Direct Connect

Product Introduction

Product Documentation

Copyright Notice

Trademark Notice

Tencent Cloud

Service Statement

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

Contents

Product Introduction

Overview

Last updated：2024-01-13 16:02:36

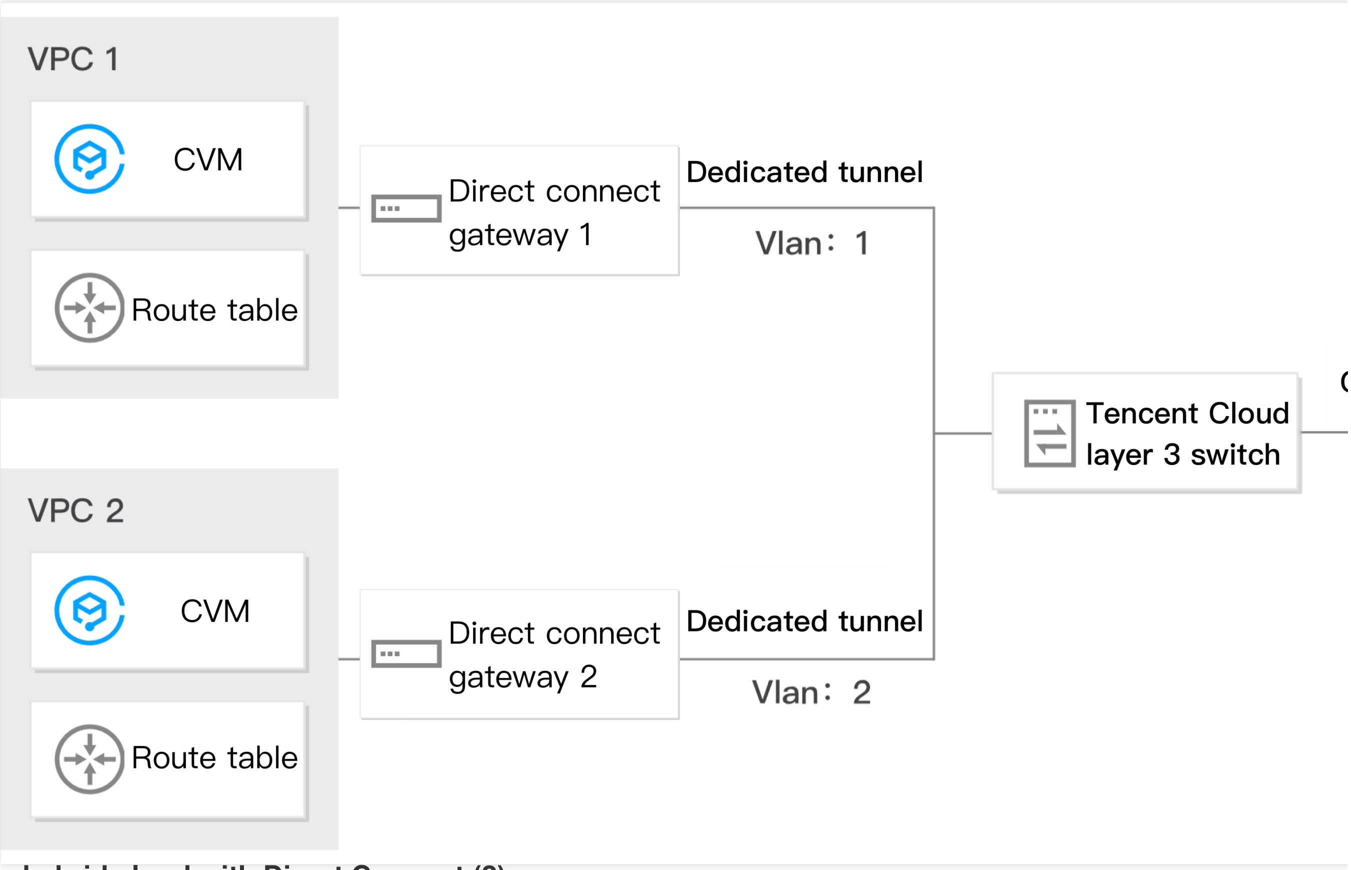
Direct Connect Overview

Direct Connect provides a fast and secure connection between Tencent Cloud and your local IDC. You can connect Tencent Cloud computing resources in multiple regions with a single connection to implement flexible and reliable hybrid cloud deployment.

Deploy hybrid cloud with Direct Connect (1)

Connect your IDCs with cloud VPCs using traditional dedicated tunnels.

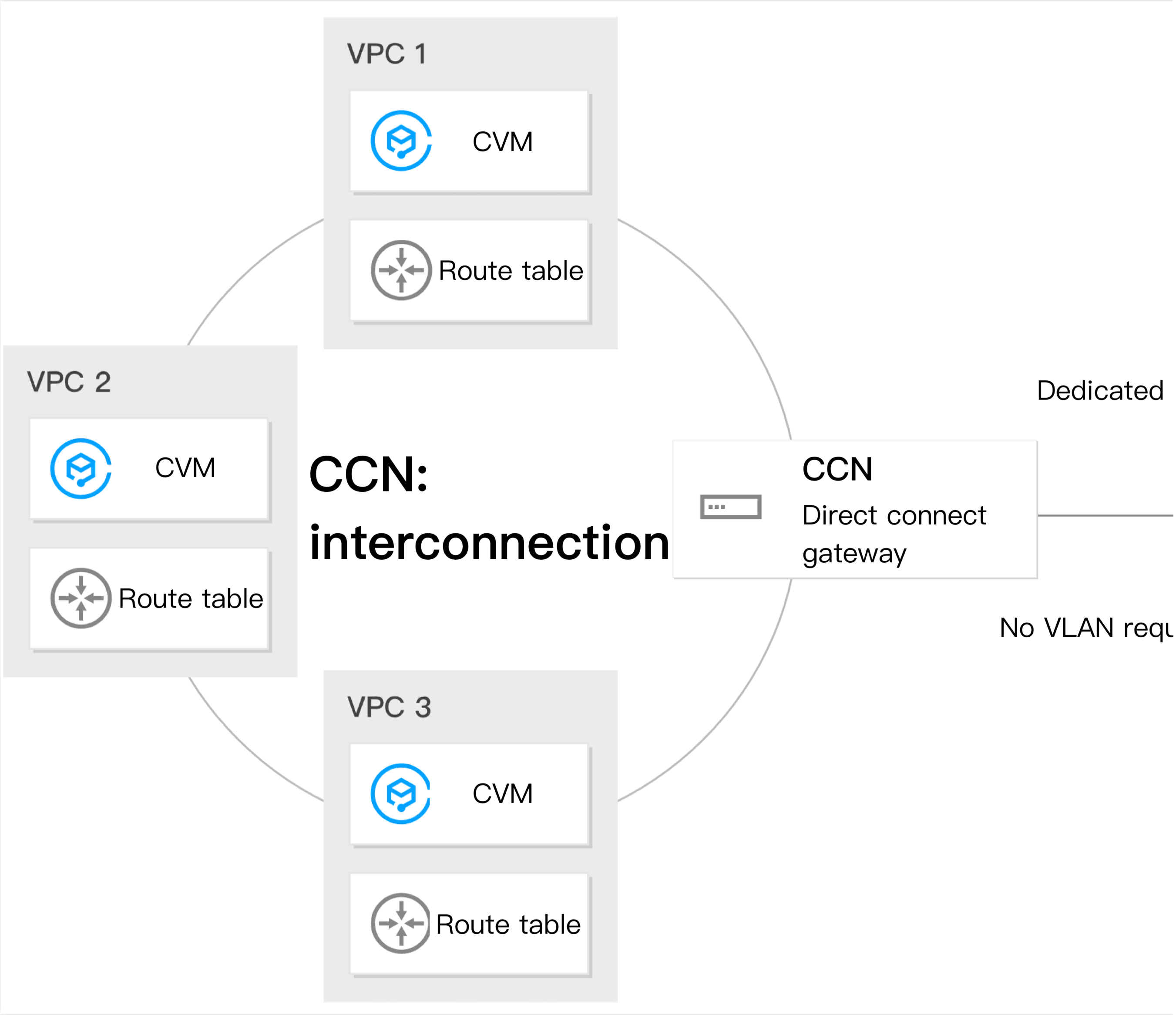
If you want to connect to multiple VPCs over one connection, you need to create dedicated tunnels with different VLAN IDs.



Deploy hybrid cloud with Direct Connect (2)

Interconnect your network instances using Cloud Connect Network (CCN).

Advantage: you just need to create one connection to the CCN-based direct connect gateway and associate the gateway with CCN to enable interconnection within the CCN.



Components

Direct Connect is composed of connections, dedicated tunnels, and direct connect gateways.

Connection

A connection is a physical line that connects customer’s local IDC to Tencent Cloud. Connections support dual-line hot backup access, dual-line access point power supply, and completely isolated network pipes.

Dedicated tunnel

A dedicated tunnel is a network link 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.

Direct connect gateway

Direct connect gateway acts as the Direct Connect traffic ingress and egress for a VPC to which multiple dedicated tunnels can be connected for communication with multiple local IDCs. This cluster-based gateway eliminates the risk of single point of failure, and meets the interconnection requirements of the finance industry.

Direct connect gateway is used to connect VPC with connections. You can create a dedicated tunnel of connections and associate it with a direct connect gateway.

Direct connect gateway can connect to dedicated tunnels of connections to enable interconnection with multiple local IDCs.

You can create up to two direct connect gateways (one standard and the other supports NAT) for each VPC in the Direct Connect Gateway console. The direct connect gateway can connect with dedicated tunnels of different connections.

Advantages over IPsec VPN

Advantage	Direct Connect	IPsec VPN Connection
Stable network latency	Network latency is stable and guaranteed. A Direct Connect instance accesses the network through dedicated links, and supports fixed routes, removing the pain of unstable latency caused by network congestion or failure bypass.	Network latency is unstable. An IPsec VPN connection accesses the network over the Internet, which may be exposed to bypass due to network congestion.
Highly reliable disaster recovery access	Access devices and network forwarding devices are deployed in distributed clusters to ensure high reliability of all links. It also supports dual-line access with protection to provide more than 99.95% of uptime.	Features a dual-server hot backup architecture with high availability at the gateway layer. However, it cannot provide the same network availability as dedicated lines due to the unreliable Internet links.
High bandwidth	Each link provides a bandwidth of up to 100 Gbps. You can have multiple 10 Gbps links for network load balancing, so it can theoretically support unlimited bandwidth.	A single IPsec VPN gateway supports a bandwidth of up to 1 Gbps and a VPC can have multiple VPN gateways, which can meet the need for a VPN connection larger than 1 Gbps.
High security	Dedicated network links offer strong security without data leakage risks, satisfying the demanding network connection requirements of the finance and government sectors.	Network transmission is encrypted using IKE pre-shared key, which can satisfy the security requirements for most network transmission.
Network address translation	It supports configuring the network address translation service on gateways, as well as IP mapping on the two sides of Direct Connect and IP port mapping on the VPC side, to	Not supported.

	avoid address conflict in case of interconnection among multiple networks.	

Features

Last updated：2024-01-13 16:02:36

Connection

A connection is a physical line that connects customer’s local IDC to Tencent Cloud. You can establish a network connection between your IDC and Tencent Cloud Direct Connect access point through a third-party network service provider.

Dedicated Tunnel

Dedicated tunnels are the network link segmentations of a connection.
You can create dedicated tunnels that connect to different direct connect gateways, making the interconnection between your on-premises IDC and multiple VPCs possible.

Direct Connect Gateway

A direct connect gateway is the ingress and egress of the dedicated tunnel between VPC and connection. A VPC supports up to two direct connect gateways (one standard and the other supports NAT).
Direct connect gateways can connect to multiple connections through dedicated tunnels. This allows for a hybrid cloud that connects with multiple regions.

Network Address Translation (NAT)

NAT is a solution that resolves the IP address conflicts when connecting hybrid clouds. You can configure NAT rules on direct connect gateways. NAT includes IP translation and IP port translation.

IP translation

IP translation translates the source IP to a new IP address for network interconnection. IP translation includes **local IP translation** and **peer IP translation**.
IP translation does not distinguish between source and destination. A mapped IP can access or be accessed by IDC.

Local IP translation

1. Description

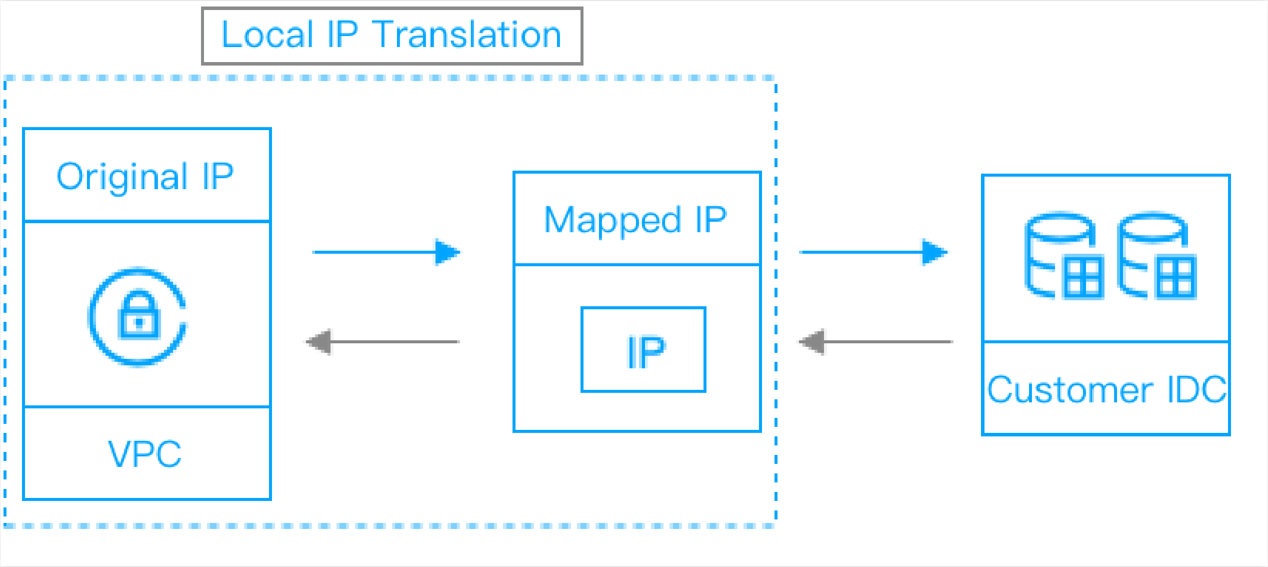
Local IP translation maps the source IP address of a resource in a Tencent Cloud VPC to a new one and use the new IP address to communicate with the IDC through Direct Connect.

You can set more than one local IP translation rule and configure network ACL for each local IP translation rule. Network ACL supports the configuration of source port, destination IP, and destination port.

Note:

NAT rules take effect only for network requests that meet ACL restriction requirements.

Local IP translation does not restrict the direction of network requests, which could be active access of the VPC to the IDC or vice versa.



2. Sample translation

If IP A `192.168.0.3` in a VPC is mapped to IP B `10.100.0.3` , the source IP address of all network packets accessing the IDC from IP A via Direct Connect is automatically translated to `10.100.0.3` . All network packets accessing `10.100.0.3` from the IDC are automatically directed to IP A `192.168.0.3` .

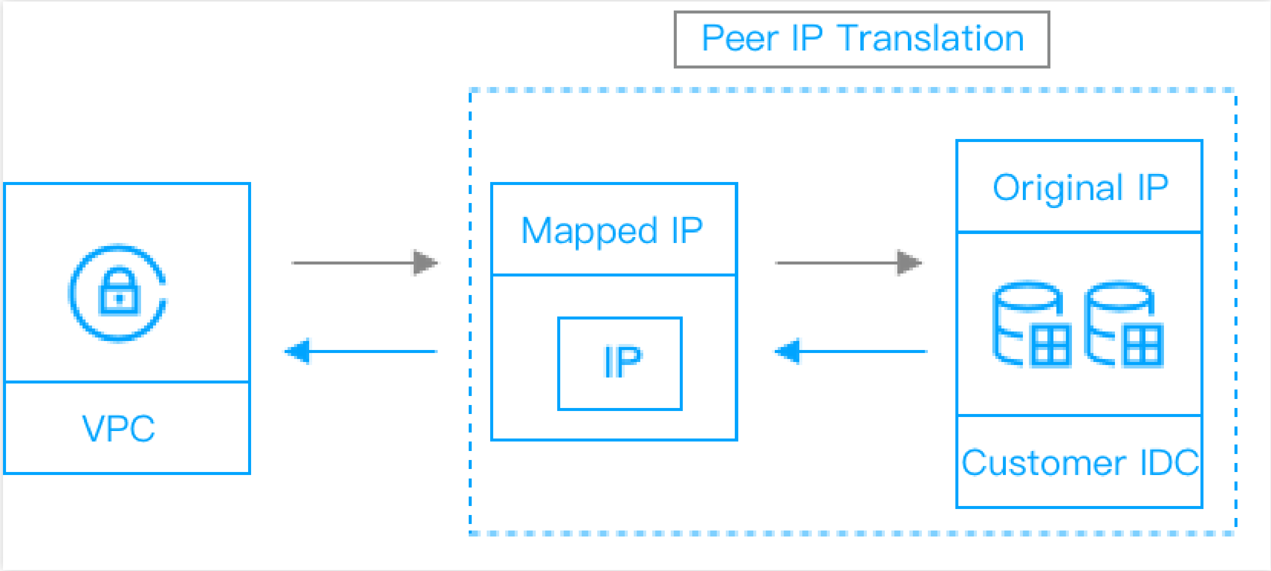
Peer IP translation

1. Description

Peer IP translation maps the source IP address of an IDC resource to a new one and uses the IP address to communicate with the VPC.

Unlike local IP translation, peer IP translation does not support network ACL restrictions. Therefore, once peer IP translation rules are configured, they take effect on all IDCs that are connected with dedicated tunnels.

Peer IP translation does not restrict the direction of network requests, which can be active access of the VPC to the IDC or vice versa.



2. Sample translation

If IP D `10.0.0.3` in an IDC is mapped to IP C `172.16.0.3` , the source IP address of all network packets accessing the VPC from IP D `10.0.0.3` is automatically translated to IP C `172.16.0.3` . All network packets accessing IP C `172.16.0.3` from the VPC are automatically directed to IP D `10.0.0.3` .

Note:

After local IP translation and peer IP translation are configured, direct connect gateway only forwards the routes of the translated IPs to the IDC. Therefore, a source IP address that has not been configured with local and peer IP translation will not be able to ping the IDC. However, a direct connect gateway is not a replacement for network firewalls. If you need advanced network protection, please configure security groups and network ACL policies within your VPC and deploy physical network firewall devices in your IDC.

When the direct connect gateway is also configured with peer IP translation, the **Destination IP** of the ACL rule for local source IP port translation should be the **mapped IP of peer IP translation**, instead of the source IP.

IP port translation

IP port translation maps the source IP port to a new one and use the new IP port for network interconnection. IP port translation includes **local source IP port translation** and **local destination IP port translation**.

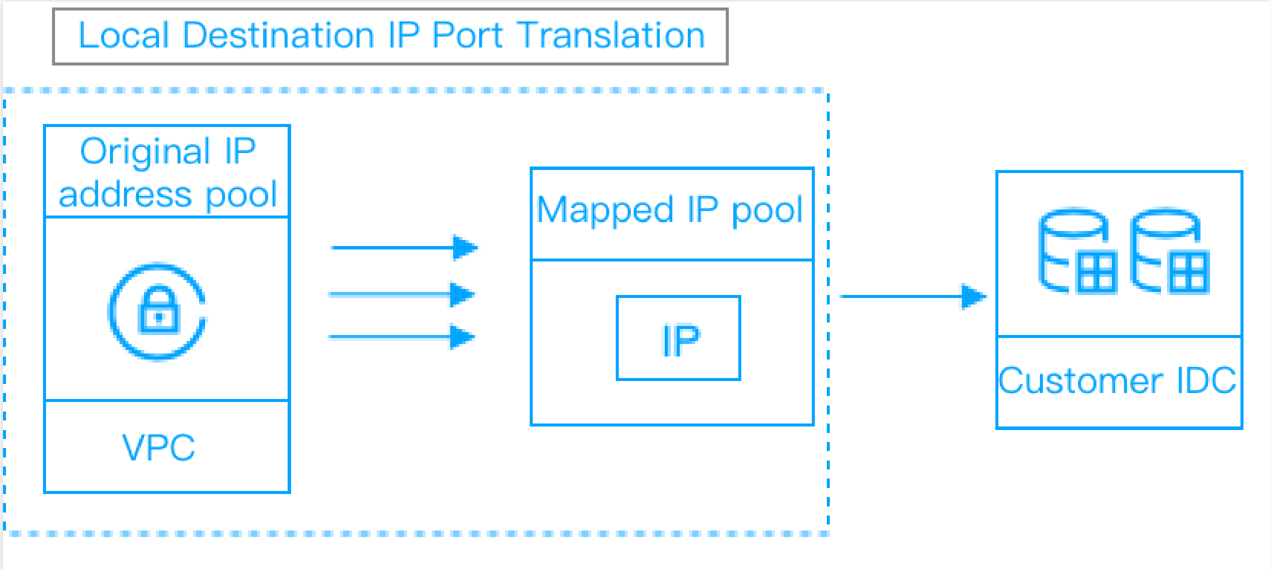
IP port translation is directional. Source IP port translation is for requests to external (to the IDC) resources, and destination IP port translation is for requests from external (to the VPC) resources.

Local source IP port translation

1. Description

Local source IP port translation translates the port of the source VPC IP address to a random port of a random IP address in the IP pool when a cloud resource accesses the IDC through a direct connect gateway.

Local source IP port translation supports ACL rules. Only outbound access requests compliant with ACL rules can be matched with address pool forwarding rules. By deploying different ACL rules for the address pool, you can flexibly configure the network address translation rules with multiple third-party access.



Local source IP port translation only supports access requests initiated by resources in a VPC. To access ports within the VPC via Direct Connect, the IDC should also be configured with local destination IP port translation. For local source IP port translation, access requests initiated by resources in a VPC are stateful connections. Therefore, response packets are not a concern.

2. Sample translation

VPC C with an IP range `172.16.0.0/16` needs to connect to third-party bank A and B via Direct Connect. Bank A with an IP range `10.0.0.0/28` needs to connect to the IP range `192.168.0.0/28` . Bank B with an IP range `10.1.0.0/28` needs to connect to the IP range `192.168.1.0/28` . For them to communicate, you need to configure the following two local source IP port translations:

Address pool A `192.168.0.1 - 192.168.0.15` ; ACL rule A: source IP `172.16.0.0/16` , destination IP `10.0.0.0/28` , destination port ALL.

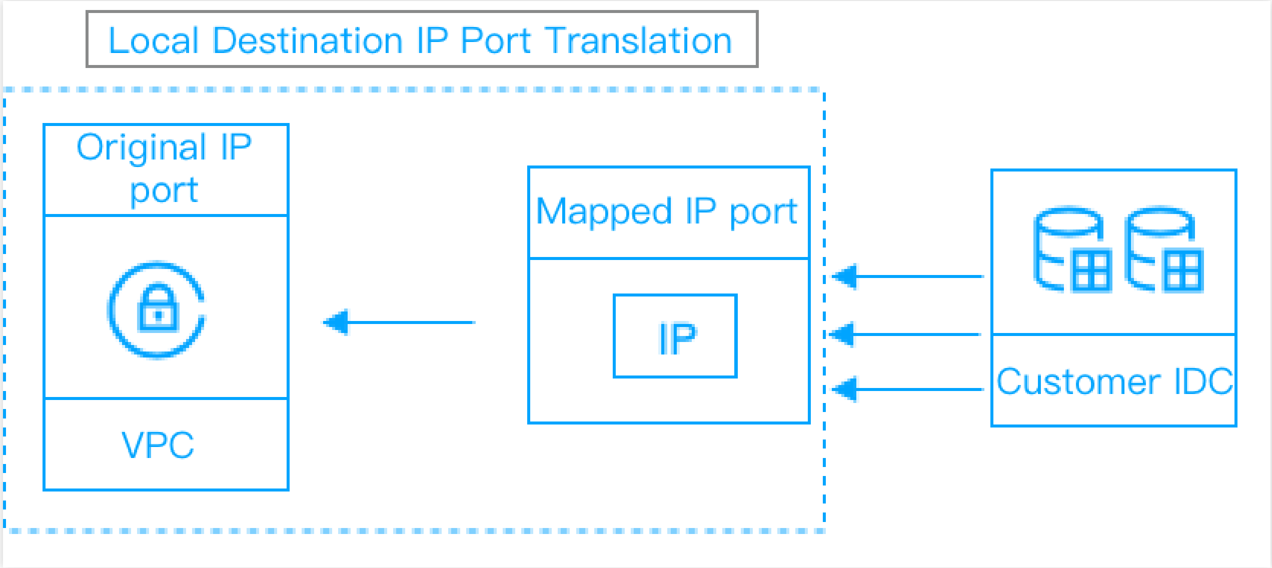
Address pool B `192.168.1.1 - 192.168.1.15` ; ACL rule B: source IP `172.16.0.0/16` , destination IP `10.1.0.0/28` , destination port ALL.

The access requests to A and B from the VPC will be translated into the random ports of corresponding address pools based on ACL rule A and B to access the appropriate dedicated tunnels.

Local destination IP port translation

1. Description

Local destination IP port translation handles requests to cloud resources in a VPC from the IDC. It translates the port of a VPC IP address to a new IP address and a new port. IDC can only communicate with VPC resources by sending requests to the mapped IP address and port, without exposing the real one.



Local destination IP port translation does not support ACL rules. Therefore, IP port translation rules will take effect on all dedicated tunnels connected to the direct connect gateway. Local destination IP port translation only takes effect on requests from IDC to a VPC via dedicated tunnels. To access an IDC, the VPC should be configured with local source IP port translation. For local destination IP port translation, the network requests are stateful connections. Therefore, response packets are not a concern.

2. Sample translation

For VPC C with an IP range `172.16.0.0/16` , if you only want to open some ports for IDC to access the VPC via Direct Connect, you can configure it as follows:

Mapping A: the source IP port is `172.16.0.1:80` and the mapped IP port is `10.0.0.1:80` .

Mapping B: the source IP port is `172.16.0.0:8080` and the mapped IP port is `10.0.0.1:8080` .

The IDC can use `10.0.0.1:80` and `10.0.0.1:8080` through Direct Connect to access `172.16.0.1:80` and `172.16.0.0:8080` in the VPC.

Note:

After local source and destination IP port translations are configured, the direct connect gateway only forwards the translated IP port routes to the IDC. Therefore, the local IP port that is not configured with translations cannot initiate requests nor receive requests. However, a direct connect gateway is not a replacement for network firewalls. If you need advanced network protection, please configure security groups and network ACL policies within your VPC and deploy physical network firewall devices in your IDC.

When both IP translation and IP port translation are configured, IP translation has priority. If there is no match for IP translation, IP port translation is used.

When the direct connect gateway is also configured with peer IP translation, the **Destination IP** of the ACL rule for local source IP port translation should be the **mapped IP of peer IP translation**, instead of the source IP.

Application Scenarios

Disaster Recovery Deployment

Last updated：2024-01-13 16:02:36

Application Scenarios

The user already has large scale applications. His/Her focus has been shifted from the balance between infrastructure deployment and business growth to the stability and reliability of the infrastructure for multi-center development.
He/She hopes to eliminate business risks caused by single IDC failure through eliminating single IDCs.

User's core pain point

How to realize multi-location disaster recovery and improve infrastructure reliability.

How to realize fast deployment while reducing infrastructure construction period.

How to re-use stock IDC to reduce operating costs (use existing servers first).

Solutions:

Hybrid cloud disaster recovery deployment

Multi-location IDC deployment: Build master/slave clusters in local IDC and public cloud IDC.

Data synchronization: Synchronize data via Direct Connect or VPN to avoid single IDC failure.

Traffic forwarding: Provide lossy but uninterrupted services by forwarding the traffic to normal IDCs.

2-region-3-DC disaster recovery deployment in cloud

Cross-availability zone deployment: You can create subnets and deploy services in different availability zones within one VPC. Data can be synchronized between subnets of different availability zones. The goal of using different availability zones is to ensure that the failures are isolated from each other.

Cross-region deployment: You can deploy the same service in the VPC of another region to achieve multi-location disaster recovery and avoid failures in one region from spreading to other regions.

Cross-region high-speed interconnection: VPCs of two different regions achieve interconnection via cross-region peering connection.

Traffic forwarding: it provides lossy but uninterrupted services by forwarding the traffic to other normal IDCs when an IDC breaks down.

Procedure

Steps of hybrid cloud disaster recovery deployment

1. Create a VPC on Tencent Cloud and deploy IDCs. For more information, please see VPC Instructions.
2. Synchronize the local IDC and the VPC IDC on the cloud via Direct Connect. For more information, please see Direct Connect Instructions.
3. Forward the traffic to other normal IDCs when an IDC breaks down.

Steps of cloud 2-region-3-DC disaster recovery deployment

1. Cross-availability zone deployment. You can create subnets and deploy master and slave synchronization service in different availability zones within one VPC. Data can be synchronized between subnets of different availability zones. The goal of using different availability zones is to ensure that the failures are isolated from each other. For more information, please see Subnet Instructions.
2. Cross-region deployment. You can deploy the same service in the VPC of another region to achieve multi-location disaster recovery and avoid failures in one region from spreading to other regions. For more information, please see VPC Instructions.
3. Cross-region high-speed interconnection. Create a cross-region peering connection to achieve high-speed data synchronization between two VPCs. For more information, please see Peering Connection Instructions.

Line access to the hybrid cloud deployment

Last updated：2024-01-13 16:02:36

According to your different connection needs, Tencent Cloud provides two services respectively to connect your enterprise IDC and VPC: VPN connection and Direct Connect. The main differences are as follows:

VPN Connection uses the public network and IPsec protocol to establish an encrypted network connection between your IDC and VPC. The purchase, enforcement and configuration of VPN gateway can be completed within minutes. But the VPN connection may be interrupted due to Internet jitter, block or other public network quality problems. If users' services have low requirement for the network connection quality, it is a highly cost-effective choice for fast deployment.

Direct Connect provides a dedicated Direct Connect network connection method. It has relatively long construction duration, but can provide high-quality, highly reliable network connection service. If your business requires high network quality and network security, you can choose to deploy this program.

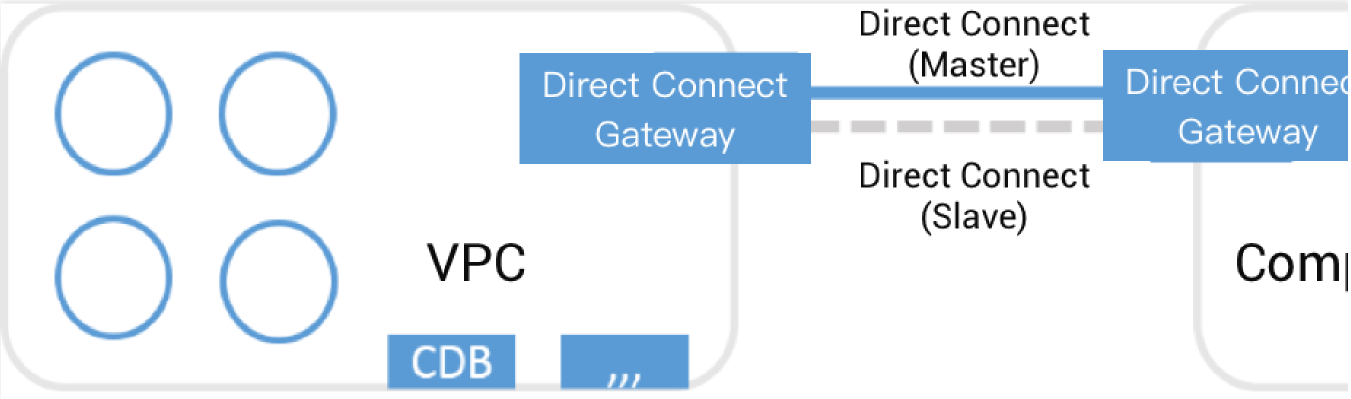
The following describes how to deploy a hybrid cloud using **Direct Connect**.

Application Scenarios

Direct Connect provides a fast and secure approach to connecting Tencent Cloud with local IDCs. Users can access to Tencent Cloud computing resources in multiple regions in one go using a Connection, to achieve a flexible and reliable hybrid cloud deployment.

There are two ways to set up a slave for Direct Connect:

Dual Direct Connect slave: Tencent Cloud supports master/slave failover configuration.



VPN connection serves as Direct Connect Linkage slave (master/slave).

Note:

Your **IP address range overlap** between VPC and IDC does not affect the communication, because Tencent Cloud Direct Connect gateway supports NAT. For more information, please see Direct Connect Features.

Solutions:

Cloud IDC: Use CVM and Cloud Database to deploy cloud IDC in a VPC created on Tencent Cloud.
Connection method: Integrate VPC IDC with your IDC private network via Connection.
Slave connection method: Dual Direct Connect/VPN connection.

Procedure

If Direct Connect is used to connect your IDC and the VPC IDC on Tencent Cloud, you need to complete the following steps:

1. Create the Connection.
2. Create the Dedicated Tunnel.
3. Create the Dedicated Tunnel for Direct Connect gateway, thus connecting your IDC to your VPC.
4. Configure the Direct Connect NAT (Optional).
5. Configure the routing table associated with the subnets requiring communication.
6. You can set up slaves for a Direct Connect by creating multiple Connection or VPN connections.

For more information, please see Getting Started.

Use Limits

Last updated：2024-01-13 16:02:36

Resource Limits

Resource	Constraints	Support Increasing Quota	Description
Connections per user	10	Yes	Each user can have up to 10 connections.
Dedicated tunnels per connection	5	Yes	Up to 5 dedicated tunnels can be created in each connection
DC gateways per VPC	2 (One standard gateway and one NAT gateway)	No	Up to 2 Direct Connect gateways can be configured in each VPC.
Local IP translations per DC gateway	100	Yes	Up to 100 local IP translations can be configured for each Direct Connect gateway.
Peer IP translations per DC gateway	100	Yes	Up to 100 peer IP translations can be configured for each Direct Connect gateway.
Local source IP port translations per DC gateway	20	Yes	Up to 20 local source IP port translations can be configured for each dedicated gateway.
Local destination IP port translations per DC gateway	100	Yes	Up to 100 local destination IP port translations can be configured for each Direct Connect gateway.
Static routes per dedicated tunnel	Dedicated tunnel 1.0: 20	No	Up to 20 static routes can be configured for a dedicated tunnel 1.0.
	Dedicated tunnel 2.0: 50	Yes	Up to 50 static routes can be configured for a dedicated tunnel 2.0. To adjust the quota, please submit a ticket.

BGP routes per dedicated tunnel	Dedicated tunnel 1.0: 100	No	Up to 100 BGP routes can be configured for a dedicated tunnel 1.0.
	Dedicated tunnel 2.0: 100	Yes	Up to 100 BGP routes can be configured for a dedicated tunnel 2.0. To adjust the quota, please submit a ticket.

Access Limits

Direct Connect

When a Direct Connect gateway is created, the content of IP translation and IP port translation are left empty by default. In this case, neither of them takes effect.

Dedicated tunnels support BGP routing and static routing.

Note the following limits for delivering routes:

To improve the fine-grained scheduling capability of your network, do not publish the following routes:

Dedicated tunnel 1.0 `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` .

Note:

The direct connect gateway will directly reject large IP ranges.

You can split the above large routes as follows for distribution:

`9.0.0.0/8`

Split as: `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` .

Dedicated tunnel 2.0

`127.0.0.0/8` , `224.0.0.0/4` , `240.0.0.0/4` , `255.255.255.255` , and `169.254.0.0/16` (excluding `169.254.64.0/23`).

Subnets and other IP addresses in the same network segment. To allow mutual access, submit a ticket to enable peer IP redistribution.

IP translation

IP address pools cannot fall within the CIDR block of the VPC in which the direct connect gateway resides.
ACL rules for multiple IP address pools should not overlap. Otherwise, this will cause network address translation conflicts.
IPs among multiple IP address pools cannot overlap.
IP address pools only support a single IP or IP ranges, and `/24` IP ranges 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.
Address pools should not contain the 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 source IP port translation supports up to 100 IP address pools, each supporting up to 20 ACL rules. You can submit a ticket to increase the quota if needed.
To switch from IP translation to IP port translation, remove the original IP translation rules and refresh the page to edit the IP port translation rules.

IP port translation

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.
Original IPs and mapped IPs do not support the 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 destination IP port translation supports up to 100 IP port mappings. You can submit a ticket to increase the quota if needed.
If both IP translation and IP port translation are configured, IP translation takes priority when both are hit.

Network Limits

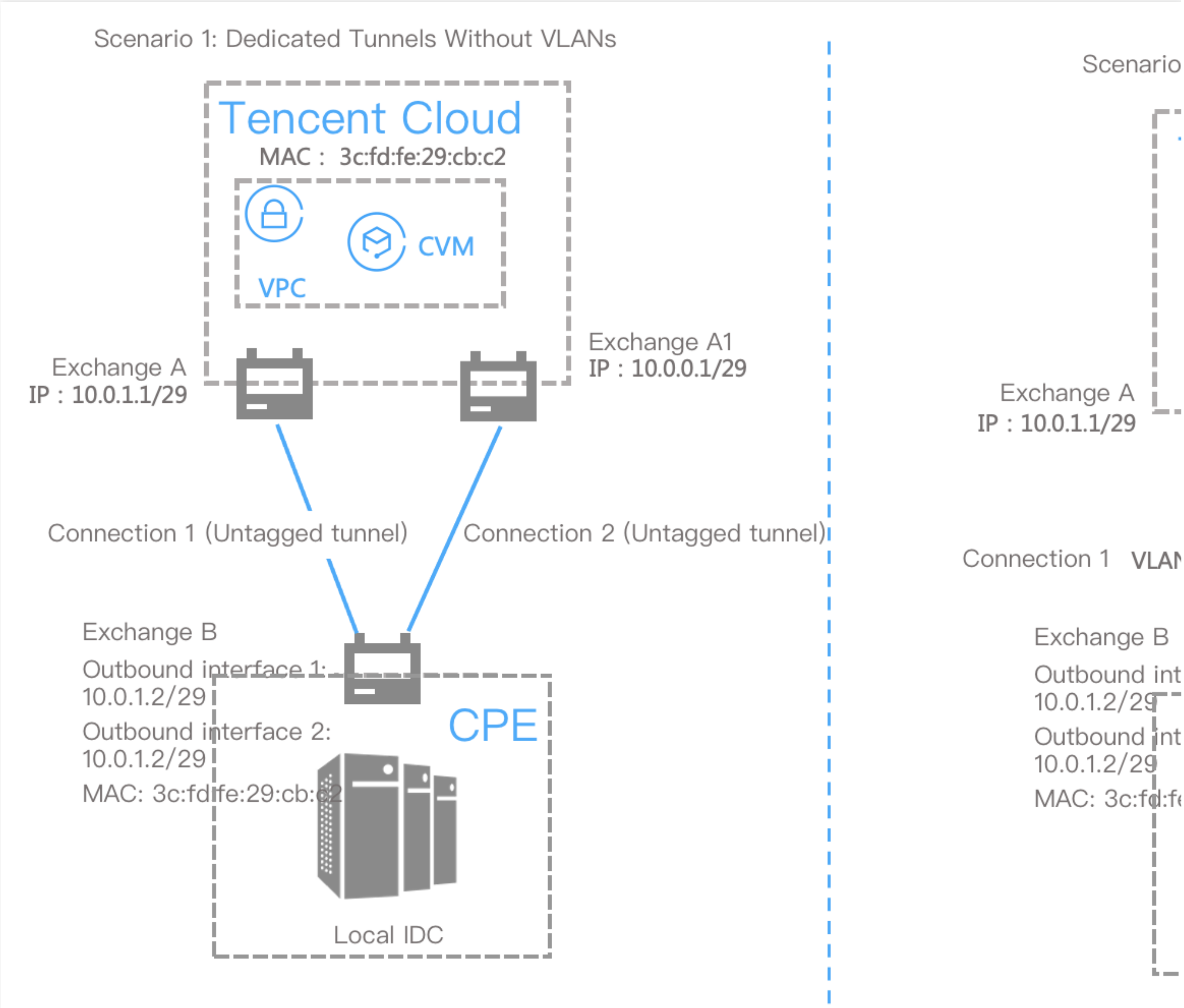
To establish a connection between the cusotmer IDC and Tencent Cloud, check that the MAC addresses of both parties meet the following requirements.

MAC

The Tencent Cloud access exchange uses a fixed MAC address of 3c:fd:fe:29:cb:c2. This MAC address cannot be used by the customer IDC access device. Otherwise, the MAC address conflict will cause MAC address flapping (switching jump), which leads to network problems such as unreachable networks, slow response, and no response.

Note:

MAC address flapping (switching jump) occurs when a MAC address is learned by two outbound interfaces in the same VLAN and the MAC address entry learned later overrides the earlier one, making the MAC address unstable. The following are scenarios where MAC address flapping occurs.



As shown in the figure above, customer exchange B connects to Tencent Cloud exchanges A and A1 through two connections (connections 1 and 2).

MAC address flapping occurs in exchange B when Tencent Cloud returns packets to the customer IDC.

Access Limits

To prevent network congestion due to network loops, you are advised to use layer-3 network sub-interfaces to connect to Tencent Cloud Direct Connect devices.

Connection Access Point

Last updated：2024-08-16 16:01:46

This document describes the approximate locations of Tencent Cloud access points, helping you choose the nearby access point for your local IDC.

Note:

The access points created after 00:00 on July 1, 2022 only support fiber optical port access, not electrical port access.

Regions in China

Region		Access point	Provider	Supported Port Types	Address
East China	Hangzhou	ap-hangzhou-a-dg	CTCC	Fiber optic port and electrical port	Building 4, Dongguan Technology Park, No. 288 Qiuyi Road, Binjiang District, Hangzhou
		ap-hangzhou-b-xh	CUCC	Fiber optic port and electrical port	Building 3113, No. 924-7, Xixi Road, Xihu District, Hangzhou
		ap-hangzhou-c-jg	CUCC	Fiber optic port and electrical port	Building 1412-1, No. 28-2, No. 4 Street, Xiasha Economic Development Zone, Qiantang New District, Hangzhou
	Shanghai	ap-shanghai-b-tz	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	No. 51, Daxiu Road, Pudong New Area, Shanghai
		ap-shanghai-c-td	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	Tencent Building, Block C, No. 1801 Hongmei Road, Shanghai

		ap-shanghai-d-wr	CUCC	Fiber optic port and electrical port	Building C, No. 1268 Wanrong Road, Jing'an District, Shanghai
		ap-shanghai-f-yh	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	No. 168, Dongxue Road, Dongjing Town, Songjiang District, Shanghai
		ap-shanghai-g-hq	CUCC	Fiber optic port and electrical port	Centrin Data Systems Co., Ltd., No. 192, Jinzhong Road, Huaqiao Town, Kunshan, Suzhou
		ap-shanghai-h-wgq	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	No. 25, Feila Road, Waigaoqiao, Shanghai
		ap-shanghai-k-sj	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	Building 8, Lane 3999, Wenxiang Road, Economic and Technological Development Zone, Songjiang District, Shanghai
		ap-shanghai-l-bx	CTCC	Electrical port	Baozhiyun Building 3, No. 500, Chuanji Road, Baoshan District, Shanghai (China Mobile Luojing Data Center)
		ap-selfdrivingcloud-a-sj	CTCC, CMCC, and CUCC	Fiber optic port	Wenxiang Road, Economic and Technological Development Zone, Songjiang District, Shanghai (Building 8, Shanghai Tencent Songjiang DC)

		ap-selfdrivingcloud-b-yh	CTCC, CMCC, and CUCC	Fiber optic port	No. 168, Dongxue Road, Dongjing Town, Songjiang District, Shanghai (Tencent Songjiang Yuehu DC2 Building)
		ap-financialcloud-a-tz	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	No.51, Daxiu Road, Pudong New Area, Shanghai
		ap-financialcloud-b-bx	CTCC, CMCC, and CUCC	Fiber optic port	Building 10, BaoCloud, No. 500, Chuanji Road, Baoshan District, Shanghai
		ap-financialcloud-shanghai-d-td	CTCC, CMCC, and CUCC	Fiber optic port	Tencent Building, Block C, No. 1801, Hongmei Road, Shanghai
		ap-financialcloud-shanghai-e-sj	CTCC, CMCC, and CUCC	Fiber optic port	Building 8, Lane 3999, Wenxiang Road, Economic and Technological Development Zone, Songjiang District, Shanghai
	Nanjing	ap-nanjing-a-js	CTCC	Fiber optic port and electrical port	150 meters north of Ginkgo Lake Avenue, Jiangning District, Nanjing
		ap-nanjing-b-xf	CMCC	Fiber optic port and electrical port	150 meters west of the intersection of Xuefu Road and Xinghuo Road, Pukou District, Nanjing (China Mobile Nanjing Jiangbei Data Center)
		ap-nanjing-c-yz	CTCC,	Fiber optic	Room 101, Building

			CMCC, and CUCC	port and electrical port	1, Tencent Yizheng Dongsheng Cloud Computing Data Center, No. 666, Keyan 2nd Road, Economic Development Zone, Yizheng, Jiangsu Province
	Jinan	ap-jinan-a-ch	CMCC	Fiber optic port and electrical port	Room 501, Building A1, Northeast corner of the intersection of Chunhui Road and Keyuan Road, Suncun Town, High-tech Zone, Jinan City, Shandong Province
	Hefei	ap-hefei-a-td	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	Room 401, Building 2, No. 204, Fanhua Avenue, Shushan District, Hefei, Anhui Province
		ap-hefei-b-gx	CTCC	Fiber optic port	2nd Floor, Building 1, Customer Service Base, Intersection of Xiyou Road and Jingui Road, High-tech Zone, Hefei City, Anhui Province
	Fuzhou	ap-fuzhou-a-ck	CTCC	Fiber optic port and electrical port	West side computer room on the 4th floor, Fuzhou Yungu Cangke Data Center, No. 1 Gaochang Road, Cangshan Science and Technology Park, Cangshan District, Fuzhou City, Fujian Province

South China	Guangzhou	ap-guangzhou-a-kyl	CTCC, CMCC, and CUCC	Fiber optic port	1st Floor, Building B1, Enterprise Accelerator Industrial Park, No. 11 Kaiyuan Avenue, Huangpu District, Guangzhou
		ap-guangzhou-b-hxy	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	Building G6, South China New Materials Innovation Park, No. 31, Kefeng Road, Luogang District, Guangzhou
		ap-guangzhou-c-dc	CTCC	Fiber optic port	Building 2, China Telecom Data Center, No. 26, Dongchong Section, Shinan Road, Nansha District, Guangzhou City, Guangdong Province
		ap-guangzhou-d-qy	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	Tencent Qingxin Cloud Computing Data Center, Longwan Yiheng Road, Qingxin District, Qingyuan City, Guangdong Province
		ap-guangzhou-e-qc	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	The end of Township Road 115, Diaojian Village, Tan Town, Qingcheng District, Qingyuan, Guangdong Province
		ap-guangzhou-f-nxg	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	No. 4, Xianning Road, Zengcheng District, Guangzhou
	Shenzhen	ap-shenzhen-a-gm	CMCC	Fiber optic port and	Building 3, Pengsen Haina Center,

				electrical port	Gongming Town, Guangming New District, Shenzhen (intersection of Guangqiao Road and Dongchang Road)
		ap-shenzhen-b-ft	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	Wanguo Data Center, Futian Free Trade Zone, Shenzhen, Guangdong
		ap-shenzhen-d-bh	CTCC, CMCC, and CUCC	Fiber optic port	7th Floor, North Tower, Tencent Binhai Building, No. 33, Haitian 2nd Road, Nanshan District, Shenzhen, Guangdong
		ap-shenzhen-e-ps	CUCC	Fiber optic port and electrical port	China Unicom Data Center, 3rd Floor, Building 1, Guoren Technology Park, Pingshan District, Shenzhen
		ap-shenzhen-f-lj	CMCC	Fiber optic port and electrical port	Junde Logistics Center, No. 6, Jinxiu West Road, Pingshan District, Shenzhen, Guangdong Province
		ap-shenzhen-financialcloud-a-ps	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	Room 0402, Building 2, Shenyu DC, Shenyu Science and Technology Park, Pingshan District, Shenzhen
		ap-financialcloud-b-jx	CTCC, CMCC, and CUCC	Fiber optic port	Building 1, Jinxiu Science Park, intersection of Wuhe Avenue and

					Guanping Road, Longhua New District, Shenzhen (No. 85, Hudi Pai, Dafu Community, Guanlan)
		ap-financialcloud-shenzhen-d-bh	CTCC, CMCC, and CUCC	Fiber optic port	North Tower, Binhai Building, No. 33, Haitian 2nd Road, Nanshan District, Shenzhen, Guangdong Province
		ap-financialcloud-shenzhen-e-lj	CMCC	Fiber optic port	Junde Logistics Center, No. 6, Jinxiu West Road, Pingshan District, Shenzhen, Guangdong Province
North China	Beijing	ap-beijing-a-kc	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	No. 15, Kechuang 9th Street, Yizhuang Economic and Technological Development Zone, Beijing
		ap-beijing-b-hx	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	No. 7, Yumin Street, Houshayu Town, Shunyi District, Beijing
		ap-beijing-c-jxq	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	Dexin Building, Building 402, Courtyard 10, Jiuxianqiao North Road, Chaoyang District, Beijing
		ap-beijing-d-zj	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	No. 1, Boxing 8th Road, Yizhuang Economic and Technological Development Zone, Beijing

		ap-beijing-f-yf	CUCC	Fiber optic port and electrical port	Zone C, Antai Science Park, No. 11, Fenghui Middle Road, Haidian District, Beijing
		ap-beijing-h-hl	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	Touerying Village, Cunrui Town, Huailai County, Zhangjiakou
		ap-beijing-l-dhm	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	Building 7, Breakthrough Technology Park, No. 56, Jiujingzhuang, Dahongmen, Fengtai District, Beijing
		ap-beijing-k-ls	CMCC	Fiber optic port and electrical port	Building 2, Lanshan Computer Room, No. 1 Niuhui Street, Shunyi District, Beijing
		ap-beijing-l-sy	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	No. 7, Yumin Street, Houshayu Town, Shunyi District, Beijing
		ap-beijing-o-tg	CTCC, CMCC, and CUCC	Fiber optic port	Courtyard 6, Tongji South Road, Yizhuang Economic and Technological Development Zone, Beijing
		ap-financialcloud-a-yf	CUCC	Fiber optic port and electrical port	AT&M Park, No. 11, Middle Fenghui Road, Haidian District, Beijing
		ap-financialcloud-a-zf	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	Beijing Hua Wei Furniture Manufacture Co. Ltd., No. 8, Zhaofeng 1st Street, Zhaofeng

					Industrial Park, Zhaoquanying Town, Shunyi District, Beijing
		ap-financialcloud-beijing-c-kch	CTCC, CMCC, and CUCC	Fiber optic port	No. 15, Kechuang 9th Street, Yizhuang Economic and Technological Development Zone, Beijing
		ap-financialcloud-beijing-d-zhg	CTCC, CMCC, and CUCC	Fiber optic port	No. 1, Boxing 8th Road, Yizhuang Economic and Technological Development Zone, Beijing
		ap-financialcloud-beijing-e-xh	CTCC, CMCC, and CUCC	Fiber optic port	No. 7, Yumin Street, Houshayu Town, Shunyi District, Beijing
		ap-financialcloud-beijing-f-sxq	CTCC, CMCC, and CUCC	Fiber optic port	Dexin Building, Building 402, Courtyard 10, Jiuxianqiao North Road, Chaoyang District, Beijing
		ap-beijing-g-zf	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	Beijing Hua Wei Furniture Manufacture Co. Ltd., No. 8, Zhaofeng 1st Street, Zhaofeng Industrial Park, Zhaoquanying Town, Shunyi District, Beijing
		ap-beijing-h-hldy	Other(China)	Fiber optic port	Dananxinbao Village, Donghuayuan Town, Huailai County, Zhangjiakou
	Tianjin	ap-c-tianjin-gx	CTCC,	Fiber optic	The intersection of

			CMCC, and CUCC	port	Gangcheng Avenue and Zhongxinzhuang Road, Binhai Hi-tech Zone, Tianjin
	Shijiazhuang	ap-shijiazhuang-a-cs	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	Go east for 300 meters from the intersection of Menglong Street and Chongyin Road, Zhengding New District, Shijiazhuang City
	Shenyang	ap-shenyang-a-tx	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	No. 10-3, Lane 10, No. 3 Street, Economic and Technological Development Zone, Shenyang
	Taiyuan	ap-taiyuan-a-zx	CMCC	Fiber optic port	Shanxi Mobile Data Center, Zexin Street, Economic and Technological Development Zone, Xiaodian District, Taiyuan, Shanxi
Central China	Wuhan	ap-wuhan-a-lkg	CTCC	Fiber optic port and electrical port	Room 203, Building 1, EC1, Wuhan Telecom Linkong Port
	Changsha	ap-changsha-a-yg	CMCC	Fiber optic port and electrical port	Zhengtong Yungu Industrial Park, Jinxing North Road, Wangcheng District, Changsha
	Xi'an	ap-xian-a-xx	CMCC	Fiber optic port and electrical port	Xi'an Data Center, Tongyi Road, Fengxi New Town, Xixian New District, Xi'an, Shaanxi Province
	Zhengzhou	ap-zhengzhou-	CMCC	Fiber optic	East of Huanglu

		a-gx		port and electrical port	Road, south of Fengxiang Street, High-tech Zone, Zhengzhou
Southwest China	Chongqing	ap-chongqing-a-th	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	No. 777, Taihe Road, High-tech Industrial Park, Shuitu Town, Beibei District, Chongqing (Chongqing Tencent Cloud Computing Data Center)
		ap-chongqing-b-yf	CTCC	Fiber optic port and electrical port	No. 15, Yunfu Road, Shuitu Town, Beibei District, Chongqing, China Unicom Southwest Data Center No. 7, Yunhan Avenue, Shuitu Town, Beibei District, Chongqing, Liangjiang Data Center (Pacific Telecom)
	Chengdu	ap-chengdu-a-xq	CTCC	Fiber optic port and electrical port	Room 301, 3rd Floor, No. 99, Tiansheng Road, West Hi-Tech Zone, Chengdu
		ap-chengdu-b-gh	CTCC, CMCC, and CUCC	Fiber optic port and electrical port	2nd Floor, No. 2007, Section 3, Guanghua Avenue, Wenjiang District, Chengdu, Sichuan Province
Special Administrative Region	Hong Kong (China)	ap-hongkong-a-kc	Local Service Provider	Fiber optic port and electrical port	Tencent (Equinix HK2) 16/F, Kerry Warehouse 3 Shing Yiu Street Kwai Chung, Hong Kong
		ap-hongkong-b-jja	Local Service	Fiber optic port and	Tencent,19 Wang Chun Street, Tseung

			Provider	electrical port	Kwun O, N.T, Hong Kong
		ap-hongkong-c-ct	Local Service Provider	Fiber optic port and electrical port	Tencent (PCCW) 15/F Sun Hung Kai Logistics Centre, No. 8 Wong Chuk Yeung Street, Fotan, NT, Hong Kong

Regions Outside China

Region		Access point	Supported port types	Address
Asia Pacific	Singapore	ap-singapore-a-ayer-rajah	Fiber optic port and electrical port	Tencent (Equinix SG3 Level-5 Hall-3) 26A Ayer Rajah Crescent, Singapore Post Code 139963
		ap-singapore-b-tai-seng	Fiber optic port and electrical port	15A Tai Seng Drive, Singapore 535 225
		ap-singapore-c-tagore	Fiber optic port and electrical port	71 Tagore Lane Singapore 787496
		ap-singapore-d-loyang	Fiber optic port and electrical port	11 Loyang Close Singapore 506756
	Japan	ap-tokyo-b-ariake	Fiber optic port and electrical port	1-2-41, Ariake, Koutou-ku, Tokyo, Japan, 135 0063
		ap-tokyo-c-Chiba	Fiber optic port	Tencent C/O Colt,Inzai Bldg, 2-3 Otsuka, Inzai, Chiba,Zip Code 270-1352
	South Korea	ap-seoul-a-yangcheon-gu	Fiber optic port and electrical port	Tencent c/o KT Mokdong 2 IDC, 323 Mokdongdong-ro, Yangcheon-gu, Seoul, South Korea.
	Thailand	ap-thailand-a-banmai	Fiber optic port and electrical port	Tencent (TRUE) 47/553-554 Moo 3,8th fl., New Geneva Industry Condominium, Popular

				3 Rd, Bannmai, Pakkrad,Nonthaburi 11120, Thailand
		ap-thailand-b-huamak	Fiber optic port and electrical port	1 Ramkamhaeng Rd, Soi Ramkhamheng 28, Huamak, Bangkok 10240
	Indonesia	ap-indonesia-c-cibitung	Fiber optic port and electrical port	Jl. Sumba Blok A-B Kav. B12-1 Kawasan Industri MM2100, Mekarwangi, Cikarang Barat – Bekasi, Jawa Barat 17530
		ap-jakarta-a-gambir	Fiber optic port and electrical port	Jl. Medan Merdeka Barat No.21, RT.2/RW.3, Gambir, Kecamatan Gambir, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10110, Indonesia
Europe	German	ap-frankfurt-b-hanauer	Fiber optic port and electrical port	Aceville(Tencent) c/o Interxion Delivery ,Hanauer Landstrasse 322D - 60314 Frankfurt am Main Germany
		ap-frankfurt-b-moerfelden	Fiber optic port and electrical port	Starkenburgstraße 12, 64546 Mörfelden, Germany
Middle East	India	ap-mumbai-b-saki-vihar	Fiber optic port and electrical port	Light Hall, ‘D’-Wing, Hiranandani Business Park, Saki Vihar Road, Saki Vihar, Mumbai-400072
		ap-mumbai-a-mahape	Fiber optic port and electrical port	GloryBird C/O CtrlS Mumbai PLOT NO-EL-72/1, P.N.WRITER COMPOUND, MAHAPE, MIDC, NEAR-NELOKO BUS STOP, Navi Mumbai - 400701, Maharashtra, India
America	United States	ap-siliconvalley-a-sanjose	Fiber optic port and electrical port	7 Great Oaks Blvd, San Jose, CA 95119
		ap-siliconvalley-b-santaclara	Fiber optic port and electrical port	3105 Alfred, St. Santa Clara, CA 95054
		ap-virginia-a-ashburn	Fiber optic port and electrical port	44790 Performance Circle, Ashburn, VA 20147, USA.
		ap-virginia-b-stirling	Fiber optic port and electrical	21350 Pacific Boulevard, Sterling, VA 20166

			port	
	Brazil	ap-saopaulo-a-Santana-de-Parnaiba	Fiber optic port and electrical port	Estrada dos Romeiros, 943 – Km 39,2, Santana de Parnaíba，São Paulo，Brazil, 06513-001

Relevant Products

Last updated：2024-01-13 16:02:36

For information on relevant products, please see the table below:

Product Name	Relationship to Direct Connect
Virtual Private Cloud (VPC)	A connection can be established with a VPC to enable communication between VPC and your own IDC over a private network
Cloud Connect Network (CCN)	CCN can be used to connect with multiple VPCs through one single dedicated tunnel
Network ACL	Multiple local IP translation rules can be created and configured with separate network ACLs
Route table	Route tables associated with subnets need to be configured for hybrid cloud deployment

Network Planning

Last updated：2024-01-13 16:09:03

Read this document to learn about the connection planning before building a network architecture for Direct Connect.

Background

A connection planning improves the stability and high availability of the network architecture for Direct Connect, and minimizes the impact from failures including device, port/fiber optic component, connection and data center at the access point. See the table below for the description and cause of failures.

Failure	Description	Cause
Connection	The connection communication fails or many packets are discarded.	The connection is damaged. For example, the cable is cut off.
Port/fiber optic component	The port/fiber optic component fails to be read or has an transfer exception due to hardware or software failures.	Hardware failure: incompatible version, contaminated or damaged port. Software failure: incorrect port status, port in UP status without receiving or sending packets, frequent port on/off, or cyclic redundancy check (CRC) error.
Network device	The exchange or router on the IDC side is unavailable.	Hardware failure: power supply, port, component or cable failures. Software failure: exchange/router error or incorrectly configured.
Data center at the access point	The data center encounters network disconnection, or the access point is unavailable.	The data center cannot function normally due to earthquakes, fires or other disasters.

Planning Ideas

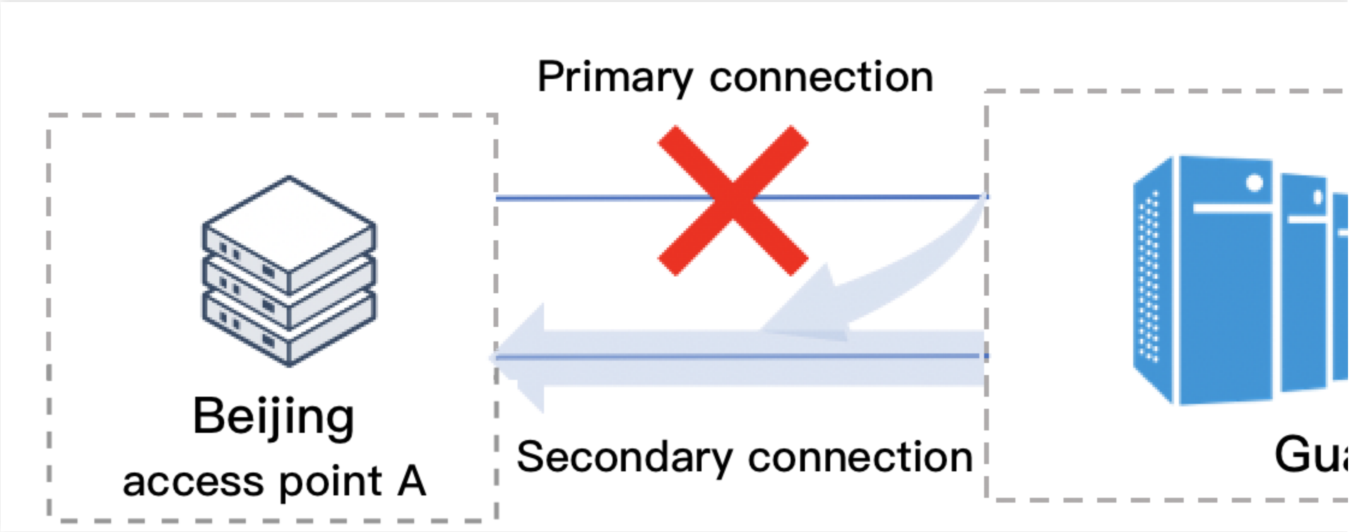
Capacity panning

The capacity planning is designed to meet business bandwidth requirements at a reasonable cost and guarantee the business operation in the event of a connection failure. To achieve this, you can:

Apply for connections twice your actual needs.

Maintain the connection utilization (current peak bandwidth/connection bandwidth * 100%) 50% or less.

Assume your business needs 3 Mpbs of bandwidth, you can apply for two connections with 5 Mpbs of bandwidth to each Tencent Cloud access point, each connection will be used about 30%. If one connection faults, the business traffic will quickly switch to the standby connection to ensure the business continuity. After the switchover, the standby connection will be used about 60%. In this way, only the connection load temporarily increases, and the business data is unaffected.



Expansion planning

The expansion planning is designed to meet the surging business demand at a reasonable cost. Depending on the expansion cycle, you need to plan differently as follows:

If you need an urgent expansion, you can apply for a connection based on the estimated business bandwidth, so that you can adjust the bandwidth limit to maintain your business when the traffic surges.

If you don’t need an expansion in the near future, you can apply for a new connection based on your actual expansion needs. The expansion will take 2-3 months.

Note:

A single expansion exceeding 100 Gbps of bandwidth requires a longer period. Please develop an expansion plan in advance for high-bandwidth businesses.

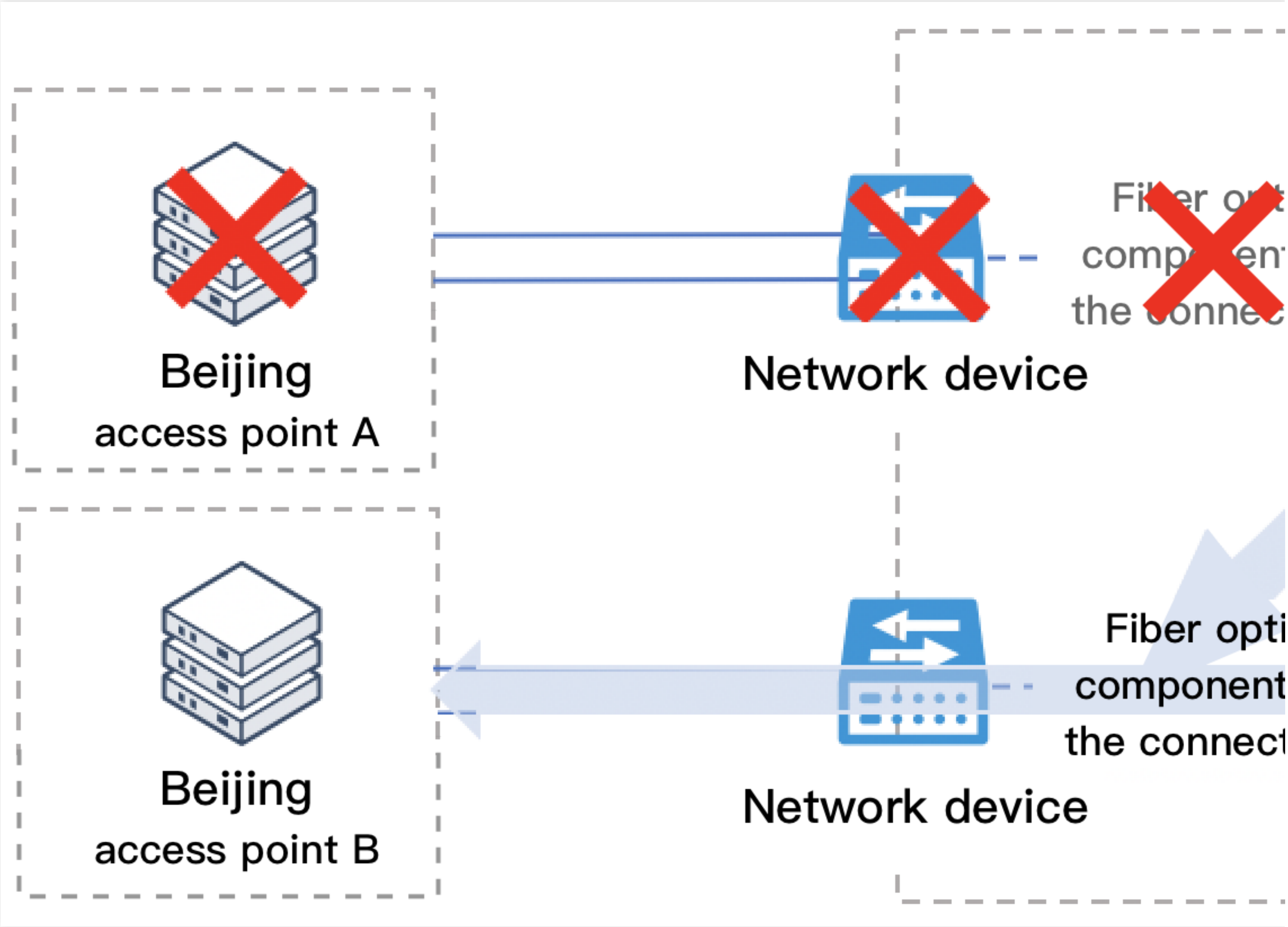
Disaster recovery planning

The disaster recovery is designed to improve the high availability of a network architecture and minimize the failure (including port/fiber optic component, network device, and data center at the access point) impact on business operations.

To avoid single points of failures, we recommend that you develop a disaster recovery plan for access points, physical lines, and hardware devices.

Access point: the local IDC uses connections of different physical lines to two intra-region Tencent Cloud access points.

Physical line: different physical lines provided by carriers are used to connect to a Tencent Cloud access point.
Hardware devices: both network devices and fiber optic components have redundant backups.
Assume you connect your local IDC to two intra-region Tencent Cloud access points according to [capacity planning (#capacity) requirements, as shown in the figure below. If the connection to access point A is disconnected due to port/fiber optic component, network devices or data center failures, the business traffic will quickly switch to the connection to access point B, without losing business data or interrupting businesses.



Sample Architectures

Tencent Cloud provides the following four network architectures for Direct Connect to facilitate your network planning.

Architecture	Use Case	Business Elasticity	Availability	Cost
Four connections to two access points (recommended)	Suitable for use cases that require excellent business availability and elasticity, including the key production and real-time data transaction.	Highest	Highest	Highest
Two connections to	Suitable for key business that requires	Medium	Higher	Medium

two access points (recommended)	high availability and elasticity.			
Two connections to one access point	Suitable for non-critical business, including the cloud development and testing environments.	Medium	Medium	Medium
Connection to one access point	Suitable for non-critical business that does not require high elasticity and availability.	Low	Low	Low

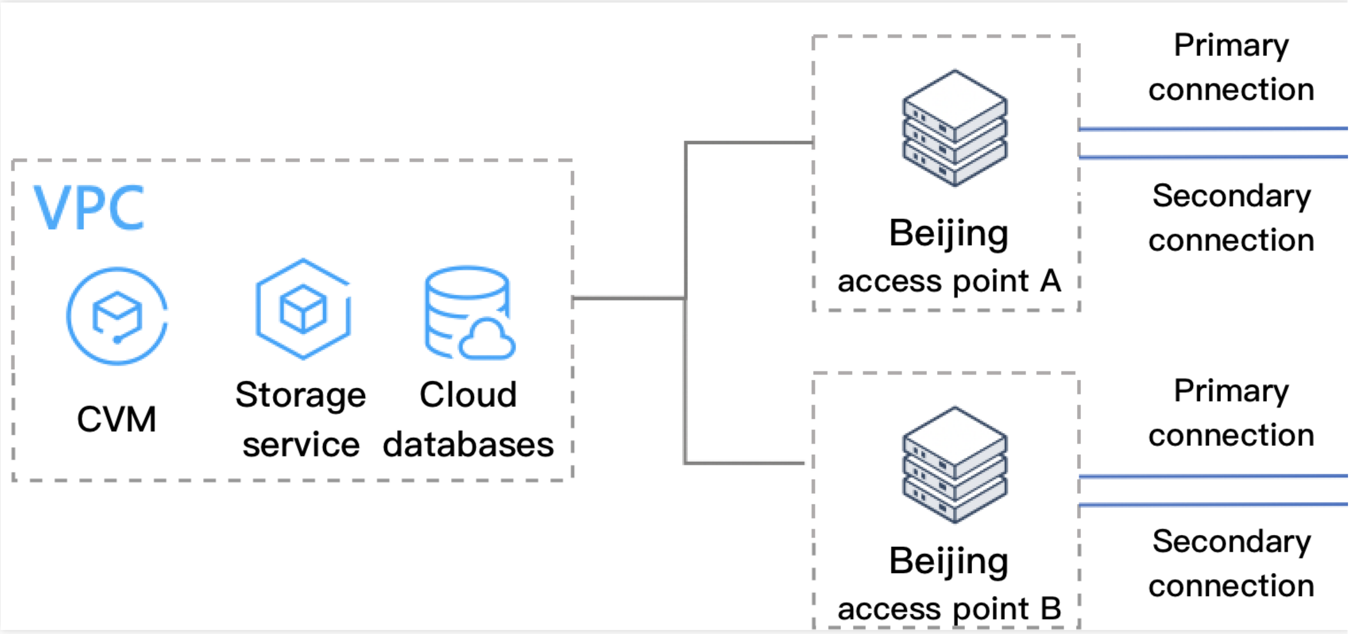
Four Connections to Two Access Points (Recommended)

Overview

Description: this architecture connects your IDC to two intra-region Tencent Cloud access points using primary and secondary connections respectively, and then accesses Tencent Cloud VPCs.

Use cases: suitable for use cases that require excellent business availability and elasticity, including the key production and real-time data transaction.

Cost: high.



Disaster recovery

The following table describes the impact of this network architecture on business under various failures when the planning ideas are met.

Failure	Business Impact
Connection	The connections loads increase, and the business continues.

Port/fiber optic component	The connections loads increase, and the business continues.
Network device	The connections loads increase, and the business continues.
Data center at the access point	The connections loads increase, and the business continues.

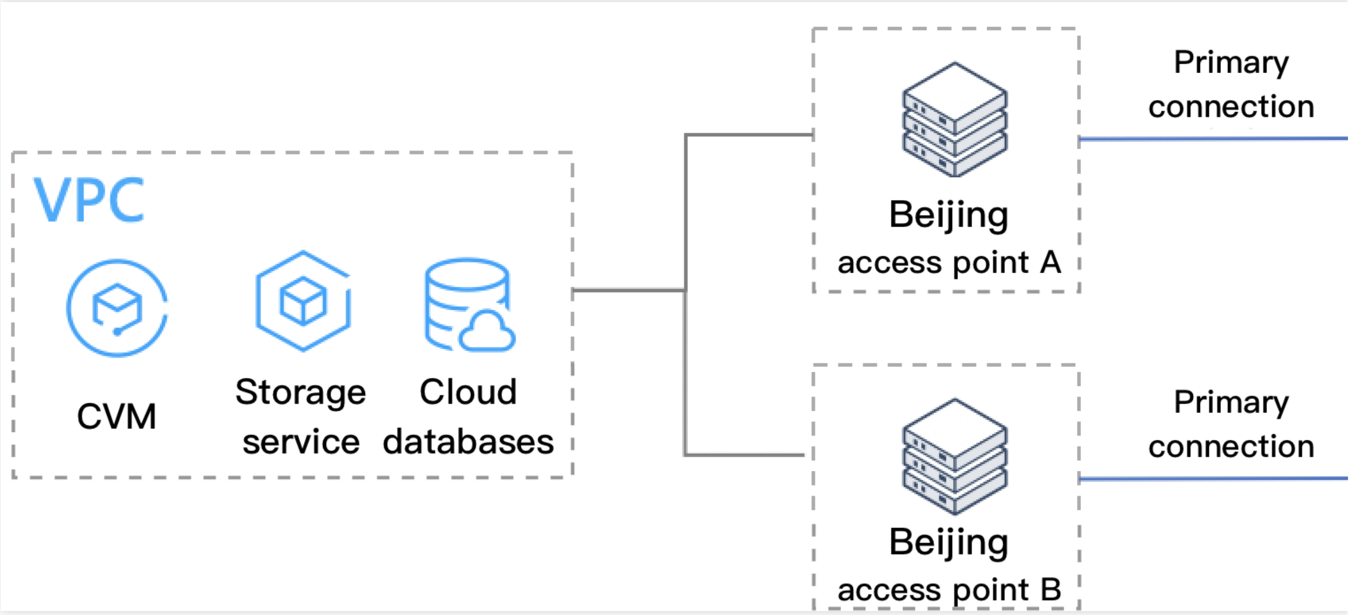
Two Connections to Two Access Points (Recommended)

Overview

Description: this architecture connects your IDC to two intra-region Tencent Cloud access points using one connection respectively, and then accesses Tencent Cloud VPCs.

Use cases: suitable for key business that requires high availability and elasticity.

Cost: medium.



Disaster recovery

The following table describes the impact of this network architecture on businesses under various failures.

Failure	Business Impact	Recovery Measures
Connection	If each connection is used 50% or less, the connection loads burst and the business continues. If each connection is used greater than 50%, the connection will be full-loaded, some data will be lost, and the business continues.	If the business data is lost, you need to apply for a new connection and spend 2-3 months to restore the business.
Network device	If each connection is used 50% or less, the connection loads burst and the business continues.	If business data is lost, you need to check and repair the network

	If each connection is used greater than 50%, the connection will be full-loaded, some data will be lost, and the business continues.	devices. The recovery time depends on the specific failure.
Port/fiber optic component	If each connection is used 50% or less, the connection loads burst and the business continues. If each connection is used greater than 50%, the connection will be full-loaded, some data will be lost, and the business continues.	If business data is lost, you need to check and repair the ports or fiber optic components. The recovery time depends on the specific failure.
Data center at the access point	If each connection is used 50% or less, the connection loads burst and the business continues. If each connection is used greater than 50%, the connection will be full-loaded, some data will be lost, and the business continues.	If business data is lost, you can: Contact the data center carrier to repair the failure. The recovery time depends on the specific failure. Reapply connections to other access points. The recovery takes about 2-3 months.

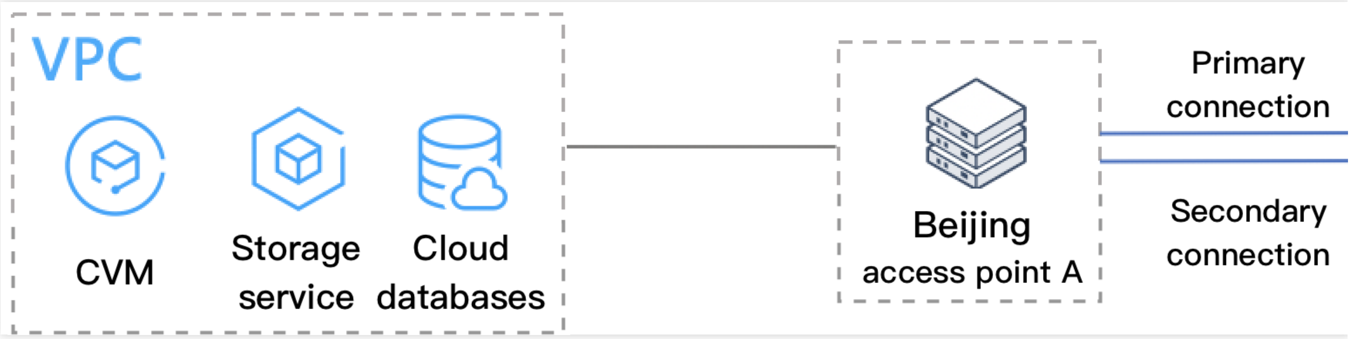
Two Connections to One Access Point

Overview

Description: this architecture connects your IDC to one Tencent Cloud access point using two connections, and then accesses Tencent Cloud VPCs.

Use cases: suitable for non-critical business, such as cloud development and testing environments.

Cost: medium.



Disaster recovery

The following table describes the impact of this network architecture on businesses under various failures.

Failure	Business Impact	Recovery Measures
Connection	If each connection is used 50% or less, the connection loads burst and the business continues.	If the business data is lost, you need to apply for a new connection and spend 2-3 months to restore the business.

	If each connection is used greater than 50%, the connection will be full-loaded, some data will be lost, and the business continues.	
Network device	The business will be interrupted.	You need to troubleshoot and repair the faulty network devices. The recovery time depends on the specific failure.
Port/fiber optic module	The business will be interrupted.	You need to troubleshoot and repair the faulty local ports or fiber optic components. The recovery time depends on the specific failure.
Data center at the access point	The business will be interrupted.	Contact the data center carrier to fix the failure. The recovery time depends on the specific failure.Reapply connections to other access points. The recovery takes about 2-3 months.

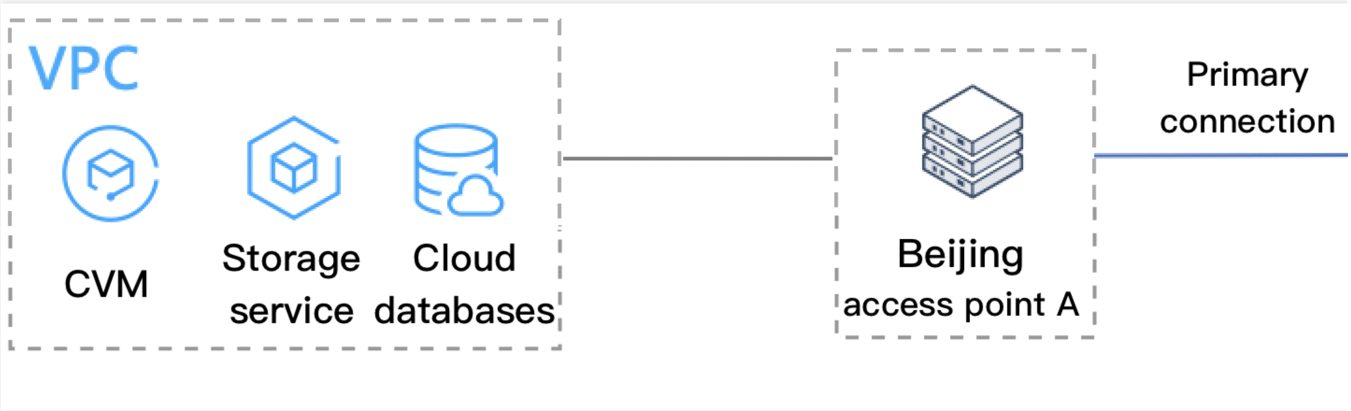
A Connection to One Access Point

Overview

Description: this architecture connects your IDC to one Tencent Cloud access point using a connection, and then accesses Tencent Cloud VPCs.

Use cases: suitable for non-critical business that does not require high elasticity and availability.

Cost: medium.



Disaster recovery

The following table describes the impact of this network architecture on businesses under various failures.

Failure	Business Impact	Recovery Measures
Connection	The business will be interrupted.	Reapply for a connection. The recovery takes about 2-3 months.

Network device	The business will be interrupted.	You need to troubleshoot and repair the faulty network devices. The recovery time depends on the specific failure.
Port/fiber optic module	The business will be interrupted.	You need to troubleshoot and repair the faulty local ports or fiber optic components. The recovery time depends on the specific failure.
Data center at the access point	The business will be interrupted.	Contact the data center ISP to fix the failure. The recovery time depends on the specific failure. Reapply connections to other access points. The recovery takes about 2-3 months.