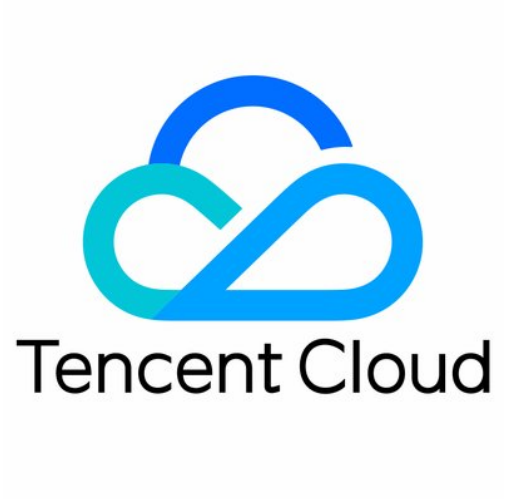
Direct Connect

Operation Guide

Product Documentation



Contents

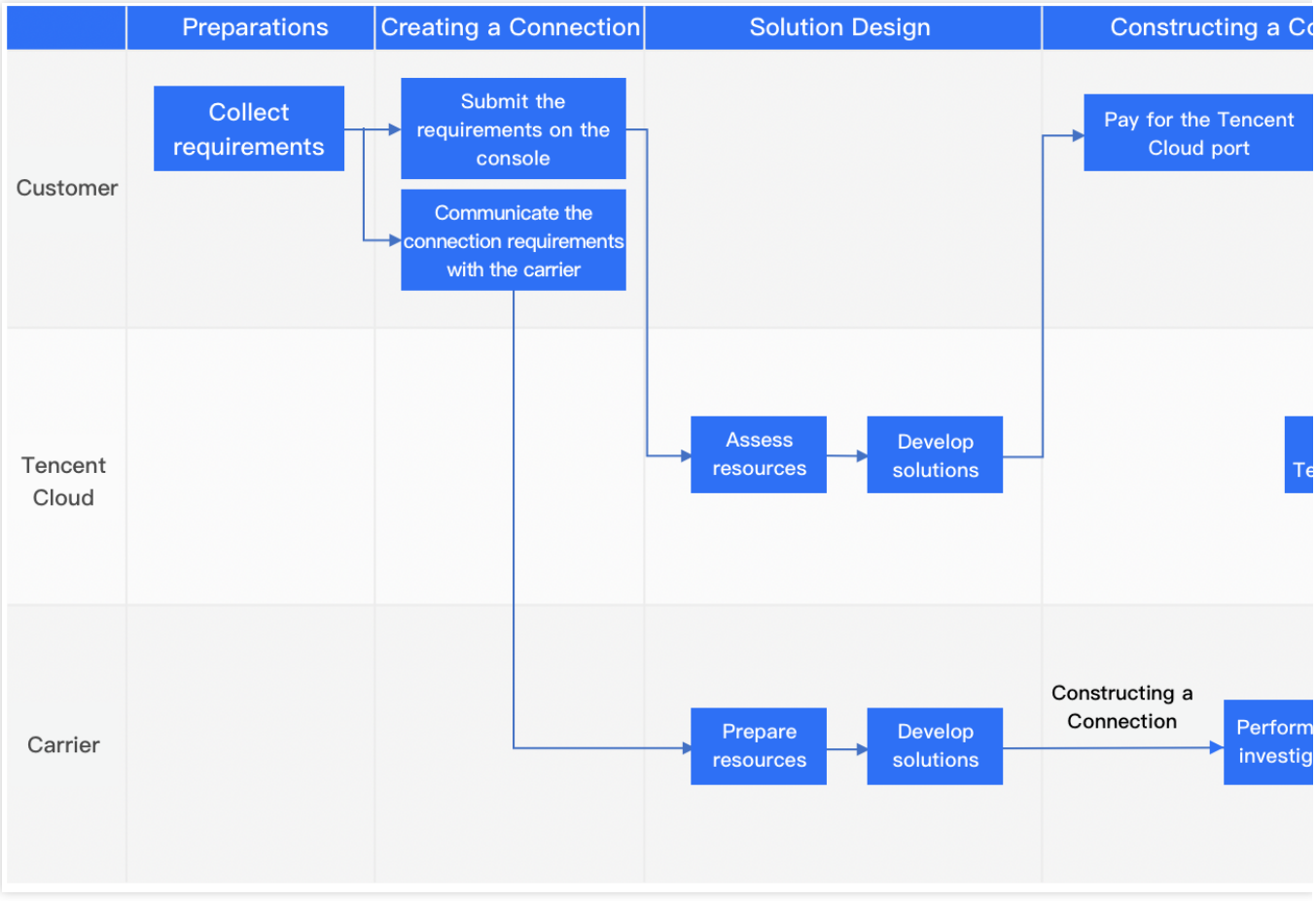
Operation Guide
Connections
Connection Overview

Last updated：2024-01-13 16:40:45

A DC connection connects customer's local IDC to Tencent Cloud. To create a connection, you need to first confirm the information and submit an application on the console, and then the carrier will start the engineering investigation and wiring. This process takes about 2-3 months; therefore, please plan ahead to guarantee the cloudification progress.

Flowchart

The following flowchart describes how to create a connection.



1. Preparations: confirm the access points and collect requirements from Tencent Cloud and the carrier before creating a connection.
2. Creating a connection: if your local IDC and Tencent Cloud access points are in different data centers, please apply for a connection in the Tencent Cloud console, and communicate your needs with the carrier. If your local IDC resides in the same data center as a Tencent Cloud access point, you only need the Tencent Cloud solution to start the connection construction.
3. Designing a solution: after receiving your application, Tencent Cloud will access resources, develop solutions, and confirm with you. The carrier also needs to prepare resources and develop solutions. Please contact the carrier for relevant fees.
4. Constructing a connection: if your local IDC and Tencent Cloud access points are in different data centers, the carrier will perform the engineering investigation and wiring based on the solution. Meanwhile, you need to pay for the port in the Tencent Cloud console. Then Tencent Cloud will complete the access port configuration, and help the carrier connect the connection to Tencent Cloud. If your local IDC resides in the same data center as a Tencent Cloud access port, directly contact the Direct Connect representative for assistance.

Note:

Starting from February 1, 2021, all the new connections will be exempted from the initial installation fee.

5. Accepting a connection: you need to check and test the links of the completed connection. Accept the connection that passes the test.

Preparations

Determine the access point before creating a connection.

An access point is the location where you can access to Tencent Cloud connection's network services. Nearby access is recommended to ensure network quality and reduce connection costs. Generally, two or more access points are available in one Tencent Cloud region, implementing multi-connection disaster recovery. You can submit a ticket to obtain the specific location of each access point. The following information helps you choose a proper access point:

Region: a region is the physical location of an IDC. In Tencent Cloud, regions are fully isolated from each other, ensuring cross-region stability and fault tolerance. We recommend selecting the region closest to your end users to minimize access latency and improve download speed.

Carrier: the provider of connection resources, such as China Mobile, China Unicom, and China Telecom.

Note:

According to the relevant national laws, regulations and the Notice on Regulating the Internet Network Access Marketplace (MIIT [2017] No. 32), you should choose an eligible connection provider to complete the construction of the Direct Connect service.

Using an illegal line may expose you to administrative penalty by the State regulatory authority and cause the line unavailability. In this case, Tencent Cloud accepts no responsibility.

Port: choose a fiber optic port or electrical port as needed.

Fiber optic port: a physical port used to connect fiber optic cables. Tencent Cloud provides three port types: 1, 10, and 100 Gbps.
Electrical port: general ports (such as RJ45) in server and network for twisted pairs (ordinary cables). Tencent Cloud provides gigabit electrical ports (10/100/1000BASE-T), which are suitable for low bandwidth use cases.
Note:
To use a 100 Gbps port, please submit a ticket.
When constructing a connection, make sure that the IDC port specification is the same as that of Tencent Cloud; otherwise, the communication may fail.
In case of inconsistency, we recommend changing the IDC port. If you want to use another Tencent Cloud port, you need to resubmit an application and initiate a new process to access the connection.

Port type		Specifications
Fiber optic port	1 Gbps	SFP-GE-LX-Sm1310, 10KM
		SFP-GE-LH80-SM1550, 80KM
	10 Gbps	SFP-XG-LX-SM1310, 10KM
		SFP-XG-LH80-SM1550, 80KM
	100 Gbps	QSFP-100G-LR4-WDM1300, 10KM
Electrical port		10/100/1000BASE - T

Creating a Connection

Use Case	Action
Local IDC and Tencent Cloud access point in different data centers	Apply for a connection in the Tencent Cloud console as instructed in Applying for Connection, and communicate your requirements with an eligible carrier.
Local IDC and Tencent Cloud access point in the same data center	Apply for a connection in the Tencent Cloud console. For detailed directions, please see Applying for Connection.

Constructing a Connection

Local IDC and Tencent Cloud access point in different data centers
Both the carrier and Tencent Cloud are responsible for the connection construction as follows:

Responsibilities of the carrier

1.1.1 Perform the engineering investigation.

1.1.2 Confirm the construction solution and relevant fees.

1.1.3 Initiate the connection construction.

Note:

During the construction, fiber-to-the-building (FTTB) and in-house wiring rental fees may incur. For more information, consult your property operator or wiring provider.

1.1.4 Access the data center.

1.1.4.1 Apply to the Direct Connect representative and provide the name, ID card and contact information of engineers who need to investigate the access point's data center.

1.1.4.2 After the application is approved, the Direct Connect representative will help engineers access the data center within two business days.

Responsibilities of Tencent Cloud

After you pay for the Tencent Cloud port in the console, Tencent Cloud will complete the access port configuration, and support the carrier for the connection to Tencent Cloud.

Local IDC and Tencent Cloud access point in the same data center

You only need to contact the Direct Connect representative for resource allocation and connection construction.

Note:

During the construction, fiber-to-the-building and in-house wiring rental fees may incur. For more information, consult your property operator or wiring provider.

Checking and Accepting the Connection

You need to complete creating a Direct Connect instance before accepting the connection. For more information, please see Quick Start. Then test the connection for its performance, latency and reliability.

Stress test: use the network test tool Iperf3 to check the interconnection between IDC and Tencent Cloud VPC.

Latency test: use the network test tool Iperf3 to check latency between IDC and Tencent Cloud VPC.

Reliability test: use the network test tool Iperf3 to check the packet loss during the communication between IDC and Tencent Cloud VPC.

This test consists of two metrics: size 1500 and count 2000, size 5000 and count 2000.

Note:

The parameter `size` is the number of packets, and `count` is the sending times. For example, size 1500 and count 2000 means 1500 packets are sent 2000 times.

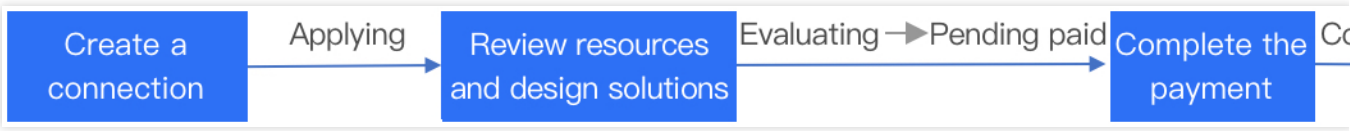
For more information about how to use the Iperf3 tool, see iPerf 3 user documentation.

Applying for Connection

Last updated：2024-01-13 16:40:45

This document introduces how to create a connection in the Tencent Cloud console.

Process



Note:

After creating a connection, contact your Tencent Cloud sales rep promptly to further configure it. If you don't have a sales rep, submit a ticket for application.

1. Create a connection: Synchronize your connection application in the console. Then, the connection status will become **Applying**.

2. Review resources and design solutions: Tencent Cloud will review resources after receiving your connection application. The connection status becomes **Evaluating**. Then, the connection manager will confirm the connection design with you synchronously. After confirmation, the connection status turns to be **Pending paid**.

3. Complete the payment: After the payment is completed in the console, the connection status will be changed to **Constructing**. You also need to contact the carrier and Tencent Cloud to complete the connection construction and acceptance, and confirm the acceptance in the console. The accepted connection will be in **Running** status.

Note:

From February 1, 2021, Tencent Cloud permanently reduces or exempts the initial installation fee for all newly created connections. During the application process, the connection status will be directly transferred from **Evaluating** to **Constructing**, with **Pending paid** status being cancelled.

Directions

Step 1. Create a connection

After the application is submitted, the connection status will become **Applying**. Tencent Cloud will assess resources and provide solutions within three business days.

1. Log in to the Direct Connect console and click **+New** on the **Connections** page.

2. Complete the following configurations and click **OK**.

Parameter	Description	Remarks

Connection name	Set a name for your connection.	You can rename your connection.
Region	Select the geographic area of a physical data center. Tencent Cloud regions are completely isolated from each other to ensure maximum stability and fault tolerance between different regions.	To reduce the access delay and improve the download speed, we recommend you choose the nearest region.
Access point	Select the network service provider of Tencent Cloud connection. We recommend you choose the nearest access point. For details, see Connection Access Point.	A region supported by Tencent Cloud generally has more than two access points, which can realize two-line disaster recovery.
Connection provider	Select a carrier with compliant telecommunication business operation qualifications.	CTCC, CMCC, CUCC, local connection carriers, other carriers in/outside the Chinese mainland.
Cloud port	Supported specifications: 1G, 10G and 100G.	To use 100G ports, submit a ticket.
Port type	Choose fiber optic port or electrical port as needed. The available ports vary with the port type. For example, 1G ports include fiber optic port and electrical port, while 10G ports only include fiber optic port.	Select the appropriate interface based on your bandwidth. For technical support, consult your connection service provider or Tencent Cloud architect/after-sales manager.
Bandwidth cap	Set a bandwidth cap between 1-1,000 Mbps for a 1G port. Set a bandwidth cap between 1-10,000 Mbps for a 10G port.	-
IDC address	Select the specific address of the user IDC.	-
Contact person	Enter the name of customer-side contact person for applying for a connection.	For example, John Smith.
Contact details	Enter the contact details of customer-side contact person for applying for a connection.	-
Applicant email	Enter the email address of the connection applicant.	XXXX@XXXX.com.

Step 2. Review resources and design solutions

After your application for a connection is submitted, Tencent Cloud's 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, its status becomes **Pending paid**. Your connection application may be rejected for any of the following reasons:
Inaccurate information: The access information you entered is incomplete. Modify your application according to the feedback of the Direct Connect representative, and submit again.
Insufficient resources: The access port or uplink bandwidth resources are insufficient. Submit a new application after the Direct Connect representative confirms the resource availability.
Ineligibility: The connection is only available to large-scale organizational customers. After you are eligible, resubmit an application.

Step 3. Complete the payment

After your application is approved, you need to complete the payment on the console. Then the Direct Connect representative will accept the access request and coordinate resources for the connection construction. After the connection is completed and accepted, the connection status becomes **Running**. Perform the following steps to make the payment:
1. Log in to the Direct Connect console.
2. Locate the connection to be paid for in the connection list, and click **Pay Now**.
3. Confirm the Direct Connect information in the pop-up window, and click **OK**.
4. Access the billing platform to complete the payment.

Step 4. Configure the alarm recipient

After a connection is created, Tencent Cloud automatically configures the following metric alarm for its bandwidth utilization, helping you monitor and manage your connection.

Metric	Statistical Period	Condition	Threshold	Duration	Policy
dc_band_rate	One minute	>=	80%	At five consecutive data points	Alarm once a day

The automatically created default alarm policy is not configured with recipient information, and only supports console alarms. You can configure alarm recipients by yourself. For details, see Configuring Alarm Policies.

Subsequent Operations

After the carrier completes the connection construction, you need to test and accept it by creating a direct connect gateway and a dedicated tunnel. The accepted connection will be in **Running** status.
Creating Direct Connect Gateway
Creating a Dedicated Tunnel

Configuring a Route Table

Managing Connections

Last updated：2024-01-13 16:40:45

After the connection is running, you can view or delete the connection, modify its bandwidth, add tags, or perform other operations in the console.

Viewing the Connection

1. Log in to the Direct Connect console and click **Connections** on the left sidebar.
2. In the list, click the **ID**/**Name** of the connection that you want to view.
3. The **Basic info** tab displays the connection details, including connection provider, port type, access point, bandwidth, and other information.

Modifying the Connection Bandwidth

You can change the connection bandwidth in the console to meet your business requirements.

1. Log in to the Direct Connect console and click **Connections** on the left sidebar.
2. Locate the target connection, and click  under the **Bandwidth** column.
3. Specify a new bandwidth value in the edit box and click **OK**.

Note:

If no dedicated tunnel is created, the connection bandwidth should be no less than 1 Mbps, and cannot exceed the port bandwidth.

If there are dedicated tunnels created, the connection bandwidth should be no less than the total bandwidth caps of all tunnels, and cannot exceed the port bandwidth.

The maximum port bandwidth varies with port types as follows:

1 Gbps electronic port: 1,000 Mbps

1 Gbps fiber optic port: 1,000 Mbps

10 Gbps fiber optic port: 10,000 Mbps

100 Gbps fiber optic port: 100,000 Mbps

Adding Tags

To easily locate and manage the connections under your account, perform the following steps to add tags to your connections.

1. Log in to the Direct Connect console and click **Connections** on the left sidebar.
2. Select the connection to which a tag is added, and click **Edit Tags** in the **Operation** column.
3. Select a tag key and tag value in the corresponding drop-down list. You can also click **Manage Tags** to create a tag.
4. Use a tag to locate the connection.
5. Click the edit box in the upper-right corner of the **Connections** page, and select **Tag** in the drop-down list.
6. Enter the tag in the edit box and click the magnifying glass icon.
7. Use a tag to manage the connections.
8. Click

in the upper-right corner of the **Connections** page.

9. In the pop-up window, select the target tags, and click **OK**.

Then the tag keys will appear in the connection list.

Deleting a Connection

You can delete a connection when you no longer need it.

1. Log in to the Direct Connect console and click **Connections** on the left sidebar.
2. Select the connection to delete, and click **Delete** in the **Operation** column.
3. In the pop-up window, check **Confirm Deletion** and click **Confirm**.

Note:

The port monthly rental fees will no longer incur.

Sharing Connection

Last updated：2024-01-13 16:40:45

You can use connections from other accounts to set up dedicated tunnels and also share your connections with other Tencent Cloud customers.
If you are purchasing connection service from a Tencent Cloud partner, normally a shared connection, you need to ask service provider for the UIN of your service provider’s account, the connection instance ID, and the VLANID. For more information, refer to Applying for a Tunnel.

Direct Connect Gateways
Direct Connect Gateway Overview

Last updated：2024-01-13 16:40:45

A direct connect gateway is a traffic entry for Direct Connect that is used to connect Tencent Cloud VPCs with connections (dedicated tunnels). There are two types: VPC-based direct connect gateway and CCN-based direct connect gateway, which are suitable for different use cases.

Use Limits

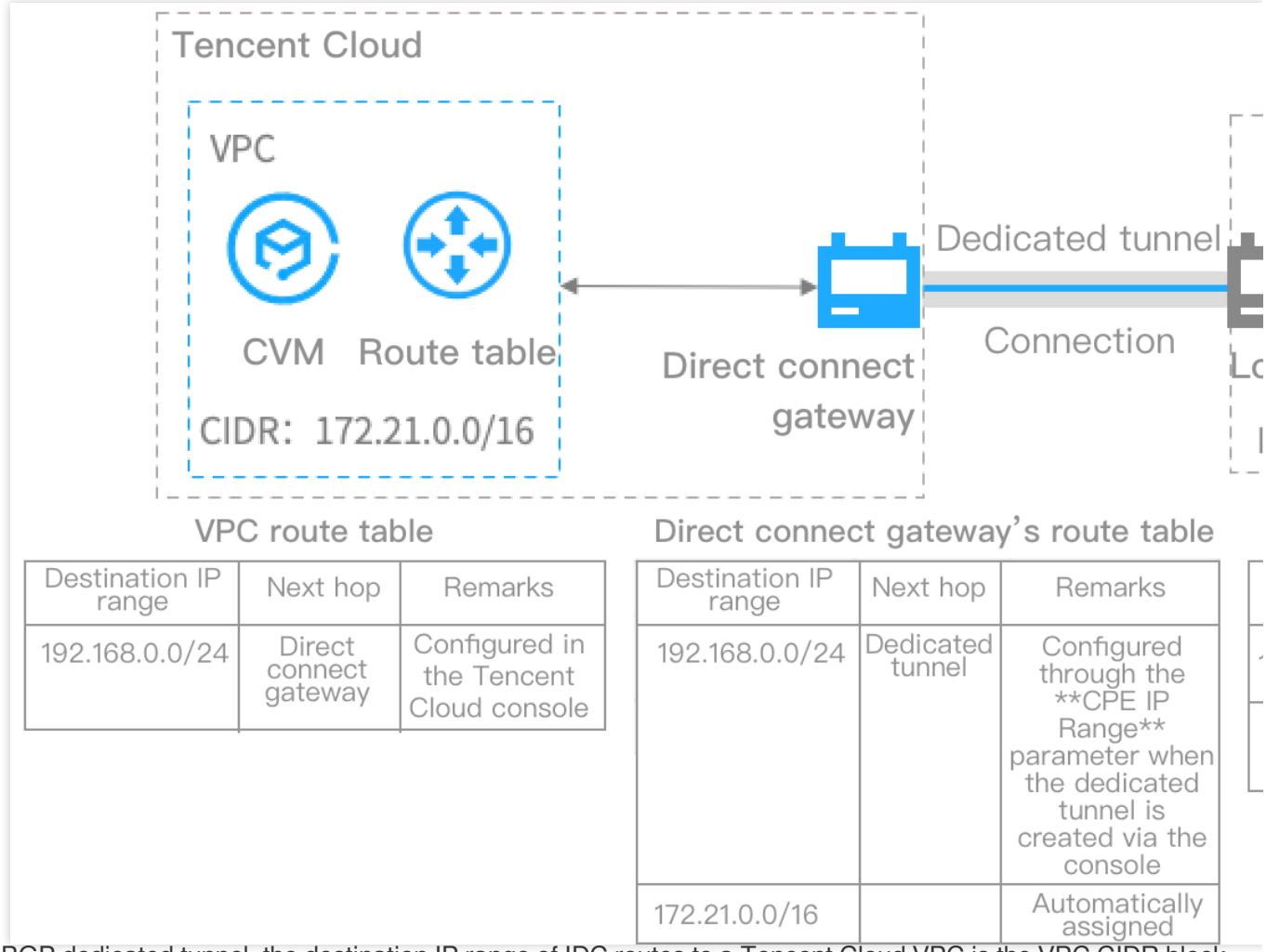
A standard direct connect gateway supports propagating secondary CIDR blocks. Note the following limits:
Up to 10 secondary CIDR blocks can be propagated.
This feature is unavailable to a NAT direct connect gateway.
Direct Connect clears gateway resources that meet all of the following conditions:
Resources created more than 180 days ago.
Resources not bound to a dedicated tunnel for over 90 consecutive days.
Resources generating no business traffic for over 90 consecutive days.

VPC-based Direct Connect Gateway

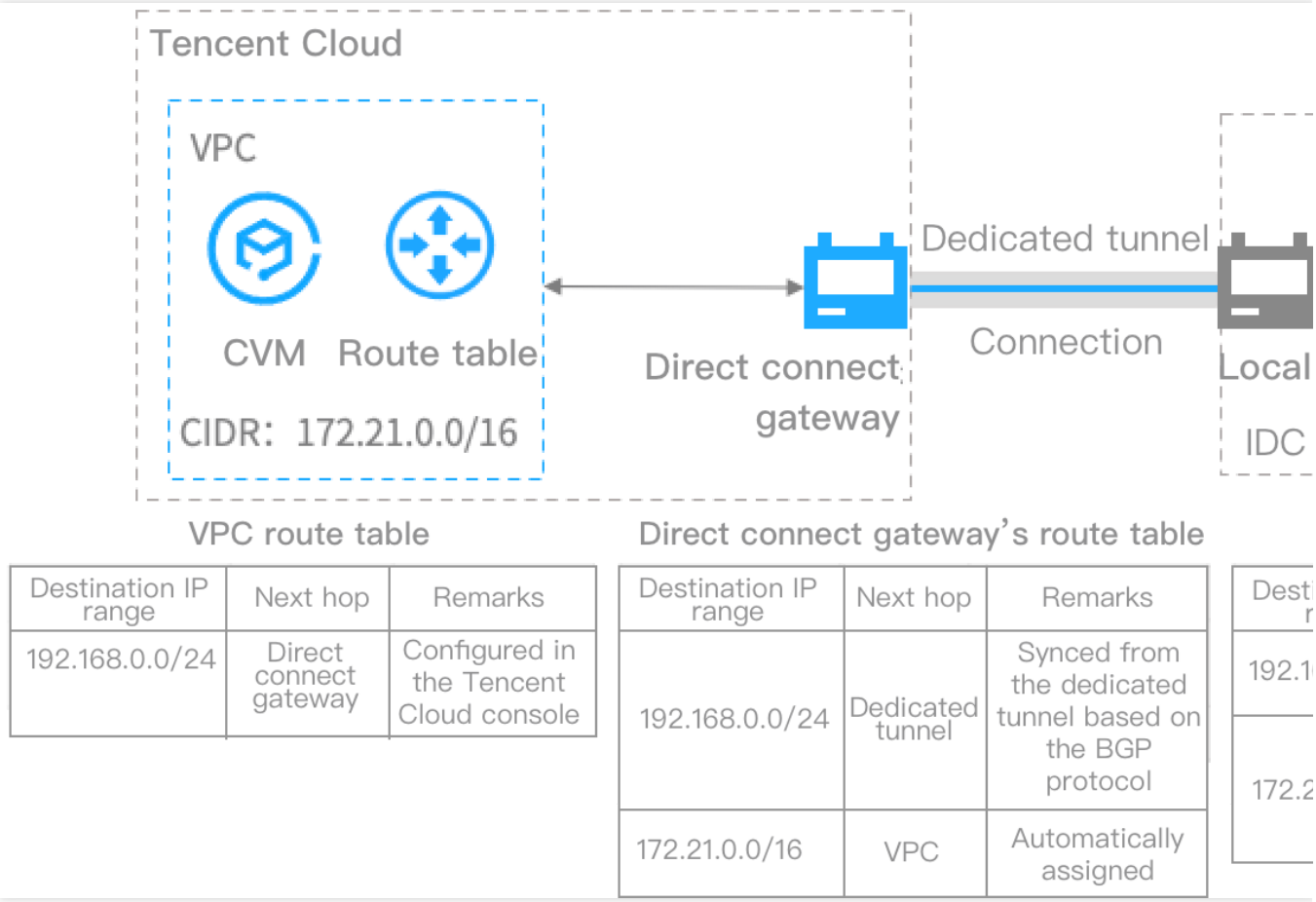
As shown in the Direct Connect network architecture, dedicated tunnel mode will affect the destination IP range of the IDC routes to Tencent Cloud VPCs. See the following table for details.

Dedicated Tunnel Mode	IDC Routes to Tencent Cloud
Static	The IDC routes to Tencent Cloud VPCs are configured in the local router.
BGP	The IDC automatically obtains the VPC CIDR block based on the BGP protocol.

For example, if a VPC-based direct connect gateway is used between a Tencent Cloud VPC and an IDC in the Direct Connect network architecture, the routes for different dedicated tunnels are configured as follows:
For a static dedicated tunnel, the destination IP range of IDC routes to a Tencent Cloud VPC is configured in the local router, such as VPC CIDR block (`172.21.0.0/16`).



For a BGP dedicated tunnel, the destination IP range of IDC routes to a Tencent Cloud VPC is the VPC CIDR block (`172.21.0.0/16`) obtained by the local router based on the BGP protocol.

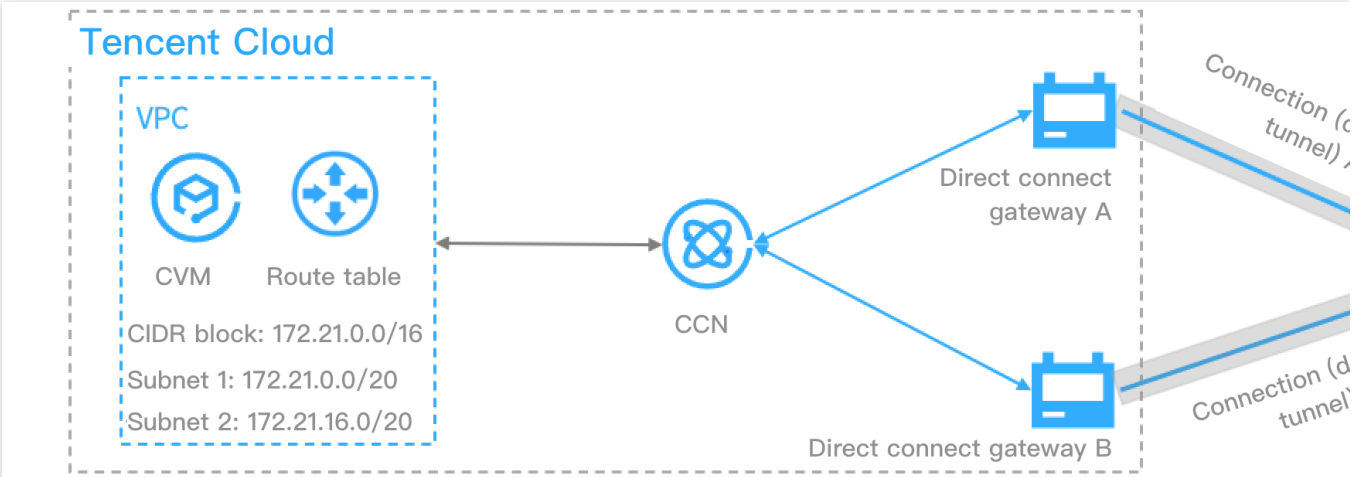


CCN-based Direct Connect Gateway

A CCN-based direct connect gateway can associate one CCN with multiple dedicated tunnels to implement the interconnection between VPCs in the CCN and IDCs. As shown in the Direct Connect network architecture, both the creation time of the direct connect gateway and dedicated tunnel mode will affect the destination IP range of the IDC routes to Tencent Cloud VPCs. See the following table for details.

Creation Time	Dedicated Tunnel Mode	IDC Routes to Tencent Cloud
Before 00:00:00 on September 15, 2020	Static	The IDC routes to Tencent Cloud VPCs are configured in the local router.
	BGP	The IDC automatically obtains the VPC subnet CIDR block based on the BGP protocol.
After 00:00:00 on September 15, 2020	Static	The IDC routes to Tencent Cloud VPCs are configured in the local router.
	BGP	The IDC automatically obtains the VPC CIDR block based on the BGP protocol.

In a Direct Connect network architecture, if the direct connect gateways A and B are created before and after September 15, 2020, 00:00:00 respectively, the routes for different dedicated tunnel modes are as follows:
When both dedicated tunnels are static, the destination IP range of IDC routes to Tencent Cloud VPCs is the VPC CIDR block (`172.21.0.0/16`) configured in the local router. The direct connect gateways A and B have the same routes and receive local IDC traffic evenly.



VPC route table

Destination IP range	Next hop	Remarks
192.168.0.0/24	Direct connect gateway	Automatically synced

CCN route table

Destination IP range	Next hop	Remarks
192.168.0.0/24	Direct connect gateway A	Configured on the **IDC IP Range** page of the direct connect gateway
192.168.0.0/24	Direct connect gateway B	Configured on the **IDC IP Range** page of the direct connect gateway
172.21.0.0/20	VPC	Automatically synced the subnet route from the VPC
172.21.16.0/20	VPC	Automatically synced the subnet route from the VPC

Direct connect gateway A

Destination IP range	Next hop	Ren
192.168.0.0/24	Tunnel A	Conf throu **CPE IP parame the de tunnel i via the
172.21.0.0/16	CCN	Autom ass

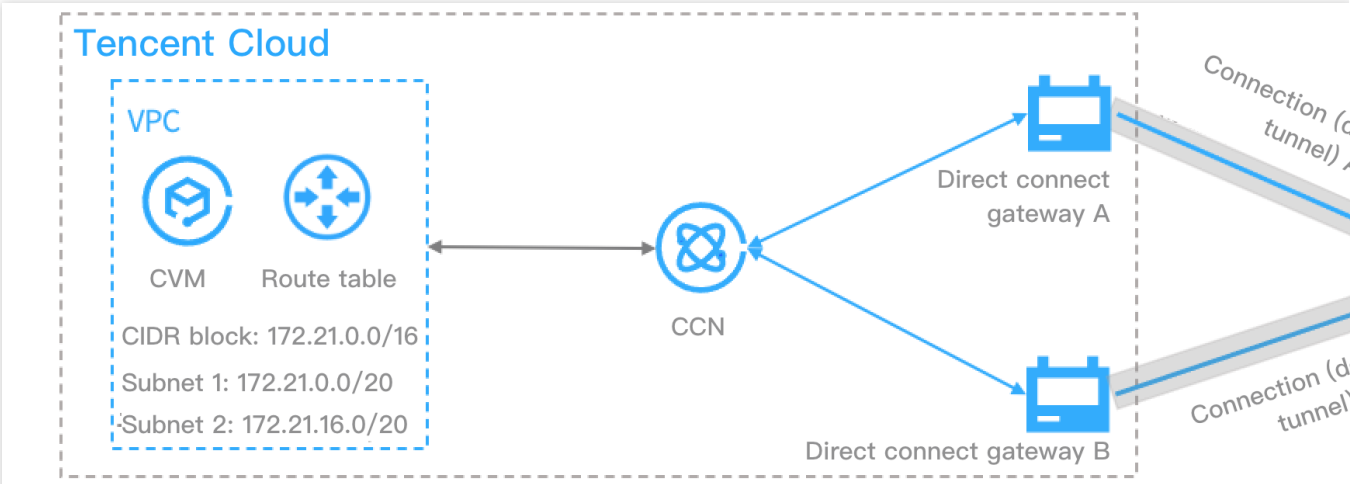
Direct connect gateway B

Destination IP range	Next hop	Ren
192.168.0.0/24	Tunnel A	Conf throu **CPE IP parame the de tunnel i via the
172.21.0.0/16	CCN	Autom ass

When both dedicated tunnels are BGP, the destination IP range synced from the direct connect gateway A to the local router based on the BGP protocol is the subnet CIDR blocks (`172.21.0.0/20` , `172.21.16.0/20`), while that synced from the direct connect gateway B is the VPC CIDR block (`172.21.0.0/16`). The route with the longest mask will be matched and used for forwarding. Therefore, the local router will forward all traffic to the direct connect gateway A. The traffic will be forwarded to the direct connect gateway B only when the direct connect gateway A fails and loses routes.

Note:

For a direct connect gateway created before September 15, 2020, 00:00:00, you can submit a ticket to change its routing policy to VPC CIDR block.



VPC route table

Destination IP range	Next hop	Remarks
192.168.0.0/24	Direct connect gateway	Automatically synced

CCN route table

Destination IP range	Next hop	Remarks
192.168.0.0/24	Direct connect gateway A	Configured on the **IDC IP Range** page of the direct connect gateway
192.168.0.0/24	Direct connect gateway B	Configured on the **IDC IP Range** page of the direct connect gateway
172.21.0.0/20	VPC	Automatically synced the subnet route from the VPC
172.21.16.0/20	VPC	Automatically synced the subnet route from the VPC

Direct connect gateway A

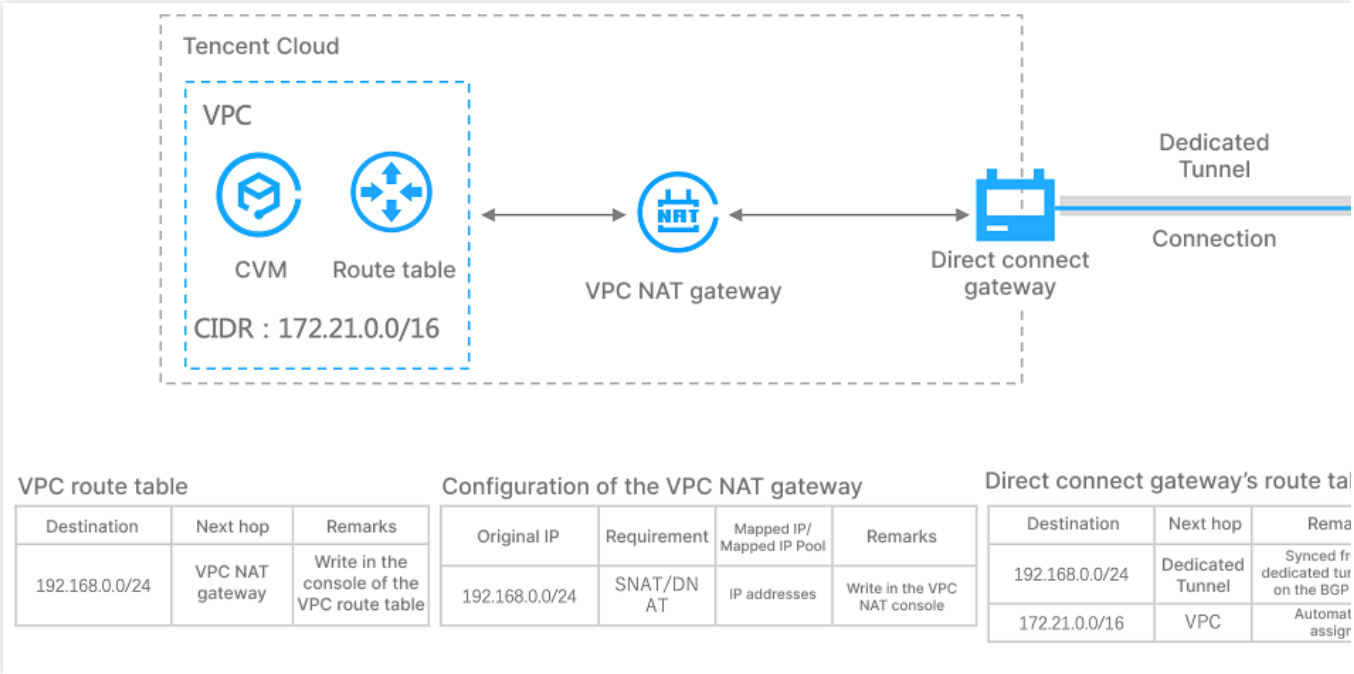
Destination IP range	Next hop	Ren
192.168.0.0/24	Tunnel A	Synced dedicat based o pro
172.21.0.0/20	CCN	Autom assi
172.21.16.0/20	CCN	Autom ass

Direct connect gateway B

Destination IP range	Next hop	Ren
192.168.0.0/24	Tunnel A	Synced dedicat based o pro
172.21.0.0/16	CCN	Autom assi

NAT Direct Connect Gateway

A NAT direct connect gateway prevents IP conflicts between your cloud network space and local IDCs by translating IP addresses.



VPC route table

Destination	Next hop	Remarks
192.168.0.0/24	VPC NAT gateway	Write in the console of the VPC route table

Configuration of the VPC NAT gateway

Original IP	Requirement	Mapped IP/ Mapped IP Pool	Remarks
192.168.0.0/24	SNAT/DNAT	IP addresses	Write in the VPC NAT console

Direct connect gateway's route tal

Destination	Next hop	Rema
192.168.0.0/24	Dedicated Tunnel	Synced fr dedicated tur on the BGP
172.21.0.0/16	VPC	Automat assigr

We recommend that you use BGP dedicated tunnels, so that a local IDC automatically obtains the CIDR block for traffic to the destination VPC.

When you configure routing rules for a VPC NAT gateway, SNAT-Local-Layer-3, SNAT-Local-Layer-4, and DNAT-Peer-Layer-4 rules are mapped automatically. Peer-Layer-3 rules cannot be mapped. In addition, the VPC CIDR block is not published by default. Therefore, you must use a Peer-Layer-3 rule with a Local-Layer-3 or Local-Layer-4 rule.

NAT Direct Connect Gateway was optimized in March 2023. You can bind a private NAT gateway to the direct connect gateway, and configure the IP mappings at the NAT gateway. The following table compares the old and new configuration methods:

Previous Parameter	New Parameter	
Local IP Translation	Mapping Direction: Local	Mapping Type: Layer-3
Peer IP Translation	Mapping Direction: Peer	Mapping Type: Layer-3
Local Source IP Port Translation	Mapping Direction: Local	Mapping Type: Layer-4
Local Destination IP Port Translation	Mapping Direction: Peer	Mapping Type: Layer-4

Local: translates the private IP addresses of the VPC.Peer: translates the private IP addresses of the network on the opposite end of the VPC. For example, if the peer is an IDC, IP addresses of the IDC are translated.Layer 3: translates only IP addresses.Layer 4: maps IP addresses and ports to random ports within a specified IP pool.

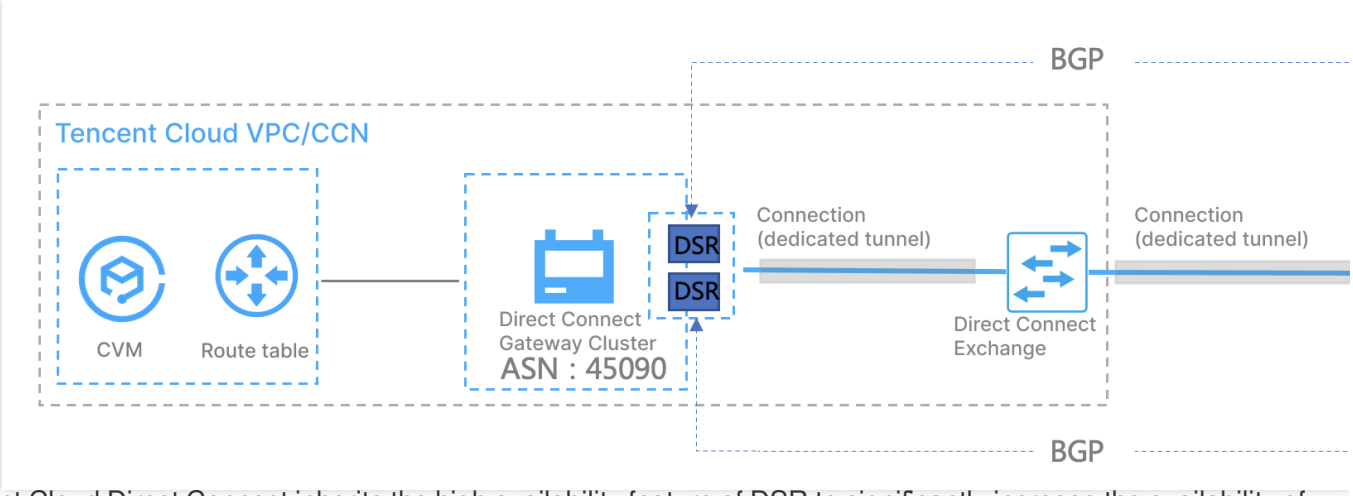
High Availability Overview

A direct connect gateway is a bridge connecting cloud network and user IDC off the cloud, thus its high availability is critical to stable operation of business.

DSR overview

Tencent's self-developed Disaggregated Software-Defined Router (DSR) is a new generation of software router system based on SDN, NFV and microservice techniques. It is used to replace classic business routers to avoid single-point failures at the layers of system architecture, routing control and data forwarding. Currently, it is broadly deployed in Tencent's large-scale, high-performance and highly elastic cloud network system.
Compared to classic network physical devices, DSR supports multiple cloud computing virtualization techniques such as NFV and microservice. It adopts a distributed architecture to effectively prevent overall impact caused by the failure of a single component, so as to discover, isolate and recover from failures at the component level automatically.

High availability design for direct connect gateways



Tencent Cloud Direct Connect inherits the high availability feature of DSR to significantly increase the availability of the direct connect gateways.
At the route forwarding plane, DSR provides two active-active routing systems for each dedicated tunnel through multi-site active-active technique with each routing system distributed independently in a different DSR cluster. Meanwhile, the DSR clusters provide two Tencent Cloud border IP addresses to implement active-active routing system at the control plane. Thus, the local router on IDC side has created BGP neighbor adjacency with the two clusters respectively via BGP protocol to effectively ensure high availability of business in case of DSR cluster upgrade or single cluster failure and avoid impact on business caused by single BGP neighbor adjacency interruption and route convergence.
At the data forwarding plane, DSR implements distributed forwarding of massive data and traffic through large-scale cluster control and self-developed cluster scaling technique. It adjusts and removes exceptional service nodes dynamically through real-time monitoring mechanism in the cluster to ensure the availability of single cluster. Meanwhile, it adopts large-scale cluster scaling technique to enable horizontal scaling among multiple clusters for the business to ensure availability across clusters.

Recommended configuration

1. Tencent Cloud side: DSR learns the routes from Tencent Cloud to user IDC via BGP protocol. The next hop is the user's local router.
2. User IDC side: user's local router learns the routes to Tencent Cloud VPC via BGP protocol. The next hop is the IP addresses of the two DSR clusters.

Creating a Direct Connect Gateway

Last updated：2024-01-13 16:40:45

This document describes how to create a direct connect gateway and provides information on the inbound route.

Prerequisites

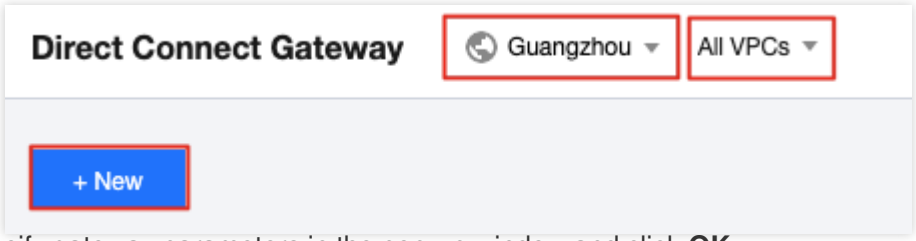
Apply for a connection. For more information, see Applying for a Connection.
If you want to use VPC, set up a VPC. For more information, see Building Up an IPv4 VPC.
If you want to use CCN, set up a CCN instance. For more information, see Creating a CCN Instance.
If you want to use NAT Direct Connect Gateway, create a VPC NAT gateway.
Note:
NAT Direct Connect Gateway is available only for users who are added to the corresponding allowlist. To use the feature, please submit a ticket. For more information about the comparison between the old and new methods for configuring the mapping parameters of NAT Direct Connect Gateway, see Overview.

Use Limits

A standard direct connect gateway supports propagating secondary CIDR blocks. Note the following limits:
Up to 10 secondary CIDR blocks can be propagated.
This feature is unavailable to a NAT direct connect gateway.

Directions

1. Log in to the Direct Connect console, and click **Direct connect gateway** in the left sidebar.
2. Select a region and VPC at the top of the **Direct connect gateway** page, and click **+ New**.



3. Specify gateway parameters in the pop-up window and click **OK**.

Field	Description
Name	Enter a name for the direct connect gateway.
AZ	Select the AZ.
Associated Network	Select the type of the direct connect gateway. Valid values: CCN, VPC, and NAT.
Network	Select an instance to which the created direct connect gateway associate based on the selected network type.
Gateway type	If `VPC` is selected for **Associated Network**, the network address translation feature is not supported. If `NAT` is selected for **Associated Network**, the network address translation feature is supported and you need to configure the translation rules for the NAT gateway.

Inbound Routes

The destination of the inbound routes (from your IDC to a Tencent Cloud VPC) are affected by both the creation time of the direct connect gateway and dedicated tunnel mode. For more information, see Direct Connect Gateway Overview.

Gateway type	Creation Time	Dedicated Tunnel Mode	IDC Routes to Tencent Cloud

VPC-based direct connect gateway	No limit	Static	The inbound routing policy is configured in the local router.
		BGP	The IDC automatically obtains the VPC CIDR block based on the BGP protocol.
CCN-based direct connect gateway	Before 00:00:00 on September 15, 2020	Static	The inbound routing policy is configured in the local router.
		BGP	The IDC automatically obtains the subnet CIDR block based on the BGP protocol.
	After 00:00:00 on September 15, 2020	Static	The inbound routing policy is configured in the local router.
		BGP	The IDC automatically obtains the VPC CIDR block based on the BGP protocol.
NAT direct connect gateway	No limit	Static	The inbound routing rule is configured in the local router.The next hop of the VPC route must point to a VPC NAT gateway.
		BGP	The next hop of the VPC route must point to a VPC NAT gateway.

Related Operations

After creating a CCN-based direct connect gateway, you need to add IDC IP ranges to the direct connect gateway to implement network communication. For more information, see Publishing IDC IP Ranges to CCN.
After creating a VPC-based direct connect gateway, you need to configure the VPC route table to implement network communication. For more information, see Configuring the Route Table.

CCN-based Direct Connect Gateways Publishing IDC IP Ranges to CCN

Last updated：2024-01-13 16:40:45

After associating a CCN instance with the direct connect gateway, you need to configure a routing policy for the CCN instance, with the direct connect gateway as the next hop and IDC IP range as the destination to implement communication. The routing policy can be either manually entered (Static) or automatically synced (BGP). For more information, see Route Overview. This document describes how to publish IP ranges on the direct connect gateway to CCN.

Note:

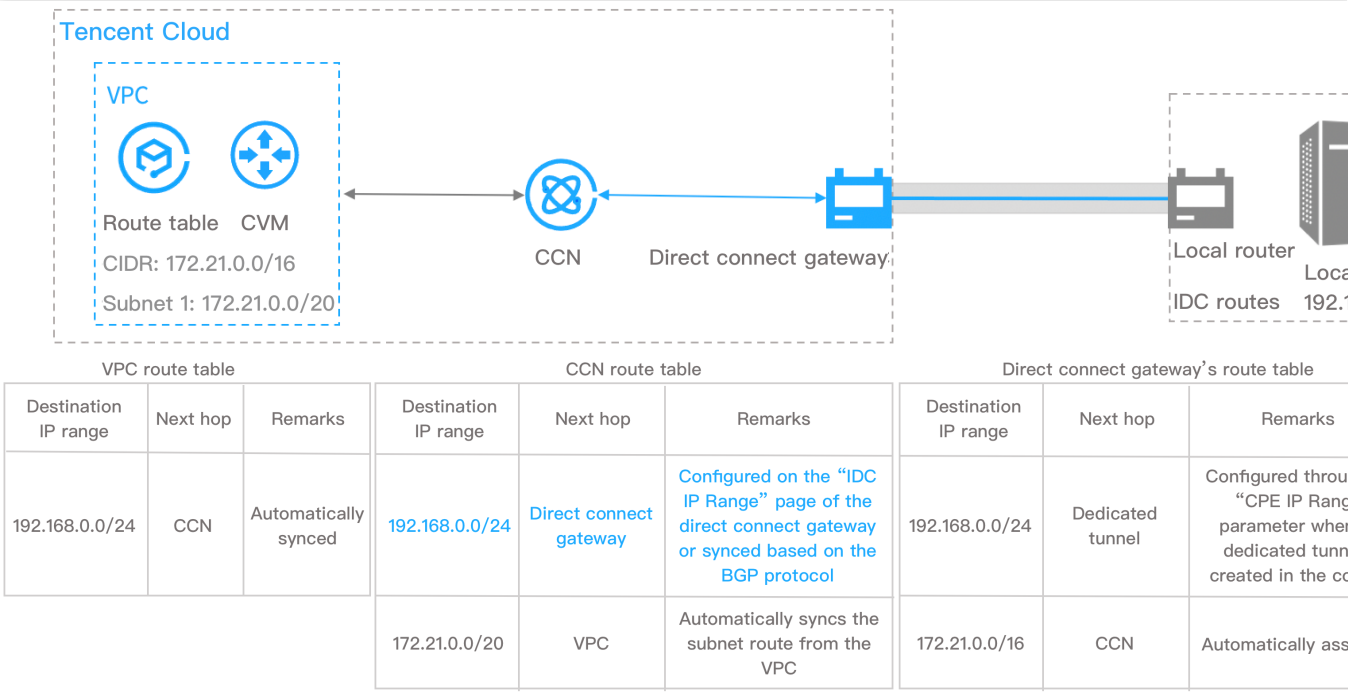
Up to 20 routes can be published to CCN through a direct connect gateway. To publish more routes, submit a ticket.

Background

As shown in the following Direct Connect network architecture, your IDC associated with the CCN-based direct connect gateway and CCN can communicate with a Tencent Cloud VPC. The destination IP range of VPC routes to IDC is `192.168.0.0/24` . After the IDC IP range is configured on the direct connect gateway, the CCN route table will add a routing policy with the direct connect gateway as the next hop and `192.168.0.0/24` as the destination to realize the route propagation.

Note:

If you configure multiple IDC IP ranges on the direct connect gateway, CCN will forward the route with the longest mask. For more information, see Route Overview.



VPC route table

Destination IP range	Next hop	Remarks
192.168.0.0/24	CCN	Automatically synced

CCN route table

Destination IP range	Next hop	Remarks
192.168.0.0/24	Direct connect gateway	Configured on the "IDC IP Range" page of the direct connect gateway or synced based on the BGP protocol
172.21.0.0/20	VPC	Automatically syncs the subnet route from the VPC

Direct connect gateway's route table

Destination IP range	Next hop	Remarks
192.168.0.0/24	Dedicated tunnel	Configured throu "CPE IP Rang parameter wher dedicated tunn created in the cc
172.21.0.0/16	CCN	Automatically ass

Prerequisite

You have created a CCN-based direct connect gateway as instructed in Creating Direct Connect Gateway.

How It Works

1. Log in to the Direct Connect console, and click **Direct Connect Gateway** in the left sidebar.
2. Select a region and a VPC at the top. Click the ID/Name of the target instance to enter its details page.
3. Click the **Publish IP range** tab on the details page.

The IP range published is an IDC IP range that specifies the direct connect gateway route to CCN. When receiving the route, CCN automatically adds a route with the direct connect gateway as the next hop and IDC IP range as the destination.

4. (Optional) Associate with CCN.

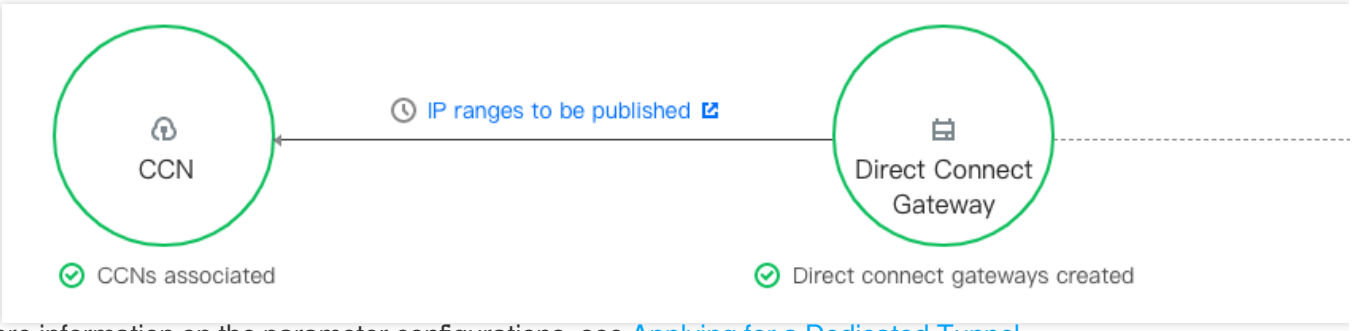
If you did not specify a CCN instance when creating the direct connect gateway, click **Associate with CCN**, select a CCN instance to be associated in the pop-up window, and click **OK**.

Then the CCN instance will be associated and the CCN icon becomes green. The dotted line between the direct connect gateway and CCN changes to solid, indicating that the interconnection between them is established.

5. Create a dedicated tunnel.

A dedicated tunnel is the network segmentation of a connection. It provides a linkage of IDC to Tencent Cloud.

Under the **Dedicated tunnels** icon connected with the direct connect gateway, click **Create dedicated tunnel** to redirect to the **Create dedicated tunnels** page, where you can configure a dedicated tunnel.



For more information on the parameter configurations, see Applying for a Dedicated Tunnel.

Then the dedicated tunnel is created and the **Dedicated tunnels** icon becomes green. The dotted line between direct connect gateway and dedicated tunnel changes to solid, indicating the direct connect gateway is configured with a dedicated tunnel.

6. Publish IDC IP ranges to CCN.

After an IDC IP range is published to CCN, the CCN route is synced to the direct connect gateway, while whether the direct connect gateway route is synced to CCN depends on the publishing method of the IDC IP range.

Custom: the manual configuration mode. CCN obtains the specified direct connect gateway route.

Auto-propagation: the BGP mode. CCN automatically obtains the direct connect gateway route published from the dedicated tunnel. But it depends on the publishing time.

Custom

Auto-propagation

Switching methods

Formerly named **Static** or manual configuration.

1. (Optional) Select a CCN instance in the **Publish rules** section.

Perform this step if you want to associate one CCN instance with the direct connect gateway or change the associated CCN instance.

Note:

The **Publishing method** defaults to **Custom**. To switch to **Auto-propagation**, submit a ticket.

2. Click the **Custom** tab on the **IP range details** page. Click **Create** and enter the information of the IP range that is published to CCN. Click **Save**.

Then the direct connect gateway will publish the IDC IP range you entered to CCN.

Note:

Up to 100 IDC IP ranges can be published. To publish more IDC IP ranges, please submit a ticket.

Formerly named **BGP mode**. To use it, please submit a ticket.

1. (Optional) Select a CCN instance in the **Publish rules** section.

Perform this step if you want to associate one CCN instance with the direct connect gateway or change the associated CCN instance.

Note:

Auto-propagation is selected after this feature is enabled. If needed, you can select **Custom** and complete the relevant configurations.

Either **Custom** or **Auto-propagation** can be checked.

2. Configure IDC IP ranges.

When **Auto-propagation** is selected, the direct connect gateway automatically obtains the IDC IP range without needing configuration.

Note:

Publishing IDC IP ranges may be delayed for one minute. If there are any updates on the IDC IP range, please refresh the current page.

You can switch between the two methods for publishing the IDC IP ranges through the direct connect gateway to CCN.

Switching to auto-propagation

Submit a ticket to enable the auto-propagation feature.

The custom IP ranges published to CCN will be withdrawn after the switching. The information of IDC IP ranges will be automatically synced to the direct connect gateway and published to CCN.

Switching to custom

Configure IP ranges to be published to CCN on the **Custom** tab on the **IP range details** page after the switching.

7. View the published IDC IP ranges.

The published IDC IP ranges are shown in the **IP range details** segment.

Viewing Route Tables

Last updated：2024-01-13 16:40:45

If you use a CCN-based direct connect gateway in the Direct Connect network architecture, you can view the IDC routes and CCN routes to the direct connect gateway on the console.

Limits

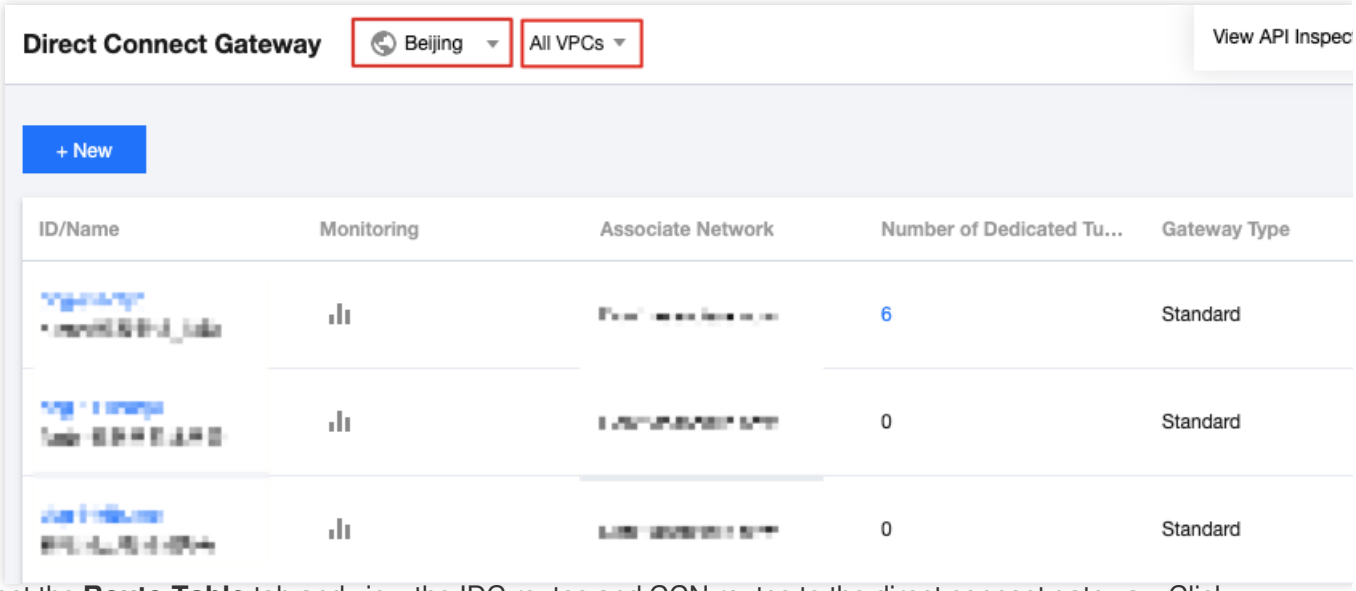
The route table feature of the direct connect gateway is currently in canary release. To try it out, please submit a ticket.
This feature is unavailable in Taiwan (China) and Canada regions.

Prerequisites

You have created a CCN-based direct connect gateway as instructed in Creating Direct Connect Gateway.
You have applied for a dedicated tunnel as instructed in Applying for a Tunnel and associated with the direct connect gateway.
You have added IDC IP ranges to the direct connect gateway as instructed in Adding IDC IP Ranges to the Direct Connect Gateway.

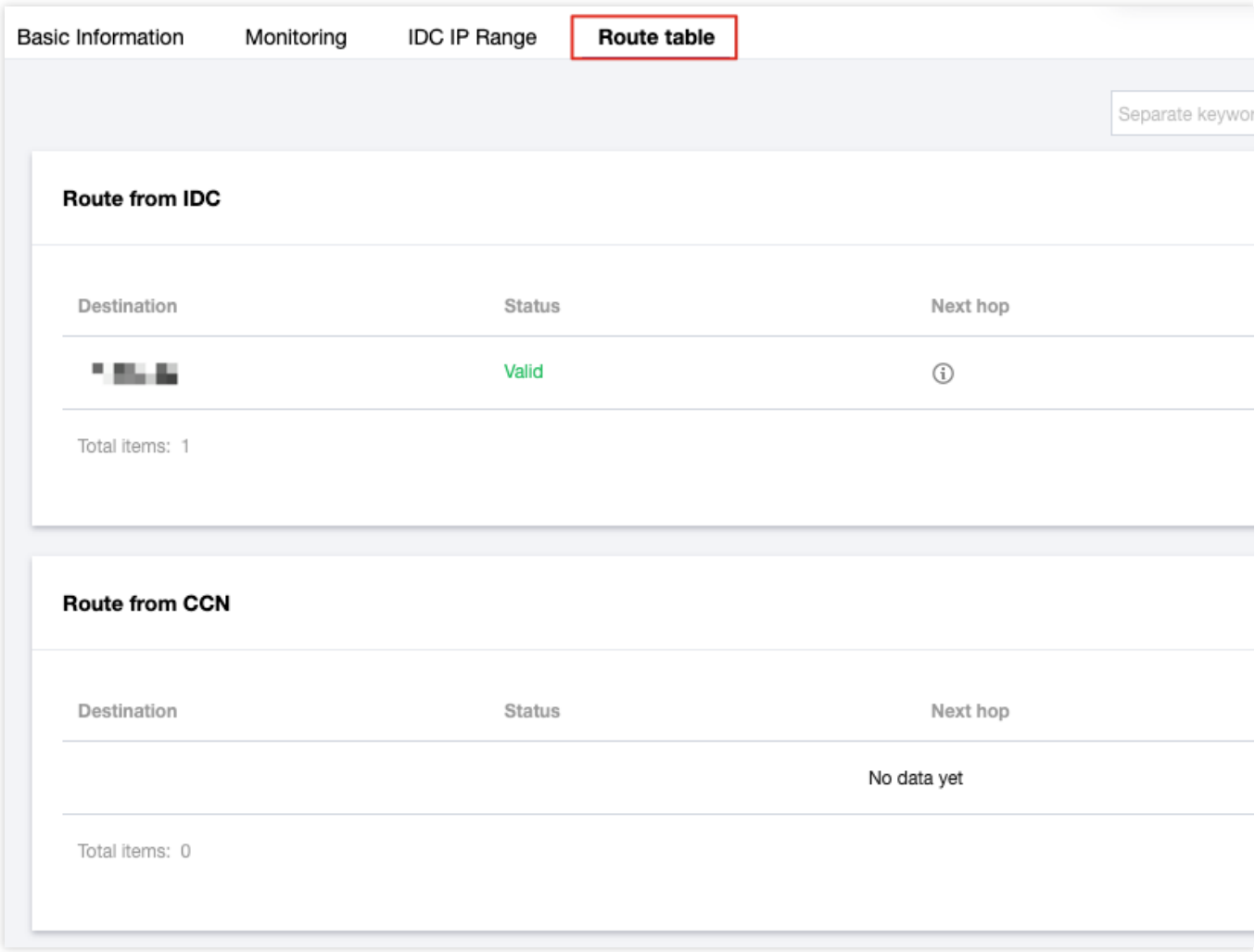
Directions

1. Log in to the Direct Connect Gateway console.
2. Select a region and VPC at the top of the **Direct Connect Gateway** page. Click the **ID/Name** of the target direct connect gateway to enter its details page.



3. Select the **Route Table** tab and view the IDC routes and CCN routes to the direct connect gateway. Click

to download the route table information.



VPC-based Direct Connect Gateways Configuring the Network Address Translation (NAT)

Last updated：2024-01-13 16:40:45

You can configure IP translation and IP port translation for Direct Connect gateways of NAT type as follows:

Note:

This document describes how to configure NAT for a V3R1 direct connect gateway of the NAT type. To do so for a V3R2 direct connect gateway, you only need to bind a private NAT gateway to the direct connect gateway when you create the direct connect gateway. The IP mappings must be configured at the NAT gateway.

Configuring IP Translation

Configuring IP Port Translation

Sample Configurations

Configuring IP Translation

Configuring local IP translation

Rules and limitations

The source IP must fall within the CIDR range of the VPC.

The mapped IP cannot fall within the CIDR range of the VPC in which the Direct Connect gateway resides.

The source IP must be unique. In other words, an IP in a VPC can only be mapped to one IP.

The mapped IP must be unique. In other words, multiple IPs in a VPC cannot be mapped to one IP.

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

The local IP translation of a Direct Connect gateway supports up to 100 IP mappings, each supporting up to 20 ACL rules. To increase the quotas, please submit a ticket.

Directions

1. Log in to the VPC console.
2. In the left sidebar, click **Direct connect gateway** to go to the management page.
3. Click the ID of the Direct Connect gateway of NAT type to go to its details page.
4. On the details page of the direct connect gateway, click the **Local IP translation** tab.
5. At the top left of the **IP mapping** page, click **Add** to add a local IP mapping.
6. In the pop-up window, enter the source IP, mapped IP, and notes, and click **OK**.

7. (Optional) When a new local IP mapping is created, an ACL rule that allows all inbound and outbound traffic is added by default, which means the local IP translation takes effect for all dedicated tunnels. You can edit the ACL rule to change the scope of the local IP translation.

Note:

When the Direct Connect gateway is also configured with peer IP translation, the **destination IP** of the ACL rule for the local IP translation should be the **mapped IP of peer IP translation**, instead of the source IP.

For a ACL rule of local IP translation, you can configure protocol (TCP or UDP), source port, destination IP, and destination port. If port and IP are left blank, they default to ALL; if ALL is selected for protocol, then All is selected for port and IP by default.

8. On the **IP mapping** page, click **Edit ACL rule** to the right of the IP mapping.
9. At the bottom of the list of existing ACL rules, click **+ New line** to add an ACL rule, and click **Save**.
10. (Optional) Modify or delete existing ACL rules when ACL rules are in the editing state, and click **Save**.
11. (Optional) Click

to show all ACL rules of the IP mapping on the **IP mapping** page, click **Modify** or **Delete** to the right of the rule that you want to manage, and confirm the action.

12. (Optional) To modify a local IP mapping, click **Modify IP mapping** to the right of the IP mapping on the **IP mapping** page. Modify the source IP, mapped IP, and notes of the local IP mapping as needed and click **OK** for the modification to take effect.
13. (Optional) To delete a local IP mapping, click **Delete** to the right of the IP mapping on the **IP mapping** page, and confirm the action. Deleting a IP mapping deletes the ACL rules associated with it.

Configuring peer IP translation

Rules and limitations

The mapped IP cannot fall within the CIDR range of the VPC in which the Direct Connect gateway resides.

The source IP must be unique. In other words, a Direct Connect peer IP can only be mapped to one IP.

The mapped IP must be unique. In other words, multiple Direct Connect peer IPs cannot be mapped to the same IP.

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

The peer IP translation of a Direct Connect gateway supports up to 100 IP mappings. To increase the quota, please submit a ticket.

Directions

1. Log in to the VPC console.
2. In the left sidebar, click **Direct connect gateway** to go to the management page.
3. Click the ID of the Direct Connect gateway of NAT type to go to its details page.

4. On the details page of the direct connect gateway, click the **Peer IP Translation** tab.
5. At the top left of the **IP mapping** page, click **Add** to add a peer IP mapping.
6. In the pop-up window, enter the source IP, mapped IP, and notes, and click **OK**.
7. (Optional) To modify a peer IP mapping, click **Modify IP mapping** to the right of the IP mapping on the **IP mapping** page. Modify the source IP, mapped IP, and notes of the peer IP mapping as needed and click **OK** for the modification to take effect.
8. (Optional) To delete a peer IP mapping, click **Delete** to the right of the IP mapping on the **IP mapping** page, and confirm the action.

Configuring IP Port Translation

Configuring local source IP port translation

Note:
If local IP translation conflicts with local IP port translation, local IP translation takes precedence.

Rules and limitations

The mapped IP pool cannot fall within the CIDR range of the VPC in which the Direct Connect gateway resides.
ACL rules for multiple mapped IP pools should not overlap. Otherwise, this will cause network address translation conflicts.
IP addresses between multiple mapped IP pools should not overlap.
Mapped IP pools only support single IPs or continuous IPs, and the /24 IP range of continuous IPs should be consistent. For example, “192.168.0.1 - 192.168.0.6” is supported, but “192.168.0.1 - 192.168.1.2” is not.
Mapped IP pools should not be broadcast address (255.255.255.255), Class D addresses (224.0.0.0 - 239.255.255.255), and Class E addresses (240.0.0.0 - 255.255.255.254).
Local source IP port translation supports up to 100 mapped IP pools, each supporting up to 20 ACL rules. To increase the quotas, please submit a ticket.

Directions

1. Log in to the VPC console.
2. In the left sidebar, click **Direct connect gateway** to go to the management page.
3. Click the ID of the Direct Connect gateway of NAT type to go to its details page.
4. On the details page of the direct connect gateway, click the **Local source IP port translation** tab.
5. At the top left of the **Mapping IP pool** page, click **Add** to add a mapped IP pool.
6. In the pop-up window, enter the mapped IP pool (IPs or IP range in the form of “A - B”) and notes, and click **OK**.
7. By default, the ACL rule of a new mapped IP pool denies all inbound and outbound traffic. You need to edit the ACL rule to implement network translation.

Note:

When the Direct Connect gateway is also configured with peer IP translation, the **destination IP** of the ACL rule for the local source IP port translation should be the **mapped IP of peer IP translation**, rather than the source IP.
For an ACL rule of local source IP port translation, you can configure protocol (TCP or UDP), source IP, source port, destination IP, and destination port.
8. On the **Mapping IP pool** page, click **Edit ACL rule** to the right of the mapped IP pool.
9. At the bottom of the list of existing ACL rules, click **+ New line** to add an ACL rule, and click **Save**.
10. (Optional) Modify or delete existing ACL rules when ACL rules are in the editing state, and click **Save**.
11. (Optional) Click

to show all ACL rules of the mapped IP pool on the **Mapping IP pool** page, click **Modify** or **Delete** to the right of the rule that you want to manage, and confirm the action.
12. (Optional) To modify a mapped IP pool, click **Modify mapping IP pool** to the right of the mapped IP pool on the **Mapping IP Pool** page, and modify the IP and notes of the mapped IP pool as needed.
13. (Optional) To delete a mapped IP pool, click **Delete** to the right of the mapped IP pool on the **Mapping IP Pool** page, and confirm the action. Deleting a mapped IP pool deletes the ACL rules associated with it.

Configuring local destination IP port translation

Rules and limitations

The source IP must fall within the CIDR range of the VPC in which the Direct Connect gateway resides.
The source IP port must be unique. In other words, an IP port in a VPC can only be mapped to one IP port.
The mapped IP port cannot fall within the CIDR range of the VPC.
The mapped IP port must be unique. In other words, multiple IP ports in a VPC cannot be mapped to one IP port.
Source IPs and mapped IPs should not be broadcast address (255.255.255.255), Class D addresses (224.0.0.0 - 239.255.255.255), or Class E addresses (240.0.0.0 - 255.255.255.254).
Local destination IP port translation supports up to 100 IP mappings. To increase the quota, you can submit a ticket.

Directions

1. Log in to the VPC console.
2. In the left sidebar, click **Direct connect gateway** to go to the management page.
3. Click the ID of the Direct Connect gateway of NAT type to go to its details page.
4. On the details page of the direct connect gateway, click the **Local destination IP port translation** tab.
5. At the top left of the **IP port mapping** page, click **Add** to add a new local destination IP port mapping.
6. In the pop-up window, select the protocol. Enter the source IP port, mapped IP port, and notes, and click **OK**.
7. (Optional) To modify a local destination IP port mapping, click **Modify IP port mapping** to the right of the IP port mapping on the **IP port mapping** page, and modify the mapping relationship and notes of the IP port mapping as needed.

8. (Optional) To delete a local destination IP port mapping, click **Delete** to the right of the IP port mapping on the **IP port mapping** page, and confirm the action.

Sample Configuration

Local IP translation configuration example

IP A `192.168.0.3` in a VPC is the source IP, and is mapped to IP B `10.100.0.3` through local IP translation:
The network packet source IP of the active access from IP A to the Direct Connect peer is automatically changed to `10.100.0.3`.
All network packets accessing `10.100.0.3` from the Direct Connect peer will automatically point to IP A `192.168.0.3`.

Peer IP translation configuration example

Direct Connect peer IP D `10.0.0.3` is the source IP, and is mapped to IP C `172.16.0.3` through peer IP translation:
The network packet source IP of the active access from IP D `10.0.0.3` to the VPC is automatically changed to IP C `172.16.0.3`.
All network packets accessing IP C `172.16.0.3` from the VPC will automatically point to IP D `10.0.0.3`.

Local source IP port translation configuration example

The VPC C network IP range `172.16.0.0/16` connects the third-party bank A and B via Direct Connect, where the peer network IP range of bank A is `10.0.0.0/28`, requiring the connected network IP range `192.168.0.0/28`, and the peer network IP range of bank B is `10.1.0.0/28`, requiring the connected network IP range `192.168.1.0/28`. Two local source IP port translations can be configured as follows:

Configuration		Local Source IP Port Translation A	Local Source IP Port Translation B
Mapped IP pool		192.168.0.1 - 192.168.0.15	192.168.1.1 - 192.168.1.15
ACL rule	Protocol	All	All
	Source IP	172.16.0.0/16	172.16.0.0/16
	Source port	-	-
	Destination IP	10.0.0.0/28	10.1.0.0/28
	Destination port	-	-

After configuration, the network requests from VPC C to access bank A and bank B will be translated to random ports in the mapped IP pools based on the corresponding ACL rules to access the corresponding dedicated tunnels.

Local destination IP port translation configuration example

For the VPC C IP range `172.16.0.0/16`, if you only want to open some of the ports to the active access of the Direct Connect peer, you can configure local destination IP port mapping A and B as follows:
Local destination IP port mapping A: source IP port is `172.16.0.1:80` and mapped IP port is `10.0.0.1:80`.
Local destination IP port mapping B: source IP port is `172.16.0.1:8080` and mapped IP port is `10.0.0.1:8080`.
After configuration, the Direct Connect peer can access ports `10.0.0.1:80` and `10.0.0.1:8080` to implement active access to ports `172.16.0.1:80` and `172.16.0.1:8080` in VPC C.

Configuring a Route Table

Last updated：2021-07-23 16:37:19

After creating a direct connect gateway and constructing a dedicated tunnel, you can configure the route table of the VPC in the console to forward the traffic passing through Direct Connect to the direct connect gateway.

1. Log in to the VPC console.
2. Click **Route Tables** on the left sidebar to access the **Route Table** page.
3. Click the **ID**/**Name** of the route table with which you want to associate the direct connect gateway to go to the details page.
4. Click **+ New routing policies**.
5. In the pop-up window, enter the destination IP range, select **Direct Connect Gateway** for **Next hop type**, and select the specific gateway instance for **Next hop**.

Configure a routing policy as instructed below.

Parameter	Configuration
Destination	Specify the destination IP range to which you want to forward traffic. Configure it as follows:Enter an IP range. If you want to enter a single IP, set the mask to 32 (for example, `172.16.1.1/32`). The destination cannot be an IP range of the VPC where the route table resides, because the local route already allows private network interconnection in this VPC.
Next hop type	Select **Direct Connect Gateway**.
Next hop	Select the specified direct connect gateway instance to which the traffic is forwarded.
Notes	Enter the route description for resource management. This parameter is optional.
Add a line	Configure multiple routing policies if needed. You can click the deletion icon in the **Operation** column to delete the unnecessary routing policies. A custom route table should contain at least one routing policy.

6. Click **Create**.

Now, you can direct the traffic from the specific destination to the direct connect gateway to associate it with your local IDC.

Binding to a NAT Gateway

Last updated：2024-01-13 16:40:45

If you have created a direct connect gateway and your business needs to access the public network through a NAT Gateway, you need to bind the direct connect gateway to the NAT Gateway. This document describes how to bind the direct connect gateway to a NAT Gateway.

Prerequisite

You have created a VPC.
You have created a VPC-based direct connect gateway.
You have created a NAT Gateway.

Binding to a NAT Gateway

1. Log in to the VPC console.
2. In the left sidebar, click **Direct Connect Gateway** to go to the management page.
3. In the list of direct connect gateways, click the name of the direct connect gateway that needs to be bound to a NAT Gateway to open the details page.
4. Select the desired NAT Gateway on the **Basic Information** page.

Unbinding from a NAT Gateway

If you do not need the NAT Gateway to which the direct connect gateway is bound, you can go to the **Basic Information** tab on the direct connect gateway details page to unbind the direct connect gateway from it.
1. Log in to the VPC console.
2. In the left sidebar, click **Direct Connect Gateway** to go to the management page.
3. In the list of direct connect gateways, click the name of the direct connect gateway that needs to be unbound from the NAT Gateway to open the details page.
4. On the **Basic Information** page, click **Unbind** in the row of **Bound NAT Gateway**, and click **OK** in the pop-up dialogue box.

Deleting Direct Connect Gateway

Last updated：2024-01-13 16:40:45

A Direct Connect gateway can be deleted if it is no longer needed. Deleting a Direct Connect gateway deletes the dedicated tunnels connected to it. Verify that deleting the Direct Connect gateway does not affect your services before deleting it.

1. Log in to Tencent Cloud console and choose **Tencent Cloud Services** > **Networking** > **Virtual Private Cloud** to open the VPC console.
2. In the leftside bar, click **Direct Connect Gateways** to go to the management page.
3. Select the Direct Connect gateway to delete, and click **Delete** in the action column.
4. Click **OK**.

Managing Direct Connect Gateways
Gateway Traffic Monitoring

Last updated：2024-01-13 16:40:45

Gateway traffic monitoring enables you to monitor and control the bandwidth between private IPs and the gateway. Gateway traffic monitoring fine-grains and visualizes traffic management to help you stay on top of the gateway traffic. Its IP-level traffic throttling capabilities help you quickly troubleshoot failures, block abnormal traffic, and safeguard key businesses.

Currently, you can enable gateway traffic monitoring in Direct Connect.

Note:

1. Sources of gateway traffic monitoring can be only CVM instances. The statistics of the traffic from other services to the gateway cannot be collected.
2. Currently, gateway traffic monitoring is in beta test. To try it out, submit a ticket.

Key Features

Gateway traffic monitoring provides accurate gateway troubleshooting, which can minimize the network failure time. It enables you to query and view top N IPs in real time based on the traffic and analyzes source IPs and key metrics to help you quickly locate abnormal traffic.

Gateway traffic monitoring provides "monitoring" and "control" at the granularity of IP-gateway. Minute-level network traffic query can be used to identify abnormal traffic that maliciously occupies bandwidth in time. Bandwidth limits can be set at the granularity of IP-gateway to guarantee the stable operation of core business.

Gateway traffic monitoring analyzes all traffic at all times to help minimize network costs. By means of QoS, it can limit the bandwidth of non-key businesses to reduce costs when the network budget is limited.

Use Cases

Gateway traffic monitoring is mainly used in scenarios where the gateway traffic of a company surges at night. By using smart gateway traffic monitoring, Ops personnel can trace the IPs that cause the traffic surge based on the time when the traffic surge occurs and quickly locate the root cause. In addition, it can control the bandwidth from an IP to a gateway to block abnormal traffic and protect key businesses.

Billing

The gateway traffic monitoring feature is free of charge.

Operation Guide

Enabling gateway traffic monitoring details

1. Log in to the VPC console.
2. Select **Direct Connect Gateway** on the left sidebar to enter the management page of the target gateway as needed. Here, a VPN gateway is used as an example.
3. Click the ID of the target gateway or connection to enter the details page.
4. Click the **Monitoring** tab and enable **Gateway Traffic Monitoring Details** in the top-right corner.
5. It takes 5–6 minutes to collect and publish data when the gateway traffic monitoring details feature is enabled. Then, you can view the details table below the monitoring charts.

Setting gateway traffic monitoring details

1. Log in to the VPC console.
2. Select **Direct Connect Gateway** on the left sidebar to enter the management page of the target gateway as needed. Here, a VPN gateway is used as an example.
3. Click the ID of the target gateway or connection to enter the details page.
4. Click the **Monitoring** tab.
5. Find the target IP address and click **Modify**.
6. Adjust the bandwidth and click **Save**.

Viewing gateway traffic monitoring details

1. Log in to the VPC console.
2. Select **Direct Connect Gateway** on the left sidebar to enter the management page of the target gateway as needed. Here, a VPN gateway is used as an example.
3. Click the ID of the target gateway or connection to enter the details page.
4. Click the **Monitoring** tab.
5. Click **View Restricted IP** in the top-right corner of the gateway traffic monitoring details table.

Gateway Traffic Analysis

Last updated：2024-01-13 16:40:45

During the operation of Tencent Cloud direct connect, each tunnel takes different traffic load for different business. If the tunnel is full of business traffic, the connection will be unavailable. To solve this issue, Tencent Cloud direct connect launches the traffic analysis feature at the gateway granularity to inform you the IPs of traffic in "Top N" ranklist and the traffic details and help you adjust your business.

Prerequisite

You have created a direct connect gateway as instructed in Creating Direct Connect Gateway.
Business traffic has flowed in the gateway.

Directions

1. Log in to the Direct Connect Gateway console, and click **Direct Connect Gateway** in the left sidebar.
2. Select a region and VPC at the top of the **Direct Connect Gateway** page. Click the **ID/Name** of the target direct connect gateway to enter its details page.
3. Click **Traffic Analysis** on the details page and enable the **Traffic collection task**.
When enabling, the system will collect statistics on all data traffic passing through the gateway and display the statistical result in about 3-5 minutes.
4. View the traffic analysis result.
Settings of time period and time granularity
For time period, you can select **3 minutes ago**, **1 hour ago** or **7 days ago**.
For time granularity, you can select **1 minute**, **1 hour** or **1 day**. This indicates the traffic statistics is collected every minute/hour/day.
Note:
If you estimate that the traffic analysis time is about 0-30 minutes, we recommend that you select **1 minute** for time granularity. If the analysis time is more than 30 minutes, we recommend that you select **1 hour**.
If you need more accurate and fine-grained traffic statistics and analysis within 3 minutes, we recommend that you select **3 minutes ago** for time period and set 1 hour for custom time span (for example, 2021-08-06 14:18 to 2021-08-06 15:17) and select **1 minute** for time granularity.
View the "TOP N" informationThe tunnel traffic ranklist can be displayed in four ways, including **Top 5**, **TOP 20**, **TOP 50** and custom top N. If you want to view the traffic of a specified IP, you can enter the IP address in the input box on the right.

Dedicated Tunnels
Overview

Last updated：2024-01-13 16:40:45

A dedicated tunnel is a network linkage segmentation of a connection. You can create dedicated tunnels that connect to different direct connect gateways to enable communication between your on-premises IDC and multiple VPCs. After a dedicated tunnel is created, its event alarms will be automatically configured to facilitate your monitoring and OPS of it. This document describes how to apply for a dedicated tunnel.

Background

You can access Tencent Cloud Direct Connect via your own connections and connections shared by partners.
Access via your own connections: You can independently connect the connection with an exclusive interface from your local IDC to the Tencent Cloud access point.
Access via connections shared by partners: You can also use our partners' connections pre-established in Tencent to access Tencent Cloud. Currently, our partners include CTCC, CMCC, CUCC, CITIC and others with A14 and A26 telecommunication qualifications.
The tunnels created on the connections vary depending on the access method.
The tunnels created on your own connections are exclusive dedicated tunnels, which are applicable to scenarios with requirements for high-bandwidth access and exclusive access. For details, see Exclusive Dedicated Tunnel.
The tunnels created on our partners' connections pre-established in Tencent are shared dedicated tunnels, which are applicable to scenarios where there is no need for high-bandwidth access and the cloudification time is short. For details, see Shared Dedicated Tunnel.

Exclusive Virtual Interface

Last updated：2024-01-13 16:40:45

Prerequisites

Apply for a connection. See Applying for a Connection.
Create a direct connect gateway. See Creating Direct Connect Gateway.

Directions

Step 1: Apply for a dedicated tunnel

1. Log in to the Direct Connect - Dedicated Tunnel console.
2. On the left sidebar, click **Dedicated tunnels** > **Exclusive virtual interface**, click **+ New**, complete basic configurations such as name, connection type, access network, gateway region and associated direct connect gateway, and click **Next**.

Field	Description
Name	Enter a name for your dedicated tunnel.
Tunnel Type	Set to 1.0 or 2.0 depending on the associated connection you select.
Connections	Select a connection you have applied for.
Access Network	For a 1.0 tunnel, select from CCN and VPC. For a 2.0 tunnel, select either CCN、Virtual Private Cloud and NAT network.
Region	If CCN is selected as the access network, the region is where the CCN-based direct connect gateway resides by default. If VPC is selected as the access network, you can only select the region where the connection resides for a 2.0 tunnel and select any region for a 1.0 tunnel.
VPC	Select the VPC instance to be connected to by the dedicated tunnel.
Direct Connect Gateway	Associate an existing direct connect gateway with the dedicated tunnel. A 2.0 tunnel does not support a NAT-type direct connect gateway.

3. Configure the following parameters on the **Advanced Configuration** page.

Field	Description

VLAN ID	One VLAN corresponds to one tunnel. Valid range: [0, 3000). If the value is 0, only 1 tunnel can be created. Use physical layer 3 interfaces for the connection. If the value is between 1 and 2999, multiple tunnels can be created. Use layer 3 sub-interfaces for the connection. When only the layer 2 connection is supported, please disable the STP protocol under the interface at the IDC side. In the case of multiple dedicated tunnels, when the MSTP connection passes through multiple VLANs, the carrier line needs to enable the Trunk mode.
Bandwidth	Specify the bandwidth cap of the dedicated tunnel, which cannot exceed the maximum bandwidth of the associated connection. If the billing mode is pay-as-you-go by monthly 95th percentile, this parameter does not mean the billable bandwidth.
Interconnection Method	By default, Manual allocation is selected for 2.0 tunnels. Both Manual allocation and Automatic Assignment are supported for 1.0 tunnels. If Automatic Assignment is selected, there is no need to configure Tencent Cloud Primary Edge IP and CPE Peer IP.
Tencent Cloud Primary IP	Enter the connection IP address on the Tencent Cloud side. Do not use the following IP ranges or IP addresses: 169.254.0.0/16, 127.0.0.0/8, 255.255.255.255, 224.0.0.0 - 239.255.255.255, 240.0.0.0 - 255.255.255.254.
Tencent Cloud Primary IP	Enter the secondary IP address of the connection on the Tencent Cloud side. The secondary IP will be automatically used to ensure the normal operation of your business when the Tencent Cloud primary IP fails and becomes unavailable. This field is not supported when the mask of the secondary IP address is 30 or 31.
CPE Peer IP	Configure the connection IP address on the user (or carrier) side.
Routing Mode	Select: BGP Routing: Applicable to the exchange of routing information and network accessibility across autonomous systems (AS). Static Routing: Applicable to a simper network environment.
Health Check	Health check is enabled by default. BFD and NQA modes are provided. For details, see Dedicated tunnel health check.
Check mode	BFD and NQA modes are provided
Health Check Interval	The interval between two health checks.
Number of Failed Health Checks	Switch the route after the configured consecutive failed health checks.
BGP ASN	Enter the BGP neighbor ASN on the CPE side. Note that the Tencent Cloud ASN is 45090. If

	this field is left empty, a random ASN will be assigned.
BGP Key	Enter the MD5 value of the BGP neighbor, which defaults to "tencent". If it is left empty, no BGP key is required. It cannot contain 6 special characters including ?, &, space, ", \\, and +.

Note:

If **Static** is selected as the routing mode, do not directly publish the following routes: `9.0.0.0/8,` 10.0.0.0/8 `,` 11.0.0.0/8 `,` 30.0.0.0/8 `,` 100.64.0.0/10 `,` 131.87.0.0/16 `,` 172.16.0.0/12 `and` 192.168.0.0/16` when configuring IDC IP ranges. Instead, you need to first split them as follows.

`9.0.0.0/8` is split into `9.0.0.0/9` + `9.128.0.0/9` .

`10.0.0.0/8` is split into `10.0.0.0/9` + `10.128.0.0/9` .

`11.0.0.0/8` is split into `11.0.0.0/9` + `11.128.0.0/9` .

`30.0.0.0/8` is split into `30.0.0.0/9` + `30.128.0.0/9` .

`100.64.0.0/10` is split into `100.64.0.0/11` + `100.96.0.0/11` .

`131.87.0.0/16` is split into `131.87.0.0/17` + `131.87.128.0/17` .

`172.16.0.0/12` is split into `172.16.0.0/13` + `172.24.0.0/13` .

`192.168.0.0/16` is split into `192.168.0.0/17` + `192.168.128.0/17` .

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

Parameter	Configuration	Remarks
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.	You can update the IP range later via "Change Tunnel" in the console.

5. Click **Submit**.

Step 2: Set the alarm recipient

After a dedicated tunnel is created, Tencent Cloud automatically configures four event alarms such as `DirectConnectTunnelDown` , `DirectConnectTunnelBFDDown` , `DirectConnectTunnelBGPSessionDown` , and `DirectConnectTunnelRouteTableOverload` , helping you monitor and manage your dedicated tunnels. For more information on the event alarms, see Alarm Overview.

The automatically created default alarm policy is not configured with recipient information, and only supports console alarms. You can configure alarm recipients by yourself. For details, see [**Configuring Alarm Policies**] (https://www.tencentcloud.com/ document/product/216/38402).

Connection Status

After the dedicated tunnel is created, it will be displayed on the **Dedicated Tunnels** page in the **Applying** status. The possible connection statuses of a dedicated channel include:

Applying

The system has received your application for a new dedicated tunnel and is ready to start the creation.

Configuring

The system is delivering the parameter configuration. If this status lasts for a long time, a failure may occur. In this case, contact your architect or submit a ticket for assistance.

Configured

The system has completed the configuration based on the specified parameters but is unable to ping to the IP address of your IDC. A dedicated tunnel in this status can be deleted.

Connected

The system pings to your IDC device successfully. However, this does not mean that your business is connected. You have to configure the route table of the VPC or CCN instance to implement the connection.

Deleting

If you delete your dedicated tunnel on the console, the connection status of the dedicated tunnel becomes **Deleting**. If this status lasts for a long time, a failure may occur. In this case, contact your architect or submit a ticket for assistance.

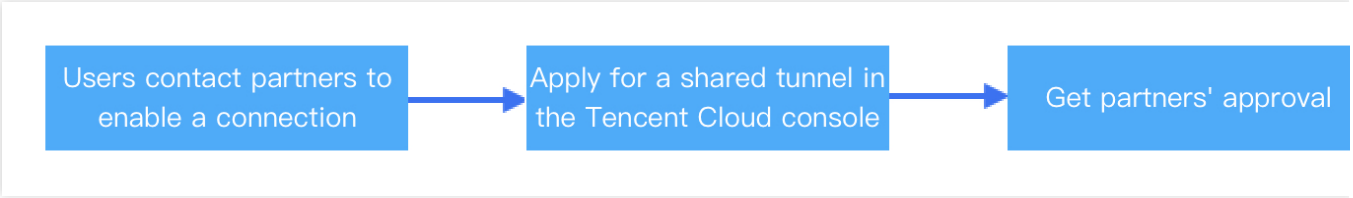
Shared Dedicated Tunnel

Last updated：2024-01-13 16:40:45

A dedicated tunnel is a network linkage segmentation of a connection. You can create dedicated tunnels that connect to different direct connect gateways to enable communication between your on-premises IDC and multiple VPCs. This document describes how to create a shared dedicated tunnel.

Overview

CTCC, CMCC, CUCC, CITIC and other partners with A14 and A26 telecommunications qualifications have pre-established connections with Tencent connection access points. You can access Tencent Cloud by sharing the partners' connections according to your actual needs.
A shared dedicated tunnel is a dedicated tunnel created using the partner's connection. It is applicable for scenarios where there is no need for high-bandwidth access and the cloudification time is short.
The procedure for enabling a shared dedicated tunnel is as follows:



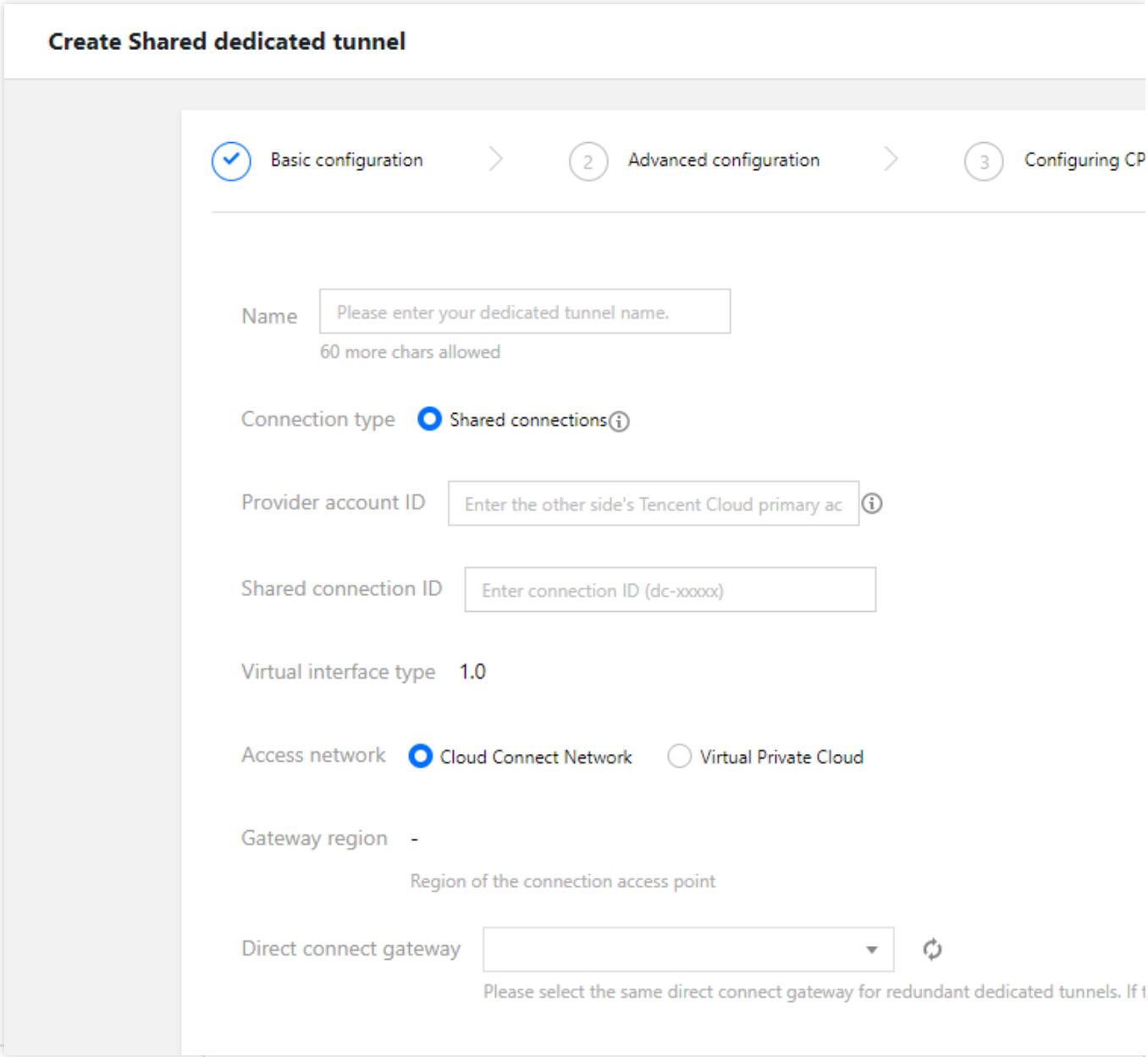
Prerequisites

You have obtained the connection instance ID for the shared dedicated tunnel and Tencent Cloud entity accounts' UINs of the connection provider from the supplier.
Create a direct connect gateway. See Creating Direct Connect Gateway.

Directions

Step 1: Apply for a dedicated tunnel

1. Log in to the Direct Connect console.
2. In the left sidebar, choose **Dedicated tunnels** > **Shared dedicated tunnel**. Click **+ New**, specify essential parameters such as the name, connection type, access network, gateway region, and associated direct connect gateway, and click **Next**.



Field	Description
Name	Enter a name for your dedicated tunnel.
Connection type	Select the shared connection.
Provider account ID	Provides a connection provider that establishes a pre-connection with Tencent: Currently, only suppliers with A14 and A26 telecommunication qualifications (such as CTCC, CMCC, CUCC, and CITIC) are supported to create a shared tunnel. If you need to share your connection with a subsidiary or your other Tencent Cloud accounts, please contact Tencent technical support for assistance. The fee of sharing the tunnel shall be borne by the tunnel user.
Shared tunnel ID	Enter the ID of the connection instance used to create the shared tunnel.
Access Network	If the tunnel type is `1.0`, you can select CCN or VPC.

	If the tunnel type is `2.0`, you can select CCN, VPC, or NAT.
Region	If you select **CCN**, the region defaults to the region where the CCN-based direct connect gateway is located. If you select **VPC**, for a 2.0 dedicated tunnel, you can only select the region where the connection is located; for a 1.0 dedicated tunnel, you can select any region.
VPC	Select the VPC instance to be connected to by the dedicated tunnel.
Direct Connect Gateway	Associate an existing direct connect gateway with the dedicated tunnel. A 2.0 tunnel does not support a NAT-type direct connect gateway.

3. Configure the following parameters on the **Advanced Configuration** page.

Field	Description
VLAN ID	One VLAN corresponds to one tunnel. Valid range: [0,3000). If the value is 0, only 1 tunnel can be created. Use physical layer 3 interfaces for the connection. If the value is between 1 and 2999, multiple tunnels can be created. Use layer 3 sub-interfaces for the connection. When only the layer 2 connection is supported, please disable the STP protocol under the interface at the IDC side. In the case of multiple dedicated tunnels, when the MSTP connection passes through multiple VLANs, the carrier line needs to enable the Trunk mode.
Bandwidth	Specify the bandwidth cap of the dedicated tunnel, which cannot exceed the maximum bandwidth of the associated connection. If the billing mode is pay-as-you-go by monthly 95th percentile, this parameter does not mean the billable bandwidth.
Tencent Cloud Primary IP1	Enter the connection IP address on the Tencent Cloud side. Do not use the following IP ranges or IP addresses: 169.254.0.0/16, 127.0.0.0/8, 255.255.255.255, 224.0.0.0 - 239.255.255.255, 240.0.0.0 - 255.255.255.254.
Tencent Cloud Primary IP2	Enter the secondary IP address of the connection on the Tencent Cloud side. The secondary IP will be automatically used to ensure the normal operation of your business when the Tencent Cloud primary IP fails and becomes unavailable. This field is not supported when the mask of the secondary IP address is 30 or 31.
User Border IP	Configure the connection IP address on the user (or carrier) side.
Routing Mode	Select: BGP Routing: Applicable to the exchange of routing information and network accessibility across autonomous systems (AS). Static Routing: Applicable to a simper network environment.
Health Check	Health check is enabled by default. BFD and NQA modes are provided. For details,

	see Dedicated tunnel health check.
Check mode	BFD and NQA modes are provided
Health Check Interval	The interval between two health checks.
Number of Failed Health Checks	Switch the route after the configured consecutive failed health checks.
BGP ASN	Enter the BGP neighbor ASN on the CPE side. Note that the Tencent Cloud ASN is 45090. If this field is left empty, a random ASN will be assigned.
BGP Key	Enter the MD5 value of the BGP neighbor, which defaults to "tencent". If it is left empty, no BGP key is required. It cannot contain 6 special characters including ?, &, space, ", \\, and +.

Note:

If **Static** is selected as the routing mode, do not directly publish the following routes: `9.0.0.0/8,` 10.0.0.0/8 `,` 11.0.0.0/8 `,` 30.0.0.0/8 `,` 100.64.0.0/10 `,` 131.87.0.0/16 `,` 172.16.0.0/12 `and` 192.168.0.0/16` when configuring IDC IP ranges. Instead, you need to first split them as follows.

`9.0.0.0/8` is split into `9.0.0.0/9` + `9.128.0.0/9`.

`10.0.0.0/8` is split into `10.0.0.0/9` + `10.128.0.0/9`.

`11.0.0.0/8` is split into `11.0.0.0/9` + `11.128.0.0/9`.

`30.0.0.0/8` is split into `30.0.0.0/9` + `30.128.0.0/9`.

`100.64.0.0/10` is split into `100.64.0.0/11` + `100.96.0.0/11`.

`131.87.0.0/16` is split into `131.87.0.0/17` + `131.87.128.0/17`.

`172.16.0.0/12` is split into `172.16.0.0/13` + `172.24.0.0/13`.

`192.168.0.0/16` is split into `192.168.0.0/17` + `192.168.128.0/17`.

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

Parameter	Description	Remarks
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.	You can update the IP range later via "Change Tunnel" in the console.

5. Click **Submit**.

After being created, the shared dedicated tunnel is in **Pending accepted** status. It will turn to be **Connected** after being approved by the connection provider.

Step 2: Set the alarm recipient

After a dedicated tunnel is created, Tencent Cloud automatically configures four event alarms such as `DirectConnectTunnelDown`, `DirectConnectTunnelBFDDown`, `DirectConnectTunnelBGPSessionDown`, and `DirectConnectTunnelRouteTableOverload`, helping you monitor and manage your dedicated tunnels. For more information on the event alarms, see Alarm Overview.
The automatically created default alarm policy is not configured with recipient information, and only supports console alarms. You can configure alarm recipients. For details, see [**Configuring Alarm Policies**] (https://www.tencentcloud.com/ document/product/216/38402).

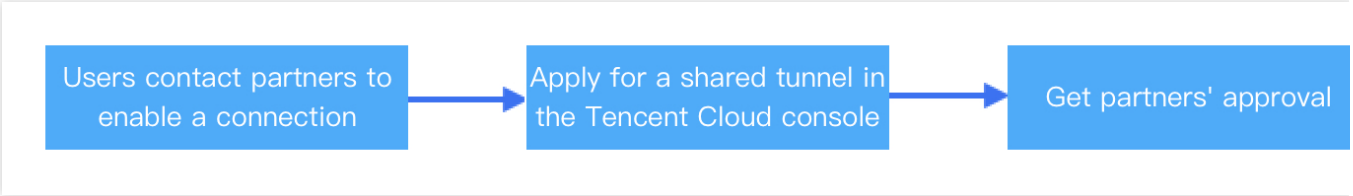
Shared Dedicated Tunnel (Partner)

Last updated：2024-01-13 16:40:45

After you share a connection to your customer, the customer will send you a request for confirmation. You need to approve the request in the console for the shared tunnel to take effect.

Background

CTCC, CMCC, CUCC, CITIC and other partners with A14 and A26 telecommunications qualifications have pre-established connections with Tencent connection access points. You can access Tencent Cloud by sharing the partners' connections according to your actual needs.
A shared dedicated tunnel is a dedicated tunnel created using the partner's connection. It is applicable for scenarios where there is no need for high-bandwidth access and the cloudification time is short.
The procedure for enabling a shared dedicated tunnel is as follows:



Prerequisites

Connect your DC connection to Tencent Cloud.
The customer submits a request for tunnel sharing. See Shared Dedicated Tunnel.

Directions

1. Log in to the Shared Dedicated Tunnel console.
2. In the Shared Dedicated Tunnels list, find the **Pending acceptance** tunnels, click **More** > **Approve now**.
3. Click **OK**. The connection status becomes **Connected** after it is approved.

Changing Tunnel Route

Last updated：2024-01-13 16:40:45

You can modify configurations including bandwidth of a connected dedicated tunnel in the Direct Connect console. This document describes how to modify configurations and routing methods of a 1.0 or 2.0 tunnel in the console.

Note:

For a shared connection, only the connection owner can modify the bandwidth of a dedicated tunnel.

Prerequisites

You have owned a tunnel before you can modify it.

Use Limits on Large IP Ranges

The direct connect gateway will directly reject a large CPE IP range. To ensure the refined scheduling capability of your network, do not publish the following routes:

`9.0.0.0/8`, `10.0.0.0/8`, `11.0.0.0/8`, `30.0.0.0/8`, `100.64.0.0/10`, `131.87.0.0/16`, `172.16.0.0/12`, and `192.168.0.0/16`.

You can split the above routes as follows for publishing:

`9.0.0.0/8`

Split into `9.0.0.0/9` + `9.128.0.0/9`.

`10.0.0.0/8`

Split into `10.0.0.0/9` + `10.128.0.0/9`.

`11.0.0.0/8`

Split into `11.0.0.0/9` + `11.128.0.0/9`.

`30.0.0.0/8`

Split into `30.0.0.0/9` + `30.128.0.0/9`.

`100.64.0.0/10`

Split into `100.64.0.0/11` + `100.96.0.0/11`.

`131.87.0.0/16`

Split into `131.87.0.0/17` + `131.87.128.0/17`.

`172.16.0.0/12`

Split into `172.16.0.0/13` + `172.24.0.0/13`.

`192.168.0.0/16`

Split into `192.168.0.0/17` + `192.168.128.0/17`.

Changing Tunnel Route

Note:

This document takes an exclusive dedicated tunnel as an example. The method also applies to a shared dedicated tunnel.

1. Log in to the Direct Connect console and click **Exclusive virtual interface** in the left sidebar.
2. On the **Exclusive virtual interface** page, find the dedicated tunnel to be modified, and click **Change tunnel** in the **Operation** column.
3. Choose the operation depending on the dedicated tunnel type, which can be checked on the **Basic Information** page.

Dedicated Tunnel 1.0

Edit the following configurations in the pop-up dialog box, and click **OK**.

Field	Description
Bandwidth cap	Specify the bandwidth cap of the dedicated tunnel, which cannot exceed the maximum bandwidth of the associated connection. If the billing mode is pay-as-you-go by monthly 95th percentile, this parameter does not mean the billable bandwidth. This feature is in canary release. To try it out, please submit a ticket.
Tencent Cloud Primary Edge IP	Enter the connection IP address on the Tencent Cloud side. Please note that changing the IP address will interrupt the service.
CPE Peer IP	Configure the connection IP address on the user (or carrier) side. Please note that changing the IP address will interrupt the service.
BGP ASN	Enter the BGP neighbor ASN on the CPE side. Note that 45090 is Tencent Cloud ASN. If this field is left empty, a random ASN will be assigned.
BGP Key	Enter the MD5 value of the BGP neighbor, which defaults to "tencent". If it is left empty, no BGP key is required. It cannot contain 6 special characters including ?, &, space, ", \\, and +.

Dedicated Tunnel 2.0

Modify the information as needed in the **Advanced Configuration** tab.

Modifying tunnel configuration

Click **Edit** on the right to modify Tencent Cloud IP, CPE peer IP, VLAN ID and Jumbo frames, and then click **Save**.

Note:

Frame, consisting of many bytes, is a protocol data unit of the data linkage layer. Ethernet frames generally have 1,500 bytes. The actual transfer frame size is usually determined by the MTU of the device, that is, the maximum number of bytes that the device can transfer at a time. Jumbo frames, also called giant frames, are larger than standard Ethernet frames in size.

Field	Description
Tencent Cloud Edge IP	Enter the connection IP address on the Tencent Cloud side. Please note that changing the IP address will interrupt the service.
CPE Peer IP	Configure the connection IP address on the user (or carrier) side. Please note that changing the IP address will interrupt the service.
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. If MSTP connection passes through to multiple VLANs, the carrier needs to enable the Trunk mode.
Jumbo frames	Jumbo frames are larger Ethernet frames and supported by dedicated tunnel 2.0.The feature of Jumbo frames is not enabled by default. In this case, the MTU includes 1,464 bytes. When this feature is enabled, the MTU can contain 9,001 bytes. To enable this feature, please submit a ticket.

Editing the routing mode

3.1 Click **Edit** on the right of the **Routing Mode** to modify the route.

Static: modify the CPE IP range. To ensure the refined scheduling capability of your network, follow the Use Limits on Large IP Range.</td>

BGP: modify BGP ASN or BGP key.

Field	Description
BGP ASN	Enter the BGP neighbor ASN on the CPE side. Note that 45090 is Tencent Cloud ASN. If this field is left empty, a random ASN will be assigned.
BGP Key	Enter the MD5 value of the BGP neighbor, which defaults to "tencent". If it is left empty, no BGP key is required. It cannot contain 6 special characters including ?, &, space, ", \\, and +.

3.2 Change health checks.

For more information, see Dedicated tunnel health check.

3.3 Click **Confirm**.

The new tunnel configuration will take effect in several minutes depending on the network.

Probing a Dedicated Tunnel

Last updated：2024-01-13 16:40:45

The Direct Connect console provides a tunnel tool that sends a detection packet from Tencent Cloud IP to customer IP to test the network connectivity. After a dedicated tunnel is created or modified, we recommend using the tunnel tool to test the connection between Tencent Cloud and IDC.

Preparation

To enable the Ping feature in a 2.0 dedicated tunnel, please submit a ticket.
The dedicated tunnel should be a 2.0 tunnel, which can be checked on the **Basic Information** page.

Directions

1. Log in to the Direct Connect console and click **Exclusive virtual interface** on the left sidebar to access the **Exclusive virtual interface** page.
2. Click the **ID/Name** of the target dedicated tunnel to enter its details page.
3. Select the **Tunnel tool** tab.
4. Configure the number and volume of the packets, and click **Start probing**. Determine if the network is connected based on the loss delay.

Deleting a Dedicated Tunnel

Last updated：2024-01-13 16:40:45

Note:

To ensure that the services of tunnel users work properly, users can only change the bandwidth of tunnels but not delete tunnels.

1. Log in to the Direct Connect console.
2. On the left sidebar, click **Exclusive virtual interface** to go to the management page.
3. In the list, locate the dedicated tunnel to delete, choose **Delete** > **Delete**.
4. You can create a dedicated tunnel with the same VLAN ID only after the deletion operation is completed.

Dedicated tunnel health check

Last updated：2024-01-13 16:40:45

You can modify configurations and bandwidths of and execute health checks for connected dedicated tunnels in the Direct Connect console. This document describes how to condut the health check of a 2.0 tunnel in the console.

Note:

For a shared connection, only the connection owner can modify the bandwidth of a dedicated tunnel.

Prerequisites

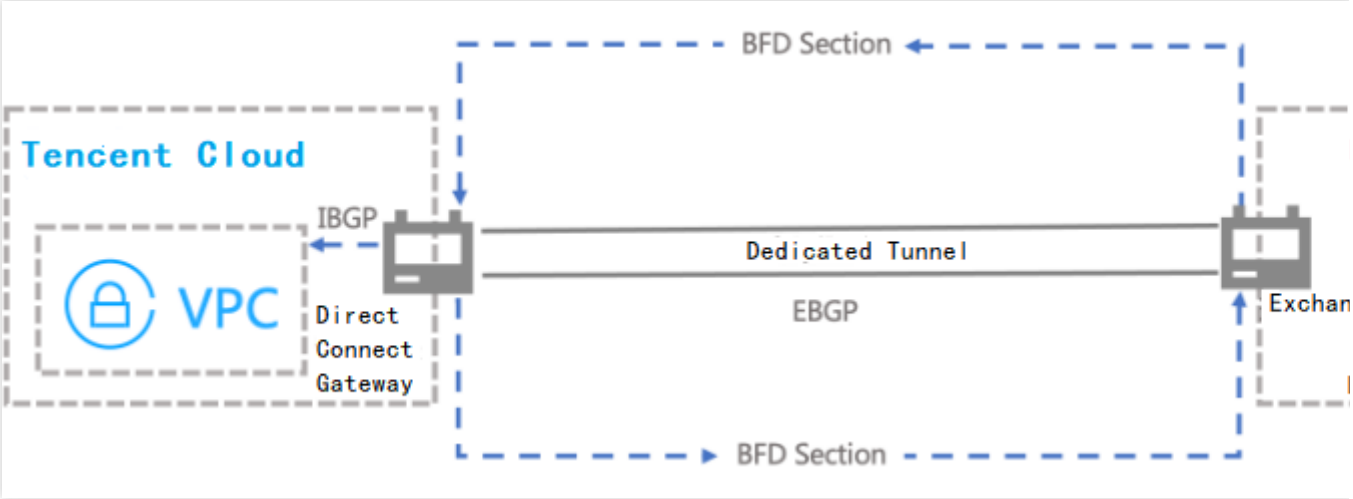
You have applied for a dedicated tunnel as instructed in Creating a Dedicated Tunnel.

You have backed up the dedicated tunnel.

Background

You can use BFD and NQA to conduct the health check for a dedicated tunnel of Tencent Cloud Direct Connect:

BFD: BFD establishes a session between network devices to detect the bidirectional forwarding path between these devices. It reports messages periodically after the session is established. The path is considered to be faulty when no messages reported during the detection. The application using the path will receives the detection result. Currently, BFD can be used in a linkage with BGP route and static route.



NQA: NQA pings the dedicated tunnel to detect whether it is connected or not. It helps you know the robustness of the tunnel in real time and locate the fault quickly.

Configuring Health Check After a Tunnel Is Created

1. Log in to the Direct Connect console and click **Exclusive virtual interface** in the left sidebar.
2. On the **Exclusive virtual interface** page, click the name of the tunnel for which you want to configure health check.
3. On the **Advanced configuration** tab of the tunnel details page, click **Edit** on the right of **Routing mode**.
4. Enable **Health check**.
5. Configure the health check parameters.

Health Check Configuration Parameters	Description	Valid Range
Health Check Interval	The interval between two health checks.	BFD: 1000 ms - 3000 ms, default value-1000 ms. NQA: 1000 ms - 5000 ms, default value-2000 ms.
Number of Failed Health Checks	Switch the route after the configured consecutive failed health checks.	BFD：3 - 8, default value-3. NQA：3 - 8, default value-5.

Note：
You shall apply different methods to conduct health checks for dedicated tunnels using different routing modes. Currently, for the health check of dedicated tunnels using the BGP routing mode, only BFD is applicable. For the health check of dedicated tunnels using the static routing mode, both BFD and NQA are applicable.
You can switch BFD and NQA to conduct the health check of a dedicated tunnel using static routing mode. The health check will be executed with the method after switching.>
6. Click **Save**.

Configuring Health Check When You Create a Tunnel

1. Log in to the Direct Connect console and click **Exclusive virtual interface** in the left sidebar.
2. Click **Create** on the **Dedicated tunnels** page. Then, specify the parameters on the **Basic configuration** tab, and specify other parameters and enable health check on the **Advanced configuration** tab as prompted.
This section describes how to configure the health check feature. For more information about other parameters, see Exclusive Virtual Interface or Shared Dedicated Tunnel.

Health Check Configuration Parameters	Description	Valid Range
Health Check Interval	The interval between two health	BFD: 1000 ms - 3000 ms, default value-

	checks.	1000 ms. NQA: 1000 ms - 5000 ms, default value-2000 ms.
Number of Failed Health Checks	Switch the route after the configured consecutive failed health checks.	BFD：3 - 8, default value-3. NQA：3 - 8, default value-5.

Note：

You shall apply different methods to conduct health checks for dedicated tunnels using different routing modes. Currently, for the health check of dedicated tunnels using the BGP routing mode, only BFD is applicable. For the health check of dedicated tunnels using the static routing mode, both BFD and NQA are applicable.

You can switch BFD and NQA to conduct the health check of a dedicated tunnel using static routing mode. The health check will be executed with the method after switching.

3. Click **Next**. Specify other parameters to create the tunnel.

Modifying the Dedicated Tunnel Bandwidth

Last updated：2024-01-13 16:40:45

You can modify configurations including bandwidth of a connected dedicated tunnel in the Direct Connect console. This document describes how to modify the bandwidth of a 1.0 or 2.0 tunnel in the console.

Note:

For a shared connection, only the connection owner can modify the bandwidth of a dedicated tunnel.

Prerequisites

You have owned a tunnel before you modify it.

Dedicated Tunnel 1.0

1. Log in to the Direct Connect console and click **Exclusive virtual interface** in the left sidebar.
2. On the **Exclusive virtual interface** page, find the dedicated tunnel to be modified, and choose **More** > **Change tunnel** in the **Operation** column.
3. Modify the bandwidth cap in the **Change tunnel** pop-up window and click **OK**.

Note:

If the tunnel bandwidth is greater than 1 Gbps, you can increase the bandwidth value by an integer multiple of 1 Gbps, such as 2 Gbps and 3 Gbps.

Dedicated Tunnel 2.0

1. Log in to the Direct Connect console and click **Exclusive virtual interface** in the left sidebar.
2. Find the target exclusive dedicated tunnel, and click

in the **Bandwidth** column.

Note:

You can modify the bandwidth only for a dedicated tunnel that is in the **Connected** state.

3. Specify a new bandwidth value in the edit box and click **OK**.

Note:

The tunnel bandwidth cap cannot exceed the maximum bandwidth of the associated connection. You can submit a ticket to increase the connection bandwidth.

Monitoring and Alarming
Viewing Monitoring Data

Last updated：2024-01-13 16:40:45

You can view the network monitoring data of a connection or dedicated tunnel via the console or an API to facilitate the troubleshooting. To use the API, see Connection Monitoring Metrics.

Directions

1. Log in to the Direct Connect console.
2. Perform the following steps to view the network monitoring data of a connection.
3. Click **Connections** on the left sidebar.
4. Locate the target connection and click


in the **Monitoring** column.

Note:

Only the monitoring data of operating connections can be viewed.

5. The **Monitoring** page displays **Network Outbound Bandwidth** and **Network Inbound Bandwidth**. Select **Last 24 hours**, **Last 7 days** or a custom time period to display the monitoring data accordingly.

Network Outbound Bandwidth: average outbound traffic of the connection per second.

Network Inbound Bandwidth: average inbound traffic of the connection per second.

Packet Loss: number of packets discarded on the port per minute.

Packet Error: number of packet errors on the port per minute.

6. Perform the following steps to view the network monitoring data of a dedicated tunnel.
7. Click **Exclusive virtual interface** on the left sidebar.
8. Locate the target dedicated tunnel and click


in the **Monitoring** column.

9. The **Monitoring** page displays **Network Outbound Bandwidth**, **Network Inbound Bandwidth**, **Packets Out**, and **Packets In**. Select **Last 24 hours**, **Last 7 days** or a custom time period to display the monitoring data accordingly.

Network Outbound Bandwidth: average outbound traffic of the dedicated tunnel per second.

Network Inbound Bandwidth: average inbound traffic of the dedicated tunnel per second.

Packets Out: total outbound traffic of the dedicated tunnel.

Packets In: total inbound traffic of the dedicated tunnel.

10. Perform the following steps to view the network monitoring data of a direct connect gateway.

11. Log in to the Direct Connect Gateway console. Click **Direct Connect Gateway** in the left sidebar.

12. Locate the target direct connect gateway and click

in the **Monitoring** column.

13. The **Monitoring** page displays **Network Outbound Bandwidth**, **Network Inbound Bandwidth**, **Packets Out**, **Packets In**, **Outbound Traffic**, and **Inbound Traffic**. Select **Last 24 hours**, **Last 7 days** or a custom time period to display the monitoring data accordingly.

Network Outbound Bandwidth: average outbound traffic of the direct connect gateway per second.

Network Inbound Bandwidth: average inbound traffic of the direct connect gateway per second.

Packets Out: total number of outbound traffic packets of the dedicated tunnel.

Packets In: total number of inbound traffic packets of the dedicated tunnel.

Outbound Traffic: total outbound traffic of the dedicated tunnel.

Inbound Traffic: total inbound traffic of the dedicated tunnel.

Packet loss (Out): total number of outbound packets discarded on the dedicated tunnel.

Packet loss (In): total number of inbound packets discarded on the dedicated tunnel.

Configuring Alarm Policies

Last updated：2024-01-13 16:40:45

You can configure alarm rules for the connection, dedicated tunnel and direct connect gateway on the Cloud Monitor console. When an alarm rule is triggered, you will receive notifications via the channel you specified, helping you take appropriate measures.

Directions

1. Log in to the Cloud Monitor console and choose **Alarm Configuration** > **Alarm Policy** on the left sidebar.
2. Click **Create** on the **Alarm Policy** page.
3. Configure a new alarm policy as instructed below.
4. Edit **Policy name** and **Remarks**. Select **Connection**, **Dedicated tunnel** or **Direct connect gateway** for **Policy type** as needed.

Note:

If **Direct connect gateway** is selected, the policy is VPC-based.

5. Choose a project to which the alarm policy belongs. Each project supports creating a maximum of 300 alarm policies.
6. Select the alarm object.

If you select **All objects**, the alarm policy will be associated with all instances under the current account.

If you select **Instance ID** and select instances in the pop-up window, the alarm policy will be associated with the selected instances.

If you select **Instance group**, the alarm policy will be associated with the selected instance group. If there is no available instance group, you can click **Create instance group** to configure one.

7. Configure the trigger condition using either of:

Template

Click **Select template** and select a configured template in the drop-down list.

Note:

You can click Add trigger condition template to configure a new trigger condition template. For more information about the configurations, please see Configuring Trigger Condition Template. If the new template is not displayed in the list, click Refresh.

Manual configuration

Set the trigger condition as needed after selecting **Manual configuration**. You can click **Add metric** to configure a new metric. For more information about metric alarms, see Alarm Overview.

For example, if you choose **Inbound bandwidth** metric and configure as follows: **statistical period: 1 minute**, **>**, **100 Mbps**, **at 2 consecutive data points**, and **Alarm once a day**, then the inbound bandwidth data will be

collected once every minute. An alarm will be triggered once a day if the inbound bandwidth of a connection, dedicated tunnel or direct connect gateway exceeds 100 Mbps for two consecutive minutes.

Note:

Click **Add metric** to configure a new trigger condition. You can choose to trigger an alarm when any or all conditions are met.

If you need to configure event alarms, see Quickly Configuring Cloud Monitor Event Alarm Push.

8. Configure alarm notification.

The notification template allows you to configure alarm recipients. You can click **Select template** and select an existing template, or click **Create template** to configure a new template as prompted.

9. (Optional) Configure the API callback.

i. Click **Create template**. In the pop-up window, click **For more configurations, please go to notification template page**.

ii. On the **New notification template** page, complete the notification template configurations, enter a URL accessible over public networks as the API callback address (domain name or IP[:port][/path]), and click **Complete**.

iii. Go to the **Alarm policy** page and select the alarm notification template you've just created.

Then Cloud Monitor will push the alarm information to this address in time.

10. Click **OK**.

Managing Alarm Policies

Once an alarm policy is created, you can enable, disable, copy, or delete it on the console.

1. Log in to the Cloud Monitor console and select **Alarm Configuration** > **Alarm Policy** on the left sidebar to access the **Alarm policy** page.

2. Perform the following steps as needed.

To enable or disable an alarm policy, toggle the switch in its **Alarm On-Off** column.

To copy an alarm policy, click **Copy** in its **Operation** column, modify the policy as needed in the pop-up window, and click **Complete**.

To view historical alarm data, locate the alarm policy and click **Alarm records** in the **Operation** column.

To delete an alarm policy, click **Delete** in its **Operation** column, and click **Confirm** in the pop-up dialog box.

Alarm Overview

Last updated：2024-01-13 16:40:45

This document describes the metric alarms and event alarms for a connection, dedicated tunnel and direct connect gateway to help you configure alarm policies.

Metric Alarms

To create a metric alarm policy, you can configure the outbound bandwidth, inbound bandwidth, and bandwidth utilization as the trigger conditions for a connection; configure the outbound bandwidth and inbound bandwidth for a dedicated tunnel; and configure the outbound bandwidth, inbound bandwidth, outbound packet, and inbound packet for a direct connect gateway.

Metric	Description
Outbound bandwidth	Average outbound traffic of the connection/dedicated tunnel/direct connect gateway per second.
Inbound bandwidth	Average inbound traffic of the connection/dedicated tunnel/direct connect gateway per second
Bandwidth utilization	Current bandwidth divided by connection bandwidth * 100%.
Outbound packet	Average outbound packets of the direct connect gateway per second
Inbound packet	Average inbound packets of the direct connect gateway per second.

Event Alarms

You can use the `DirectConnectDown` event as the trigger condition of event alarms for a dedication. You can use the `DirectConnectTunnelDown` , `DirectConnectTunnelBGPSessionDown` , `DirectConnectTunnelRouteTableOverload` , and `DirectConnectTunnelBFDDown` events as the trigger conditions of event alarms for a dedicated tunnel.

Event Name	Event Parameter	Event Type	Dimension	Recoverable	Desc
Connection downtime	DirectConnectDown	Exception	Connection	Yes	The physi

					link o conn is interr or ha excep
Dedicated tunnel downtime	DirectConnectTunnelDown	Exception	Dedicated tunnel	Yes	The physi link o conn is interr or ha excep
Dedicated tunnel BGP	DirectConnectTunnelBGPSessionDown	Exception	Dedicated tunnel	Yes	The dedic

session downtime					tunne BGP sessi interr
Alarm for exceeded number of BGP tunnel routes	DirectConnectTunnelRouteTableOverload	Exception	Dedicated tunnel	No	The numb BGP sessi route dedic tunne exce 80% thres
Dedicated tunnel BFD detection downtime	DirectConnectTunnelBFDDown	Exception	Dedicated tunnel	Yes	The dedic tunne detec is interr

Viewing Alarms

Last updated：2024-01-13 16:40:45

After a metric or event alarm policy is configured for a connection, dedicated tunnel, or direct connect gateway, you can view the alarm history and details on the Cloud Monitor console.

Prerequisites

You have configured an alarm policy.

Viewing Alarm History

1. Log in to the Cloud Monitor console and select **Alarm List** on the left sidebar to view alarm records.
2. Select a period during which alarms are generated.
The **Alarm Records** page displays the alarm details, including alarm object, alarm content, duration, and alarm status.

Viewing Product Event

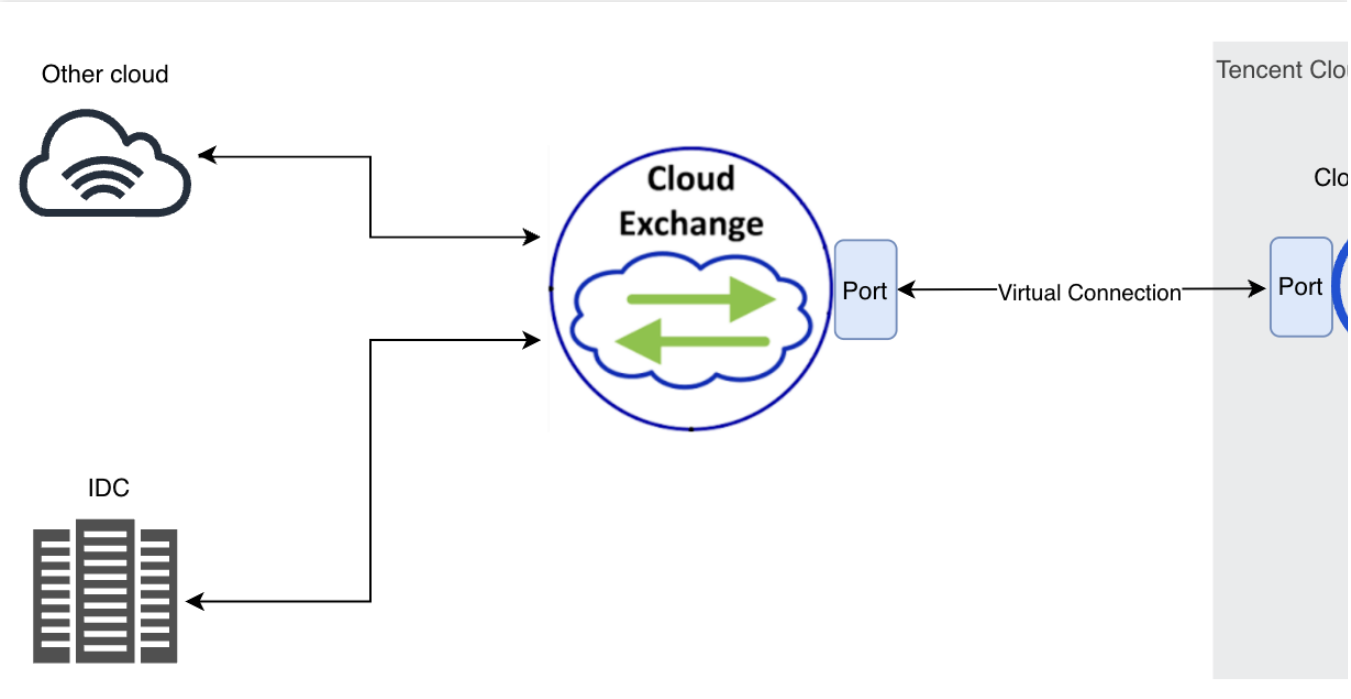
Tencent Cloud provides the automatic exception detection for connections and dedicated tunnels such as disconnected port or link, and syncs the information to the Cloud Monitor console. These product events in the last 30 days can be viewed on the console. You can also configure an alarm policy for the product event as needed.
1. Log in to the Cloud Monitor console and select **Event Center** -> **Product Event** on the left sidebar.
2. At the top of the **Product Event** page, double-click **All** of **Product Type: All** in the search bar, select Connection or Dedicated Tunnel in the drop-down list, and click **OK**.
Note:
By default, the product event lists all the connection/dedicated tunnel events under the current account during the custom period. The fields including Event, Affected Object, Object Details, Status, and Start Time are displayed.
3. To create an alarm policy for the selected product event, click **Add Configuration** in its **Alarm Configuration** column to access **Create Policy**. Complete the configurations and click **Complete**.

Cloud Exchange

Cloud Exchange Introduction

Last updated：2024-07-01 15:31:48

Cloud Exchange (CX) is a multi-cloud ecosystem community built through collaboration between Direct Connect of the Tencent Cloud and cloud service providers outside the Chinese Mainland. CX offers customers a one-stop multi-cloud interconnection service.



Note:

When accessing, use the dual-route access mode, as single-route access does not guarantee service availability.

If the number of regional access points ≥ 2, access using the dual-access point method.

If the number of regional access points < 2, connect to two different devices to enhance business disaster recovery capability.

Use Limits

A single CX instance can create only one dedicated channel.

Regions currently supported are Hong Kong (China), Japan, and Singapore, Brazil.

Strengths

Multi-cloud Deployment

Supports both hybrid and multi-cloud deployment architectures, cooperating with cloud exchange providers outside the Chinese Mainland to allow you to link your communication cloud network with cloud service providers outside the Chinese Mainland and data centers outside the Chinese Mainland.
Prevents service downtime in the event of a failure in a single cloud service.
Supports the use of a second cloud or data center for disaster recovery.
Enables interoperability with cloud services from well-known cloud providers outside the Chinese Mainland like AWS and Microsoft, avoiding dependence on a single vendor.

Rapid Cloud Adoption

In traditional connection modes, linking users' data centers outside the Chinese Mainland with the Tencent Cloud involves complex steps, including separate coordination with operations, cabling, and setting up VPC and CCN for cloud resources outside the Chinese Mainland. The Cloud Exchange is a physical interconnect link pre-established through collaboration between Direct Connect of Tencent Cloud and cloud exchange providers outside the Chinese Mainland, with the cloud exchange providers acting as a bridge to connect various cloud service providers.
Short building period. The inter-cloud interconnection can be completed in 2-3 working days.
Reduced complexity. You can build Tencent Cloud resources with just one click, sparing you the hassle of tedious configuration.

Operation Guide

Last updated：2024-07-01 15:31:41

Prerequisites

1. You already have an Equinix Fabric account.
2. Your Equinix Fabric account has a port or virtual device in the region where a connection is needed.

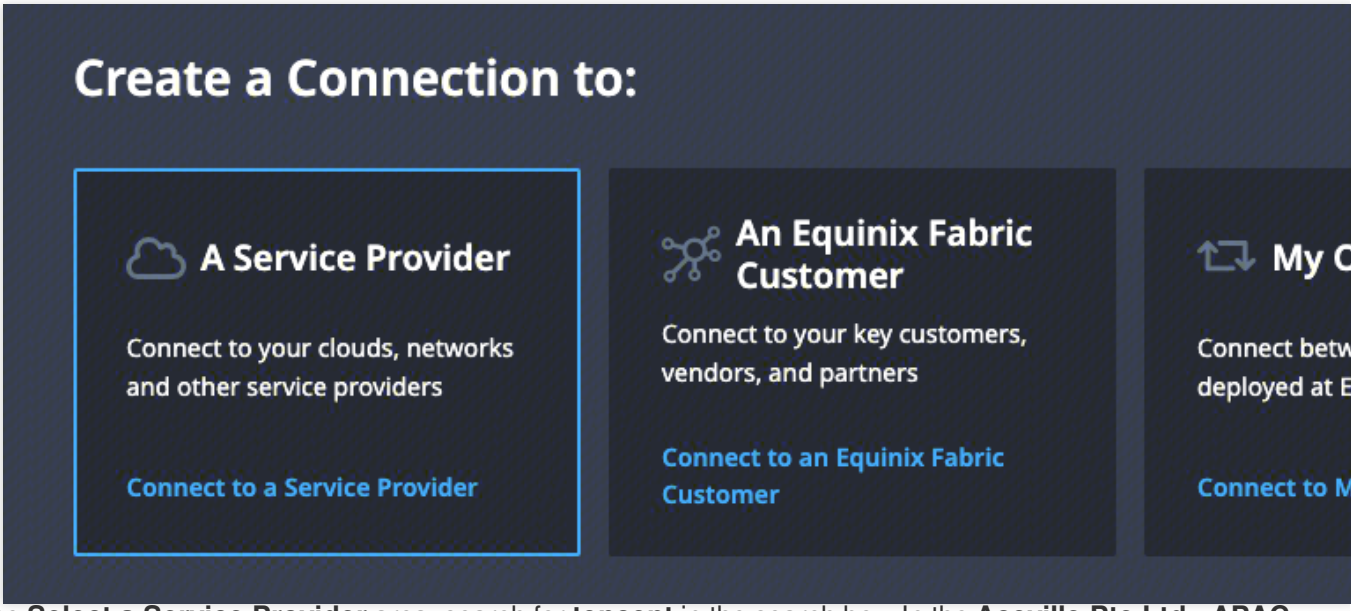
If you do not have an Equinix Fabric account, you can contact sales through the Equinix page or create one yourself. If you have questions about using the page, you can ask Equinix sales for guidance or contact Equinix online service for support.

Directions

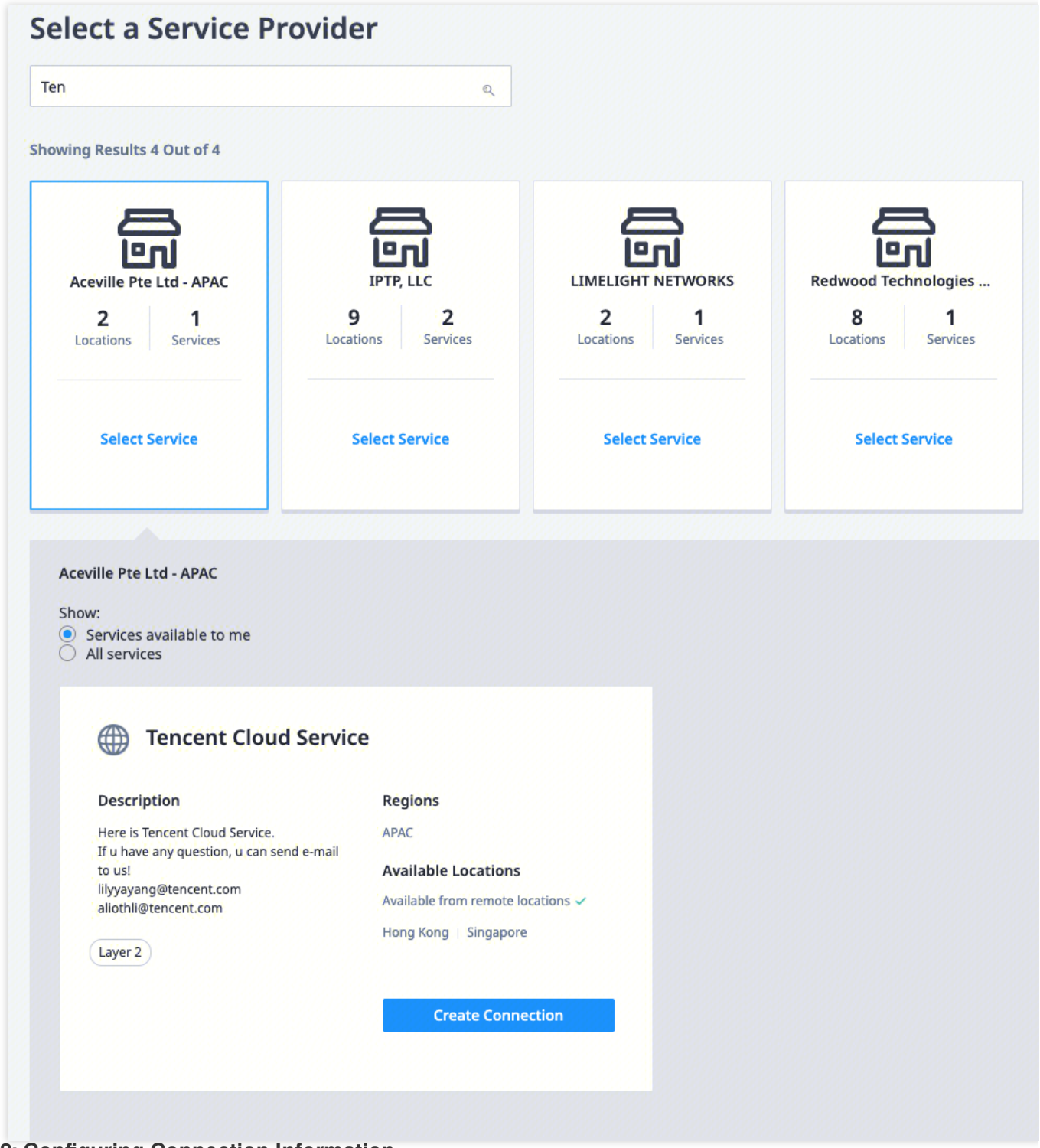
Submitting an Order on Equinix

Step 1: Selecting a Service Provider

1. Log in to Equinix Fabric. From the **Connections** menu, select **Create Connection**.
2. Click **A Service Provider**.

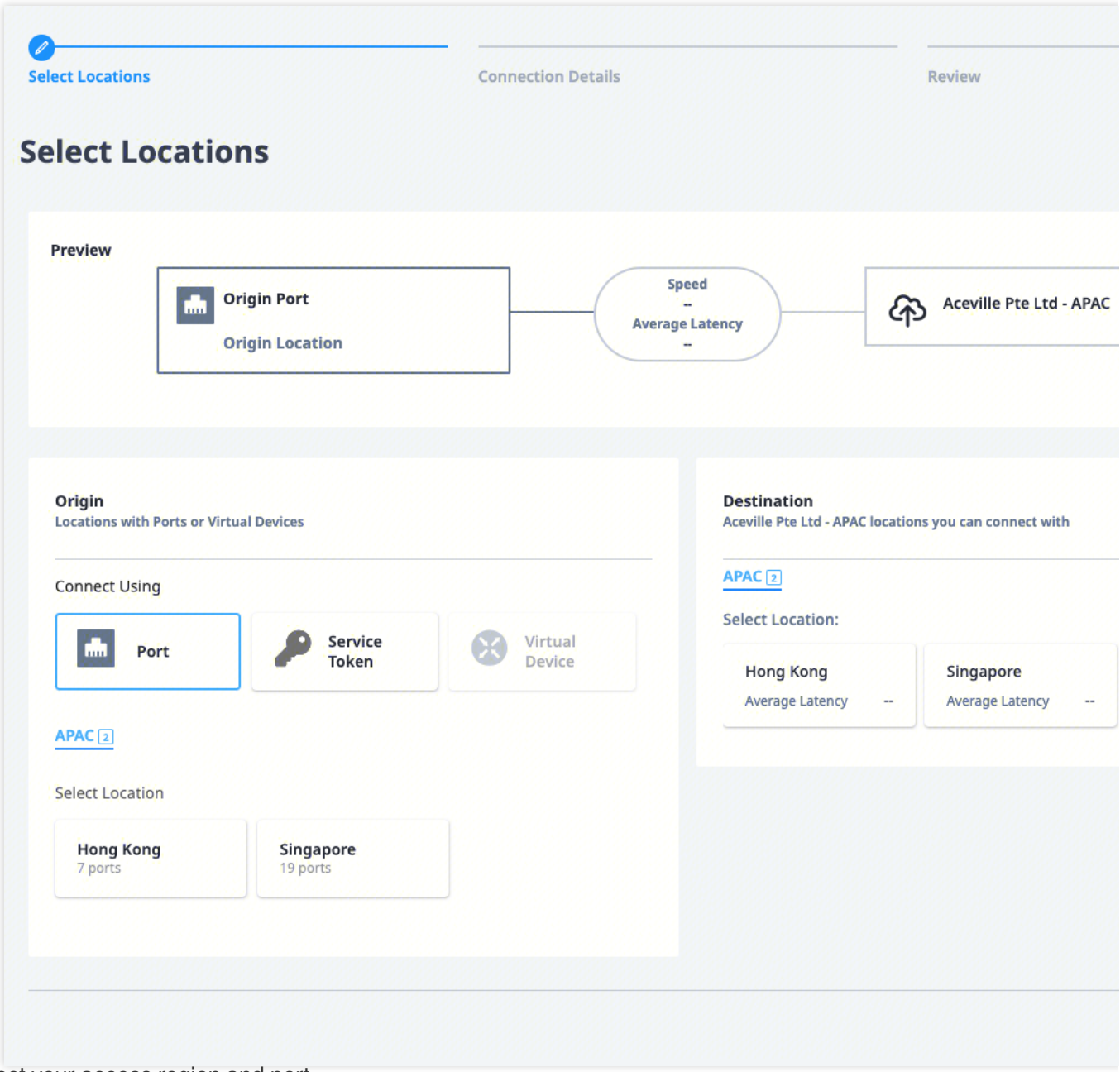


3. In the **Select a Service Provider** area, search for **tencent** in the search box. In the **Aceville Pte Ltd - APAC** selection box, click **Select Service**. In the pop-up window, select the service type **Services available to me**, and click **Create Connection**.

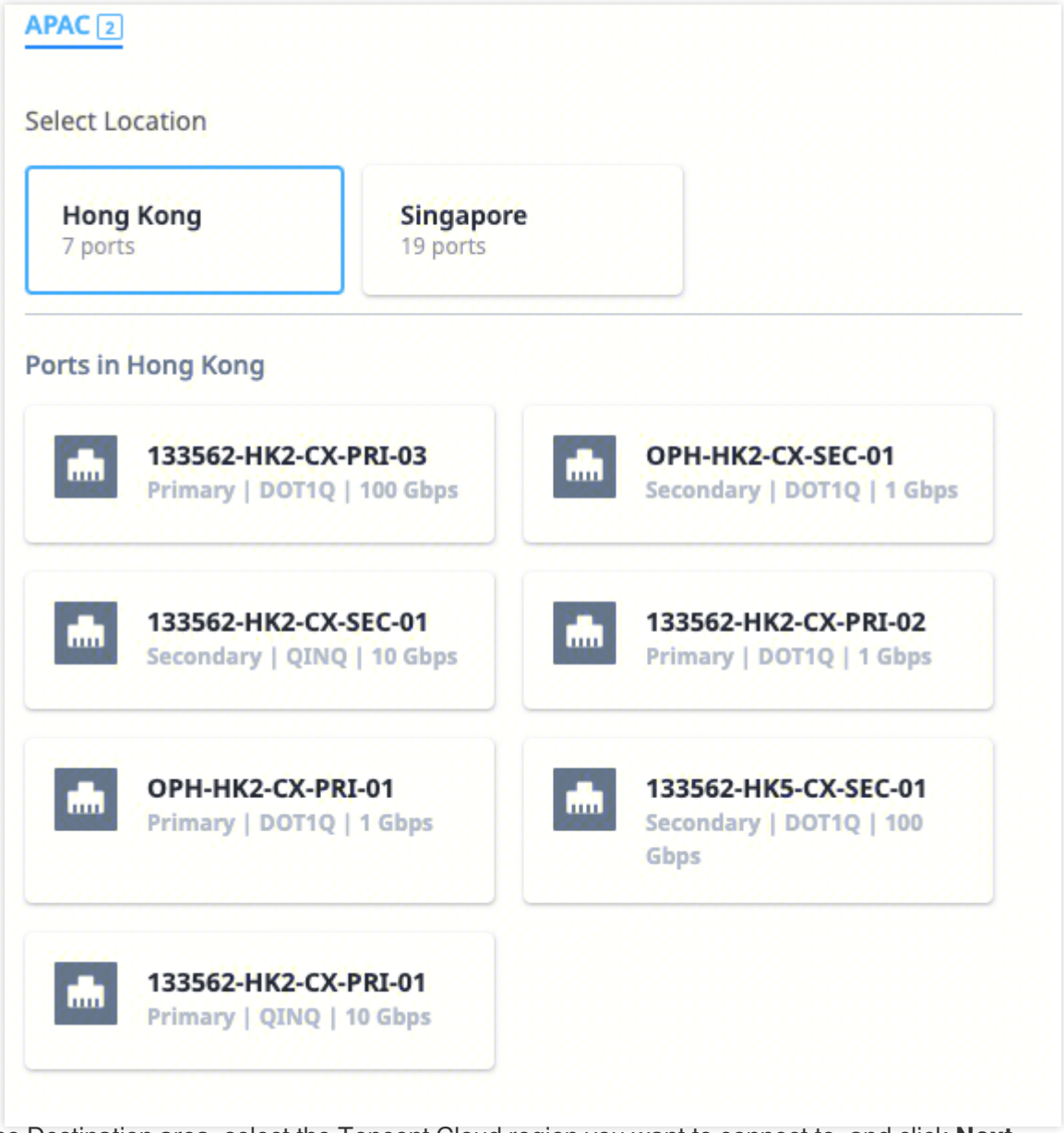


Step 2: Configuring Connection Information

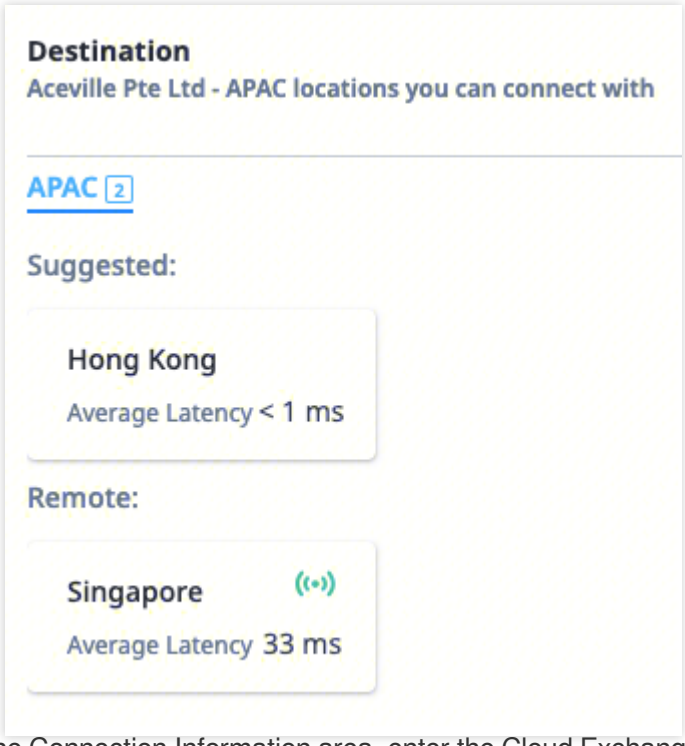
1. In the Origin configuration area of the Select Locations part, click **Port** or **Virtual Device**.



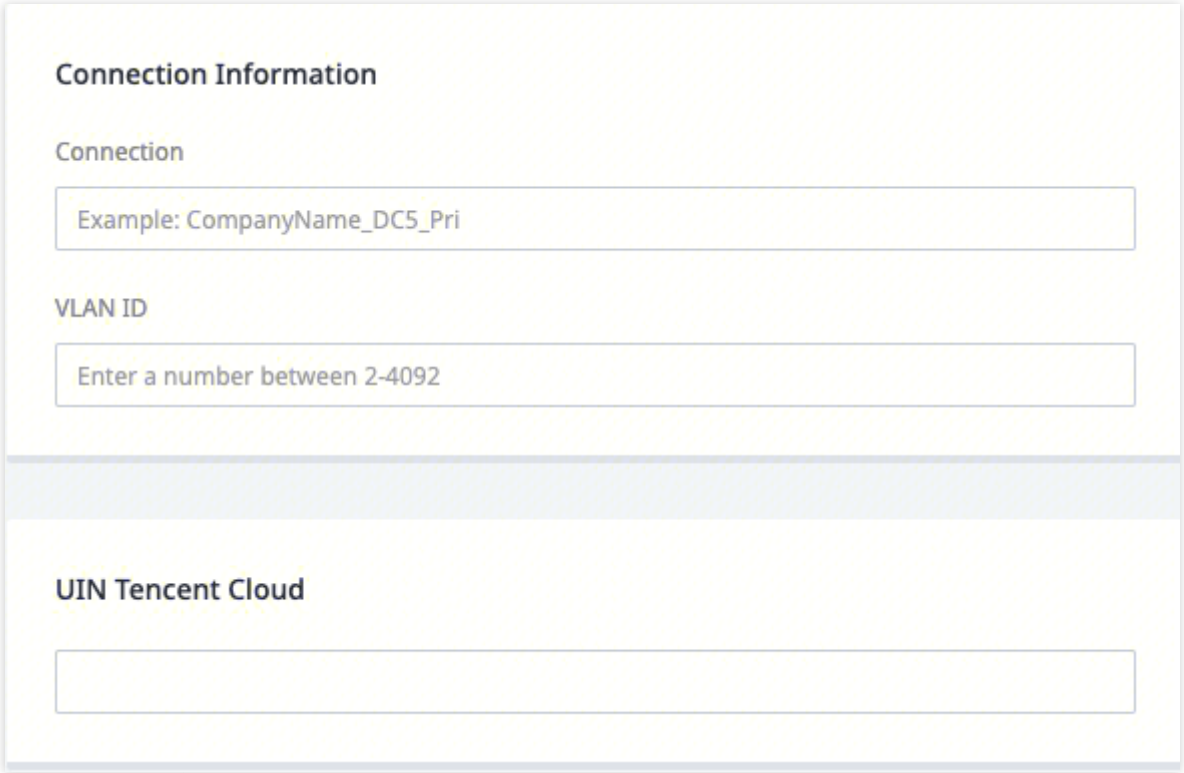
2. Select your access region and port.



3. In the Destination area, select the Tencent Cloud region you want to connect to, and click **Next**.

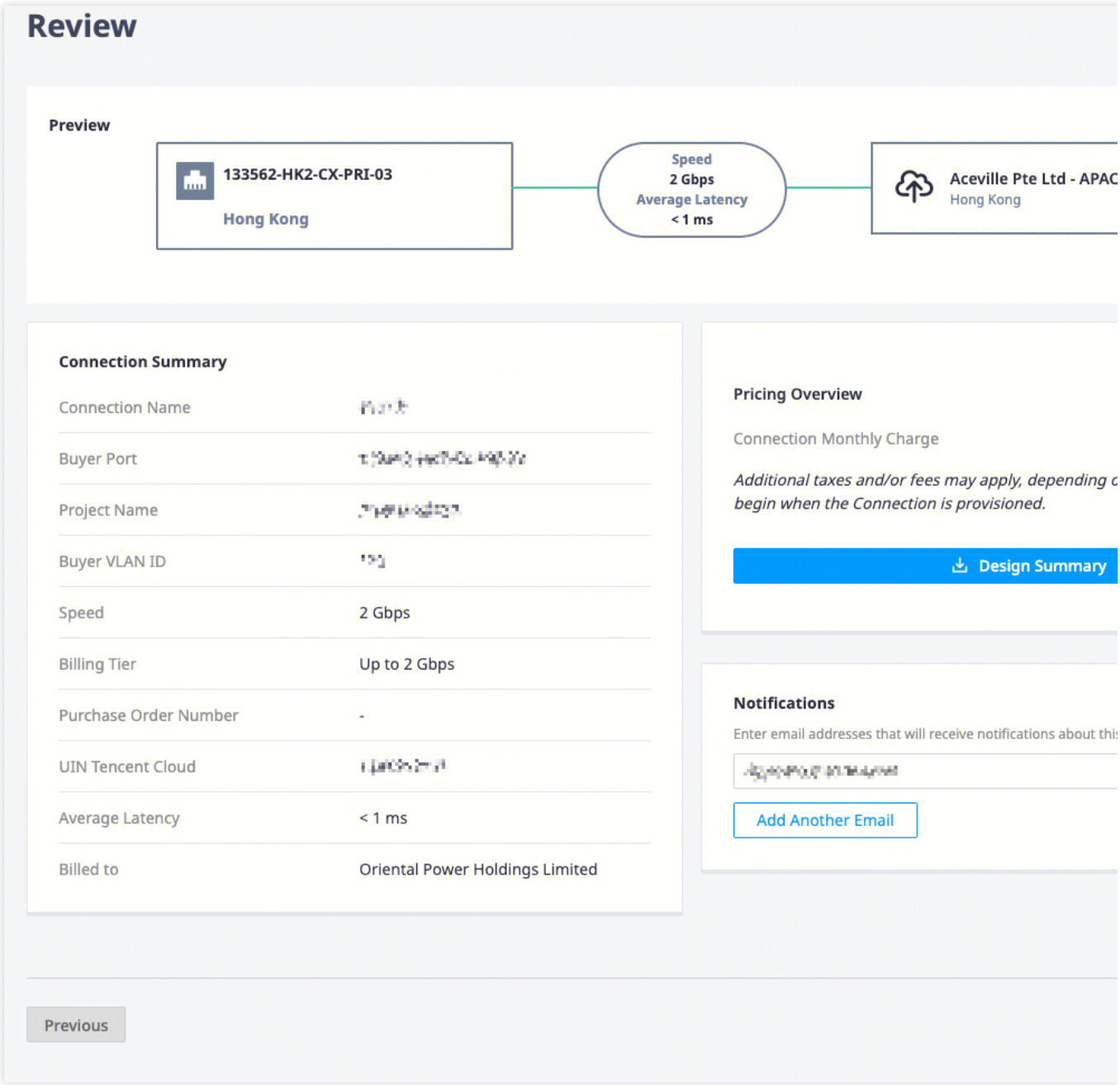


4. In the Connection Information area, enter the Cloud Exchange name and specify the VLAN ID and UIN (the Tencent Cloud account ID you use for interconnection).



5. In the Connection Speed area, select the bandwidth, and click **Next**.

6. On the **Review** page, confirm the order information, and click **Submit Order**.



Building Tencent Cloud Resources

Step 1: Confirming the Order

1. Log in to the DC console, and click **Cloud Exchange** on the left sidebar to enter the Cloud Exchange list page.
2. In the action column of the target Cloud Exchange instance, click **Confirm** to enter the resource building approval phase. A DC manager will assign a port for you.

A status change to "In Operation" indicates connectivity with Equinix, and you can create Tencent Cloud resources.

Step 2: Building Tencent Cloud Resources with One Click

When the Cloud Exchange instance status is **In Operation**, you can click **One-click Building of Cloud Resources** in the corresponding row of the instance, and configure parameters on the resource building page based the actual situation. For details on the configuration parameters, refer to Creating a Dedicated Tunnel.

Supported Equinix Regions

Equinix Region	Tencent Cloud Point
Japan	Tokyo-B-Ariake
Hong Kong (China)	Hong Kong (China)-B-Tseung Kwan O
	Hong Kong (China)-A-Kwai Chung
Singapore	Singapore-B-Tai Seng
	Singapore-A-Ayer Rajah