to creating and using tags, please keep the following best practices in mind:

  - **You can tag VPCs when creating them or later on**. You are not required to tag VPCs when you create them. That is, you can leave the tag key and tag value fields empty in the *Basic Information* settings and still create a VPC. This will result in the VPC not being tagged. As just mentioned above, you can create a VPC <u>without</u> a tag and then, later on, add a tag it.

  - **Get in the habit of tagging your VPCs (as well as your other OTC resources)**. You should make a habit of using tags to help you categorize, identify and manage your cloud resources. Using

tags quickly starts to make real sense as soon as you start to build your cloud environment by creating and using more and more cloud resources.

- **Use the predefined tag function provided by the Tag Management Service (TMS)**. It is important to remember that you can create up to 10 VPCs. And for each VPC, you can create and add up to 10 tags. There is range of other resources in your OTC environment that you can create and also tag. As a result, it is recommended that you use the predefined tag function provided by TMS to add tags to your resources.

  For users who have many cloud resources, TMS allows them to quickly locate all of their resources with a specific tag. TMS also provides a underlined tag management platform on which you can check, modify, or delete tags. **For more information about understanding and using TMS, check out the following related** user guide.

You are still on the **Create VPC page**. Directly above, the **Basic Information settings** on the upper half of the page were described. The bottom half of the **Create VPC page** contains the **Subnet settings**. The bottom half of the page and the setting are pictured and described below.

Create VPC page (bottom half)
The bottom half of the **Create VPC page** (pictured here) shows the **Subnet settings**.

These settings consist of Subnet Name; CIDR; Gateway; DNS Server Address 1 and 2; and Subnet Tag.

The settings are briefly explained below.

Create VPC page (bottom half): Subnet Settings

NOTE: By default, a subnet is automatically created when you create a VPC. After the VPC has been created, you can modify or delete the subnet as well as create additional ones in the VPC. This screen shows the default subnet settings that, just like the *Basic Information* settings, were automatically created when you clicked on the magenta *+Create VPC* button

- *Subnet Name*: This specifies the subnet name. A default name is automatically created. You can leave this as is or select a new name. You can also modify this later on after the subnet has been created.

- *CIDR*: This specifies the Classless Inter-Domain Routing (CIDR) block for the subnet. Just like with the VPC CIDR Block setting, for which a default IP address range was automatically configured, a default subnet IP address range is automatically configured here for the subnet CIDR block. The default configuration of this value ensures that the allotted subnet IP address range is within the default *VPC CIDR range*.

  When it comes to configuring CIDR settings, please keep the following important points in mind:

  - The CIDR block of a subnet can be the same as the CIDR block of the VPC (for a single subnet in the VPC) or a subset (for multiple subnets in the VPC). If we take the default CIDR block configuration in this tutorial as an example that means the following: the default VPC CIDR block has been set to *192.168.0.0/16.* The default subnet CIDR block has been set to *192.168.0.0/24.* You can now modify these default subnet CIDR setting as follows:
    ➔ The subnet IP address range must be a subset of 192.168.0.0
    ➔ The subnet mask must be an integer from 16 to 28

  - If you want to modify the default CIDR block settings of a VPC, you must ensure that the default CIDR settings of all subnets in the VPC is within the VPC's new CIDR block range. If they are not, you will not be able to modify the VPC CIDR block.

- **Subnet CIDR settings <u>cannot</u> be modified <u>after</u> a subnet has been created**. This means the following:

  ➔ If you want to modify the CIDR settings of a subnet, you will have to delete that subnet and create a new one with the desired CIDR settings. The new subnet CIDR settings must be within the VPC's CIDR block range.

  ➔ If you want to modify the CIDR settings of a VPC, you must ensure that the CIDR settings of all subnets in the VPC are <u>within</u> the VPC's new CIDR block range. If they are not, you will not be able to modify the VPC CIDR block. That means if you want to set a new range for a VPC's CIDR block that does not cover the CIDR settings of all the subnets in that VPC, you will first have to delete those subnets.

- *Gateway*: This specifies the gateway address of the subnet. By default, this is set to ***192.168.0.1***. Just like with the subnet CIDR settings, the gateway address of the subnet <u>cannot</u> be modified after the subnet has been created.

- *DNS Server Address 1*: This specifies the IP address of DNS server 1. By default, the external DNS server address is used and automatically entered for this setting. You can modify this setting later on after you have created the subnet.

- *DNS Server Address 2*: This specifies the IP address of DNS server 2. By default, the external DNS server address is used and automatically entered for this setting. You can modify this setting later on after you have created the subnet.

- *Subnet Tag*: Specifies the subnet tag that consists of a key and value pair. You can add a maximum of ten tags to each subnet. Just like with the VPC Tag setting explained above, you can leave this blank and add one or more Tags to this subnet later on. The same best practices apply to this subnet Tag setting that apply to the VPC Tag setting.

c. Click on the magenta ***Create Now*** button at the right-hand bottom of the **Create VPC page** to create the VPC. After only a few seconds the screen should confirm that the VPC has been created and then automatically take you back VPC service page in the Network Console, pictured below.

VPC service page
The **VPC service page**, pictured here, is in the **Network Console**. The VPC that was just created, which is named ***vpc-1784***, is listed here (highlighted in red).

VPC service page in the Network Console

This completes the creation of a simple default VPC. **For each OTC account, you can create a maximum of 10 VPCs**. This is a default limit and applies to each OTC account. This is one of several default limits related to the available VPC resources in your OTC account. These default limits are listed and described below in the section called VPC Limitations.

# Step 4: How to modify a default VPC

Clicking on the VPC name in the **VPC service page** picture above will provide you with an overview of the newly VPC's configuration, which is pictured below.
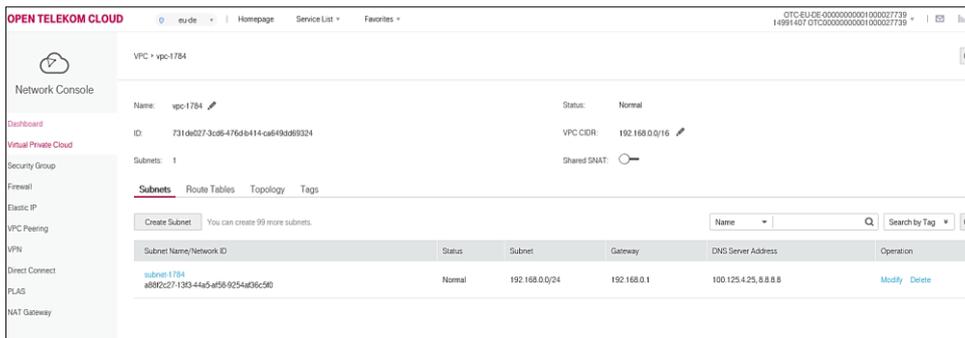
The overview pictured here shows the VPC's current configuration. Each element of the configuration shown on the screen is briefly explained below.

Overview of the newly created VPC's configuration

a. **Name**: The VPC's name is currently **vpc-1784**. This setting can be modified.
b. **ID**: Specifies the VPC ID, which uniquely identifies the VPC. This setting cannot be modified.
c. **Subnets**: This specifies the current number of subnets in the VPC, which in this example is one. By default, one subnet is automatically created when a VPC is created. **For each OTC account, it is possible to create a total of 100 subnets**. This is one of several default limits related to the available VPC resources in your OTC account. These default limits are listed and described in the next section.

   • The one default subnet that was created along with this VPC is named **subnet-1784**. It is listed at the bottom of the VPC configuration screen pictured above.

   • This subnet can easily be deleted by simply clicking on the **Delete** button.

   • It can also be modified by clicking on the **Modify** button. As already explained above in the subnet settings in step 3, the only subnet settings you can change are its name and DNS Server Addresses.

d. **Status**: This specifies the current status of the VPC, which in this example is NORMAL. The following statuses are possible for a VPC: CREATING, NORMAL, DOWN, PENDING UPDATE, PENDING DELETE, or ERROR.
e. **VPC CIDR**: This shows the VPC's current CIDR block. The VPC CIDR settings were explained in detail above in step 2. Please refer to them before you decide to modify this setting.
f. **Shared SNAT**: This specifies the shared Source Network Address Translation (SNAT) function. The Open Telekom Cloud's VPC service provides free, shared SNAT. This allows ECSs to use a limited number of public IP addresses to gain one-way access to the Internet for operations, such as updating software. However, Internet users cannot directly access the ECSs. For more about the working principles of shared SNAT and how to use it with your VPCs, click here.
g. **Route Tables**: A route table contains a set of rules that are used to determine where network traffic is directed. You can add routes to a route table to enable other ECSs in a VPC to access the Internet through the ECS that has a bound Elastic IP. For more about route tables and how to use them, click here.
h. **Topology**: This is a very helpful feature that provides a visual overview of the VPC's configuration. A screenshot of the default VPC created in this tutorial is picture below.
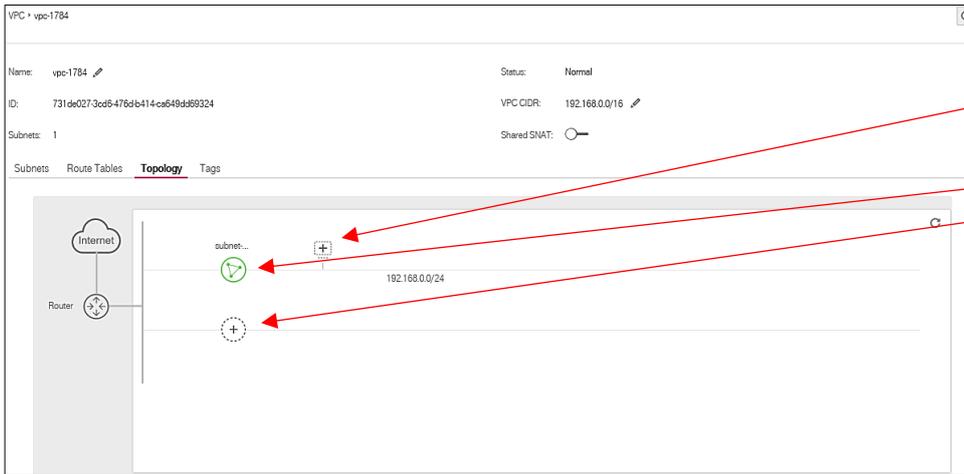
For each VPC you create, you can use the **Topology** feature to do the following:

- Click to add an Elastic Cloud Server (ECS) to an existing subnet.
- Click to modify existing subnets.
- Click to create a new subnet.

Overview of the newly created VPC's topology

i. ***Firewalls and Security Groups***: On the left-hand navigation pane of the VPC's configuration pictured at the start of this section are a number of network features that you can configure and add to the VPC. These include firewalls and security groups.

- Firewalls and security groups are provided to monitor the VPC service and improve VPC security. This is extremely important when you start adding and building Elastic Cloud Servers (ECSs). For an overview about the differences between firewalls and security groups, click here.

- A security group is a collection of access control rules for ECSs that have the same security protection requirements and are mutually trusted in a VPC. After a security group is created, you can create different access rules for the security group to protect the ECSs that are added to this security group. The default security group rule allows all outgoing data packets. ECSs in a security group can access each other without the need to add rules. For more about security groups and how to crate and configure them, click here.

- A firewall consists of one or more access control lists (ACLs). Based on inbound and outbound rules, the firewall determines whether data packets are allowed in or out of any associated subnet. You can create a custom firewall. By default, a newly created firewall is disabled. It does not have subnets associated with it nor does it have any inbound or outbound rules. Each user can create a maximum of 200 firewalls by default. For more about firewalls, click here.

- ***Tags***: This specifies the number of tags you have created for this VPC. As already explained in step 3, you do not need to create a tag when you create a VPC. Rather, you can create and add up 10 tags to an existing VPC any time later on. To do so, simply click on the ***Tags*** tab on the VPC service page and then click on the ***Add*** button. Please remember to review the best practices about VPC tags explained in step 3.

VPC Limitations

For each OTC account (tenant), there are limits to the number of VPC resources that you can utilize. These resources and their default limits are listed below. The default limits (quotas) are automatically generated by Deutsche Telekom during the setup and provisioning of the account. They apply for each OTC account (tenant) and can be increased

You can request an increase for some of these limits.

Resource	Default limit per OTC account (tenant)	Comments
VPC	10	By default, one tenant can create a maximum of 10 VPCs.
Subnet	100	By default, one tenant can create a maximum of 100 subnets. If the number of subnets does not meet your service requirements, submit a work order to increase the quota.
Security Group	100	By default, a tenant can create a maximum of 100 security groups
Security Group Rule	500	By default, a tenant can create a maximum of 500 security group rules. An excessive number of security group rules increase network latency of the first packet. It is recommended that you add a maximum of 50 rules for each security group.
Elastic IP (EIP)	10	By default, one tenant can create a maximum of 10 EIPs.
VPN	5	By default, one tenant can create a maximum of 5 VPNs.
VPN Gateway	2	By default, one tenant can create a maximum of 2 VPN Gateways.
VPN Peering Connection	50	A tenant can have a maximum of 50 VPC peering connections in one region. Accepted VPC peering connections consume the quota of both owners of a VPC peering connection. A VPC peering connection consumes the quota of only the requester (tenant of the local VPC).
Firewall	200	Each tenant can have a maximum of 200 firewalls. It is recommended that you configure a maximum of 20 inbound or outbound rules for each firewall. If more than 20 inbound or outbound rules are configured, the forwarding performance will deteriorate.

If the default quotas listed above do not meet your service requirements, you can submit a work order to increase a quota. For more information on how to submit a work order, click here.

Conclusion

By following this step-by-step tutorial, you should be able to quickly and easily create a default VPC. While default VPCs may not be ideal for a robust production environment, they often are suitable for small non-critical single tier applications and related user scenarios. Once new OTC users become familiar with the technology and resources that make up a default VPC, they can then begin to modify their default VPC configurations and even create custom (non-default) VPCs for production use. OTC provides plenty of help resources on VPCs. Please check out the list of help videos and documentation listed below under Further Resources.

Further Resources

A range of related and helpful resources is available and listed below.

- **Related Video Tutorials**
    - Create a VPC for accessing the internet through a VPN
    - How to create your own network in the Open Telekom Cloud – with just a few simple clicks

- **Related User / API Reference Guides**
    - Virtual Private Cloud User Guide
    - Virtual Private Cloud API Reference Guide

- **Open Telekom Support**
    - Toll-free hotline Germany: 0800 33 04477 (Monday through Friday, 8:00 – 17:00 CET)
    - Toll-free hotline international: 0800 445 566 00 (Monday through Friday, 8:00 – 17:00 CET)
    - Email: cloud-products@telekom.de

List of Abbreviations

- ACL: Access Control List
- API: Application Programming Interface
- AZ: Availability Zone
- CIDR: Classless Inter-Domain Routing
- DNS: Domain Name Service
- ECS: Elastic Cloud Service
- OTC: Open Telekom Cloud
- SNAT: Source Network Address Translation
- TMS: Tag Management Service
- VPC: Virtual Private Cloud

Document History

Version	Date	Changes	Author
1.0	15.06.2018	Initial version	Editorial Team