Virtual Private Cloud

Access Internet

Product Documentation

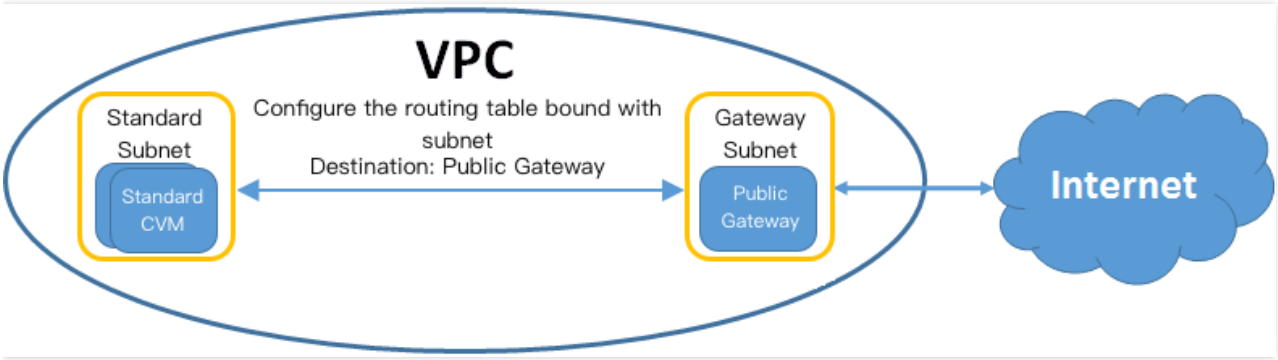
Contents

Access Internet
Public Network Gateway

Last updated：2019-07-30 18:14:32

Introduction

Public network gateway is a CVM on which the forwarding feature is enabled. CVMs without public IPs can access the Internet through a public network gateway in a different subnet. The public network gateway host will carry out source address translation for public network traffic. The IP of traffic by all other hosts accessing the public network is translated to the IP address of public network gateway host after passing through the public network gateway, as shown below:



Difference Between Public Network Gateways and CVMs with Public IPs

Public network gateways have had the public network traffic route forwarding function enabled in image, while CVMs with public IPs do not have traffic forwarding function by default. Windows public image CVMs cannot be used as public network gateways, because the traffic forwarding function is not enabled in Windows image.

Usage Constraints

- Public network gateway currently supports a maximum egress bandwidth of 100 Mbps. If you need a larger egress bandwidth, you can purchase more public network gateways to form a public network egress cluster. With the same destination route configured in routing tables, the self-adaptive load balancing for forwarding traffic can be achieved between public network gateways. (Note: The cloud load balancer does not support health checks currently. Public network gateway failures may lead to loss of traffic).
- A gateway subnet and an ordinary subnet cannot be associated with the same routing table. A separate gateway routing table needs to be created to be associated with the gateway subnet.
- Public network gateways support NAT connections, and users need to log in to the CVM to configure this. Direct Connect gateways and VPN gateways do not support NAT connections currently.

Billing

As a public network gateway is essentially a CVM instance, the billing method is the same as the CVM billing. For details, please refer to here.

Expiry Reminder

The expiry reminder mode is consistent with the CVM. For details, please refer to here.

Operating Instructions

If a CVM without a public IP in a VPC needs to access the public network through a public network gateway, the following steps should be completed:

a) Create a gateway subnet;
b) Purchase a public network gateway;
c) Create a routing table of gateway subnet;
d) Configure the routing table of ordinary subnet;

Creating a gateway subnet

The public network gateway can only forward the route forwarding request of the subnet to which it does not belong, so the public network gateway cannot be in the same subnet with the CVM which needs to access the public network through the public network gateway. Therefore, it is necessary to set up a separate gateway subnet first.

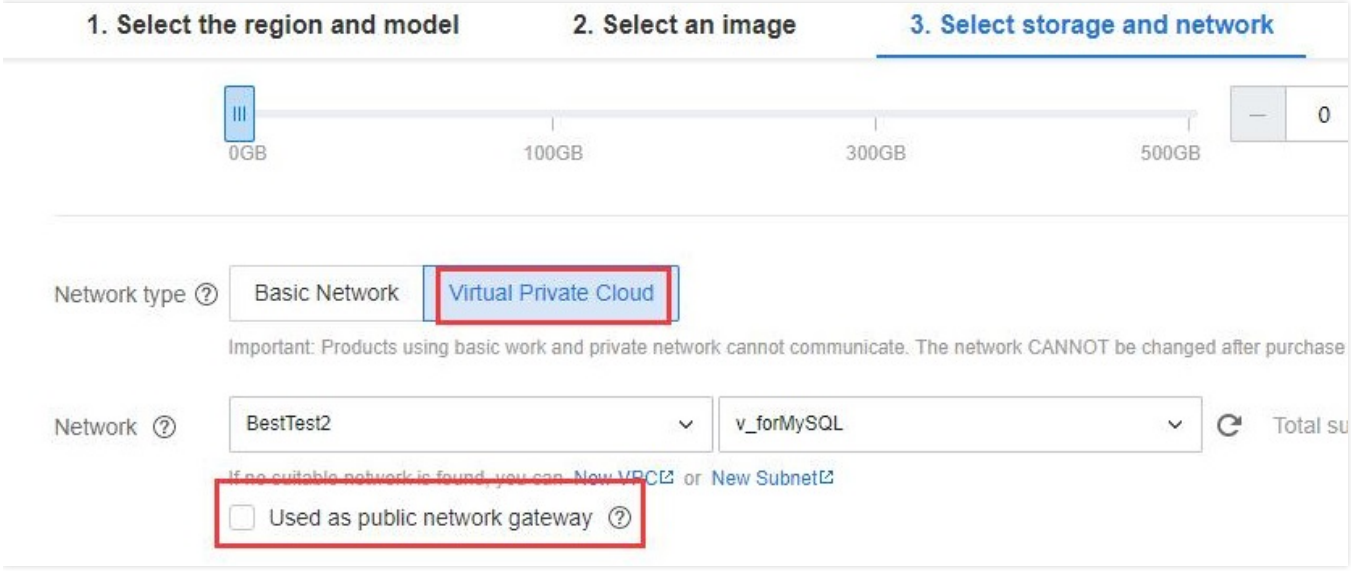
1) Click "Subnet" in the left navigation bar of VPC Console.
2) Select a region and a VPC in the top drop-down boxes.
3) Click "New", and fill in a subnet name (such as public network gateway subnet), CIDR, availability zone and associated routing table (A random routing table can be associated with at this time).
4) Click "Create", and then the newly created subnet will display in the subnet list.

Purchasing a public network gateway

Like the CVMs, public network gateways are also purchased in the Tencent Cloud CVM Purchase Page.

1) Log in to Tencent Cloud CVM Purchase Page, and select "VPC" in the Network Type on the "3. Select Storage and Network" page.
2) Select a VPC and the gateway subnet created in the previous step.

3) Check "Used as a public network gateway". The public network gateway is created upon the completion of the purchase.



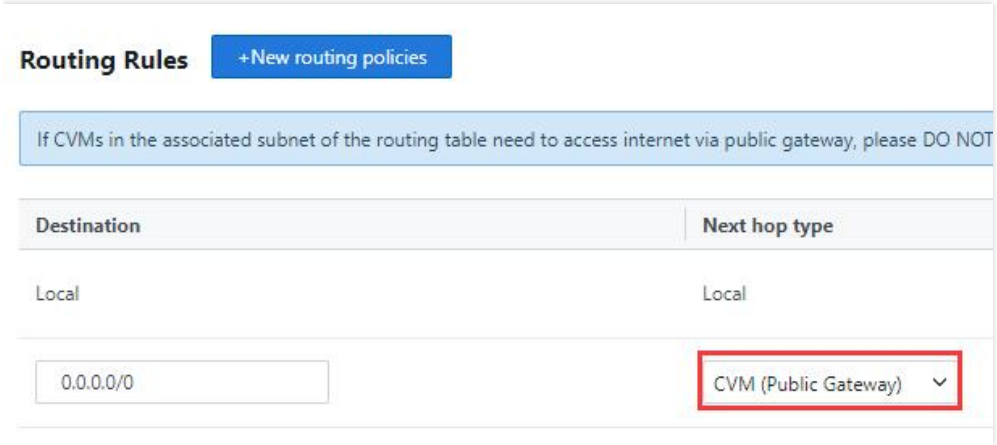
Creating a routing table of gateway subnet

A gateway subnet and an ordinary subnet cannot be associated with the same routing table. A separate gateway routing table needs to be created to be associated with the gateway subnet created in association with this routing table. The default Local policy can be retained as a routing policy. For related operations, refer to Creating Custom Routing Table and Modifying Routing Table Associated with a Subnet.

Configuring the routing table of ordinary subnet

Configure the routing table of the ordinary subnet, and direct the route to the public network gateway CVM, so that the CVM without a public IP in the ordinary subnet can access the public network through the route forwarding capability of public network gateway.

1) Click the "Routing Table" in the left navigation bar of VPC Console, and select the routing table associated with the ordinary subnet that needs to access the public network (users can find the routing table associated with the ordinary subnet in the Subnet list page.
2) Click the ID of the routing table associated with the ordinary subnet to enter the routing table details page.
3) Click the "Edit" button and configure the default route to take the public network gateway CVM, so that the CVM in the ordinary subnet can access the public network through the route forwarding capability of public network gateway.



API Overview

The public network gateway is essentially a CVM instance. Users can view related APIs in Overview of CVM APIs, or use VPC, subnet, routing table and other APIs to complete the configuration of public network gateways. For more information, refer to Overview of All VPC APIs.

NAT Gateway

Last updated：2019-07-31 11:33:42

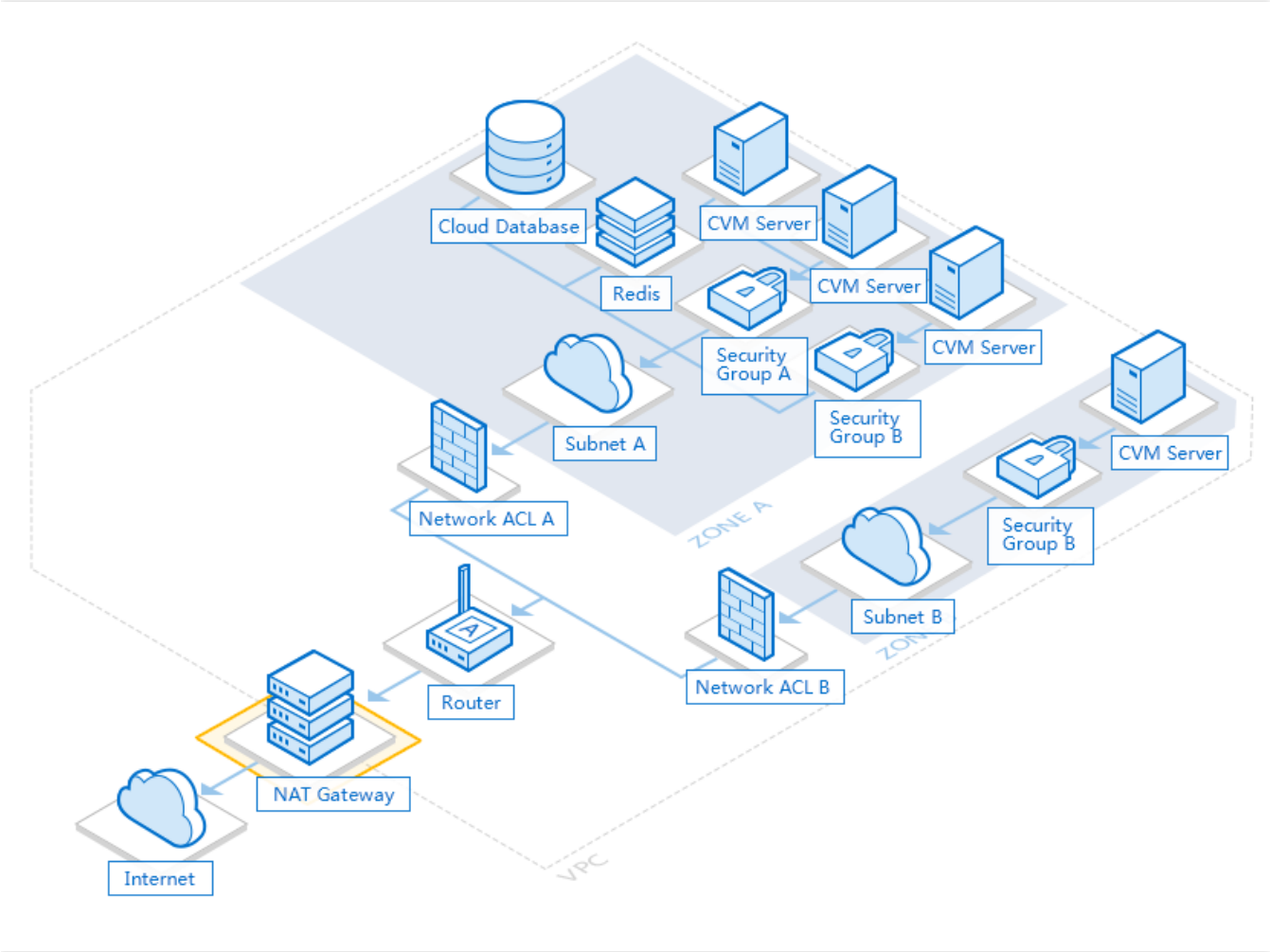
Overview

NAT gateway provides the capability to translate between private IPs and public IPs in VPC. It is an ingress/egress for public network traffic in VPC. The NAT gateway of Tencent Cloud VPC is used in the following typical scenarios:

- **Public network access with large bandwidth and high availability.** Tencent Cloud NAT gateway can meet users' demands for public network access that requires ultra-large bandwidth, massive use of public IPs, and a large number of services to be deployed.
- **Secure public network access.** The NAT gateway of Tencent Cloud VPC provides secure IP translation. If you want to hide the public IP of the CVM in the VPC to avoid exposing its network deployment while expecting to communicate with the public network, you can use Tencent Cloud NAT gateway.

Network Topology

As shown in the figure below, the NAT gateway resides on the boundary between the Internet and the VPC, and is connected to the router on the VPC. In such a topology, when resources like CVM in the VPC send data packets outwards via the NAT gateway, the data first passes through the router and makes routing selection based on routing policies. Then, the NAT gateway sends traffic to the Internet through the bound EIP as the source IP:



Features

- The NAT gateway supports SNAT and DNAT:
  - SNAT: Source network address translation. It allows multiple VPC CVMs to actively access the Internet through the same public IP.
  - DNAT: Destination network address translation (which is under internal trial. Submit a Ticket, if necessary). It is used to map [private IPs, protocols and ports] of the CVM in the VPC into [public IPs, protocols and ports], so that services on the CVM can be accessed from the public network.

- The NAT gateway supports high defense services:
  BGP high defense provides ultra-large bandwidth DDoS and CC defense for Tencent Cloud users, with a capacity of up to 310 Gbps. You can bind the high defense package to the NAT gateway that requires defense for security protection.

Difference between NAT Gateway and Public Network Gateway

Both NAT gateway and public network gateway are used for the CVM in the VPC to access the Internet. Differences between these two gateways are shown below:

Attribute	NAT Gateway	Public Network Gateway
Availability	Master/slave hot backup, automatic hot switching	Switch the failed gateway manually
Public network bandwidth	Maximum is 5 Gbps	Depend on the network bandwidth of CVM
Public IP	A maximum of 10 EIPs can be bound	One EIP or ordinary public IP
Rate limit of public network	N/A	Depend on the rate limit of CVM
Maximum number of connections	10m	500k
Private IP	Private IPs of VPC users are not occupied	Private IPs of the subnet are occupied
Security group	Binding of security group is not supported. You can bind the security group to the NAT gateway backend CVM	Support
Network ACL	Binding of network ACL is not supported. You can bind the network ACL to the subnet in which the NAT gateway backend CVM resides	Binding of network ACL is not supported. You can bind the network ACL to the subnet to which the public network gateway belongs
Charges	Mainland China: Small (a maximum of 1m connections): 0.5 CNY/hr Medium (a maximum of 3m connections): 1.5 CNY/hr Large (a maximum of 10m connections): 5 CNY/hr	Depend on the size of CVM used as a public network gateway. Take Mainland China as an example: 1-core 2 GB: 0.44 CNY/hr 4-core 8 GB: 1.76 CNY/hr 12-core 24 GB: 5.28 CNY/hr

The comparisons listed above show that Tencent Cloud NAT gateway has three advantages:

- Large capacity: It supports a maximum of 10m concurrent connections, 5 Gbps bandwidth and 10 EIPs to meet the demand of users with a large business scale.
- Highly available master/slave hot backup: Automatically switch when a single server suffers a failure to allow automatic disaster recovery and 99.99% service availability, superior to the manual switch of a public network gateway.
- Cost effectiveness: Three configuration types, high, medium and low, are available for users to choose from as needed, offering flexibility in billing and high cost effectiveness.

Configuration Types

The NAT gateway supports binding up to 10 EIPs, and a maximum of 5 Gbps traffic surge and 10m concurrent connections, while providing three configuration types.

- Small (max. 1m connections)
- Medium (max. 3m connections)
- Large (max. 10m connections)

Available values for maximum public network outbound bandwidth of NAT gateway (in Mbps): 10, 20, 50, 100, 200, 500, 1000, 2000, and 5000.

How to Use NAT Gateway and EIP

NAT gateway and EIP are two ways for the CVM to access the Internet. You can use either one of them or both of them to design your public network access architecture.

Method 1: Use NAT Gateway Only

The CVM is not bound to an EIP, and all the traffic for accessing the Internet is forwarded via the NAT gateway. In this way, the CVM traffic for accessing the Internet is forwarded to the NAT gateway via the private network. This means that the traffic is not restricted by the upper limit of public network bandwidth specified when you purchase the CVM, and the traffic generated from the NAT gateway doesn't occupy the public network bandwidth egress of the CVM.

Method 2: Use EIP Only

CVM is only bound with EIP, instead of using NAT gateway. With this solution, all the traffic of the CVM accessing the Internet flows via the EIP and is restricted by the upper limit of public network bandwidth specified when you purchase the CVM. The fees for accessing the public network depends on the billing method of the CVM's network.

Method 3: Use Both NAT gateway and EIP

The CVM is bound to an EIP, and the traffic of the subnet route for accessing the Internet is directed to the NAT gateway. In this way, all the traffic of the CVM for accessing the Internet is **forwarded to the NAT gateway via the private network only**, and the response packets are returned to the CVM via the NAT gateway. This means that the traffic is not restricted by the upper limit of public network bandwidth specified when you purchase the CVM, and the traffic generated from the NAT gateway does not occupy the public network bandwidth outlet of the CVM. If the traffic from the Internet accesses the EIP of the CVM, the response packets of the CVM are all returned through the EIP. In this case, the resulting outbound traffic of the public network is restricted by the upper limit of public network bandwidth specified when you purchase the CVM. The fees for accessing the public network depend on the billing method of the CVM's network.

> **Note:**
> For the accounts with a bandwidth package for bandwidth sharing, the fee for the outbound traffic from NAT gateway is covered by the bandwidth package (the network traffic fee of 0.8 CNY/GB is not charged additionally). You're recommended to set a limit on the outbound bandwidth of the NAT gateway, so as to avoid a high bandwidth package fee due to the excessive use of outbound bandwidth of NAT gateway.

Key Features

The followings are some key features of NAT gateway:

- SNAT: Source network address translation. It allows multiple VPC CVMs to actively access the Internet through the same public IP.
- DNAT: Destination network address translation. It is used to map [private IPs, protocols and ports] of the CVM in the VPC into [public IPs, protocols and ports], so that services on the CVM can be accessed from the public network.
- High performance: NAT gateway supports forwarding up to 5 Gbps of data to a single instance.
- High availability: NAT gateway provides master/slave hot backup to switch automatically when a single server suffers a failure, without affecting your use of services.
- Monitoring details display: All the key metrics for private IPs flowing to the NAT gateway are displayed, to help you implement rapid troubleshooting and exceptional traffic location. The monitoring details data can be kept for 7 days.

- Refined gateway traffic control: The bandwidth between a private IP and the NAT gateway can be limited to guarantee key businesses.

NAT Gateway Traffic Control

NAT gateway traffic control provides the "monitoring" and "controlling" capabilities at **IP-gateway** granularity. Refined gateway traffic visualization enables network OPS personnel to get a clear picture of the traffic in the gateway. The speed restricting capability at IP-gateway granularity helps block exceptional traffic.
For example, in the early morning of one day, the gateway traffic of a company surges. With intelligent gateway traffic control, the OPS personnel can trace data to find which IPs cause this traffic surge according to the time when the traffic surge occurs, so as to rapidly locate its source. In addition, the gateway traffic control provides bandwidth control based on IP-gateway granularity, which can restrict the bandwidth from an IP to the gateway and block exceptional traffic to guarantee key businesses.

The advantages of gateway traffic control are as follows:

- Featured with the capability for accurate gateway troubleshooting, it can minimize the network failure time. It can also analyze the source IP and its key metrics by combining real-time traffic query and TOP N ranking features, to rapidly locate the exceptional traffic.
- With "monitoring" and "controlling" capabilities based on IP-gateway granularity and by using the minute-level network traffic query, it can find the exceptional traffic that maliciously occupies the bandwidth in real time, and set bandwidth limits at IP-gateway granularity, so as to guarantee the stable operation of core businesses.
- It has full-time and full-traffic gateway traffic analysis capability, to help reduce cloud network cost. It controls the cost through qos, thus restricting the bandwidth of non-key businesses to reduce cost in case of limited network budget.

Service Limits

When you use the NAT gateway, note the followings:

- If the NAT gateway is deleted, its EIP is disassociated from it, but not released from the account.
- Although the NAT gateway cannot be associated with security groups, they can be used for the instances in the private subnet to control the traffic that flows in and out of these instances.
- You cannot use the network ACL to control the traffic that flows in and out of the NAT gateway, but you can use it to control the traffic of the associated subnet that flows in and out of the NAT gateway.
- Users can not use VPC peering connection, VPN connection or direct connection to route traffic to the NAT gateway which cannot be used for these resources that are connected to the other end. For example, all the traffic of VPC 1 can be sent to the Internet through the NAT gateway. Since a peering connection has been established between VPC 1 and VPC 2, all the resources within VPC 2 can access all the resources within VPC 1, but no resources within VPC 2 can access the Internet through the NAT gateway.
- Supported protocols for the NAT gateway include TCP, UDP and ICMP, while ESP and AH for the GRE tunnel and IPSec cannot be used for the NAT gateway. This is a result of the characteristics of the NAT gateway itself, which has nothing to do with the service provider. Luckily, TCP is a dominant type of application in the Internet world, and, together with UDP, accounts for 99% of all Internet applications.
- For more information about the restrictions on the supported resources for the NAT gateway, please see Service Limits of Other VPC Products.

Resource	Limit

Resource	Limit
Number of NAT gateways per VPC	3
Number of EIPs per NAT gateway	10
Maximum forwarding capacity per NAT gateway	5 Gbps

Billing Method

NAT gateway charges include the gateway rental fee (billed hourly) and Internet access traffic fees. For traffic fees , you can refer to CVM's bill-by-traffic method. See below for NAT gateway fees.

Feature	Billing Model	Configuration	Price						
			Beijing Shanghai Guangzhou	Hong Kong	Singapore	Toronto	Korea	Frankfurt	Silicon Valley
NAT Gateway	Rental fee for gateway (USD/hour)	Small	0.089	0.13	0.13	0.14	0.13	0.13	0.13
		Medium	0.28	0.39	0.39	0.42	0.39	0.39	0.39
		Large	0.89	1.3	1.3	1.4	1.3	1.3	1.3

Note:
For those who have a bandwidth sharing package, NAT gateway-generated outbound traffic will be covered by the package (network traffic will not be charged again). It is recommended that you limit the NAT gateway outbound bandwidth to avoid excessive bandwidth package fee. For more information, see Bandwidth Package billing details
Arrears measures are the same as pay-as-you-go CVM instances, please see VPC Pricing List more information.

Arrears Reminder

- When your balance falls below zero, you can continue to use NAT gateway for the next **2** hours. We will also continue to bill you for this usage.
- After 2 hours, if your account is not topped up to a positive balance, NAT gateway service and billing will automatically be stopped.
- Your service will remain unavailable if your balance is not positive within 24 hours after automatic shutdown. If your balance is positive, NAT gateway service and billing can be resumed.
- If your balance remains negative more than 24 hours after automatic shutdown, NAT gateway will be repossessed.
- Email and SMS notifications will be sent to the Tencent Cloud account creator and all collaborators.

Operation Instructions

If you want to allow the resources within the subnet of a VPC to access the Internet through an NAT gateway, you need not only to create the NAT gateway, but also to configure the routing rules in the routing table with which the subnet that needs route

forwarding is associated.

Quick Start

You can access the Internet through an NAT gateway by following the steps below:

Step 1: Create NAT Gateway

1. Log in to Tencent Cloud Console, select "Virtual Private Cloud" tab, and then select "NAT Gateway".
2. Click the "New" button at the upper left corner, and enter or specify the following parameters in the pop-up box:
   - Gateway name
   - Gateway type (which can be changed after creation)
   - VPC of NAT gateway service
   - Assign an EIP to NAT gateway. You can choose an existing EIP, or purchase and assign a new EIP.
3. After selection, click "OK" to complete the creation of NAT gateway.
4. After the creation of the NAT gateway, you need to configure the routing rules on the Routing Table page of the VPC Console to direct the subnet traffic to the NAT gateway.

> **Note:**
> The rental fee will be frozen for 1 hour during the creation of NAT gateway.

Step 2: Configure the Routing Table Associated with the Subnet

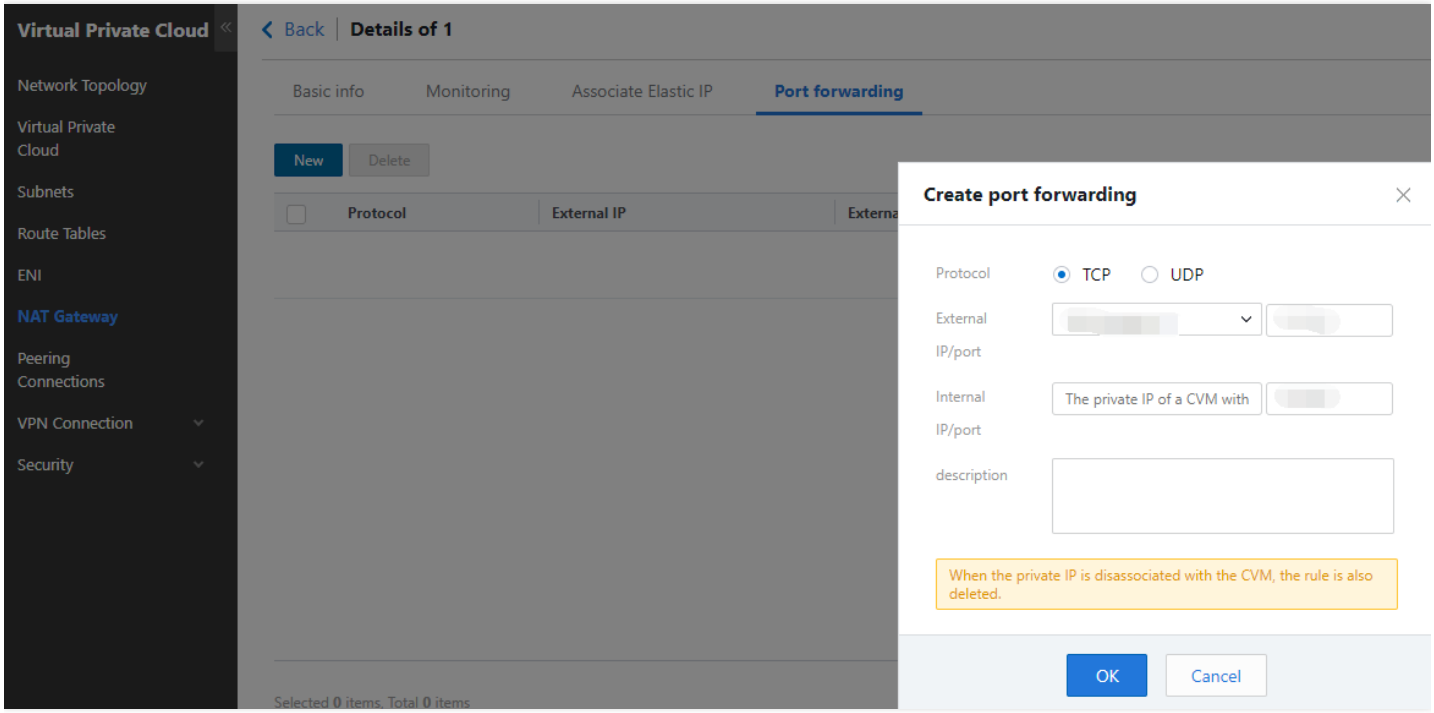
1. Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "Routing Table".
2. In the routing table list, click the ID of the routing table associated to the subnet that needs to access the Internet to go to the details page of the routing table, and then click "Edit" button in the "Routing Policies".
3. Click "New line", enter the "Destination" field, select "NAT Gateway" in "Next Hop Type", and select the ID of the created NAT gateway.
4. Click "OK". After the configuration, the traffic generated when the CVM in the subnet associated with the routing table accesses the Internet is directed to the NAT gateway.

Creating Port Forwarding Rule

The port forwarding table is a configuration table on the NAT gateway, which is used to configure the DNAT feature on the NAT gateway. It map [private IPs, protocols and ports] of the CVM in the VPC into [public IPs, protocols and ports], so that services on the CVM can be accessed from the public network. (It is under internal trial. Submit a Ticket, if necessary).

1. Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "NAT Gateway".
2. In the NAT gateway list page, click the ID of the NAT gateway to be modified to go to its details page, and select "Port Forwarding".
3. Click "New", and select the protocol, external IP port and internal IP port.

> **Note:**
> The internal IP only supports the private IP of the CVM in this VPC.



Querying Port Forwarding Rule

1. Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "NAT Gateway".
2. In the NAT gateway list page, click the ID of the NAT gateway to be modified to go to its details page, and select "Port Forwarding".
3. In the search box, select the protocol\IP\port, and enter related attribute values to query related port forwarding rules.

Modifying NAT Gateway Configuration

You can modify the attributes of a created NAT gateway.

1. Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "NAT Gateway".
2. In the NAT gateway list page, click the ID of the NAT gateway to be modified to go to its details page, where you can make modifications to the following attributes:
   - Change the custom name of NAT gateway
   - Change the NAT gateway specifications. Specification changes take effect immediately (the network connection is not broken)

Managing EIPs bound to the NAT Gateway

1. Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "NAT Gateway".
2. In the NAT gateway list page, click the NAT gateway ID to go to its details page.
3. In the list of associated EIPs, you can "Add" or "Unbind" an EIP.

Viewing Monitoring Information of NAT Gateway

1. Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "NAT Gateway".

2. In the NAT gateway list page, click the "Monitor" button in an NAT gateway entry to view its monitoring information.
   (Alternatively) In the NAT gateway list page, click the ID of an NAT gateway to go to its details page, and then click "Monitoring" tab to view its monitoring information.

Setting the Alarm

1. Log in to Tencent Cloud Console, click "Cloud Products" -> "Monitor & Management" -> "Cloud Monitor" in the top navigation bar, and select "My Alarms" -> "Alarm Policy" in the left navigation bar, and then click "Add Alarm Policy".
2. Enter the alarm "Policy Name", select "NAT Gateway" in "Policy Type", and then add alarm triggering condition.
3. **Associate alarm objects**: Select the alarm receiver group, and when it is saved, you can view the set alarm polices in Policy List.
4. **View the alarm information**: When the alarm is triggered, you can receive a notification sent via SMS/email/internal message. You can also view it in "My Alarms" -> "Alarm List" in the left navigation bar.

Deleting NAT Gateway

NAT Gateway can be deleted when it is not needed. The routing table and routing rules containing the NAT gateway is deleted with the NAT gateway. Upon the deletion, the request forwarded over Internet is interrupted immediately. Be prepared for the network interruption in advance.

1. Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "NAT Gateway".
2. Select the NAT gateway to be deleted, click "Delete" button and confirm the action, and then the NAT gateway is deleted.

Enabling Gateway Traffic Control Details

After it is enabled, you can view the metrics of IP traffic passing through an NAT gateway over the last 7 days, and also set the outbound bandwidth for an IP to flow to a specific NAT gateway.

1. Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "NAT Gateway".
2. In the NAT gateway list page, click the NAT gateway ID to go to its details page.
3. Click the "Monitor" tab, and enable the switch of "Gateway Traffic Control Details" on the upper right corner.
   After the Gateway Traffic Control Details are enabled, it takes 5 to 6 days to collect and publish data. During this period, you can view the monitoring details table at the lower part of the monitoring chart.

> **Note:**
> This feature is under internal trial. Submit a ticket to apply for it.

Setting Gateway Traffic Control Details

After Gateway Traffic Control Details is enabled, you can set the outbound bandwidth for an IP to flow to a specific NAT gateway.

1. Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "NAT Gateway".
2. In the NAT gateway list page, click the NAT gateway ID to go to its details page.
3. Click the "Monitor" tab, find the IP for which monitoring details need to be set, and set a limit on its outbound bandwidth.

Viewing Gateway Traffic Control Details

1. Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "NAT Gateway".

2. In the NAT gateway list page, click the NAT gateway ID to go to its details page.
3. Click the "Monitor" tab, and then click "View Restricted IP" in the upper right of the gateway traffic control details table.

Binding High Defense Package

1. Log in to Tencent Cloud Console, click "Security" -> "Dayu Distributed Defense" in the navigation bar, and select BGP High Defense Package on the left navigation bar.
2. Select an existing high defense package instance, click "Change Device" and select the EIP on the NAT gateway that needs to be used repeatedly.
3. Click "OK" to associate the high defense package feature to this NAT gateway.

API Overview

You can use APIs to configure and manage your NAT gateway. For more information about other VPC resources, please see Overview of All VPC APIs.

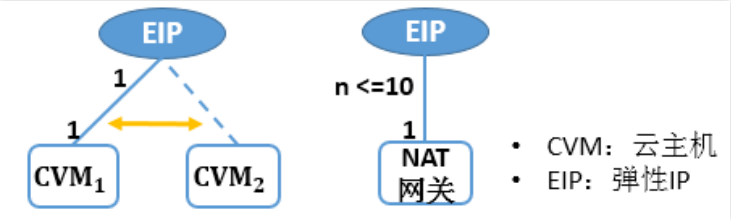
Feature	Action ID	Description
Create NAT Gateway	CreateNatGateway	Create an NAT gateway.
Query NAT gateway creation status	QueryNatGatewayProductionStatus	Query the creation status of an NAT gateway.
Delete NAT gateway	DeleteNatGateway	Delete an NAT gateway.
Modify NAT gateway	ModifyNatGateway	Modify an NAT gateway.
Query NAT gateway	DescribeNatGateway	Query an NAT gateway.
Bind EIP for NAT gateway	EipBindNatGateway	Bind an EIP for an NAT gateway.
Unbind EIP for NAT gateway	EipUnBindNatGateway	Unbind an EIP for an NAT gateway.
Upgrade NAT gateway specifications	CreateNatGateway	Upgrade the specifications of an NAT gateway.

Elastic Public IP

Last updated：2018-10-18 15:49:32

Basic Concepts

Elastic IP (EIP) is a public IP address that can be applied for independently. It supports dynamic binding and unbinding to CVM/NAT gateway instances. As shown in the figure below, you can bind or unbind it to a CVM (or NAT gateway instance) in the account. It is mainly used to shield off instance failures. For example, a DNS name is mapped to an IP address through the dynamic DNS mapping. It may take up to 24 hours to propagate this mapping to the entire Internet, while elastic IP enables the drift of an IP from one CVM to another. In case of a CVM failure, all you need to do is start another instance and remap it, thus responding rapidly to the instance failure.
Your EIP is associated with a Tencent Cloud account, instead of a CVM instance, until you choose to explicitly release it or your payment is more than 7 days overdue.



Range of Application

The elastic public IP address applies to the CVM instances of both basic networks and VPCs, and the NAT gateway instances in VPCs. It supports dynamic binding and unbinding. Please note that:

- There is a one-to-one relationship between EIPs and CVM/NAT gateways. As shown in the above figure, one EIP can only be bound to one CVM/NAT gateway instance in the same region at the same time. One CVM instance can only be bound to one EIP at the same time, while one NAT gateway can be bound to up to 10 EIPs at the same time.
- When an EIP is bound to a CVM instance, the current public IP address of the instance will be released.
- If you choose to reassign a public IP when unbinding an EIP from a CVM instance, the instance will be automatically assigned to the new public IP.
- Terminating a CVM/NAT gateway instance will disassociate it from its EIP.
- If a CVM instance in a VPC is bound to an EIP and also resides in a subnet that is associated with a NAT gateway, the data packets accessing the public network will go through the NAT gateway instead of the EIP.

Releasing an EIP

There are two ways to release an EIP:

- Users can actively release an elastic public IP through the console or cloud API;
- Release under arrears: A fee will be calculated by hour when the elastic IP is bound to no resource. After the account is negative for 2 hours and still not renewed, the elastic public IP will be inoperable within the following (24 x 7) hours (until the account balance is greater than 0), that is, if the amount is still negative after (2+24 x 7) hours, the elastic public IP will be automatically released.

Reasons for Unavailable Elastic Public IPs

Reasons for unavailable elastic public IPs include:

- The elastic public IP is not bound to a cloud resource. For specific binding method, refer to Binding a CVM to an EIP
- Check whether there is a security policy inside the CVM instance. If the CVM instance has a security group policy, for example: 8080 port access is denied, the 8080 port of the elastic public IP is also inaccessible.

How to Use NAT Gateway and Elastic Public IP

NAT gateway and elastic public IP are the two ways for the CVM to access the Internet. You can use either one of them or both of them to design your public network access architecture.

Method 1: Use NAT gateway only

The CVM is not bound to an elastic public IP; all traffic from accessing the Internet is forwarded through the NAT gateway. With this method, the traffic from the CVM accessing the Internet will be forwarded to the NAT gateway through the private network. That means this traffic will not be subject to the public bandwidth limit specified when the CVM was purchased, nor will the traffic generated at the NAT gateway occupy the public bandwidth egress of the CVM.

Method 2: Use elastic public IP only

The CVM is only bound to an elastic public IP, and the NAT gateway will not be used. With this method, all traffic from the CVM accessing the Internet will go out from the elastic public IP. That means this traffic will not be subject to the public bandwidth limit specified when the CVM was purchased. The cost resulting from accessing the public network will be charged based on the network billing mode of the CVM.

Method 3: Use both the NAT gateway and the elastic public IP

The CVM is bound to an elastic public IP; meanwhile all traffic from the subnet route accessing the Internet is directed to the NAT gateway. With this method, all traffic from the CVM actively accessing the Internet **can only be forwarded to the NAT gateway through the private network**, and the returning packets will be returned to the CVM through the NAT gateway as well. This traffic will not be subject to the public bandwidth limit specified when the CVM was purchased, nor will the traffic generated at the NAT gateway occupy the public bandwidth egress of the CVM. If the traffic from the Internet actively accesses the elastic public IP of the CVM, the returning packets of the CVM will be uniformly returned through the elastic public IP. This way, the resulting outbound traffic of the public network will be subject to the public bandwidth limit specified when the CVM was purchased. The cost resulting from accessing the public network will be charged based on the network billing mode of the CVM.

> Note: For users with a Bandwidth Package for bandwidth sharing, the outbound traffic generated at the NAT gateway will be billed as per the Bandwidth Package (the RMB 0.8/GB network traffic fee will not be charged separately). It's recommended that you set a limit on the outbound bandwidth of the NAT gateway, so as to avoid any high Bandwidth Package charge due to excessively high amount of such bandwidth.

Usage Restrictions

Note: Click to view the usage restrictions of other products within the VPC.

Resources	Limit
Quota of elastic public IPs for each Tencent Cloud account in each region	20

Resources	Limit
Number of purchases that can be made by each Tencent Cloud account in each region per day	Quota X 2 (times)
Number of reassignments of public IPs that can be made for free by each account in a day when an EIP is unbound	10 times

EIP Billing Method

The EIPs that are bound to CVMs (or NAT gateways) are free. To ensure the effective use of elastic IP addresses, the elastic IPs that are not bound to CVM or NAT instances will be charged a resource occupancy fee by hour (Less than 1 hour will be counted as 1 hour. Settlement is made per hour). The detailed billing standard is listed in the table below. It is recommended that you release the elastic public IPs that are not used in a timely manner so as to ensure the rational use of IP resources and save your cost.

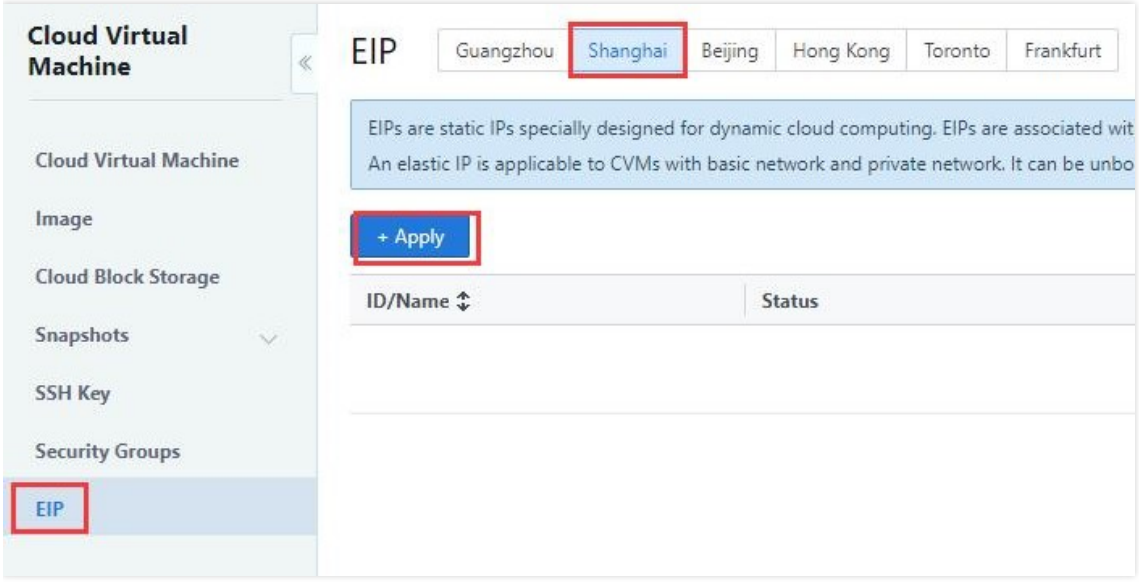
Region of the Elastic Public IP	Price for No Binding
Beijing, Shanghai, and Guangzhou	RMB 0.20/hour
Hong Kong	RMB 0.30/hour
North America	RMB 0.25/hour

Note: Click to view the billing method for other products within the VPC

Operating Instructions

Applying for an EIP

1) Open the CVM Console.
2) In the left navigation pane, click "Elastic Public IP".
3) Select a region in the list and click the "Apply" button.
3) After the application is successful, the EIP you applied for will display in the EIP list.



Modifying the EIP Name

1) Open the CVM Console.
2) In the left navigation pane, click "Elastic Public IP".
3) Click the Rename button in the EIP entry to be modified.
4) Enter a new name and click the "OK" button.

Binding a CVM to an EIP

1) Open the CVM Console.
2) In the left navigation pane, click "Elastic Public IP".
3) Click the "Bind" button at the end of the EIP to which a CVM needs to be bound. If this EIP is already bound to a CVM, this button will be unavailable. Please unbind it first.
4) In the pop-up box, select the CVM for binding according to CVM instance ID.
5) Click "Bind".

Or:

1) Open the CVM Console, and enter the CVM instance list.
2) Click "Bind EIP" under the Operation column on the right side of the CVM to which an EIP needs to be bound.
3) In the pop-up Bind EIP box, select the EIP you want to bind, and click the "OK" button.

Unbinding a CVM from an EIP

1) Open the CVM Console.
2) In the left navigation pane, click "Elastic Public IP".
3) Click the "Unbind" button at the end of the EIP which is already bound to a CVM.
4) Click "OK".

Or:

1) Open the CVM Console.
2) Click "Unbind EIP" under the Operation column on the right side of the CVM from which an EIP needs to be unbound.
3) In the pop-up Unbind EIP box, select whether you need to assign public IPs for free, and then click the "OK" button.

Releasing an EIP

1) Open the CVM Console.
2) In the left navigation pane, click "Elastic Public IP".
3) Click the "Release" button at the end of the EIP to be released.
4) Click "OK".