Date published: 30.08.2018 Estimated reading time: 20 minutes Authors: Editorial Team

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

How to set up an IPsec VPN connection

1. Introduction

This tutorial provides Open Telekom Cloud (OTC) users with a step-by-step overview of how to create an Internet Protocol Security (IPsec) Virtual Private Network (VPN) connection between their OTC account and a remote network such as a company or home network.

Who should read this tutorial?
This tutorial was created for both new and existing OTC users who need to start setting up secure VPN connections between their OTC account and their company or home network. It is designed and structured to help users quickly get acquainted with what OTC VPNs 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 VPNs.

What will you gain from reading this tutorial?
In this tutorial, you will learn how to create a basic *default* VPN in easy-to-understand steps. You will learn about the individual features and default settings that make up a default VPN. A default VPN 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.

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.

2. Prerequisites

You will need the following in order to set up your IPsec VPN connection:

- **Internet Protocol Version 4** (**IPv4)**: Currently, the type of internet protocol communication over a VPN connection that OTC supports is IPv4. IPv6 (Internet Protocol Version 6) support for VPN is not possible. Please check to make sure that your internet connection supports IPv4.

- **Site-to-site / hub-and-spoke VPN:** Currently, the types of VPN connection that OTC supports are site-to-site and hub-and-spoke VPN. The next section briefly describes these two types of VPN connections. Please check to make sure that your network firewall or router supports site-to-site VPN.

- **Internet Protocol Security (IPsec) VPN**: Currently, the type of VPN protocol that OTC supports is Internet Protocol Security VPN (IPsec VPN). That means that your company or home network (router or firewall) must also support IPsec VPN. The next section briefly describes what an IPsec VPN is. Other types of site-to-site connections including Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2TP) are not supported.

- **Virtual Private Cloud (VPC)**: You will need to have already created at least one Virtual Private Cloud (VPC) in your OTC account. Please see directly below to understand more about how to create VPCs.

If you have determined that your network meets the prerequisites listed above and you have also already set up at least one Virtual Private Cloud (VPC) in your OTC account, please now proceed to the next section, which provides a step-by-step walkthrough for setting up a VPN connection. If you have not yet set up a VPC, please continue reading the prerequisite information below.

First thing's first: Before you can set up a VPN in your OTC account, you first need to create a VPC.
A VPC is a private, secure network environment in which you can define and create the virtual networks you need. It is essentially your own exclusive cloud datacenter within the OTC. A VPC forms the basis for most of the further work you will be doing to set up and configure your environment and resources in the OTC. With your own VPC, you reserve a private, secure IP address range within the OTC that belongs solely to you. A VPC is a basic yet extremely important security measure to prevent unauthorized access to your cloud resources. **Every OTC user who wants to create a VPN requires at least one VPC.**

Once you have created at least one VPC in your OTC account, you can connect it with other external networks. These include not only public networks such as the internet, but also private ones such as a company or home network. And to do this, you need to set up a VPN. Your VPN thus connects your VPC with other external networks.

The OTC provides plenty of helpful information on gaining a better understanding of VPCs and how to create, configure and use them. The process of setting up and configuring a VPC is covered extensively in separate tutorials. For a simple step-by-step guide to creating a VPC, check out this tutorial. For more detailed information on VPCs, please see the links provided under Further Resources at the end of this tutorial.

Once you have set up a VPC, please proceed with the steps below for setting up a VPN.

3. Setting up an IPsec VPN connection

a. Step 1: Understand what an IPsec VPN is and what you can do with it

Understanding what an IPsec VPN is

By default, resources you configure and launch into a VPC in your OTC account cannot communicate with your own remote network. One of the most common and secure methods you can use to enable access to your remote network from your VPC is by creating a VPN connection.

Simply put, a VPN connection refers to the connection between a VPC in your OTC account and your own remote network. OTC supports IPsec VPN. An IPSec VPN is a standards-based, encrypted tunneling technology that uses encrypted security services to establish confidential and secure communication tunnels between different networks (in this case, between your OTC account and your remote network).

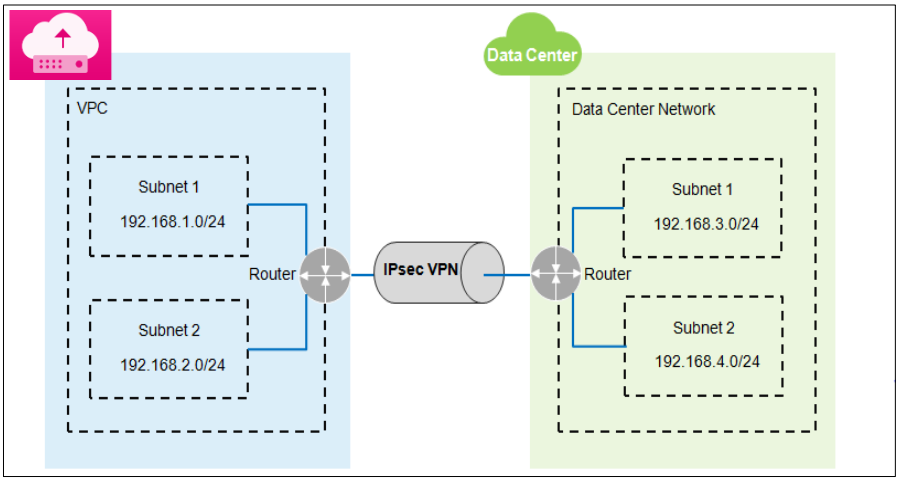
Understanding what you can do with a VPN

By default, Elastic Cloud Services (ECSs) in a VPC cannot communicate with your datacenter or private network. To enable communication between them, you need to use a VPN.

Specifically, a VPN connection enables you to do the following:

- With a VPN between a VPC in your OTC account and your datacenter, you can easily access and use an ECS and block storage resources provided in your OTC environment.
- You can migrate applications to the cloud and deploy additional web servers to increase the computing capacity in your network.
- You can build and develop a hybrid cloud environment, which reduces IT operations and maintenance costs and protects enterprise core data from being leaked.

The figure below illustrates a typical topology of a simple IPsec VPN connection between a VPC in a customer's OTC account and the customer's datacenter. In the customer's OTC account, a VPC has been created that has two subnets, 192.168.1.0/24 and 192.168.2.0/24. There are also two subnets on the router deployed in the customer's datacenter, 192.168.3.0/24 and 192.168.4.0/24. It is now possible to create an IPsec VPN to securely connect the VPC subnets to the datacenter subnets.



Topology of a simple IPsec VPN connection between a VPC in an OTC account and a remote network

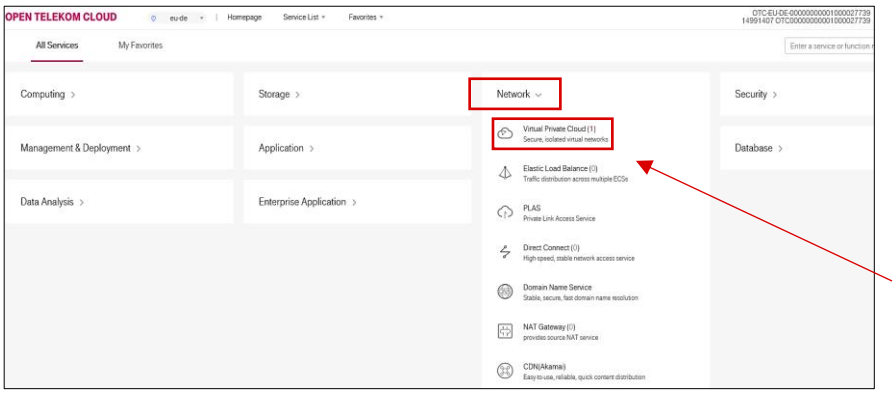
OTC currently supports **site-to-site VPNs** and **hub-spoke VPNs**.

- Site-to-site VPN: The local side is a VPC on the public cloud platform, and the remote side is the user data center. A site-to-site VPN establishes a communications tunnel between a user data center network and a single VPC.

- Hub-and-spoke VPN: The local side is multiple VPCs on the public cloud platform, and the remote side is the user data center network. A hub-and-spoke VPN establishes a communications tunnel between a user data center network and multiple VPCs.

b. Step 2: Go to the Network Service Console in your OTC account

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



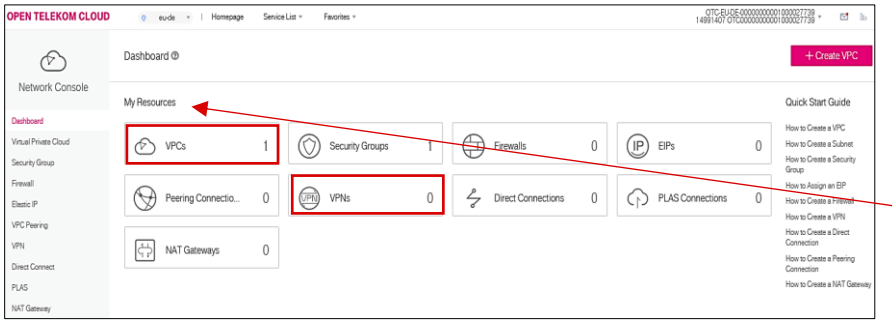
Your OTC account's Management Console homepage

- **Management Console homepage**
  The first thing you will see after accessing your OTC account is your **Management Console** homepage.
- **Individual Service Consoles**
  The **Console** homepage provides an overview of the individual service consoles. Clicking on a service console will expand it to display its specific services.
- **Network Service Console**
  On the **Console** homepage pictured on the left, the Network service console has been expanded to display its services, which includes Virtual Private Cloud.

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

c. Step 3: Create a default IPsec VPN in your VPC

Clicking on ***Virtual Private Cloud*** in step 2 above will take you to the **Network Console** dashboard, pictured below.



The Network Console page

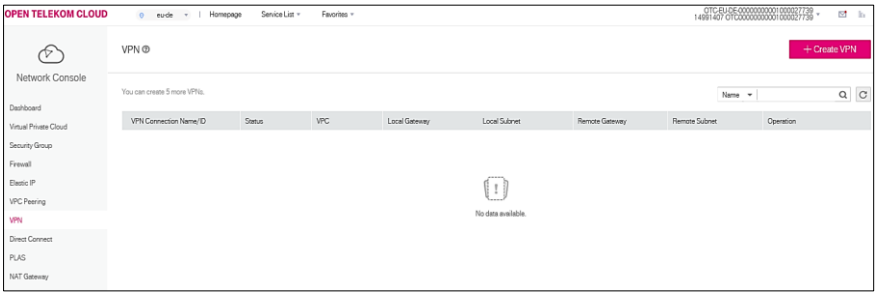
- **Network Console page**
  Clicking on dashboard at the top of the navigation pane on the left-hand side of the screen will give you an overview of all the resources that are available in the **Network Console**. These include VPC and VPN.
- Under ***My Resources***, the dashboard overview shows you the status of each available resource. This includes the current number of VPCs and VPNs that have been configured.

On the **Network Console** page pictured above, both the current number of VPCs and VPNs that have been created can be seen. Both are highlighted in red and located directly under ***My Resources***. In this example, the current number of VPCs is one, while the current number of VPNs is still zero.

Since at least one VPC has already been created, you can now begin to create a default VPN. As explained above under Prerequisites, it is important to understand that part of the step-by-step process described below for creating a VPN requires you to allocate it to an existing VPC.

Now follow the steps below to set up a VPN.

(1) Create a VPN: To create a VPN, start by clicking on VPN in the navigation pane on the left side of the **Network Console** page (pictured above). This will take you to the **VPN service page**, which is pictured below. The **VPN service page** is where you need to go to view the status of and modify any existing VPNs as well as create new VPNs. By default, OTC allows you to create a maximum of 5 VPNs in each OTC account.

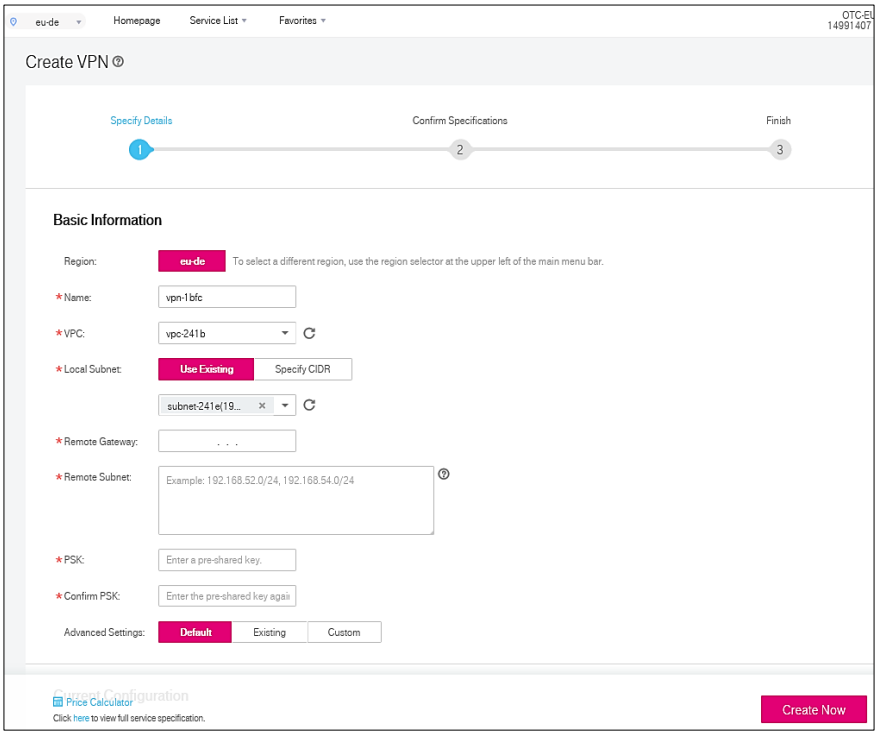


The VPN service page

- **The VPN service page**
  The **VPN service page**, pictured here, is one of the services contained in the **Network Console**. The page allow you to view the status of and modify existing VPNs as well as create new VPNs.
- On the page pictured here, there are currently no existing VPNs.

(2) Now click on the magenta ***+Create VPN*** button, which is easy to spot in the upper right-hand corner of the **VPN service page** pictured above.

(3) Clicking on the ***+Create VPN*** button will open a new browser window displaying the **Create VPN page** pictured below.



The Create VPN page

- **The Create VPN page**
  This page contains a number of basic and advanced settings for your new VPN. These settings will allow you to specify the necessary parameters of your VPN.

- Below, the basic and advanced setting are briefly explained.

(4) **Basic Information Settings** (under Basic Information on the Create VPN page pictured above)

- *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 VPN. A default name is automatically created and entered here. You can leave this as is or select a new name of your choice.
- *VPC*: This specifies which VPC the new VPN will connect to. As already explained above under Prerequisites, you will need to have already created at least one VPC before you can create a VPN. In this example, the only existing VPC with the name **vpc-b379** has been entered by default. If you have created more than one VPC, you can specify here which one you would like the new VPN to connect to.
- *Local Subnet*: Starting here, it is important to understand the difference between Local and Remote settings. Local always refers to the settings in your OTC account. Remote always refers to the settings in your external network (i.e. such as your company network). For this setting Local Subnet, we are referring to the subnet setting in your OTC account. This specifies the VPC subnets that need to communicate with your company or private network. Here, you have a choice between using an existing local subnet or specifying a new Classless Inter-Domain Routing (CIDR) block.
  - *Use Existing*: Select this option if you want to use the existing subnet of the VPC you have selected. When you create a VPC, a default subnet is created automatically. If required, you can create additional subnets for each VPC. For an overview on to do create additional subnets, click here.
  - *Specify CIDR*: Alternatively, you can opt to create a new Classless Inter-Domain Routing (CIDR) block for the VPC you have selected for the VPN to connect to. Specifies the CIDR block for the subnet. This value must be within the VPC CIDR range.

- *Remote Gateway*: This specifies the public IP address of the VPN in your company or home network. This IP address is used for communicating with the VPN in the VPC.
- *Remote Subnet*: This specifies the subnets of your company or home network for communicating with the VPC. The remote and local subnets cannot have overlapping or matching CIDR blocks. The remote subnet CIDR block cannot overlap with CIDR blocks involved in existing VPC peering connections created for the local VPC.
- *PSK* (pre-shared key): This specifies the pre-shared key. The value must be a string of between 6 and 128 characters. This value must also be the same on both ends of the VPN. That is, the value entered here must match with the value you enter when configuring the VPN connection in your company or home network.
- *Confirm PSK* (pre-shared key): Here, you need to confirm the PSK value.

(5) **Advanced Settings**: The advanced settings consist of the IKE (Internet Key Exchange) and IPsec policy options. The IKE policy specifies the encryption and authentication algorithms to use in the negotiation phase of an IPsec tunnel. The IPsec policy specifies the protocol, encryption algorithm and authentication algorithm to use in the data transmission phase of an IPsec tunnel. These policy options must be the same for the VPN in your VPC and the VPN in your company or home network. If they are different, the VPN tunnel cannot be set up. As a result, you must ensure that the VPN in your VPC and the VPN in your company or home network use the same IKE and IPsec policy configurations.

The advanced settings give you three main configuration options to choose from: ***Default, Existing*** and ***Custom***.

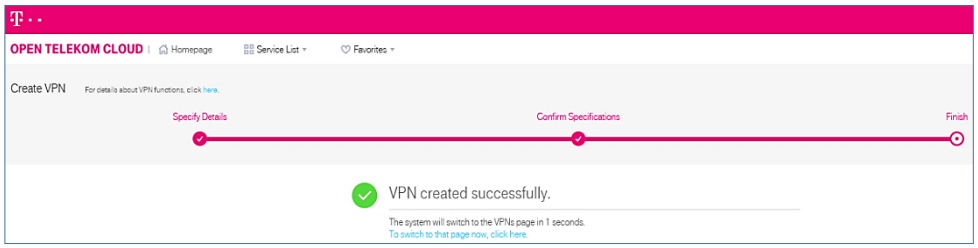
- *Default*: This specifies that a default configuration for IKE and IPsec policies will be created and used.
- *Existing*: This specifies that existing IKE and IPsec policies you have already defined for the VPC will be used.
- *Custom*: This allows you to customize the IKE and IPsec policies. Clicking on Custom will let you configure each of the available IKE and IPsec policy options.

For detailed information about all of the basic and advanced settings listed here and how to configure them, click here.

Once you have configured all of the basic and advanced settings, click the magenta ***Create Now*** button at the bottom right-hand of the screen of the **Create VPN page** (pictured above in step 3).

(6) Your screen should now show a ***Confirm Specifications*** overview of your configuration. Confirm your VPN configuration by clicking on the magenta ***Submit*** button. An IPsec VPN will now be created, and a public network egress IP address will be assigned to it. The IP address is the local gateway address of a created VPN on the **Network Console**. When configuring the peer tunnel in your company or home network, you must set the remote gateway address to this IP address.

(7) This will take you to the screen below, informing you that your VPN has been created successfully. You will then be automatically switched back to **Network Console page**.



Screen showing that your new VPN hast been created successfully

(8) You are now back in the **Network Console**, which shows your newly configured VPN. The status of your VPN will show ***Not connected***. This means that while the VPN has been configured on the local (i.e. OTC) side, you still need to configure it on the peer (i.e. remote) side.

Note: Due to the symmetry of the tunnel that is required for a VPN connection, you also need to configure the IPsec VPN on your router or firewall. In step 4 below, we provide some guidance and examples to help you with this.

d. Step 4: Tips for setting up an IPsec VPN in your remote network

Now that you have created a default IPsec VPN in one of your VPCs, you need to create an IPsec VPN in your remote (i.e. company or home) network. You also must ensure that the VPN in your remote network uses the same IKE and IPsec policy configurations that you have set for the VPN in your VPC. Once this has been achieved, the two VPNs should connect to establish a VPN connection.

After the IPsec VPN is created, a public network egress IP address is assigned to the IPsec VPN. The IP address is the local gateway address of a created VPN on the **Network Console**. When configuring the peer tunnel in your data center or home network, you must set the remote gateway address to this IP address.

When configuring the VPN in the router or firewall of your company or home network, make sure that the following requirements are met:

The Access Control List (ACL) of the remote firewall/router must be configured to allow a connection to the Open Telekom Cloud VPN remote gateway.

- The local and remote subnets cannot overlap.
- Different local subnets cannot overlap.
- The local and remote sides use the same IKE policy.
- The local and remote sides use the same IPsec policy.
- The local and remote subnet and gateway parameters must be symmetric.
- The local and remote sides use the same PSK.
- The ECS security group in a VPC allows traffic from and to the remote side.
- After a VPN is created, its status changes to Normal only after the ECSs or physical servers on the two sides of the VPN communicate with each other.

Please see below under Further Resources for further details about configuring a remote device for your OTC VPN and a list of protocols supported by VPN connections.

4. VPN Limitations

For each OTC account (tenant), there are limits to the number of VPC, VPN and other resources within the **Network** service console that you can utilize. These resources and their default limits are listed in the table below. The default limits (quotas) listed in the table below 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.

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.

5. Conclusion

By following this step-by-step tutorial, you should be able to create and configure a VPN both in your OTC account as well as in your company network, and then establish a VPN connection between the two networks. Once OTC users become familiar with the features and steps required to set up a default VPN, they can then begin to modify their default VPN configurations and create non-default VPNs.

If, after carefully following the steps described in this tutorial, you are still not able to establish a VPN connection, please check out the extensive list help video and documentation listed directly below under Further Resources.

6. Further Resources

A range of related and helpful OTC resources on IPsec VPN connections is available and listed below.

- **Related tutorials**
  - VPN between a CISCO Router and the Open Telekom Cloud
  - Extend your cloud and your options - creating a Virtual Private Network VPN connection between Open Telekom Cloud and DSI vCloud
  - Virtual Private Network: Open Telekom Cloud optimal nutzen (German only)

- **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 in the OTC Help Center**
  - Virtual Private Cloud User Guide (includes extensive “how to” info on VPN)
    - VPN Application Scenarios
    - Creating a VPN
    - Configuring the Remote Device for a VPN, with two detailed examples:
      - Configuring the VPN on a Huawei USG6600 Series Firewall
      - Configuring the VPN on a Cisco 2900 Firewall
    - Reference Standards and Protocols for the IPsec VPN
    - Extensive VPC & VPN FAQs

  - Virtual Private Cloud API Reference Guide
    - This guide includes an extensive section on VPNs related to Native OpenStack API. The section describes operations for the VPN services, including creating, querying, deleting, and updating IPsec VPN connections and IPsec policies, creating VPN endpoint groups, VPNs, and IKE policies.

- **Open Telekom Cloud Support**
  - Toll-free hotline Germany: 0800 33 04477 (Monday through Friday, 8:00 – 17:00 CET)
  - Toll-free hotline international: +49 800 445 566 00 (Monday through Friday, 8:00 – 17:00 CET)
  - Email: cloud-products@telekom.de

7. 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
- IKE: Internet Key Exchange
- IP: Internet Protocol
- IPsec: Internet Protocol Security
- L2TP: Layer Two Tunneling
- OTC: Open Telekom Cloud
- PPTP: Point-to-Point Tunneling Protocol
- PSK: Pre-shared Key
- SNAT: Source Network Address Translation
- TMS: Tag Management Service
- VPC: Virtual Private Cloud
- VPN: Virtual Private Network

8. Document History

Version	Date	Changes	Author
1.0	03.08.2018	Initial version	Editorial Team
2.0	30.08.2018	Updated Section 6 (Further Resources) with links to related VPN tutorials (English and German) accessible on www.cloud.telekom.de.	Editorial Team