

NAT Gateway

FAQ

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

 Tencent Cloud

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

FAQ

Concepts

Billing

Features

FAQ

Concepts

Last updated : 2020-07-09 14:43:01

What is a NAT Gateway?

A [NAT Gateway](#) can translate the private IP address in a Virtual Private Cloud (VPC) to a public IP address if the private and public networks are isolated from each other, enabling the VPC to access the Internet. The NAT Gateway supports a maximum of 5 Gbps traffic surge and 10,000,000 concurrent connections. As a highly available gateway, the NAT Gateway also provides master/slave hot backup. When one server fails, its automatic switchover helps ensure your businesses intact. As a gateway with the ability to translate private IP addresses in a VPC to public IP addresses, the NAT Gateway provides a way for cloud resources that reside in a VPC without a public IP address to access the Internet. For more information about the typical use cases of the NAT Gateway, see [Use Cases](#).

What are the differences between NAT Gateways and public gateways?

Both are used for CVMs in a VPC to access the Internet, but there are some differences. For more information, see the “Differences Between the NAT Gateway and the Public Gateway” section in [Overview](#).

What types of configuration do NAT Gateways provide?

Each NAT Gateway can bind up to 10 EIPs, and provides three configuration types. For more information, see the “Configuration Specifications” section in [Product Specifications](#).

What are the key features of NAT Gateways?

NAT Gateways highlight features including SNAT, DNAT, high performance, high availability, monitoring details display, and refined gateway traffic control. For more information, see [Features](#).

What are the constraints of NAT Gateways?

Notice the constraints when you are using the NAT Gateway. For example, if you delete a NAT Gateway, its EIP will be disassociated, but not released from the account. For more information, see [Use Limits](#).

What is the network topology of NAT Gateways?

When resources like CVMs in a VPC send out data packets through the NAT Gateway, the data will first travel through the router and select a route based on the routing policies. For more information,

see the “Network Topology” section in [Overview](#).

What are the key features of NAT Gateways?

- SNAT and DNAT are supported.
- The Anti-DDoS service is supported.
For more information, see [Features](#).

What is an EIP?

An EIP is a static IP address designed for dynamic cloud computing, and is a fixed public IP address in a region. You can use EIP to quickly remap an address to another NAT Gateway under your account to shield instance failures. For more information, see [Elastic Public IP \(EIP\)](#).

What can the NAT Gateway bandwidth limit do?

- Role: NAT Gateway bandwidth limit provides **monitoring** and **control** capabilities at **IP-gateway** granularity. The visualization helps network OPS personnel get a clear picture of the gateway traffic. The speed limiting capability at IP-gateway granularity helps block unhealthy traffic. The gateway bandwidth limit has the following advantages:
 - It can accurately troubleshoot gateway exceptions to minimize network downtime. Using real-time traffic query and Top-N ranking features, it can analyze the source IP and its key metrics to quickly locate unhealthy traffic.
 - With **monitoring** and **control** capabilities at IP-gateway granularity as well as minute-level network traffic queries, it can efficiently identify unhealthy traffic that consumes the bandwidth. The bandwidth limit at IP-gateway granularity ensures the stable operation of key businesses.
 - With gateway traffic analysis capability for all traffic at all times, it helps minimize network costs. By means of QoS, it can limit the bandwidth of non-key businesses to reduce costs.
- For example, the gateway traffic of an enterprise surges on one morning. With intelligent gateway bandwidth limit, the OPS personnel can trace the IP that caused this surge based on a point in time. The gateway bandwidth limit features IP-gateway granularity to control the bandwidth from an IP to the gateway, blocking unhealthy traffic to protect key businesses.

What is a region?

Different regions of Tencent Cloud are completely isolated to ensure maximal stability and fault tolerance across regions. The South China, East China, and North China nodes cover China Mainland. The Hong Kong (China) and Singapore nodes for South East Asia, the Toronto node for the North America, and the Silicon Valley node for the Western U.S, are also available. In the future, we will make more nodes available and cover more regions. We recommend you select a region closest to your customer to reduce access latency and increase access speed.

How do I select the most Suitable region?

Select a region under the principles below:

- Close to your users.

Select the CVM region based on the user's geographical location. The closer the CVM is to your users who will access it, the shorter the access latency and the higher the access speed will be.

- In the same region.

CVMs are interconnected in the same region over a private network, but cannot communicate with each other across regions. To enable interconnection among multiple CVMs over a private network, you need to reside them in the same region. The intra-region interconnection over a private network is free of charge, while the cross-region communication is only available over a public network at a cost.

How are availability zones isolated from each other?

Each availability zone operates in its own separate, physically distinct infrastructure and has been designed to feature high reliability. Common points of failure like generators and cooling devices are not shared between availability zones. In addition, availability zones are physically independent of one another, so even in the case of rare disasters such as fires, tornadoes, or floods, only a single availability zone will be affected.

How many NAT Gateways can I create?

It depends on the use limits of resources. To increase the quota, please [submit a ticket](#).

Billing

Last updated : 2020-05-12 15:09:55

How is NAT gateway billed?

NAT gateway fees consist of the following:

- Gateway fees (billed by the hour).
- Public network traffic fees

For more information on billing, see [Billing and Pricing](#).

For additional VPC pricing information, see [VPC Price Overview](#).

Why am I charged for a NAT gateway I did not use?

NAT gateways feature dual-server hot backup. The system sends a 5 KB detection packet to the master and slave NAT gateways every 3 seconds, thereby generating 0.2747 GB of traffic each day. The prices of traffic in Mainland China (not including Hong Kong, Macao, and Taiwan), Hong Kong, and North America are: 0.12 USD/GB, 0.12 USD/GB, and 0.077 USD/GB.

Will I receive a reminder when my NAT gateway expires?

When the balance in your account becomes 0, you can still use your NAT gateway for 2 hours, but you will be charged for that time. If your account balance is still not greater than 0 after two hours, your NAT gateway stops to function and billing stops. If your account balance is still not greater than zero 24 hours after your NAT gateway stops working, the NAT gateway becomes unavailable, which means you cannot access it anymore. As soon as your account balance is greater than 0, your NAT gateway functions again and billing starts. If your account balance remains at or below 0 for more than 24 hours after your NAT gateway stops functioning, your NAT gateway is repossessed. We will alert the account owner and all collaborators via email and SMS when we repossess the NAT gateway.

If I configure the routing table to allow one of my subnets to access the public network through a NAT gateway and the CVM instances in that subnet are configured with EIPs. Will these CVM instances access the public network through the NAT gateways or EIPs?

When there are multiple routing policies in a route table, the following routing priority applies, from high to low:

- VPC traffic
- Exact match routing

- Public IP

For more details, refer to [Route Tables](#).

Features

Last updated : 2020-07-09 14:43:39

How do I use the NAT Gateway and EIP?

- The NAT Gateway can translate the private IP address in a VPC to a public IP address. It is an ingress or egress for public network traffic in a VPC. For more information about how to use Tencent Cloud's NAT Gateway service, see [NAT Gateway](#).
- The NAT Gateway and EIP are two ways for CVMs to access the Internet. You can use either or both of them to design your public network access architecture.

How can I learn more information about security?

Tencent Cloud provides various network and security services such as security groups, encrypted login, and EIPs to back up your instances on the provision of secure and efficient services. For more information about CVM security, see [Network and Security Overview](#).

How do I prevent others from querying my system?

You have full control over the visibility of your system, and the CVM allows you to place running instances into any security group of choice. In the [Security Group Console](#), you can specify inter-group communication and IP subnets on the network that can communicate with the CVM.

How do I troubleshoot security issues?

If you perceive any security event or adverse event, see [Cloud Workload Protection](#) for troubleshooting.