Direct Connect
Operation Guidelines
Product Documentation
Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud’s the prior written consent.

Trademark Notice

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud’s products and services only and does not form part of Tencent Cloud’s terms and conditions. Tencent Cloud’s products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud’s applicable terms and conditions.
Contents

Operation Guidelines
  Operations Overview
  Managing Connection
    Applying for Connection
    Cancelling Connection
    Sharing Connection
    Viewing Monitoring Data
    Configuring Alarm Policies
  Managing a Tunnel
    Applying for a Tunnel
    Changing a Tunnel
    Deleting a Tunnel
    Viewing Monitoring Data
    Configuring Alarm Policies
  Managing Direct Connect Gateway
    Creating Direct Connect Gateway
    Configuring the Network Address Translation (NAT)
    Deleting Direct Connect Gateway
  Configure The Routing Table
Operation Guidelines

Operations Overview

When you use Direct Connect, you may need to apply for, cancel, and share connections, apply for dedicated tunnels, or set alarms. This document describes the common operations of Direct Connect and relevant products for your reference.

Managing Connections
- Applying for a connection
- Canceling a connection
- Sharing a connection
- Viewing monitoring data
- Configuring an alarm

Managing Dedicated Tunnels
- Applying for a tunnel
- Changing a tunnel
- Deleting a tunnel
- Viewing monitoring data
- Configuring an alarm

Managing Direct Connect Gateways
- Creating a Direct Connect gateway
- Configuring network address translation (NAT)
- [Deleting a Direct Connect gateway](https://intl.cloud.tencent.com/document/product/216/19258)

Managing Routers
- Configure a routing table
Managing Connection
Applying for Connection

Last updated: 2019-08-07 12:30:20

All applications for Tencent Cloud Connection shall be initiated and completed in the console. Tencent Cloud Direct Connect is only available to enterprise customers verified by Tencent Cloud. For more information on enterprise verification, please see how to complete enterprise verification.

Complete the application for and setup of Tencent Cloud Connection by following the steps below:

Apply in the console

1. Open Tencent Cloud Direct Connect Console - Connection.
2. Click + New to initiate an application for Connection. You will be required to fill in the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Name</td>
<td>You can define the name of your Connection</td>
<td>Modification allowed</td>
</tr>
<tr>
<td>Connection Provider</td>
<td>Available options: China Telecom, China Unicom, China Mobile, other providers in Mainland China (select this if your Connection is provided by a provider in Mainland China other than China Telecom, China Unicom and China Mobile), and providers outside Mainland China (select this if your direct connect is provided by a provider outside Mainland China)</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Remarks</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cloud Port Type</td>
<td>Indicates the Cloud port type for connecting the Connection with the Tencent Cloud access device</td>
<td>Select the port type based on your bandwidth. You can consult with your Connection provider or Tencent Cloud’s architect or after-sales manager</td>
</tr>
<tr>
<td>Access Point</td>
<td>The access point for Tencent Cloud Connection. We recommend that you select the one nearest to you</td>
<td>The city where the access point locates should at least have two access points for dual-line disaster recovery</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Supports 2-100,000 Mbps</td>
<td></td>
</tr>
<tr>
<td>Your premise</td>
<td>Detailed address</td>
<td>The floor of the IDC should be provided in the address</td>
</tr>
<tr>
<td>CPE Port Type</td>
<td>The port type for connecting your CPE with Connection</td>
<td></td>
</tr>
<tr>
<td>Redundant</td>
<td>Determining the master/slave relation between Connections can avoid single point of failure caused by two Connections connecting to the same access device</td>
<td>Determining the master/slave relation is to avoid two lines connecting to the same access point. The master/slave relation of Dedicated Tunnel needs to be applied for on the Dedicated Tunnel product page</td>
</tr>
<tr>
<td>Contact Number</td>
<td>The mobile number of the contact for Direct Connect</td>
<td></td>
</tr>
<tr>
<td>Contact Email</td>
<td>The email of the contact for Direct Connect</td>
<td></td>
</tr>
</tbody>
</table>

After a setup application is submitted, the Connection will go into the "Applying" status, and Tencent Cloud’s Direct Connect engineer will evaluate your application for Direct Connect within 3 work days.
Resource review and confirmation by Tencent Cloud

After receiving your application for Direct Connect, Tencent Cloud’s Direct Connect engineer will execute a comprehensive assessment on Direct Connect resources and check with you the details of the Direct Connect service via telephone. After the Connection is verified and approved, the manager will change its status to "To Be Paid".

However, the application for Connection may be rejected under the following circumstances:

- Inaccurate information: The access information you entered is incomplete. Please update the information according to the feedback of the Direct Connect engineer and resubmit an application.
- Insufficient resources: Access port or uplink bandwidth resources are insufficient. Please resubmit an application according to the Direct Connect engineer’s feedback after the resources are sufficient.
- Disqualification: Connection is only available to large-scale enterprise customers. Please resubmit an application after updating the enterprise qualification.

Payment and acceptance

After your application for Connection is approved by Tencent Cloud’s Direct Connect engineer, you can complete the payment in the console.

1. Open Tencent Cloud Direct Connect Console - Connection.
2. Find the Connection to be paid in the Connection list, and click Pay.
3. Confirm the Direct Connect information in the pop-up window, and click OK.
4. Enter the billing platform to complete the payment.

Once the payment is completed, the Direct Connect engineer will handle the access application and allocate related resources for the setup. The Connection will go into the "Running" status automatically after set up.
Cancelling Connection

You cannot cancel a physical direct connect in the console, but you can do this offline by contacting your dedicated physical Direct Connect manager. If you intend to cancel a physical direct connect, you must submit an application to the Direct Connect manager two months in advance.
Sharing Connection

Last updated: 2019-08-07 12:31:24

You can set up a Dedicated Tunnel by using the Connection under other Tencent Cloud account, which is known as hosted connection. You can also share your own Connection with other Tencent Cloud customers, especially, all by your own without any Tencent Cloud’s permission. For more how-to information, please see the Direct Connect documentation.
Viewing Monitoring Data

Last updated: 2019-08-07 12:31:49

You can query the monitoring data (outbound and inbound bandwidth, packet loss, and latency) of Connections in the console or via API. The console operations are as follows:

1. Open Tencent Cloud Direct Connect Console - Connections.
2. Click your Connection in the list, and click the Monitoring button to query the monitoring data of the Connection.
Configuring Alarm Policies

Last updated: 2019-09-26 18:37:24

You can configure monitoring alarms for a Connection by following the steps below:


2. Enter the alarm policy name.

3. Click Add and edit the alarm policy:
   - Select Connection for Policy Type.
   - Select Outbound Bandwidth, Inbound Bandwidth, or Packet Loss for Trigger Condition.

4. Click Next: Associate Alarm Object, and select the Connection to be associated.

5. Set the Alarm Receiver Group, and then click OK to complete the alarm policy configuration.

After the Connection alarm is configured, you can receive system alarms according to the setting of the alarm receiver group. For more information on monitoring, please see Cloud Monitor.
Managing a Tunnel
Applying for a Tunnel

Last updated: 2019-08-07 12:32:20

1. Open Tencent Cloud Direct Connect Console - Dedicated Tunnel;
2. Click + New to initiate the application for Dedicated Tunnel. You need to enter the following information to create a Dedicated Tunnel:

If you would use the Connection under your own Tencent account, steps as below:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedicated Tunnel name</td>
<td>Create your Dedicated Tunnel name</td>
<td>-</td>
</tr>
<tr>
<td>Connection Type</td>
<td>Select My Connection, which means the Connection under your account. Or shared Connection, which is under other accounts</td>
<td>-</td>
</tr>
<tr>
<td>Connection ID</td>
<td>Select the ID of the Connection by which you want to setup a tunnel</td>
<td>-</td>
</tr>
<tr>
<td>Target Network</td>
<td>VPC and CCN network are available in Tencent Cloud International station</td>
<td>-</td>
</tr>
<tr>
<td>VPC</td>
<td>Select the ID of the network accessed via the Dedicated tunnel</td>
<td>-</td>
</tr>
<tr>
<td>DC Gateway</td>
<td>The gateway type is displayed on the left of the gateway name. Check if it meets you need</td>
<td>-</td>
</tr>
<tr>
<td>VLANID</td>
<td>Specify the non-conflicted VLANID, 0 indicates that the sub-interface is not enabled for the Connection and only one tunnel can be created</td>
<td>-</td>
</tr>
<tr>
<td>Peer IP</td>
<td>&quot;Specific&quot; means the peering IP should be specified on your own. &quot;Random&quot; means Tencent Cloud will allocate the non-conflict Peer IP for you. You can find it in tunnel details after you create it.</td>
<td>-</td>
</tr>
<tr>
<td>Routing Method</td>
<td>BGP and static. Routing information is required for static route</td>
<td>-</td>
</tr>
<tr>
<td>BGP ASN</td>
<td>Optional, automatically assigned if not specified.</td>
<td>-</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Remarks</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>BGP Key</td>
<td>Optional, &quot;Tencent&quot; is displayed at frontend by default. Leave it empty means no key needed.</td>
<td></td>
</tr>
<tr>
<td>IDC Routes</td>
<td>Enter the user's IDC IP address range, which cannot conflict with that of VPC except in NAT mode</td>
<td>Only valid for static route</td>
</tr>
</tbody>
</table>

If you would use the Connection under other Tencent account, steps as below:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedicated Tunnel name</td>
<td>Create your Dedicated Tunnel name</td>
<td></td>
</tr>
<tr>
<td>Connection Type</td>
<td>Select shared Connection, which is under other accounts</td>
<td></td>
</tr>
<tr>
<td>Provider Account ID</td>
<td>You should ask the Connection provider for his Tencent Cloud ID.</td>
<td>Only valid for shared Connection</td>
</tr>
<tr>
<td>Connection ID</td>
<td>Enter the ID of the Shared Connection for which you want to setup a tunnel</td>
<td>Only valid for shared Connection</td>
</tr>
<tr>
<td>Target Network</td>
<td>VPC and CCN network are available in Tencent Cloud International station</td>
<td></td>
</tr>
<tr>
<td>VPC</td>
<td>Select the ID of the network accessed via the Dedicated tunnel</td>
<td></td>
</tr>
<tr>
<td>DC Gateway</td>
<td>The gateway type(standard or NAT) is displayed on the left of the gateway name. Please double check if it meets you need</td>
<td></td>
</tr>
<tr>
<td>VLANID</td>
<td>Specify the non-conflicted VLANID, 0 indicates that the sub-interface is not enabled for the Connection and only one tunnel can be created</td>
<td></td>
</tr>
<tr>
<td>Peer IP</td>
<td>&quot;Specific&quot; means the peering IP should be specified on your own. &quot;Random&quot; means Tencent Cloud will allocate the non-conflict Peer IP for you. You can find it in tunnel details after you create it.</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Remarks</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Routing Method</td>
<td>BPG and static. Routing information is required for static route</td>
<td>-</td>
</tr>
<tr>
<td>BGP ASN</td>
<td>Optional, automatically assigned if not specified.</td>
<td>-</td>
</tr>
<tr>
<td>BGP Key</td>
<td>Optional, &quot;Tencent&quot; is displayed at frontend by default. Leave it empty means no key needed.</td>
<td>-</td>
</tr>
<tr>
<td>IDC Routes</td>
<td>Enter the user’s IDC IP address range, which cannot conflict with that of VPC except in NAT mode</td>
<td>Only valid for static route</td>
</tr>
</tbody>
</table>

**Note:**
The following CIDR will be rejected by Tencent Cloud, 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 and 100.64.0.0/10, due to the restriction of Tencent Cloud Network.

You can divide the CIDR into 2 subnets of them and broadcast:

- 10.0.0.0/8 = 10.0.0.0/9 + 10.128.0.0/9;
- 172.16.0.0/12 = 172.16.0.0/13 + 172.24.0.0/13;
- 192.168.0.0/16 = 192.168.0.0/17 + 192.168.128.0/17;
- 100.64.0.0/10 = 100.64.0.0/11 + 100.96.0.0/11.
Changing a Tunnel

Descriptions of Parameter Changes

The following parameters can be changed for a dedicated tunnel:

- **IP address:**
  Changing the IP address will interrupt the service.

- **BGP ASN:**
  Changing the BGP ASN will interrupt the service.

- **Bandwidth:**
  Changing the bandwidth will not interrupt the service, and the system will automatically overwrite the configuration.

  In the Shared Connection mode, you cannot apply for a bandwidth change for a dedicated tunnel; instead, such a change can only be applied for by the connection owner.

- **BGP KEY:**
  Changing the BGP KEY will not interrupt the service, and the system will automatically overwrite the configuration.

- **User IDC IP range:**
  The user IDC IP range can be modified, and the system will automatically distribute the configuration.

After a tunnel change request is submitted, the system will complete the device configuration in a few minutes.

Use Limits on Large IP Range

In order to improve the fine-grained scheduling capabilities of your network, please avoid distributing the following routes:

10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10.

You can split the above large routes into the following ones for distribution:
- **10.0.0.0/8** 
  should be split into **10.0.0.0/9** + **10.128.0.0/9**.

- **172.16.0.0/12** 
  should be split into **172.16.0.0/13** + **172.24.0.0/13**.

- **192.168.0.0/16** 
  should be split into **192.168.0.0/17** + **192.168.128.0/17**.

- **100.64.0.0/10** 
  should be split into **100.64.0.0/11** + **100.96.0.0/11**.
Deleting a Tunnel

Last updated: 2019-08-07 12:32:46

1. Open Tencent Cloud Direct Connect Console - Dedicated Tunnel;
2. Locate the Dedicated Tunnel to be deleted in the list, click Delete and then OK.
3. The Dedicated Tunnel will be deleted within 10 minutes.
Viewing Monitoring Data

Last updated: 2019-08-07 12:33:16

You can query monitoring information (outbound and inbound bandwidth, latency) of a Dedicated Tunnel via console or APIs. The console operations are as follows:

1. Open Tencent Cloud Direct Connect Console - Dedicated Tunnel;
2. Locate the Dedicated Tunnel in the list, and click the Monitoring button to query its monitoring information.
You can configure alarms for a Dedicated Tunnel. The configuration steps are as follows:

2. Enter the alarm policy name.
3. Click **Add** and edit the alarm policy:
   - Select "Dedicated Tunnel" for "Policy Type".
   - Select "Outbound Bandwidth", "Inbound Bandwidth", "Packet Loss", and "Latency" for "Alarm Triggering Conditions".
4. Click **Next: Associate Alarm Object**, and select the associated Dedicated Tunnel.
5. Set the **Alarm Receiver Group**, and then click **OK** to complete the alarm policy configuration.

After the Dedicated Tunnel alarm is configured, you can receive the system alarm according to the setting of the alarm receiving group. For more information on monitoring, please see Cloud Monitoring.
Managing Direct Connect Gateway

Creating Direct Connect Gateway

Last updated: 2019-01-21 17:58:51

1. Open the Tencent Cloud Console, select Virtual Private Cloud in the top navigation bar, and click the Direct Connect Gateway tab in the left navigation bar.
2. Click the + New button to enter the Direct Connect creation page.
3. Enter the name, VPC and address mapping mode, and select whether to enable the network address translation feature. (This feature is only available in the beta test for now. Please activate it via a ticket or your customer manager.)
4. Click OK to confirm the information and complete the creation of the Direct Connect gateway.
Configuring IP translation

The specific procedure is as follows:

1. Open the Tencent Cloud Console, select Virtual Private Cloud in the top navigation bar, and click the Direct Connect Gateway tab in the left navigation bar.

2. Click the ID of the Direct Connect gateway to enter its details page.

3. Configure local IP translation.

   On the Direct Connect gateway details page, click Local IP Translation tab. There are two steps for configuring local IP translation:
   (1) Edit the rules for local IP translation.
   - Adding: In the top-left corner of the IP mapping page, click the New blue button and enter the original IP, mapping IP and note. ACL rule for the new local IP translation rule is ALL PASS by default, which means the local IP translation is valid for all Dedicated Tunnels. You can edit the ACL rule for the local ACL translation to change the applicable scope of the local IP translation.
   - Deleting: Click Delete to the right of the IP translation rule and click OK to confirm the deletion. When the IP translation rule is deleted, all the ACL rules under it will also be deleted.
   - Modifying: Click the Modify IP Mapping to the right of the IP translation rule to edit the original IP, mapping IP and comments of the local IP translation rule. Click OK, and the modified IP translation rule takes effect immediately.
   (2) Configure the network ACL rules for local IP translation.

   ACL rules support TCP and UDP protocol. The local IP mapping ACL rules support the source port, destination IP, and destination port. If the port and the IP are left blank, it means ALL. When ALL is selected for the protocol, both the port and the IP will be set to ALL by default.
   - Adding: Click Edit ACL Rule to the right of the IP mapping rule and click Add next to the existing ACL rules.
Deleting: Click **Edit ACL Rule** to the right of an IP mapping rule for editing. Click **Delete** and OK to delete the ACL rule. You can also click the **Delete** button next to the ACL rule to delete it.

Modifying: Click **Edit ACL Rule** to the right of an IP mapping rule to modify an ACL rule. You can also click the **Modify** button next to the ACL rule to modify it.

---

**Note:**

When the Direct Connect gateway is also configured with **Peer IP Translation**, the Destination IP of the ACL rule for local IP translation should be the mapping IP of peer IP translation, instead of the original IP.

**Restrictions on rule:**

- The original IP must be within the CIDR range of VPC.
- The mapping IP cannot be within the CIDR range of VPC to which the Direct Connect gateway belongs.
- The original IP is unique and cannot be replicated. That means an IP in a VPC can only be mapped to one IP.
- Mapping IP is unique and cannot be replicated. That means multiple IPs in a VPC cannot be mapped to the same IP.
- Original or destination IP should not be broadcast address (255.255.255.255), Class D address (224.0.0.0 - 239.255.255.255), and Class E address (240.0.0.0 - 255.255.255.254).
- The maximum number of local IP translation rules for Direct Connect gateway is 100, and a maximum of 20 ACL rules is supported for each local IP translation (the quota can be raised in the backend on demand).

1. **Configuring peer IP translation.**

On the Direct Connect gateway details page, click **Peer IP Translation** tab:

- Adding: In the top left corner of the IP mapping page, click the **New** button in blue and enter the original IP, mapping IP and comments.
- Deleting: Click the **Delete** to the right of the IP translation rule and confirm it.
- Modifying: Click the **Modify IP Mapping** to the right of the IP translation rule to edit the original IP, mapping IP and comments of the local IP translation rule. Click **OK**, and the modified IP translation rule takes effect immediately.

**Restrictions on rule:**
The mapping IP cannot be within the CIDR range of VPC to which the Direct Connect gateway belongs.

The original IP is unique and cannot be replicated. That means a peer IP of the Direct Connect can only be mapped to one IP.

Mapping IP is unique and cannot be replicated. That means multiple peer IPs of the Direct Connect cannot be mapped to the same IP.

Original or destination IP should not be broadcast address (255.255.255.255), Class D address (224.0.0.0 - 239.255.255.255), and Class E address (240.0.0.0 - 255.255.255.254).

The maximum number of peer IP translation rules for Direct Connect gateway is 100 (the quota can be raised in the backend on demand).

Configuring IP port translation

1. Open the Tencent Cloud Console, select Virtual Private Cloud in the top navigation bar, and click the Direct Connect Gateway tab in the left navigation bar.

2. Click the ID of the Direct Connect gateway to enter its details page.

3. Configure local source IP port translation.
   On the Direct Connect gateway details page, click Local Source IP Port Translation. There are two steps for configuring local source IP port translation:

   i. Configuring the local IP port translation address pool.
      - Adding: Click New in the mapping IP pool page, enter the mapping IP pool (IP or IP segment is supported, and IP segment is indicated in "A-B").) and comments (optional); ACL rule for the new IP pool is ALL DROP, and you need to additionally edit ACL Rules to implement Network Translation.
      - Deleting: Click Delete to the right of the IP address pool to delete the address pool.
        Deleting an address pool will delete the ACL rules associated with the address pool automatically.
      - Modifying: Click Modify Mapping IP Pool to the right of the IP address pool to edit the IPs and comments of the mapping IP pool.

   ii. Configuring the network ACL rule for the IP address pool.
      ACL rules support configuration protocol (TCP or UDP), source IP, source port, destination IP, and destination port.
      - Adding: Click Edit ACL Rule to the right of the IP address pool for editing. Click New Line at the bottom of the rule to add a new ACL rule.
Deleting: Click **Edit ACL Rule** to the right of the IP address pool for editing. Click **Delete** to the right most of an ACL rule to delete it. You can also delete an ACL rule by expanding it and clicking **Delete** to the right most of it.

Modifying: Click **Edit ACL Rule** to the right of the IP address pool for editing. You can also modify an ACL rule by expanding it and clicking **Modify** to the right most of it.

**Note:**
When the Direct Connect gateway is also configured with **Peer IP Translation**, the **Destination IP** of the ACL rule for local source IP port translation should be the mapping IP of peer IP translation, instead of the original IP.

**Restrictions on rule:**
- The IP address pool cannot be within the CIDR range of VPC to which the Direct Connect gateway belongs.
- ACL rules for multiple IP address pools should not overlap. Otherwise, this will cause network address translation conflicts.
- IP addresses between multiple IP addresses should not overlap.
- IP address pool only supports single IP or continuous IPs, and /24 IP address range of continuous IPs should be consistent, that is, "192.168.0.1 - 192.168.0.6" is supported but "192.168.0.1 - 192.168.1.2" is not.
- Address pool should not contain broadcast address (255.255.255.255), Class D address (224.0.0.0 - 239.255.255.255), and Class E address (240.0.0.0 - 255.255.255.254).
- The local source IP port translation supports a maximum of 100 IP address pools, and each address pool supports a maximum of 20 ACL rules (the quota can be raised in the backend on demand).

4. **Configuring the local destination IP port translation.**
On the Direct Connect gateway details page, click the **Local Destination IP Port Translation** tab:

- Adding: Click **Add** on the IP port mapping page to add a new IP port mapping.
- Deleting: Click **Delete** to the right of the line where the IP port mapping is located to delete the mapping.
- Modifying: Click **Modify IP Port Mapping** to the right of the line where the IP port mapping is located to modify the mapping and note of this IP port mapping.

**Restrictions on rule:**
- The original IP must be within the CIDR range of VPC to which the Direct Connect gateway belongs.
- The original IP port should be unique. In other words, the same IP port within the VPC can only be mapped to one IP port.
- The mapping IP port cannot be within the CIDR range of VPC.
- Mapping IP port should be unique. In other words, multiple IP ports in a VPC cannot be mapped to the same IP port.
- Original or mapping IP should not be broadcast address (255.255.255.255), Class D address (224.0.0.0 - 239.255.255.255), and Class E address (240.0.0.0 - 255.255.255.254).
- The local destination IP port translation supports a maximum of 100 IP port mappings (the quota can be raised in the backend on demand).

**Note:**
If both IP translation and IP port translation are configured, IP mapping will be matched with first if any conflicts.
Deleting Direct Connect Gateway

You can delete the Direct Connect gateway which you don’t want to use again. Deleting a Direct Connect gateway will also delete its associated tunnel. Please make sure that this will not affect your normal service.

1. Open the Tencent Cloud Console, select Virtual Private Cloud in the top navigation bar, and click the Direct Connect Gateway tab.
2. Select the Direct Connect gateway you want to delete, and click the Delete button in the Operation column.
3. The deletion will be completed after you confirm it.
Configure The Routing Table

After creating a Direct Connect gateway and setting a Dedicated Tunnel, you can configure the routing table of the VPC in the console to direct the desired traffic to the Direct Connect gateway.

1. Log in to the Tencent Cloud Console, select Virtual Private Cloud in the top navigation bar, and click the Routing Tables tab.

2. Click the ID of the routing table to be associated with the Direct Connect gateway to enter the routing table details page.

3. Click the Edit button and add a policy in the routing policies. Enter the Destination, and select "Direct Connect Gateway" for the Next hop type to filter out the Direct Connect gateway you created.

4. Save the routing table.

Now, you can direct the traffic of the specific destination to the Direct Connect gateway to associate it with your local IDC.