

# **Cloud Load Balancer**

## **CLB Instances**

### **Product Documentation**



## Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

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

## Trademark Notice



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

## Service Statement

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

# Contents

## CLB Instances

- Creating IPv6 CLB Instance

- Creating IPv6 NAT64 CLB Instances

- Creating an Anycast Instance

- Creating CLB Instances

- Deleting CLB Instances

- Configuring CLB Security Group

# CLB Instances

## Creating IPv6 CLB Instance

Last updated : 2020-11-05 14:19:26

### Note :

- IPv6 CLB is currently in beta test. If you want to use it, please [submit a ticket](#) for application.
- Currently, IPv6 CLB instances can be created in Beijing, Shanghai, Guangzhou, Nanjing, Chengdu, Singapore, and Virginia regions.
- IPv6 CLB does not support classic CLB.
- IPv6 CLB supports obtaining the client's IPv6 source address, which can be directly obtained by layer-4 IPv6 CLB or through the `X-Forwarded-For` header of HTTP layer-7 IPv6 CLB.
- Currently, IPv6 CLB is completely implemented on the public network, so clients in the same VPC cannot access IPv6 CLB over the private network.
- IPv6 implementations are still at the primary stage across the internet. In case of access failure, please [submit a ticket](#). SLA is not guaranteed during the beta test period.

## Overview

IPv6 CLB is load balancing implemented based on the IPv6 single stack technology. It can collaborate with IPv4 CLB to implement IPv6/IPv4 dual-stack communication. An IPv6 CLB instance is bound to an IPv6 address of a CVM instance and provides an IPv6 VIP address.

### IPv6 CLB advantages

IPv6 CLB has the following advantages when helping your business quickly connect to IPv6:

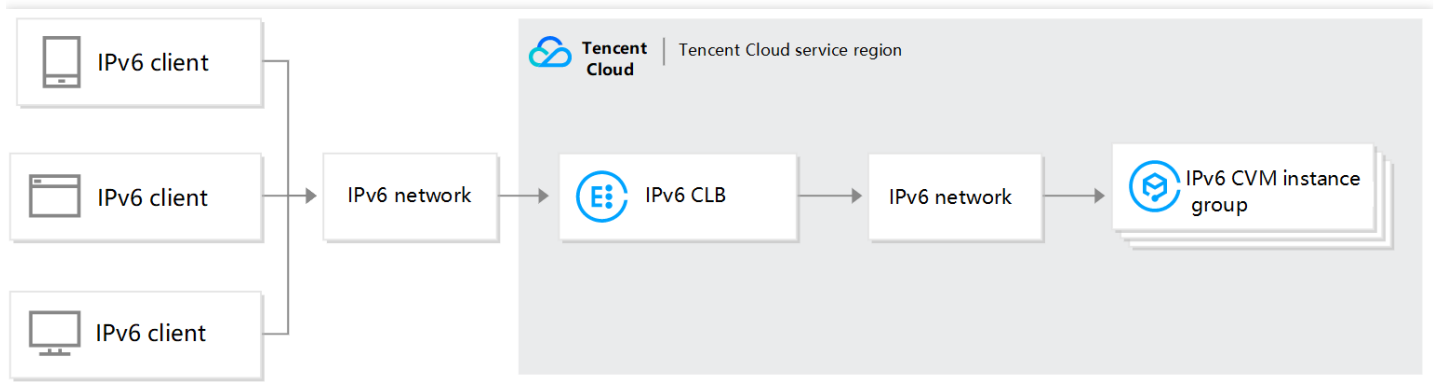
- Quick connection: CLB enables connection to IPv6 in a matter of seconds and is available upon purchase.
- Ease of use: IPv6 CLB is compatible with IPv4 CLB operation process and easy to use with no additional learning costs incurred.
- End-to-end IPv6 communication: IPv6 CLB communicates with CVM instances over IPv6, which helps applications deployed on the CVM instances quickly upgrade to IPv6 and implement end-to-end IPv6 communication.

### IPv6 CLB architecture

CLB supports creating IPv6 CLB instances. Tencent Cloud will assign an IPv6 public IP address, i.e., VIP of the IPv6 edition, to an IPv6 CLB instance, and the VIP will forward requests from IPv6 clients to the real IPv6 CVM instance.

An IPv6 CLB instance can support IPv6 public network user's quick access and communicate with real servers over IPv6, which helps in-cloud applications quickly upgrade to IPv6 and implement end-to-end IPv6 communication.

The IPv6 CLB architecture is as shown below.



## Operation Guide

### Step 1. Create an IPv6 CLB instance

1. Log in to the Tencent Cloud's official website and enter the [CLB purchase page](#).
2. Select options for the following parameters correctly:
  - Billing Mode: only pay-as-you-go billing is supported.
  - Region: Beijing, Shanghai, Guangzhou or Singapore.
  - IP Version: IPv6.
  - ISP Type: BGP.
  - Network: please select a VPC and subnet that have already obtained IPv6 CIDR.
3. After setting the configuration items on the purchase page, click **Buy Now** to return to the [CLB instance list page](#), where you can view the IPv6 CLB instance you just purchased.

Billing Mode Pay per usage [Pricing Sample](#)

Region Guangzhou Qingyuan Shanghai Nanjing Beijing Chengdu Chongqing Hong Kong, China

Singapore Bangkok Mumbai Seoul Tokyo Silicon Valley Virginia Toronto



Frankfurt Moscow

Tencent Cloud products in different regions can not communicate with each other

Availability Zone Availability Zone cannot be selected for IPv6

Network type Public network Private network

IP Version IPv4 IPv6 NAT64 IPv6

Network vpc- subnet- ? ↺

If you want to change the network, please go to the Console to [Create a VPC](#) or [Create a Subnet](#)

Project DEFAULT PROJECT

Tag


Tag Key	Tag Value	Operat...
<span>Please select a tag key</span>	<span>Please select a tag value</span>	<span>Delete</span>

[Add](#)

If there is no desired tag key or value, you can go to the console to [Create](#)

Instance name Automatic generation is performed if it is left empty 60 more chars allowed. chars; allowing letters, digits, Chinese characters, "-", ".", and "\_".

Cost:

Instance Fee	Network Fee
 USD/hour	The network fee will be charged on CVM instances

Buy Now

## Step 2. Create an IPv6 CLB listener

1. Log in to the [CLB Console](#) and click the IPv6 CLB instance ID to enter the details page.
2. Select the **Listener Management** tab and click **Create** to create a listener, e.g., a TCP listener.

### Note :

CLB supports creating layer-4 (TCP/UDP/TCP SSL) and layer-7 (HTTP/HTTPS) IPv6 CLB listeners. For more information, please see [CLB Listener Overview](#).

3. In "Basic Configurations", configure the name, listening protocol ports, and balancing method, and click **Next**.

**CreateListener** ×

1 **Basic Configuration** >

2 Health Check >

3 Session Persistence

Name

ipv6-ssh

Listen Protocol Ports

TCP

:

22

Balance Method

Weighted Round Robin

If you set a same weighted value for all CVMs, requests will be distributed by a simple pooling policy.

Close

Next

4. Configure health check and click **Next**.

**CreateListener** ×

✓

 Basic Configuration >

2 **Health Check** >

3 Session Persistence

Health Check ⓘ

☒

Show advanced options ▼

Back

Next

5. Configure session persistence and click **Submit**.

## CreateListener

✓ Basic Configuration >

✓ Health Check >

**3 Session Persistence**

---

Session Persistence ⓘ☒

Hold Time ⓘ

III

-

54

+

Seconds

30 Seconds3600 Seconds

Session persistence based on the source IP

Back

Submit

6. After the listener is created, select it and click **Bind** on the right.

**Note :**

Before binding the listener to a CVM instance, please check whether the instance has obtained an IPv6 address.

TCP/UDP/TCP SSL Listener

Create

ipv6-ssh(TCP:22)

Listener Details [Expand](#)




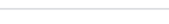
Bound Real Server

Bind

Modify Port

Modify Weight

Unbind

<input type="checkbox"/>	CVM ID/Name	Port Health Status	IP Address	Port	Weight	Oper...
<input type="checkbox"/>		<div>s①</div> <div>Healthy</div>		22	10	<a href="#">Unbind</a>
<input type="checkbox"/>		<div></div> <div>Healthy</div>		22	10	<a href="#">Unbind</a>



7. In the pop-up box, select the real IPv6 CVM instance that needs to be communicated with, configure the service port and weight, and click **OK**.

**TCP/UDP/TCP SSL Listener**






Create

ipv6-ssh(TCP:22)

**Listener Details** Expand ▾

**Bound Real Server**

Bind Modify Port Modify Weight Unbind

<input type="checkbox"/>	CVM ID/Name	Port Health Statu	IP Address	Port	Weight	Ope...
<input type="checkbox"/>		 Healthy		22	10	Unbind
<input type="checkbox"/>		Healthy		22	10	Unbind

# Creating IPv6 NAT64 CLB Instances

Last updated : 2020-06-28 15:18:05

- IPv6 NAT64 CLB can only be created in three regions: Beijing, Shanghai, and Guangzhou.
- IPv6 NAT64 CLB does not support classic CLB.
- IPv6 NAT64 CLB does not support getting client IPs.
- IPv6 implementations are still at the primary stage across the internet, and SLA is not guaranteed. In case of access failure, please [submit a ticket](#) for assistance.

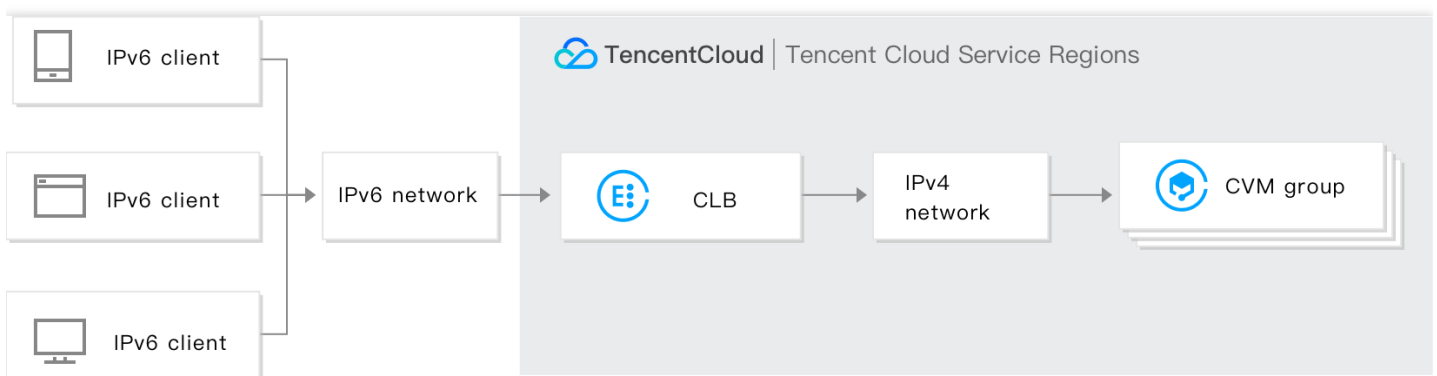
CLB supports creating IPv6 NAT64 CLB instances. Tencent Cloud will assign an IPv6 public IP address, i.e., VIP of the IPv6 edition, to an instance, and the VIP will forward requests from IPv6 clients to the real IPv4 CVM instance.

## IPv6 NAT64 CLB Instance Overview

An IPv6 NAT64 CLB instance is a load balancer implemented based on the IPv6 NAT64 transition technology. Through an IPv6 NAT64 CLB instance, real servers can be quickly accessed by IPv6 users without any IPv6 modification required.

## IPv6 NAT64 CLB Architecture

The IPv6 NAT64 CLB architecture is as shown below.



When IPv6 NAT64 CLB is accessed from an IPv6 network, CLB can smoothly convert IPv6 addresses to IPv4 addresses to adapt to existing services and quickly implement IPv6 transformation.

## IPv6 NAT64 CLB Advantages

Tencent Cloud IPv6 NAT64 CLB has the following advantages when helping your business quickly connect to IPv6:

- **Quick connection:** CLB enables connection to IPv6 in a matter of seconds and is available upon purchase.
- **Smooth business transition:** in order to smoothly transit your business to IPv6, you only need to transform the client with no modifications required for real servers. IPv6 NAT64 CLB supports access from IPv6 clients and converts IPv6 messages into IPv4 messages. IPv6 transition is imperceptible to applications on real servers, which still work in their original way.
- **Ease of use:** IPv6 NAT64 CLB is compatible with IPv4 CLB operation process and easy to use with no additional learning costs incurred.

## Operation Guide

### Creating IPv6 NAT64 CLB instance

1. Log in at Tencent Cloud's official website and go to the [CLB purchase page](#).
2. Select options for the following parameters correctly:
  - Region: only Beijing, Shanghai, and Guangzhou are supported.
  - Instance Type: CLB.
  - Network Type: public network.
  - IP version: IPv6 NAT64.
  - Network: VPC.
  - Other configurations are the same as general instance configurations.
3. After setting the configuration items on the purchase page, click **Buy Now** to return to the [CLB instance list page](#), where you can view the IPv6 NAT64 CLB instance you just purchased.

Billing Mode

Pay per usage

Pricing Sample

Region

Guangzhou

Shanghai

Nanjing

Beijing

Chengdu

Chongqing

Taipei, China

Hong Kong, China

Singapore

Bangkok

Mumbai

Seoul

Tokyo

Silicon Valley

Virginia

Toronto

Frankfurt

Moscow

Tencent Cloud products in different regions can not communicate with each other

Instance type

Cloud Load Balancer (former "Application Load Balancer")

Recommended

Details

✓ Support HTTP(S)/TCP/UDP Protocol

✓ Support the forwarding based on domain name + URL

App Full coverage of classic CLB features named to "Cloud Load Balancer".

Classic Cloud Load Balancer

Details

HTTP(S) Protocol is not supported in private network

Do not support the forwarding based on domain name + URL

Network type

Public network

Private network

IP Version

IPv4

IPv6 NAT64

Network

vpc-k9gii1kb | Default-VPC (Default)

If you want to change the network, please go to the Console to [Create a VPC](#)

Project

DEFAULT PROJECT

Tag

Tag Key	Tag Value	Operation
Please select a tag key	Please select a tag value	Delete

Add

Cost:

Instance Fee

Network Fee

The network fee will be charged on CVM instances

Buy Now

## Using IPv6 NAT64 CLB

Log in to the [CLB Console](#) and click an instance ID to enter the details page. On the "Listener Management" tab, you can configure listeners and forwarding rules and bind CVM instances. For

more information, please see [Getting Started with CLB](#).

Instance Management

[Guangzhou\(8\)](#) Shanghai Nanjing Beijing Chengdu Chongqing Taipei, China Hong Kong, China Singapore Bangkok Mumbai Seoul Tokyo Silicon Valley Virginia Toronto Frankfurt Moscow

Cloud Load Balancer(7)

Classic Cloud Load Balancer(1)

CreateDeleteChange ProjectEdit Tags

Project: All ProjectsUse 'f' to split more than one keywords

ID/Name	Monito...	Status	VIP	Networ...	Network	Health Status	Project	Tag	Operation
		Normal	72 (IPv6 NAT64)	Public Network	6)	Health check not enabled (Configuration)	DEFAULT PROJECT	-	<a href="#">Configure listener</a> <a href="#">More</a>

# Creating an Anycast Instance

Last updated : 2020-08-25 17:58:08

CLB supports creating Anycast CLB instances. Anycast CLB is a load balancing service that supports cross-region dynamic acceleration. CLB VIP is published in multiple regions. The client connects to the nearest POP and forwards traffic to a CVM instance through the high-speed internet of Tencent Cloud IDC.

Anycast CLB can achieve network transfer optimization and multi-entry nearby access and reduce network jitter and packet loss, which can ultimately improve the service quality of in-cloud applications, expand the service scope, and streamline backend deployment.

This feature is currently in beta test. To apply for a trial, submit an application for beta test eligibility.

## What is Anycast?

Anycast means that when the same IP publishes a route in multiple locations simultaneously, the routing algorithm will deliver user traffic to the nearest router.

Advantages of Anycast CLB:

- **Low latency**

Anycast CLB publishes the VIP to multiple regions simultaneously by means of Anycast. According to transfer protocol, a request package will arrive at the optimal VIP publishing region to gain privileged access to Tencent Cloud and then get to the CVM instance through Tencent Cloud private network, avoiding public network congestion and reducing latency.

- **Reduced jitter and packet loss**

The transmission instability of cross-border or cross-carrier public networks can result in network jitter and packet loss, undermining the service experience. By contrast, Anycast CLB boasts high transmission stability. It gives client requests nearby access to Tencent Cloud and enables cross-region transmission via Tencent Cloud dedicated private network connection, helping eliminate jitter and packet loss.

- **High reliability**

Transmission over public networks can be unreliable. When ISP-specific line problems make services inaccessible, users generally have to wait until services are resumed. With the aid of Anycast CLB, Tencent Cloud private network, ISP networks, and Tencent Cloud POPs can achieve

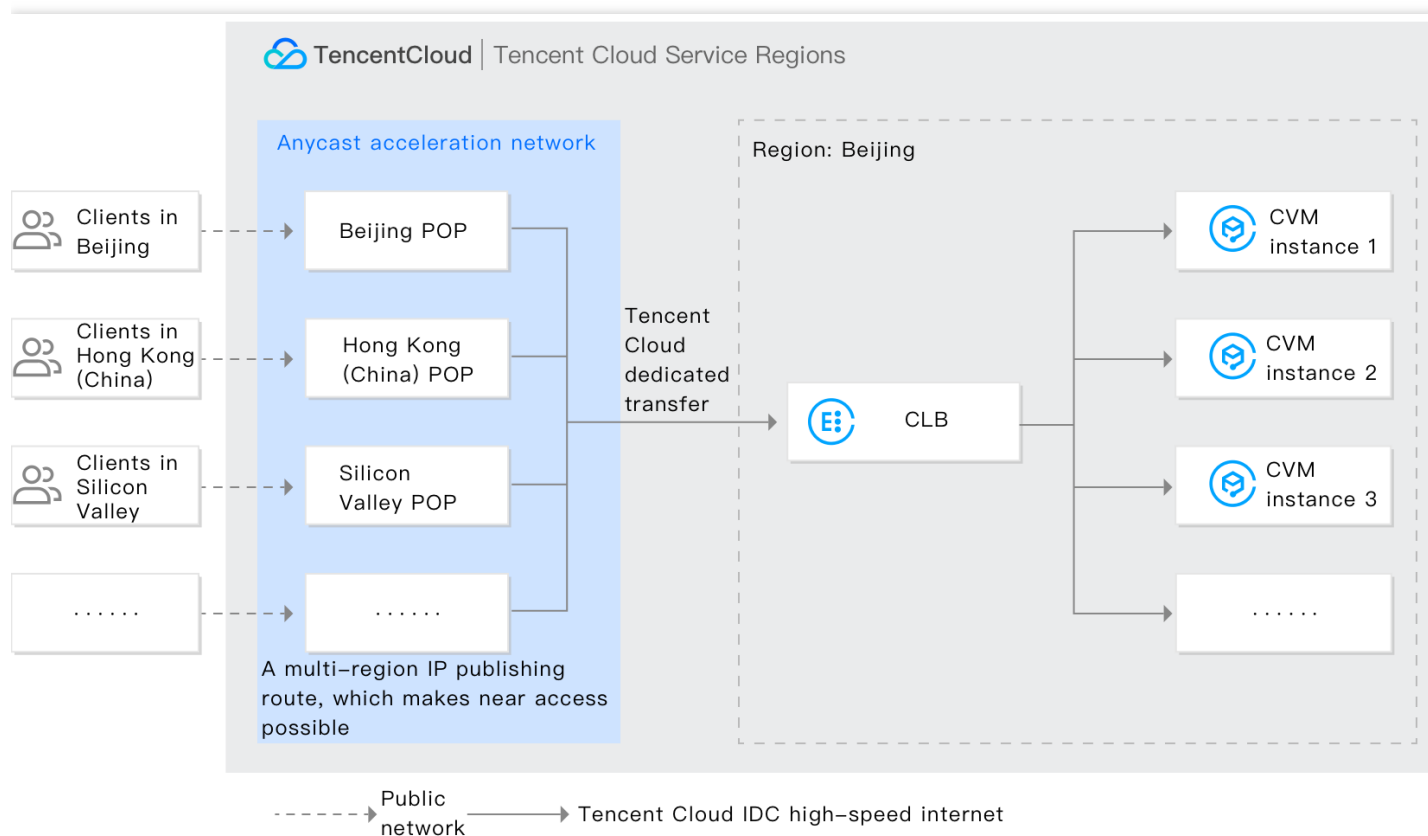
multiple network paths and entries to eliminate failures caused by single region or line and improve network stability.

- **Simplified deployment**

When your clients are distributed across regions and need nearby access, you have to deploy servers in all of those regions and configure DNS to achieve load balancing, and the IPs vary by region, making the deployment even more complicated. Through Anycast CLB, the region attribute is converged at the IP level, eliminating the need to configure IPs for every region. Moreover, you only need to maintain one set of business logic on the backend, and requests from different regions are directly routed to real servers through private network acceleration.

## Anycast CLB Architecture

The Anycast CLB architecture is as shown below:



The VIP of Anycast CLB is published to multiple regions around the world. The client connects to the nearest POP and forwards access traffic in an ultra-fast manner to a CVM instance over Tencent Cloud private network.

### Anycast publishing region

An Anycast publishing region is where an accelerated IP address is published, i.e., the POP where Anycast CLB VIP is published. The client accesses the nearest POP. Currently, Anycast CLB supports simultaneous publishing in the following regions: Beijing, Shanghai, Guangzhou, Hong Kong (China), Toronto, Silicon Valley, Frankfurt, Virginia, Moscow, Singapore, Seoul, Mumbai, Bangkok, and Tokyo.

## Anycast CLB region

Just like a region of generic CLB instances, an Anycast CLB region is the one you selected when purchasing an Anycast CLB instance or the region where your real server resides. Currently, Anycast CLB is available in most regions.

- China: Beijing, Shanghai, Guangzhou, and Hong Kong SAR.
- Europe and the North America: Toronto, Silicon Valley, Frankfurt, Virginia, and Moscow.
- Southeast Asia: Singapore, Seoul, Mumbai, Bangkok, and Tokyo.

- The anycast capability of Anycast CLB is implemented by binding an Anycast EIP to a private network CLB instance.
- Anycast EIP can be bound to private network CLB instances but not classic private network CLB instances.

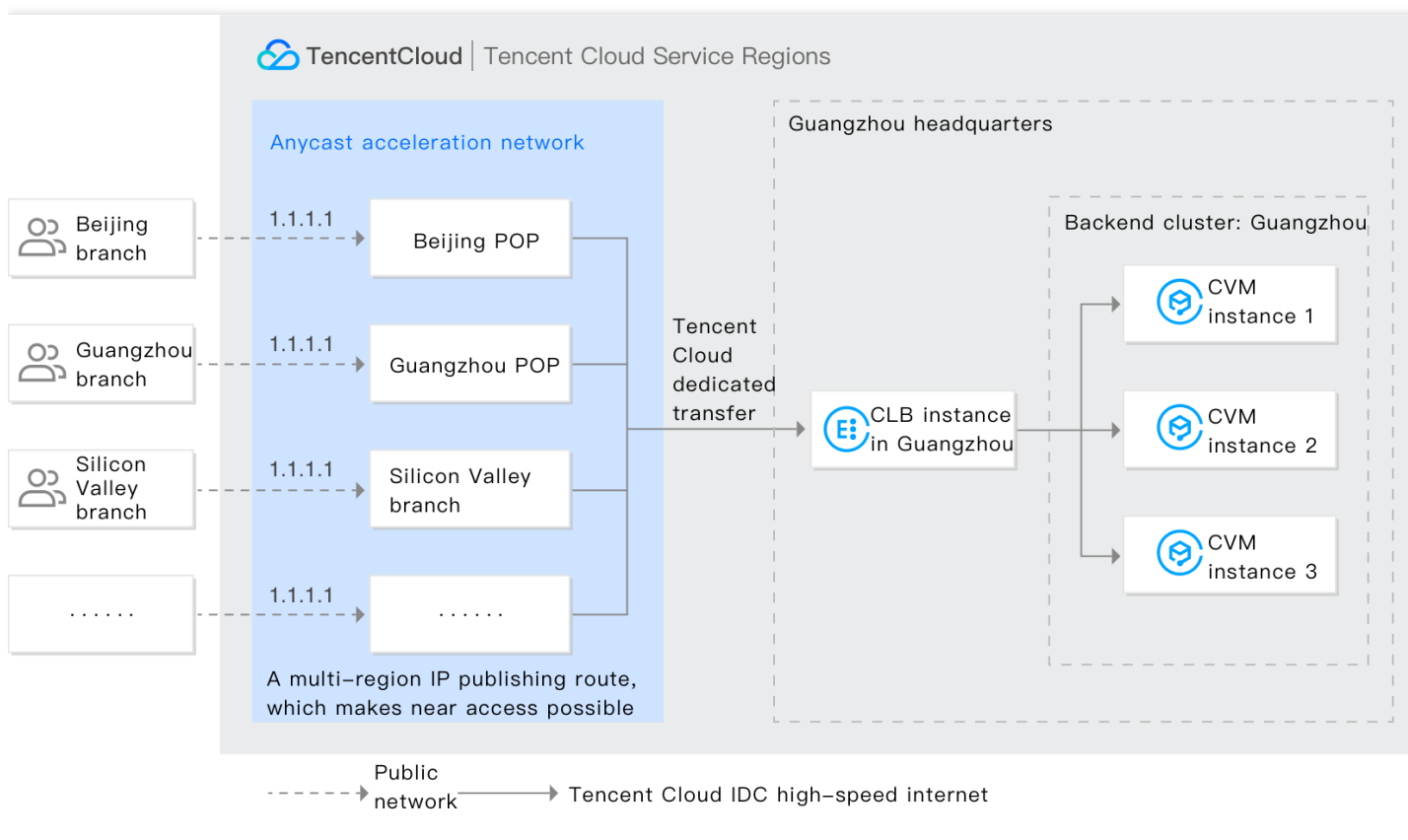
## Anycast CLB Use Cases

### Unified server for cross-region access

If you are in the gaming industry, you may hope that the players from different places are in the same server region or that your branches around the globe can share the same IDC. You can use Anycast CLB to deploy real servers in one region (such as Guangzhou), purchase an Anycast CLB instance in that region and select the publishing regions as needed. In this way, players or



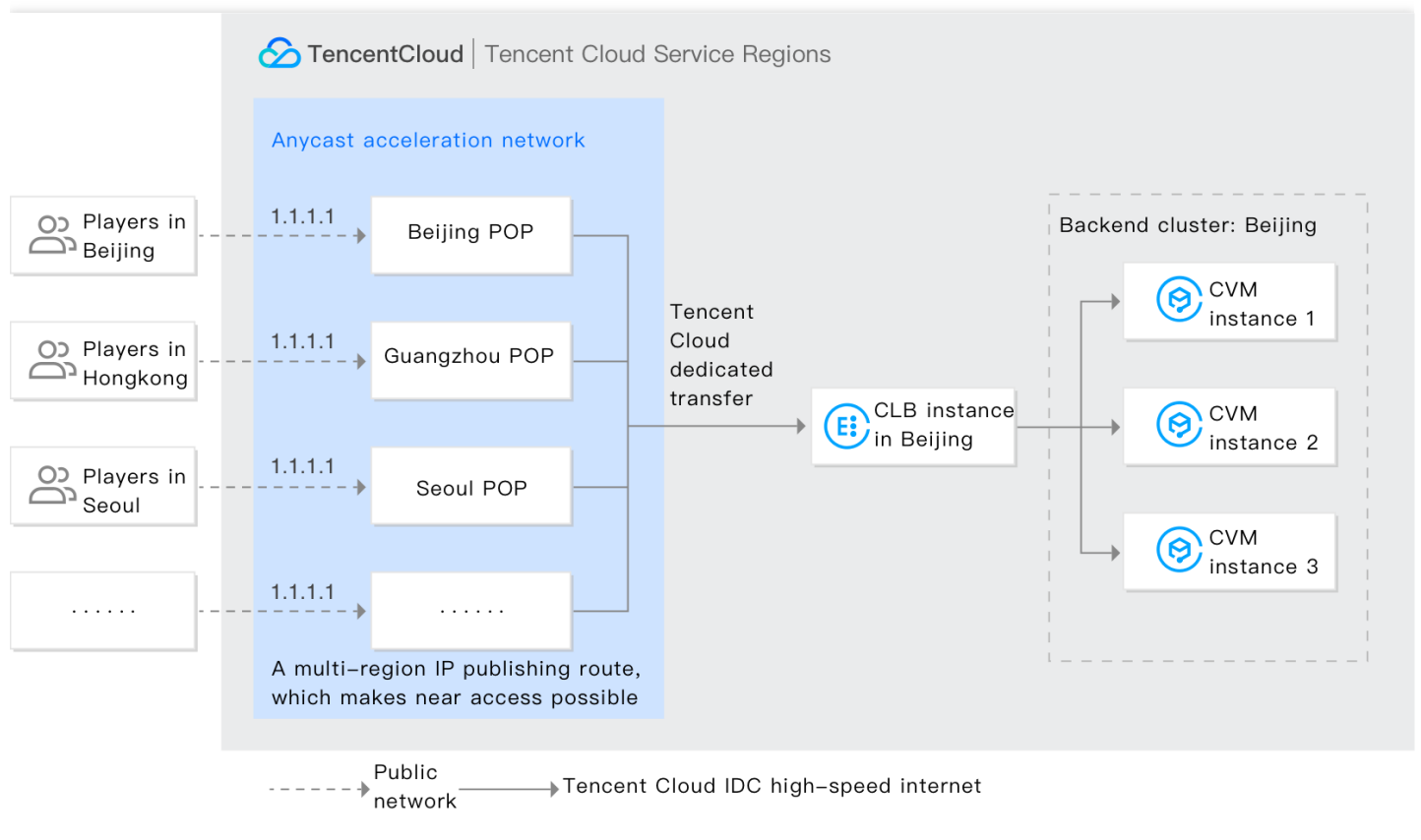
employees can obtain the nearby access to the same real servers.



## Gaming acceleration

Anycast CLB has been widely used in gaming acceleration. Through Anycast CLB, game requests can have nearby access to Tencent Cloud and get to game servers through Tencent Cloud private network, greatly shortening the public network path and reducing problems such as delay, jitter, and packet loss. Compared to the traditional acceleration, Anycast CLB requires no extra deployment of

traffic receivers at the entry and eliminates the need for zoning, thus simplifying DNS deployment.



## Operation Guide

### Prerequisites

This feature is currently in beta. Make sure that your application for beta test eligibility has been approved before using it.

### Directions

1. Log in to the [CVM Console](#).
2. On the left sidebar, click **EIP** to enter the EIP management page.

3. Click **Apply**. In the pop-up window, select **Accelerated IP** as the IP address type and click **OK**.

**Apply for EIP**

IP address type

☐ Normal IP  
Ordinary BGP IP, balancing network quality and costs

☒ Acceleration IP **Recommended**  
Adopts Anycast acceleration, providing stable, reliable the low-latency internet access

Region South China(Guangzhou)

Accelerated Region Global

Amount  1  4/20

Advanced ▼ Tag

Fee






(Preview price)  
Billed by the total bandwidth usage in all regions. An idle EIP will incur an idle fee of [blurred] No charges incur if it's bound with an instance.

**OK** Cancel

4. Log in to the [CLB Console](#), select a private network CLB instance (classic CLB instances are not supported), and click **More** > **Bind Accelerated IP** in the "Operation" column.

<input type="checkbox"/>	ID/Name ↕	Monitor...	Status	VIP	Network... ▼	Network	Health Status	Creation Time ↕	Operation
<input type="checkbox"/>	[blurred]	[blurred]	Normal	[blurred]	Private Network	[blurred]	Health check not enabled(Configuration)	2019-12-17 16:26:12	Configure listener <b>More</b> ▼
<input type="checkbox"/>	[blurred]	[blurred]	Normal	[blurred]	Public Network	[blurred]	Abnormal(Abnormal ports: 1)	2019-12-17 16:26:12	Bind Accelerated IP Edit Tags Delete

5. After the private network CLB instance is bound to an accelerated IP, it can provide Anycast CLB service. For more information on CLB configuration, please see [CLB Listener Overview](#).

<input type="checkbox"/>	ID/Name ↕	Monitor...	Status	VIP	Network... ▾	Network	Health Status	Creation Time ↕	Operation
<input type="checkbox"/>			Normal	<div>1  (Accelerated IP)</div> <div>1  (Private)</div>	Private Network		Health check not enabled (Configuration)	2019-12-17 16:26:12	<a href="#">Configure listener</a> <a href="#">More ▾</a>

# Creating CLB Instances

Last updated : 2020-07-16 16:06:30

Tencent Cloud allows you to create a CLB instance on the official purchase page or via API. The two methods are detailed below:

## Creating a CLB instance on the official purchase page

You can purchase a CLB instance on [Tencent Cloud official website](#). Private network CLB is free of charge, while public network CLB only charges instance fees on an hourly pay-as-you-go basis. You can purchase public network on [CVM](#). For more information on network billing modes, please see [Public Network Billing Mode](#).

You can purchase a CLB instance on the official website as follows:

1. Log into Tencent Cloud official website and go to [CLB purchase page](#).
2. Select "CLB" (recommended) as the instance type.
3. Select attributes as needed, such as network and project to which the instance belongs. For more information on attributes, please see [Product Attribute Selection](#).
4. Complete payment after confirming the purchase.
5. CLB service is enabled after the payment completes. You can now configure and use the CLB instance.

Billing Mode

Pay per usage

Pricing Sample

Region

Guangzhou

Shanghai

Nanjing

Beijing

Chengdu

Chongqing

Hong Kong, China

Singapore

Bangkok

Mumbai

Seoul

Tokyo

Silicon Valley

Virginia

Toronto

Frankfurt

Moscow

Tencent Cloud products in different regions can not communicate with each other

Instance type

Cloud Load Balancer (former "Application Load Balancer")

Recommended

Details

Support HTTP(S)/TCP/UDP Protocol

Support the forwarding based on domain name + URL

Full coverage of classic CLB features

Classic Cloud Load Balancer

Details

HTTP(S) Protocol is not supported in private network

Do not support the forwarding based on domain name + URL

"Application Load Balancer" has been renamed to "Cloud Load Balancer".

Network type

Public network

Private network

IP Version

IPv4

IPv6 NAT64

Network

?

↺

If you want to change the network, please go to the Console to [Create a VPC](#)

ISP

BGP

China CMCC

China CTCC

China CUCC

Project

DEFAULT PROJECT

▼

Instance name

Automatic generation is performed if it is left empty

50 more chars allowed. Allowing letters, numbers, '-', '\_', '.'

Quantity

-

1

+

Cost:

Buy Now

## Creating a CLB instance via API

If you want to purchase a CLB instance via API, you can create a CLB instance as instructed in [CLB API](#).

©2013-2019 Tencent Cloud. All rights reserved.

Page 22 of 33

# Deleting CLB Instances

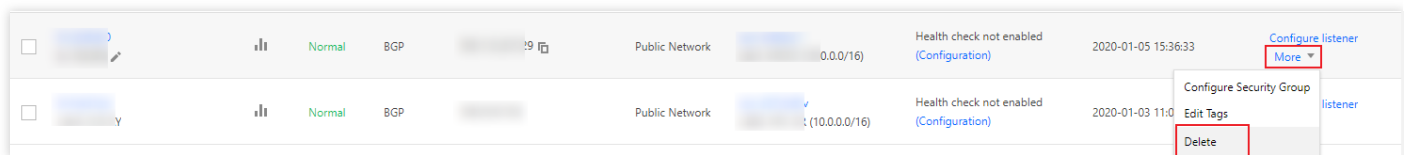
Last updated : 2020-07-16 16:06:48

After you confirm that a CLB instance has no traffic and is no longer needed, you can delete it via CLB Console or API.

Once deleted, the CLB instance will be completely terminated and cannot be recovered. We strongly recommend you unbind all real servers and wait for while before deleting any instance.

## Deleting CLB instance via the console

1. Log into the [CLB Console](#).
2. Find the CLB instance you want to delete and click **Delete** in the "Operation" column on the right.



3. The confirmation dialog box will pop up. After you read the operation security prompt, click **OK** to confirm the deletion.

The confirmation dialog box is as shown below. We strongly recommend you first confirm that the number of servers is **"0"**, CVM instance is **none**, and the security prompt is **green** before deleting

the instance.

**Confirm to delete the following load balancers?** ×

ID/Name	Bound rules	Bound CVM	Notes About Oper...
lb-2jrl6dv0 lb-162309	0	None	✓

Submit

Close

## Deleting CLB instance via API

For more information on detailed steps, please see [Deleting CLB Instances](#).



# Configuring CLB Security Group

Last updated : 2020-11-13 14:49:44

After a CLB instance is created, you can configure a CLB security group to isolate public network traffic. This document describes how to configure CLB security groups in different modes.

## Use Limits

- One CLB instance can be bound to five security groups at most.
- There can be 0-65535 security group rules.
- Security groups cannot be bound to classic private network CLB instances and private network CLB instances in the classic network. If a private network CLB instance is bound to an [Anycast EIP](#), security groups bound to the instance will not take effect.
- The "Allow Traffic by Default in Security Group" feature is currently in beta test. To try it out, please submit a ticket for application. This feature is not supported for classic private network CLB and CLB in the classic network.

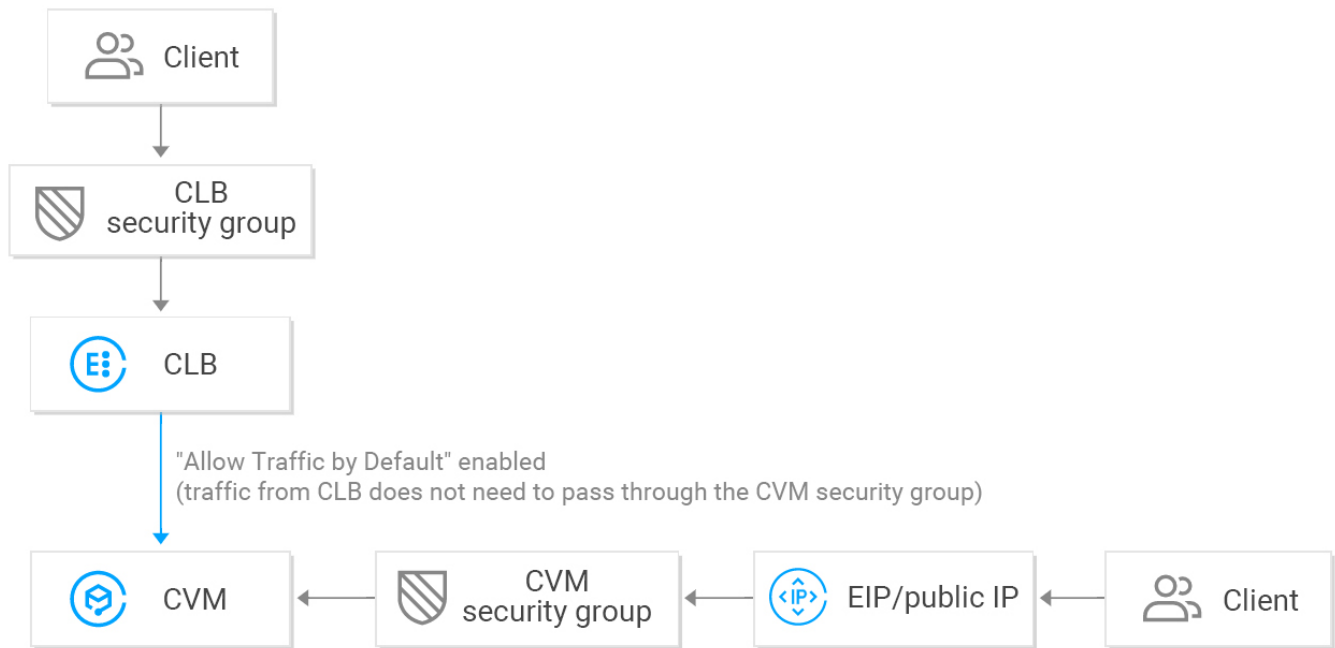
## Background

A security group is a virtual firewall that can filter stateful data packets and control outbound and inbound traffic at the instance level. For more information, please see [Security Group Overview](#).

A CLB security group is bound to a CLB instance, while a CVM security group is bound to a CVM instance. They target at different objects. CLB security groups can be generally configured in the following two modes:

- [Enable "Allow Traffic by Default in Security Group"](#)
- [Disable "Allow Traffic by Default in Security Group"](#)

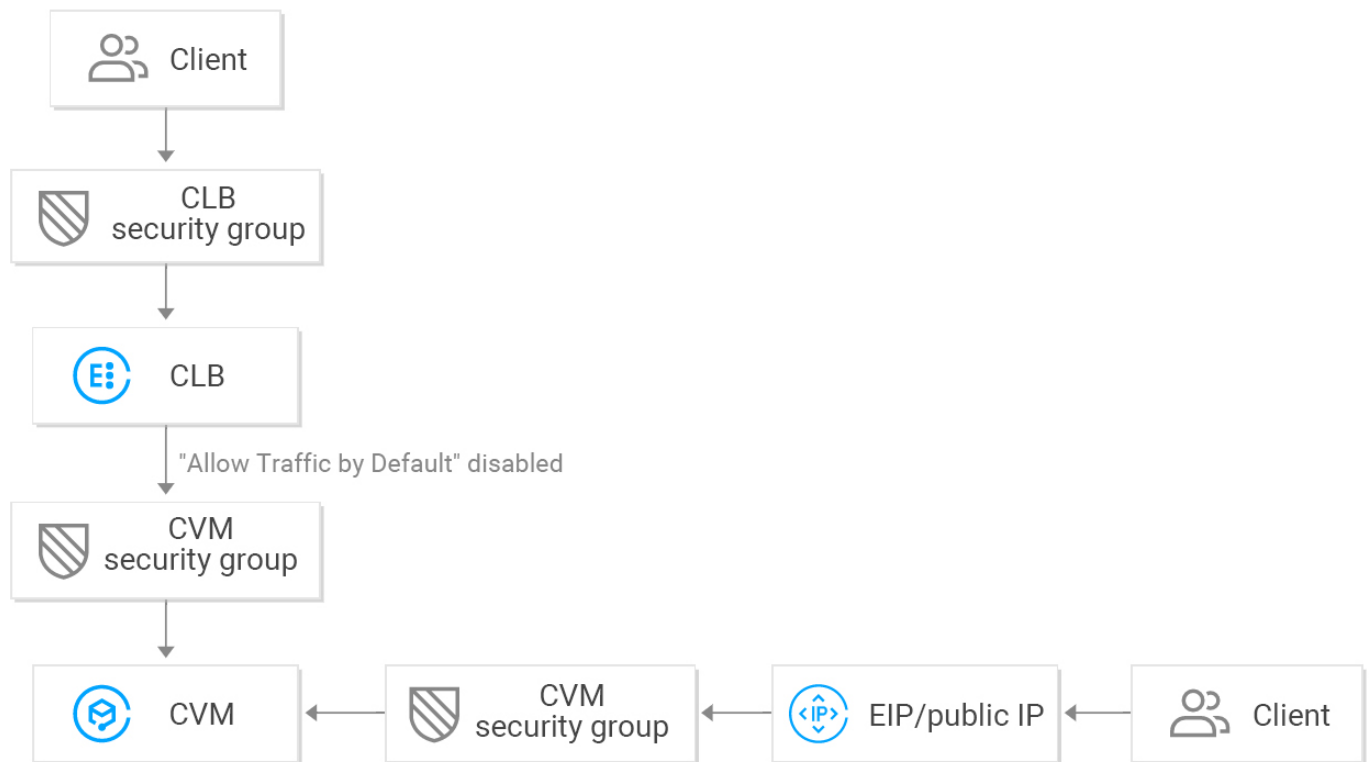
### Enabling "Allow Traffic by Default in Security Group"



After "Allow Traffic by Default in Security Group" is enabled:

- If you want to allow access only from a specified client IP, you **need to open** the client IP and listening port to the internet in the CLB security group, but you **don't need to open** the client IP and service port in the backend CVM security group. Access traffic from CLB only needs to pass through the CLB security group, as the real server allows traffic from CLB by default and doesn't need to open the port.
- Traffic from public IPs (including general public IPs and EIPs) still needs to pass through the CVM security group.
- If a CLB instance has no security group configured, all traffic will be allowed, and only ports configured with listeners on the VIP of the CLB instance can be accessed; therefore, the listening port will allow traffic from all IPs.
- To reject traffic from a specified client IP, you must do so in the CLB security group, as doing so in the CVM security group takes effect only for traffic from public IPs (including general public IPs and EIPs) but **not** for traffic from CLB.

## Disabling "Allow Traffic by Default in Security Group"



After "Allow Traffic by Default in Security Group" is disabled:

- If you want to only allow access from the specified client IP, you **need to open** the client IP and listening port to the internet in the CLB security group and **open** the client IP and service port in the CVM security group; therefore, business traffic passing through CLB will be double checked by both the CLB security group and CVM security group.
- Traffic from public IPs (including general public IPs and EIPs) still needs to pass through the CVM security group.
- If a CLB instance has no security group configured, all traffic will be allowed, and only ports configured with listeners on the VIP of the CLB instance can be accessed; therefore, the listening port will allow traffic from all IPs.
- You can reject access in either the CLB security group or the CVM security group to reject traffic from a specified client IP.

After "Allow Traffic by Default in Security Group" is disabled, the CVM security group should be configured as follows to ensure effective health checks:

#### 1. Configure public network CLB

You need to open the CLB VIP to the internet on the backend CVM security group, so that CLB can use the VIP to detect the backend CVM health status.

#### 2. Configure private network CLB

- For private network CLB (formerly "private network application CLB"), if your CLB instance is in a VPC, the CLB VIP needs to be opened to the internet in the backend CVM security group for health checks; if your CLB instance is in the classic network, no additional configuration is needed as the health check IP is opened to the internet by default.
- For private network classic CLB, if your CLB instance was created before December 5, 2016 and is in a VPC, the CLB VIP needs to be opened to the internet (for health checks) in the backend CVM security group; otherwise, no additional configuration is needed as the health check IP is opened to the internet by default.

## Directions

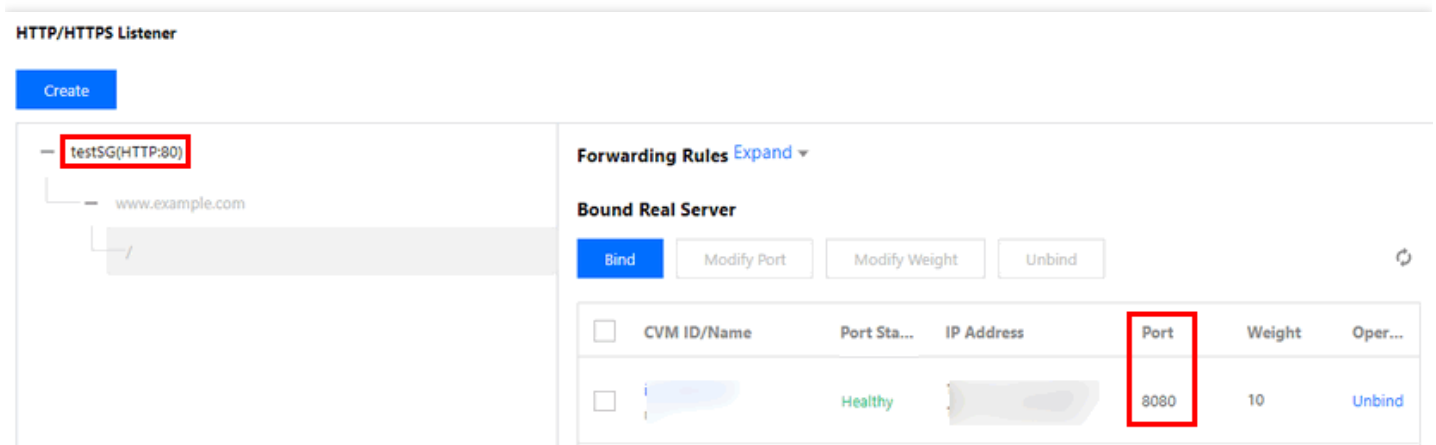
The following public network CLB security group configuration example only allows business traffic to enter from CLB port 80 and make CVM port 8080 provide services. It does not limit the client IP but supports access from any IP.

### Note :

For the public network CLB instance used in this example, the CLB VIP needs to be opened to the internet in the backend CVM security group for health checks. The current IP `0.0.0.0/0` already contains the CLB VIP.

### Step 1. Create a CLB instance and listener and bind a CVM instance

For more information, please see [Getting Started with CLB](#). An HTTP:80 listener is created and bound to a backend CVM instance whose service port is 8080 in this example.



**HTTP/HTTPS Listener**

Create

testSG(HTTP:80)

www.example.com

Forwarding Rules Expand

Bound Real Server

Bind Modify Port Modify Weight Unbind

<input type="checkbox"/>	CVM ID/Name	Port Sta...	IP Address	Port	Weight	Oper...
<input type="checkbox"/>		Healthy		8080	10	Unbind

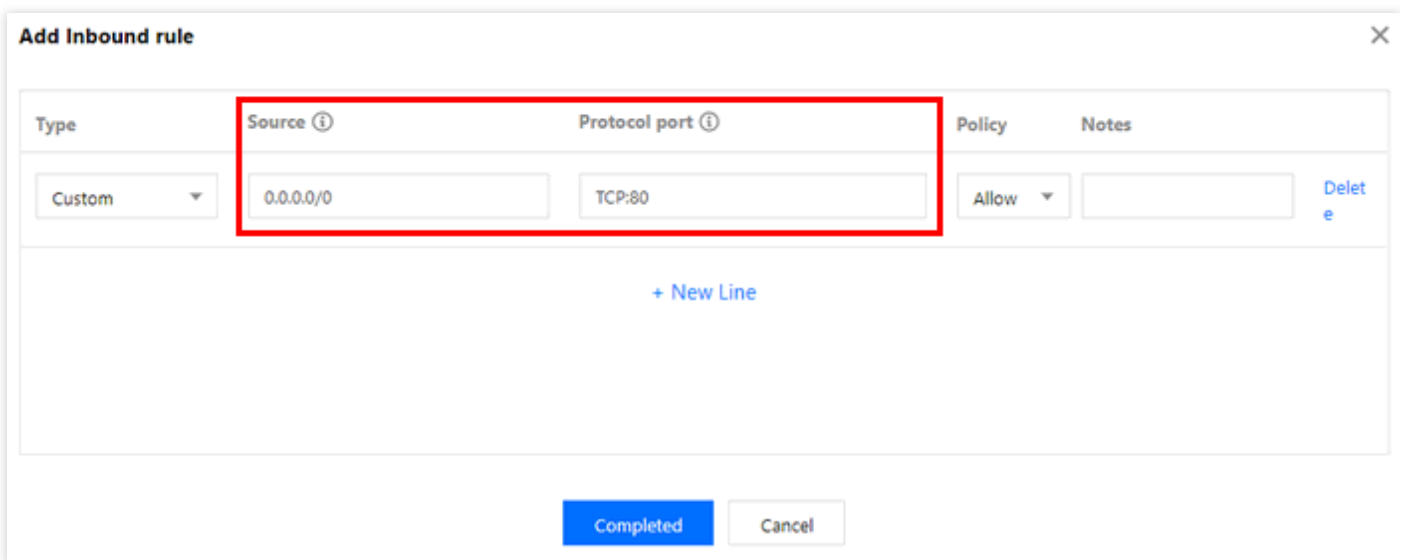
### Step 2. Configure a CLB security group

## 1. Configure a CLB security group rule.

Log in to the [Security Group Console](#) to configure a security group rule. In the inbound rule, open port 80 of all IPs (i.e., 0.0.0.0/0 ) to the internet and reject traffic from other ports.

### Note :

- Security group rules are screened to take effect from top to bottom. If the new rule is put into effect, other rules will be denied by default; therefore, pay attention to their order.
- A security group has inbound and outbound rules. The above configuration is intended to restrict inbound traffic and is therefore an **inbound rule**, while the outbound rule does not need to be specially configured.



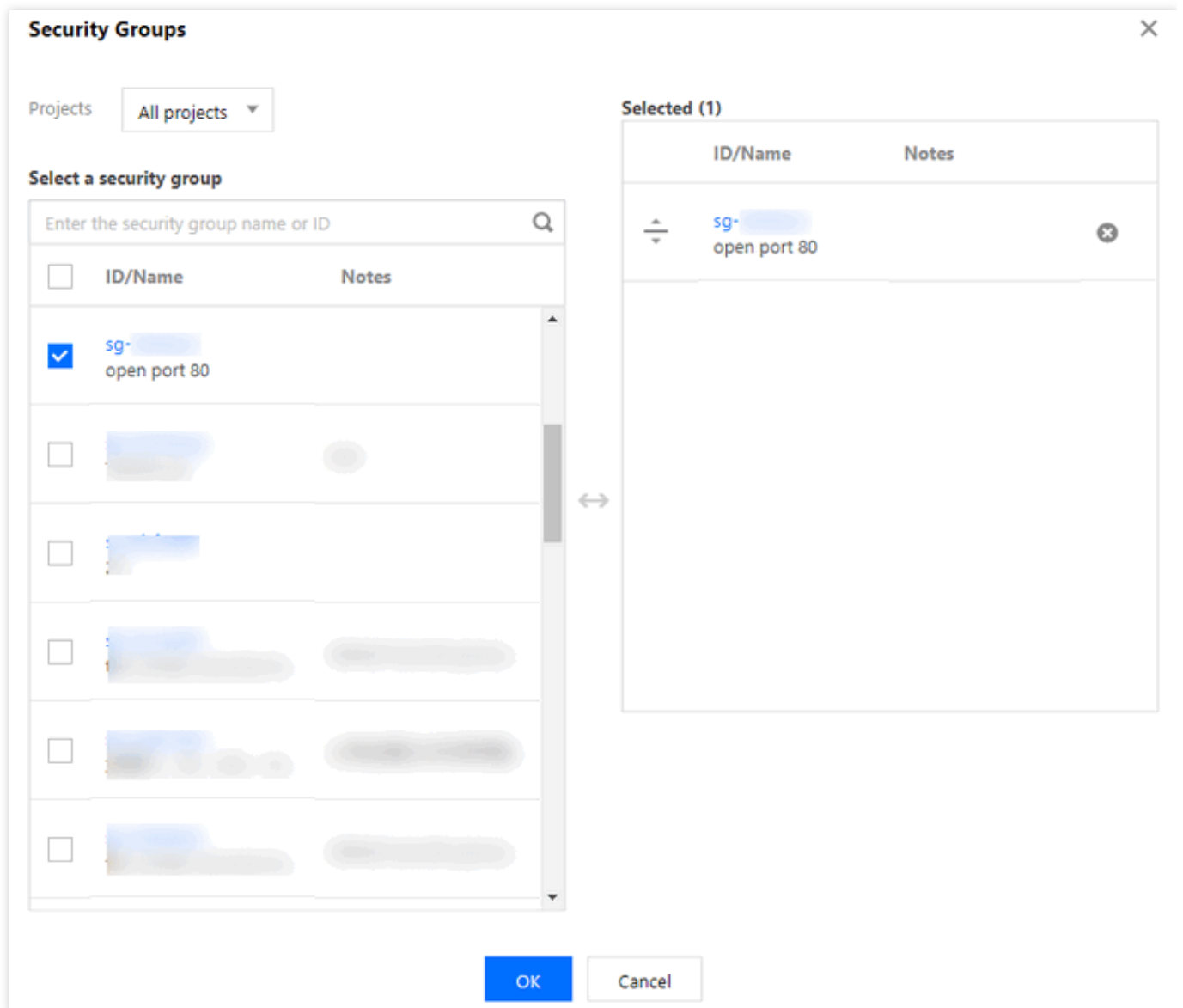
Type	Source ⓘ	Protocol port ⓘ	Policy	Notes
Custom ▼	0.0.0.0/0	TCP:80	Allow ▼	

+ New Line

Completed Cancel

## 2. Bind the security group to the CLB instance

- Log in to the [CLB Console](#).
- On the "Instance Management" page, click the ID of the target CLB instance.
- On the instance details page, click the **Security Group** tab and click **Bind** in the **Bound Security Groups** module.
- In the **Configure Security Group** window that pops up, select the security group bound to the CLB instance and click **OK**.



The CLB security group configuration is completed, which only allows access to CLB from port

80.

Note: from Dec 17, 2019, Tencent Cloud adds limits on the max number of security groups bound with an instance, instances bound to a security group, and rules referenced by a security group. For details, please see [Details of Limit](#).

**Bound to security group** [Sort](#) [Bind](#)

Priority①	Security Group...	Operation
1	sg-xxxx open port 80	Unbind

**Rule preview**  
**Inbound rule** [Outbound rule](#)

sg-xxxx | open port 80 [Edit rule](#)

Source	Port Protocol	Policy	Notes
0.0.0.0/0	TCP:80	Allow	open port 80
ALL	ALL	Refuse	If there is no rule, all traffic is rejected by default (system added, cannot be modified)

### Step 3. Configure "Allow Traffic by Default in Security Group"

You can choose to enable or disable "Allow Traffic by Default in Security Group" with different configurations as follows:


- Method 1. Enable "Allow Traffic by Default in Security Group", so that the real server does not need to open the port to the internet.

#### **Note :**

The "Allow Traffic by Default in Security Group" feature is currently in beta test. To try it out, please submit a ticket for application. This feature is not supported for classic private network CLB and CLB in the classic network.

- Method 2. Disable "Allow Traffic by Default in Security Group", and you also need to open the client IP to the internet (0.0.0.0/0 in this example) in the CVM security group.

### Method 1. Enable "Allow Traffic by Default in Security Group"

- Log in to the [CLB Console](#).
- On the "Instance Management" page, click the ID of the target CLB instance.
- On the instance details page, click the **Security Group** tab.
- On the "Security Group" tab, click  to enable "Allow Traffic by Default".

5. After the "Allow Traffic by Default" feature is enabled, only security group rules in the **rule preview** as shown below need to be verified.

**Allow by Default** ☒

When it's enabled, the access between CLB and CVM is allowed by default. Requests from CLB only need to be verified by the CLB security group. When it's disabled, requests from CLBs need to be verified by both security groups of CLB and CVM. If the CLB is not bound with a security group, all its listening ports allow requests from all IPs.

**Bound to security group** [Sort](#) [Bind](#)

Priority①	Security Group...	Operation
1	xx-allow80	<a href="#">Unbind</a>

**Rule preview** ⓘ

Inbound rule Outbound rule

xx-allow80

[Edit rule](#)

Source	Port Protocol	Policy	Notes
0.0.0.0/0	TCP:80	Allow	-
ALL	ALL	Refuse	If there is no rule, all traffic is rejected by default (system added, cannot be modified)

## Method 2. Disable "Allow Traffic by Default in Security Group"

If "Allow Traffic by Default" is disabled, you need to open the client IP to the internet in the CVM security group. Business traffic is allowed to access CVM only from CLB port 80 and use services provided by CVM port 8080.

### ⓘ Note :

Traffic from a specified client IP can be allowed, but that must be done in both the CLB security group and CVM security group. In the absence of the former, only the latter needs to be opened to the internet.

#### 1. Configure a CVM security group rule

A CVM security group can be configured to only allow access from service ports for traffic accessing the backend CVM instance.

Go to the [Security Group Console](#) to configure a security group policy. In the inbound rule, open port 8080 of all IPs to the internet. To ensure smooth remote CVM login and ping services, open 22, 3389, and ICMP services in the security group.

#### 2. Bind the security group to the CVM instance

- In the [CVM Console](#), click the ID of CVM instance bound to the CLB instance to enter the details page.



- ii. Select the **Security Group** tab and click **Bind** in the **Bound Security Groups** module.
- iii. In the **Configure Security Group** window that pops up, select the security group bound to the CVM instance and click **OK**.

Note: from Dec 17, 2019, Tencent Cloud adds limits on the max number of security groups bound with an instance, instances bound to a security group, and rules referenced by a security group. For details, please see [Details of Limit](#).

**Bound to security group** [Sort](#) [Bind](#)

Priority①	Security Group...	Operation
1	sg-... TCP port 22,...	Unbind

**Rule preview** [Inbound rule](#) [Outbound rule](#)

sg-... | TCP port 22, 8 [Edit rule](#)

Source	Port Protocol	Policy	Notes
0.0.0.0/0	TCP:8080	Allow	port 8080 open for CVMs
0.0.0.0/0	TCP:3389	Allow	TCP port 3389 open for ...