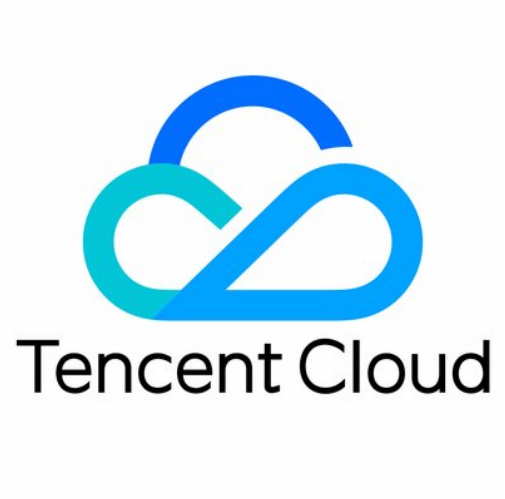
Direct Connect

Getting Started

Product Documentation



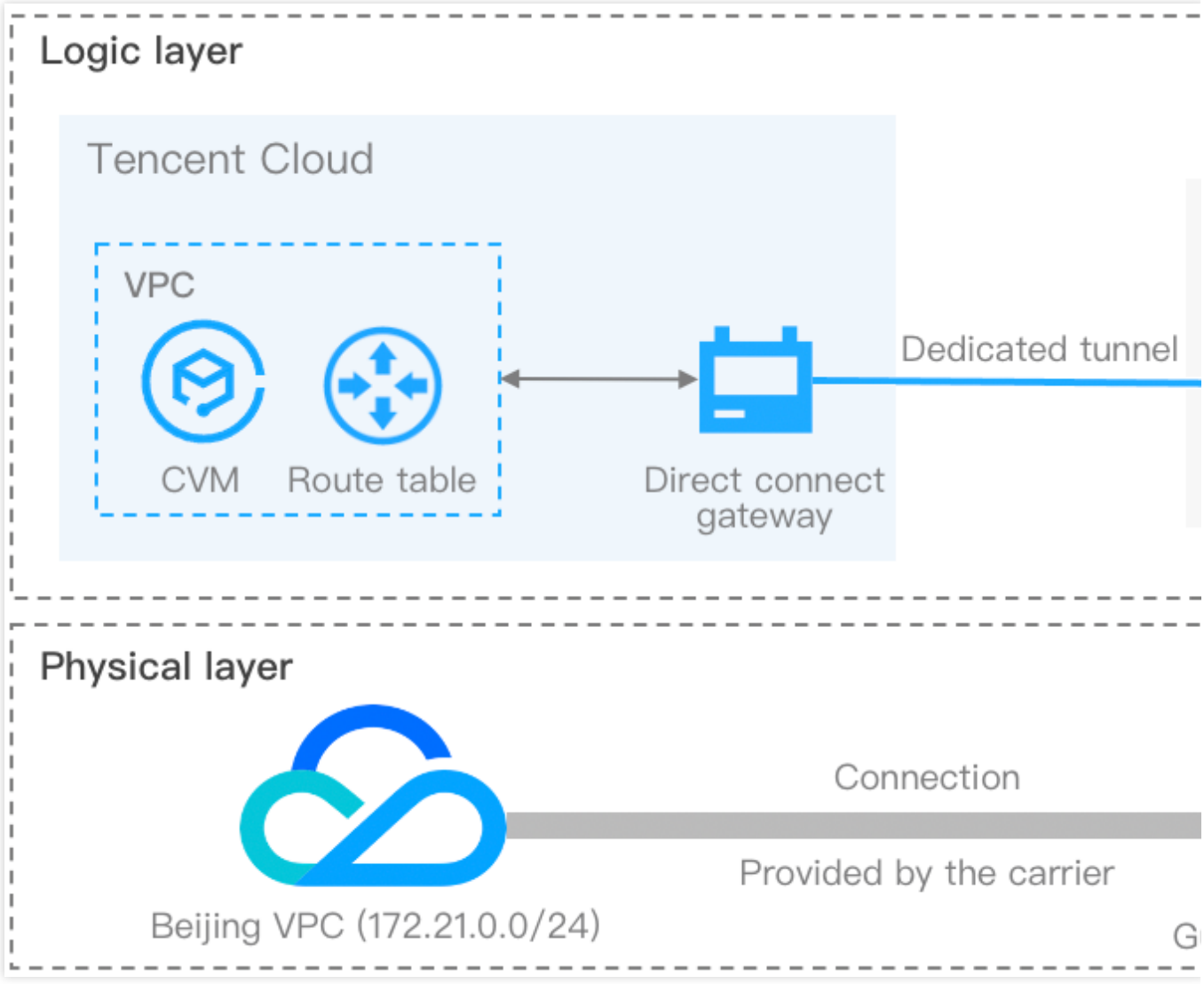
Getting Started

Last updated：2024-01-13 16:02:36

A VPC-based direct connect gateway can be used to interconnect one Tencent Cloud VPC with one or more local IDCs. This document describes how to use a VPC-based direct connect gateway to build the Direct Connect network architecture that connects a VPC in Beijing to an IDC in Guangzhou.

Background

The following figure shows you how to interconnect a Tencent Cloud VPC (`172.21.0.0/24`) and a local IDC (`192.168.0.0/24`) with a bandwidth of 2 Mbps.



Follow the steps below:

1. Create a connection: connects customer's local IDC to Tencent Cloud.
2. Create a direct connect gateway: as the traffic entry of the Direct Connect, connects a Tencent Cloud VPC to connections (dedicated tunnels).
3. Create a dedicated tunnel: acts as the network segmentations of a connection.
4. Configure the route table: configures a routing policy in the route table of a VPC subnet to enable connection.
5. Set alarms: configures recipients for alarm policies automatically created together with the connection and dedicated tunnel.

Prerequisites

You have built a Tencent Cloud VPC in the Beijing region as instructed in Building Up an IPv4 VPC.

How It Works

Step 1: create a connection

To create a connection, you need to first confirm the information and submit an application in the console, and then the carrier will start the engineering investigation and wiring. This process takes about 2-3 months. For more information, see Connection Overview. Perform the following steps to apply for a connection in the console.

1. Log in to the Direct Connect console.
2. Click **Connections** on the left sidebar to access the **Connections** page. Click **+New**.
3. In the pop-up window, read **Tencent Cloud Direct Connect Service Level Agreement**, select **Read and Agreed**, and click **Next**.
4. Complete the following configurations and click **OK**。

Parameter	Description
Connection Name	Enter a name for the connection, such as "Connection to Beijing IDC".
Region	Select Beijing.
Access point	We recommend you first search for access points and check their distances to your IDC, and then select the nearest access point. For more information, see Connection Access Point.
Connection provider	Select an eligible carrier, such as CTCC.
Cloud port	Ports in 1, 10, and 100 Gbps are available. To use a 100 Gbps port, please submit a ticket. Select 1 Gbps as an example.

Port type	Choose fiber optic port or electrical port as needed. The available ports vary with the port type. For example, 1 Gbps ports include fiber optic port and electrical port, while 10 Gbps ports only include fiber optic port. Select Fiber optic port as an example.
Bandwidth Cap	Select 998 Mbps as an example.

Note:

For more information on parameter configurations, see Applying for Connection

5. After your application is submitted, Tencent Cloud Direct Connect representative will comprehensively assess Direct Connect resources and then check with you the service details over the phone. After the connection is confirmed to be accessible, you should complete the payment in the console.

Step 2: create a direct connect gateway

1. Log in to the Direct Connect console.
2. Select **Beijing** in the region at the top of the **Direct Connect Gateway** page, and click **+New**.
3. Complete the configurations in the pop-up window and click **OK**.

Parameter	Description
Name	Enter a name for the direct connect gateway, such as "Beijing VPC - Guangzhou IDC".
Associate Network	Select VPC.
Network	Select an existing VPC instance.
Gateway type	Select Standard as an example. Standard: does not support the network address translation feature. NAT Type: supports the network address translation feature. You should also configure the network address translation (NAT) if you want to use a NAT direct connect gateway.

Step 3: create a dedicated tunnel

1. Log in to the Direct Connect console.
2. Click **Dedicated Tunnels** on the left sidebar to access the **Dedicated Tunnels** page. Click **+New**.
3. Complete basic configurations such as name, connection type, access network, region and associated direct connect gateway, and click **Next**.

Parameter	Description
Name	Enter a name for the dedicated tunnel, such as "Beijing VPC - Guangzhou IDC".
Connection	Select the connection created in Step 1.

Access Network	Select VPC.
VPC	Select an existing VPC instance.
Direct Connect Gateway	Select the direct connect gateway created in Step 2.

Note:

For more information on the parameter configurations, see Creating a Dedicated Tunnel

4. Configure the following parameters in the **Advanced Configuration** tab, and click **Next**.

Parameter	Definition
VLAN ID	A VLAN corresponds to a tunnel. Enter a value within the range of 0-3000. Entering 0 means one dedicated tunnel can be created. Enter “0” as an example.
Peer IP	Peer IP addresses need to be manually configured by default.
Bandwidth	Specify the bandwidth cap of the dedicated tunnel, which cannot exceed the maximum bandwidth of the associated connection. Set it to “2 Mbps” as an example.
Tencent Cloud Primary IP	Enter the connection IP address on the Tencent Cloud side. Set it to “172.21.0.0/24” as an example.
Tencent Cloud Secondary IP	Enter the secondary IP address of the connection on the Tencent Cloud side. Set it to “172.21.0.2/24” as an example.
CPE Peer IP	Configure the connection IP address on the user (or carrier) side. Set it to “172.21.0.1/24” as an example.
Routing Mode	Select **Static**.
Health Check	Health check is disabled by default. To enable it, see Dedicated tunnel health check.
CPE IP range	Select `192.168.0.0/24` as an example.

5. Configure IDC devices. You can click **Download configuration guide** to download related files and complete the configurations as instructed in the guide.

Parameter	Description
CPE IP range	Enter the customer IP range if **Static** is selected as the routing mode. This parameter cannot conflict with the VPC IP range in a non-NAT mode.

6. Click **Submit**.

Step 4: configure the route table

To use a VPC-based direct connect gateway, configure a routing policy with direct connect gateway as the next hop and IDC IP range as the destination in the route table of the VPC subnet to enable communication.

1. Log in to the VPC console.
2. Select **Route Tables** on the left sidebar, and click the **ID/Name** of the target VPC to enter its details page.
3. Click **+New routing policies** on the **Basic Information** page.
4. In the pop-up window, enter “192.168.0.0/24” for the **Destination**, select “Direct Connect Gateway” for the **Next hop type**, locate the direct connect gateway created in Step 2 for the **Next hop**, and click **Create**.
5. Click **Confirm**.

Step 5: set alarms

After a connection and a dedicated tunnel are created, Cloud Monitor will automatically create a default alarm policy for each service. This default alarm policy does not configure recipient information, so you can only view alarms on the console. To configure a recipient, take the following steps.

Default alarm policy for connections

Metric	Statistical Period	Condition	Condition Value	Consecutive Periods	Policy
Bandwidth utilization	1 minute	>=	80%	5 periods	Alarm once a day

Default alarm policy for dedicated tunnels: available event alarms are DirectConnectTunnelDown, DirectConnectTunnelBFDDown, DirectConnectTunnelBGPSessionDown, and DirectConnectTunnelRouteTableOverload.

1. Log in to the cloud monitor console. View Monitoring Overview
2. Select **Alarm Configuration** > **Alarm Policy** on the left sidebar. Click **Advanced Filter**, select **All** for **Monitoring Type**, and select the relevant product for **Policy type**.
3. Click the name of the target default policy in the **Alarm Management** list.
4. On the **Manage alarm policy** page, select a notification template.

Click **Edit Recipient** to configure alarm recipients in the template. If existing templates are not suitable, you can click **Create Template** and configure the template to create as prompted. Then you can select the template to configure alarm recipients.