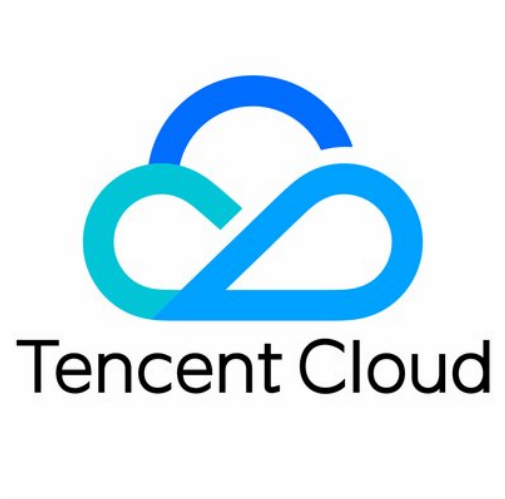
VPN Connections

Operation Guide

Product Documentation



Contents

Operation Guide

Operations Overview

Last updated : 2021-06-15 15:15:24

Through an encrypted public network channel, a VPN connection can facilitate the safe communication between the user IDC and internal office network and Tencent Cloud Virtual Private Cloud (VPC). A VPN gateway provides IPsec VPN connections. You can configure and manage VPN connections, such as viewing monitoring data, modifying VPN tunnels and binding anti-DDoS products, on the VPN console. This document provides the console operation guides of VPN connections.

VPN Gateway
Creating VPN Gateways

Last updated : 2021-06-15 15:22:25

A VPN gateway is a VPN connection instance. Therefore, please create an IPsec VPN gateway before using a VPN connection to securely access the Tencent Cloud Virtual Private Cloud (VPC) from external networks. This document shows you how to create a VPN gateway on the console.

Prerequisites

Please create a VPC network in the same region in advance if you want to create a VPN gateway for VPC. For more information, see Create VPC.

Operation Directions

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Gateway** on the left sidebar to go to the management page.
3. Click **+New** on the VPN gateway management page.
4. Configure the following gateway parameters in the pop-up **Create VPN Gateway** dialog box.

Parameter Name	Description
Gateway Name	Enter the VPN gateway name with 60 characters or less.
Region	Show the region of the VPN gateway.
Associated Network	This shows whether you will create a cloud connect network (CCN) VPN or a private network VPN, which is commonly known as VPN gateway for CCN or VPN gateway for VPC respectively. ◦ Choose **CCN** if you need to use VPN to connect to multiple VPC networks or other direct connect networks. Note: when being created, the VPN gateway for CCN cannot be directly associated with the CCN instance. After it is created, you can edit the associated network on the VPN gateway details page and choose the CCN instance. ◦ Choose **VPC** if you need to use the VPN to connect to a single VPC network.
Network	Choose the private network to be associated with the VPN gateway only when

	the associated network is **VPC**.
Bandwidth Cap	Please set a reasonable bandwidth cap for the VPN gateway according to the actual application scenarios.
Tag	Tags mark VPN gateway resources so that these resources can be queried and managed efficiently. Tag is not a required configuration. You can decide whether to configure it according to your demand.
Billing Mode	Bill-by-traffic mode is supported. This billing mode is applicable to scenarios with significant bandwidth fluctuations.

5. After configuring gateway parameters, click **Create** to create a VPN gateway, and the **Status** will be **In Progress**. About 1-2 minutes later, the status of the successfully created VPN gateway will be **In Service**. The system will assign the VPN gateway a public IP.

Modifying VPN Gateways

Last updated : 2021-06-15 15:25:01

After a VPN gateway is created, the VPN gateway name, tag and bandwidth cap can be modified.

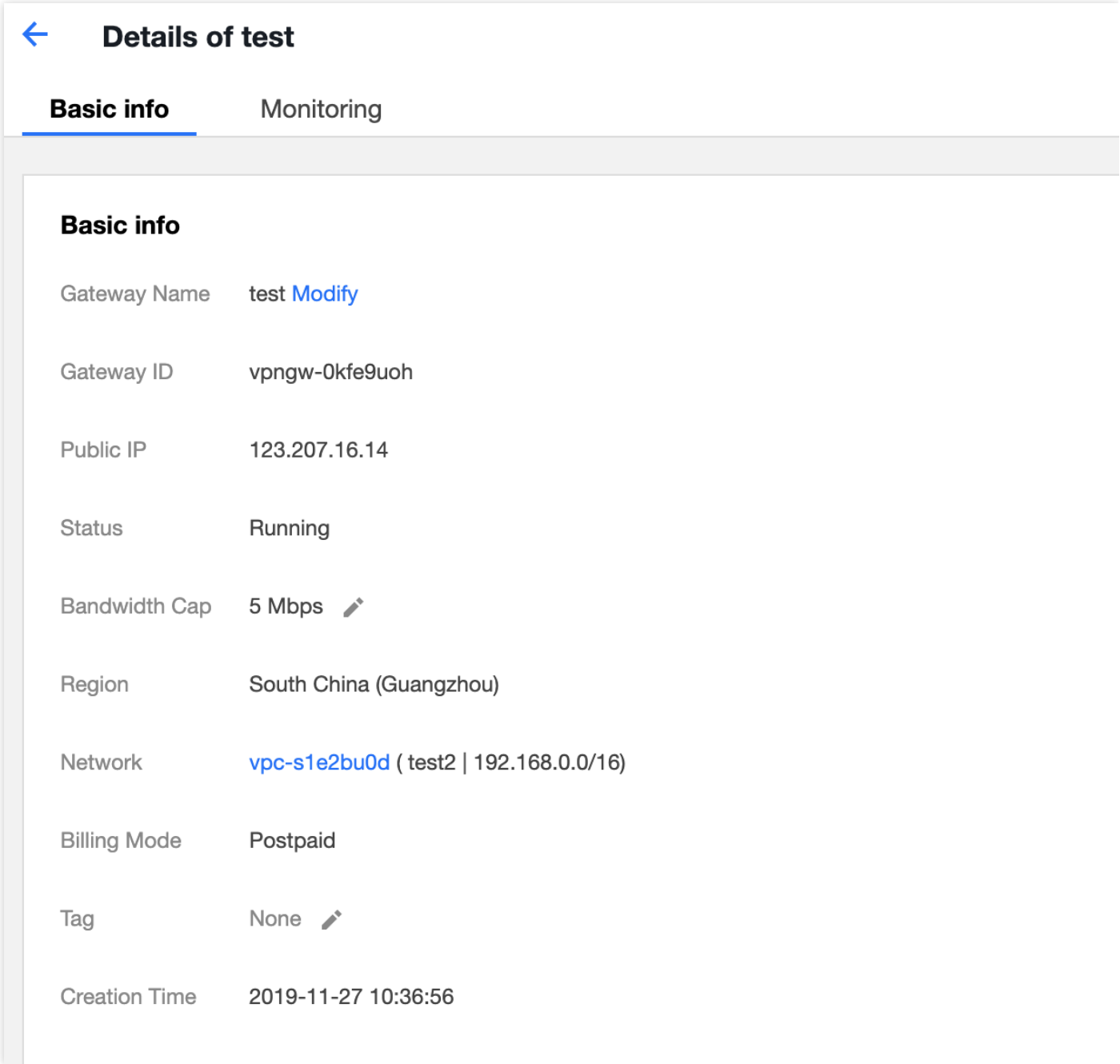
Operation Directions

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Gateway** on the left sidebar to go to the management page.
3. Modify the VPN gateway name on the “VPN Gateway” page.
   - Click the “Edit” icon next to the VPN gateway name to modify the name.
   - Click the gateway ID to go to the gateway details page, and then you can click **Modify** to modify the gateway name.
4. Modify the bandwidth cap.
   - To modify the bandwidth cap of a bill-by-traffic gateway, you can click the “Edit” icon next to the “bandwidth” on the gateway list or directly go to the details page.
5. To modify tags, click **Edit Tag** on the “Gateway List” page or click the “Edit” icon on the gateway details page.

Viewing a VPN Gateway

Last updated : 2021-04-07 15:01:47

1. Log in to VPC Console.
2. In the left sidebar, choose **VPN Connection** > **VPN Gateway** to go to the management page.
3. Click the ID of the target VPN gateway to go to the details page.
4. View the details of the VPN gateway.



Configuring VPN Routing Policies

Last updated : 2021-07-05 11:09:47

Prerequisites

You have completed the configurations of VPN gateway, customer gateway and VPN tunnel before configuring a routing policy.

Directions

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Gateway** on the left sidebar.
3. On the **VPN Gateway** page, select the target region and VPC, and click the **ID/Name** of the VPN gateway to go to its details page.
4. Click the **Route Table** tab.
5. Click **Add a route** and configure routing policies.

Configuration Item	Description
Destination	Enter the IP range of the network to access.
Next hop type	Select **VPN tunnel** or **CCN**. Note: if the VPN gateway for CCN is associates with a CCN instance, the routing policy with **CCN** as the next hop will be automatically obtained and displayed in the route table. Do not manually configure it.
Next hop	Select the instance ID of the next hop. ◦ If you select **VPN tunnel** for the **Next hop type**, select a VPN tunnel that has been created. ◦ If you select **CCN** for the **Next hop type**, the CCN instance associated with the VPN gateway will be automatically displayed.
Weight	Choose the weighted values of VPN tunnels: ◦ 0: high priority ◦ 100: low priority
Add a line	Configure multiple routing policies as needed.
Delete	Delete the routing policies, except for the last one.

6. Click **OK**.
7. Perform other operations as needed.
   i. Enable or disable routing policies.
   ii. Delete the disabled routing policies.

Binding an Anti-DDoS Instance

Last updated : 2020-02-25 18:19:44

1. Log in to Anti-DDoS Pro Console, choose **Resource List**, and select a region.
   - For single IP instances, select the **Single IP Instance** tab.
   - For multi-IP instances, select the **Multi-IP Instance** tab.
2. Find the Anti-DDoS Pro instance to be bound in the list, and click **Change Resource** in the **Operation** column for the instance.
3. Select the associated device type and associated device from the pop-up box. Select **VPN Gateway** as the device type and select the VPN gateway you want to associate from the list.
4. Click **OK**.

Deleting a VPN Gateway

Last updated : 2021-08-06 17:58:08

You can delete VPN gateways that are no longer used.

Prerequisites

- The associated VPN tunnels have been deleted. For detailed directions, see Deleting VPN Tunnel.
- The associated customer gateways have been deleted. For detailed directions, see Deleting Customer Gateways.

Directions

1. Log in to the VPC console.
2. Select **VPN Connection** > **VPN Gateway** on the left sidebar to access the **VPN Gateway** page.
3. Locate the VPN to be deleted, click **Delete** under the **Operation** column, and click **Delete** in the pop-up.

> Note :
> Note that all the associated connections will be immediately interrupted after the VPN gateway is deleted.

Customer Gateway
Creating Customer Gateways

Last updated : 2021-06-15 15:41:26

1. Log in to the VPC console.
2. Click **VPN Connection** > **Customer Gateway** on the left sidebar to go to the management page.
3. Choose the region and click **+New** on the “Customer Gateway” management page.
4. Enter the name of the customer gateway and public IP. Public IP refers to the static public IP of the VPN gateway device of the customer IDC. Configure tags according to demand.
5. Click **Create**. A successfully created customer gateway is shown in the picture below.

Modifying Customer Gateways

Last updated : 2021-06-15 15:43:01

After creating a customer gateway, you can modify the name and descriptions of it.

Operation Directions.

1. Log in to the VPC console.
2. Click **VPN Connection** > **Customer Gateway** on the left sidebar to go to the management page.
3. On the “Customer Gateway” management page, click the “Edit” icon on the right of the gateway name to modify the name, and then click **Save**.
4. Click **Edit Tag** on the right to modify the tag information.

Deleting Customer Gateways

Last updated : 2021-06-15 15:44:23

If you do not use the customer gateway anymore and haven’t created any VPN tunnels, you can delete the customer gateway.

Operation Directions.

1. Log in to the VPC console.
2. Choose **VPN Connection** > **Customer Gateway** on the left sidebar to go to the management page.
3. On the “Customer Gateway” management page, click **Delete** on the right of the customer gateway instance to be deleted.
4. Click **Delete** in the confirmation dialog box.

VPN Tunnel
Creating VPN Tunnel

Last updated : 2021-04-16 16:53:12

A VPN tunnel is an encrypted public network tunnel used to transmit data packets in a VPN connection. The VPN tunnel on Tencent Cloud uses the IKE (Internet Key Exchange) protocol to establish a session when implementing IPsec. Featuring a self-protection mechanism, IKE can securely verify identities, distribute keys, and establish IPSec sessions on insecure networks. This document describes how to create a VPN tunnel on the VPC console.

The following configuration information is required to create a VPN tunnel:

- Basic information
- SPD (Security Policy Database) policy
- IKE configuration (Optional)
- IPsec configuration (Optional)

Prerequisites

- The VPN gateway and customer gateway have been configured.
- The VPN gateway IP range and customer IP range cannot overlap.
- The customer IDC must be configure with a static public IP.

Directions

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Tunnel** on the left sidebar to go to the management page.
3. Click **Create** on the **VPN Tunnel** management page.
4. Configure the basic information of the VPN tunnel in the pop-up dialog box.

Parameter Name	Notes
Tunnel Name	A custom tunnel name with up to 60 characters
Region	It is the same as the region of VPN gateway.

VPN Gateway Type	VPC or CCN
VPC	Select the VPC of the VPN gateway only when the **VPN Gateway Type** is **VPC**. This parameter is not available for CCN-based VPN gateways.
VPN Gateway	Select a VPN gateway from the list.
Customer Gateway	Select an existing customer gateway. Or you can create a new one.
Customer Gateway IP	The public IP address of the customer gateway.
Pre-shared Key	Used for identity authentication between the VPN gateway and customer gateway. The two peers must use the same pre-shared key.
Enable Health Check	Used to enable/disable health check and check the health status of the linkage. **Disabled** by default.
VPN Gateway IP Address for Health Check	It's only required when the health check is enabled. It should be an available IP outside the VPC IP range.
Customer Gateway IP Address for Health Check	It's only required when the health check is enabled. It should be an available IP within the IDC IP range. Note that the following IP addresses are not allowed: 169.254.0.0/16, 224.0.0.0-239.255.255.255, and 0.0.0.0.
Tag	(Optional) Attach a tag to the network resource as you need for easy management.

5. Click **Next** to go to the **SPD Policy** configuration page.

6. Configure the SPD policy.

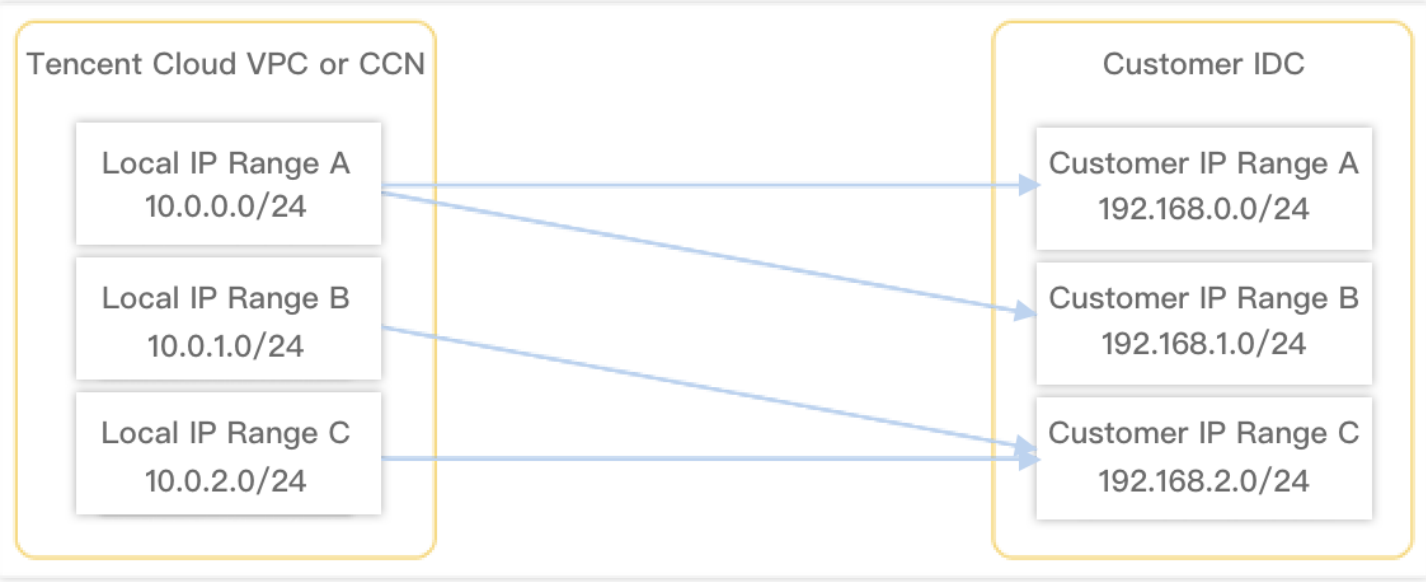
Note :

- An SPD policy consists of a series of SPD rules to specify the IP ranges in a VPC or CCN and an IDC that can communicate with each other. Each SPD rule contains one VPN gateway CIDR block and at least one customer gateway CIDR block. A CIDR block and a customer gateway CIDR block form a mapping. An SPD rule may involve multiple mappings.
- The rules for all tunnels of the same VPN gateway cannot contain overlapped mappings. In other words, the VPN gateway IP range and customer gateway IP range in a mapping

cannot have a duplicate address range.

Example:

As shown in the figure below, a VPN gateway has the following SPD rules:



- SPD rule 1: the VPN gateway IP range is 10.0.0.0/24, and the customer gateway IP ranges are 192.168.0.0/24 and 192.168.1.0/24. Two mappings are formed.
- SPD rule 2: the VPN gateway IP range is 10.0.1.0/24, and the customer gateway IP range is 192.168.2.0/24. One mapping is formed.
- SPD rule 3: the VPN gateway IP range is 10.0.1.0/24, and the customer gateway IP range is 192.168.2.0/24. One mapping is formed.

  There are four mappings as follows:
- 10.0.0.0/24-----192.168.0.0/24
- 10.0.0.0/24-----192.168.1.0/24
- 10.0.1.0/24-----192.168.2.0/24
- 10.0.2.0/24-----192.168.2.0/24

  Note that the mapping rules cannot overlap with each other, which means that the VPN and customer gateway IP range of a rule cannot be both overlapped with the two corresponding IP ranges of another rule.
- Suppose that you want to add a new mapping between 10.0.0.0/24-----192.168.1.0/24. The operation fails as the combination of VPN gateway IP and customer gateway IP already exists.
- You can add a new mapping between 10.0.1.0/24 and 192.168.1.0/24 as it does not overlap with any of the existing mappings.

7.Click **Next** to go to the **IKE Configuration (Optional)** page. If no advanced configuration is required, click **Next** directly.

Configuration Item	Notes
Version	IKE V1, IKE V2
Identity Verification Method	Default pre-shared key
Encryption Algorithm	The encryption algorithm supports AES-128, AES-192, AES-256, 3DES, and DES
Verification Algorithm	The identity verification algorithm. MD5 and SHA1 supported.
Negotiation Mode	**Main** mode and **Aggressive** mode supported In **aggressive** mode, more information can be sent with fewer packets so that a connection can be established quickly, but the identity of a security gateway is sent in plain text. The configuration parameters such as Diffie-Hellman and PFS cannot be negotiated and they must have compatible configurations.
VPN Gateway Identifier	IP Address and FQDN (full domain name) supported. IP Address by default
Customer Gateway Identifier	IP Address and FQDN supported. IP Address by default
DH group	Specifies the DH group used during IKE. The security of key exchange increases as the DH group expands, but the exchange may take a longer period. DH1: DH group that uses the 768-bit modular exponential (MODP) algorithm DH 2: DH group that uses the 1,024-bit MODP algorithm DH5: DH group that uses the 1,536-bit MODP algorithm DH14: DH group that uses the 2,048-bit MODP algorithm. Dynamic VPN is not supported for this option DH 24: DH group that uses the 2,048-bit MODP algorithm with a 256-bit prime order subgroup.
IKE SA Lifetime	Unit: second SA lifetime proposed for IKE security. Before a preset lifetime expires, another SA is negotiated in advance to replace the old one. The old SA is used before a new one is negotiated. The new SA is used immediately after

	establishment, and the old one is automatically cleared after its lifetime expires.

8.Go to the **IPsec configuration (Optional)** page. Directly click **Finish** if no advanced configuration is required.

Configuration Item	Notes
Encryption Algorithm	3DES, AES-128, AES-192, and AES-256 supported
Verification Algorithm	MD5 and SHA1 supported
Packet Encapsulation Mode	Tunnel
Security Protocol	ESP
PFS	disable, DH-GROUP1, DH-GROUP2, DH-GROUP5, DH-GROUP14, and DH-GROUP24 supported
IPsec SA lifetime(s)	Unit: s
IPsec SA lifetime(KB	Unit: KB

9. After the VPN tunnel is successfully created, return to the VPN tunnel list page and click **More**. Choose **Download config file** to complete the download.
0. Other operations:
   i. Clicking **Reset** will clear existing tunnel configurations. This operation will interrupt data transmission over the existing VPN tunnel and reestablish the connection. Please get ready for network change in advance.
   ii. Click **More** > **Log** to view the tunnel log.
   iii. Click **More** > **Delete** to delete the tunnel. Unconnected tunnels can be deleted.
   iv. Click **More** > **Download config file** to download the tunnel configuration file. This file can be uploaded to the customer VPN device.
   v. Click **More** > **Edit Tag** to modify tags.

Modifying VPN Tunnel

Last updated : 2021-03-31 10:11:39

After a VPN tunnel is created, you can modify the basic information of it, such as the tunnel name, pre-shared key, tag information, and SPD policy, as well as advanced configurations such as IKE configuration and IPsec configuration. You can also reset all the configurations of the VPN tunnel.

Impact on the System

The reset operation will interrupt data transmission over the existing VPN tunnel and reestablish the connection. Please get ready for network change in advance.

Directions

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Tunnel** on the left sidebar to go to the management page.
3. On the **VPN Tunnel** page, click the ID of the target VPN tunnel to go to the details page.
4. Click the **Edit** icon on the **Basic Info** page to modify the tunnel name, pre-shared key, tag information and SPD policy rules. Then click **Save**.

   You can also modify the tunnel name and pre-shared key by clicking the edit icon on the VPN tunnel list page, as shown in the figure below.
5. Click the **Advanced Configuration** tab to modify the IKE and IPsec configurations, and click **Save**.
6. Please be aware that, by clicking **Reset**, all your custom tunnel configurations will be cleared.

Downloading Config File

Last updated : 2021-03-31 10:13:09

After the local VPN tunnel is configured, you can download the VPN tunnel configuration and upload it to the local gateway device on the IDC side.

Directions

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Tunnel** on the left sidebar to go to the management page.
3. On the **VPN Tunnel** page, click **More** > **Download config file** on the right of the target tunnel.
4. In the pop-up download dialog box, select the type of the customer gateway device, platform, version, API name, and then click **Download**.

Viewing Log Information

Last updated : 2021-03-31 10:13:49

You can query logs on the VPN tunnel management page and troubleshoot failures during the VPN tunnel connection according to the log information.

Directions

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Tunnel** on the left sidebar to go to the management page.
3. On the **VPN Tunnel** management page, click **More** > **Logs** on the right of the tunnel to go to the log retrieval page.
4. You can view the log details in different time frames on the log retrieval page.

Deleting VPN Tunnel

Last updated : 2021-03-31 10:14:16

You can delete VPN tunnels that are no longer used.

Directions

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Tunnel** on the left sidebar to go to the management page.
3. In the **VPN Tunnel** page, click **More** > **Delete** on the right of the target tunnel.
4. Click **Delete** in the confirmation dialog box to delete the VPN tunnel.

Alarming and Monitoring
Setting Alarms

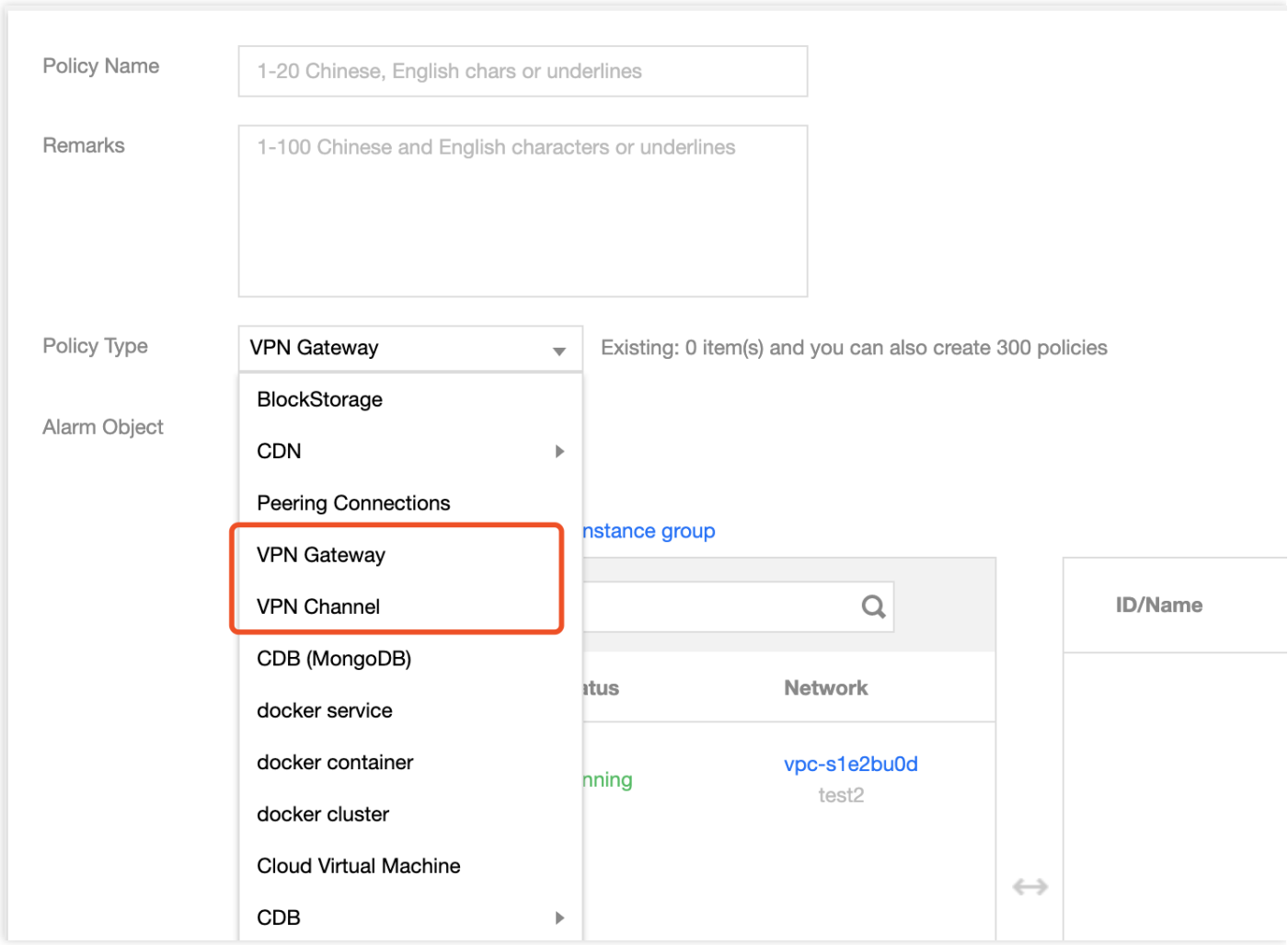
Last updated : 2021-09-01 16:40:57

You can customize traffic alarms for VPN connections. When a metric value exceeds its threshold, alarm notifications are sent to you automatically via email and SMS. Alarm services are free of charge, helping you quickly locate problems.

Operation Directions

1. Log in to Cloud Monitor Console.
2. On the left sidebar, choose **Alarm Configuration** > **Alarm Policy** to go to the alarm policy configuration page, and then click **Add**.
3. Enter the alarm policy name, choose **VPC** > **VPN Tunnel** for **Policy Type**, select an alarm object, set an alarm policy, select a recipient group and an alarm channel, and click **Complete**. You can

view the alarm policy in the alarm policy list.



4. View alarm information
   When the alarm condition is triggered, you will receive an alarm notification via SMS, email, or WeChat. You can also click **Alarm History** on the left sidebar to find the alarm. For more information about alarms, see Alarm Configuration.

Viewing Monitoring Data

Last updated : 2021-06-15 15:48:18

With VPN tunnels and VPN gateways, you can view monitoring data, and quickly locate failures if they occur. The monitoring service is free of additional charges.

VPN Gateway

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Gateway** on the left navigation bar.
3. Select a region and a VPC, and click the monitoring icon of a VPN gateway in the list to view its monitoring data.
   You can also view the monitoring data on the **Monitoring** tab by clicking the gateway ID.
4. Click **VPN Connection** > **VPN Tunnel** on the left navigation bar.

VPN Tunnel

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Tunnel** on the left navigation bar.
3. Select a region and a VPC, and click the monitoring icon of a VPN tunnel in the list to view its monitoring data.

Documentation

VPN Gateway Monitoring Metrics
VPN Tunnel Monitoring Metrics