

NAT Gateway

FAQ

Product Documentation



Copyright Notice

©2013-2024 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

FAQ

Billing

Concepts

Features

FAQ

Billing

Last updated : 2024-01-04 21:49:21

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](#).

Concepts

Last updated : 2024-01-04 21:49:21

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 G bps traffic surge and 10,000,000 concurrent connections. As a highly available gateway, the NAT gateway also provides master/slave hot backup, enabling automatic switching in the event of a single point of failure with an imperceptible impact on your use of the services. As a gateway with the ability to translate private and public IP addresses within a VPC, 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 application scenarios of the gateway, please see [NAT Gateway-Application Scenarios](#).

What are the differences between NAT gateways and public gateways?

Both NAT gateways and public gateways are used by CVMs within the VPC to access the Internet. However, there are some differences between them. For more information, please see [Differences Between NAT Gateways and Public Gateways](#).

What types of configuration do NAT gateways provide?

NAT gateways support the binding of up to 10 EIPs, and provide three configuration types. For more information, please see [Configuration Types of NAT Gateways](#).

What are the key features of NAT gateways?

NAT gateways feature SNAT, DNAT, high performance, high availability, monitoring details display, and refined gateway traffic control. For more information, please see [Features of NAT Gateways](#).

What are the constraints on the use of NAT gateways?

There are constraints on the use of NAT gateways. If a NAT gateway is deleted, its EIP is disassociated from it, but not released from the account. For more information, please see [Use Limits of NAT Gateways](#).

What is the network topology of NAT gateways?

When resources like CVMs within the VPC send outbound 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, please see [Network Topology of NAT Gateways](#).

What are the main features of NAT gateways?

SNAT and DNAT are supported.

The Anti-DDoS service is supported.

For more information, please see [Features of NAT Gateways](#).

What is an EIP?

An EIP is a static IP address designed for dynamic cloud computing, and is a static public IP address in certain regions. By using EIPs, you can quickly remap an address to another NAT gateway in your account to fail over instance failures. For more information, please see [Elastic Public IP \(EIP\)](#).

What can NAT Gateway Traffic Control do?

NAT Gateway Traffic Control provides the **monitoring** and **controlling** capabilities at IP-gateway granularity. The refined gateway traffic visualization enables network OPS personnel to get a clear picture of the traffic in the gateway. In addition, the speed limiting capability at IP-gateway granularity helps to block abnormal traffic. The advantages of gateway traffic control are as follows:

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 the **monitoring** and **control** capabilities at IP-gateway granularity and by using minute-level network traffic query, it can identify abnormal traffic that maliciously consumes the bandwidth in real time, and set bandwidth limits at IP-gateway granularity to ensure the stable operation of core 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, in an early morning, the gateway traffic of an enterprise surges. With intelligent gateway traffic control, the OPS personnel can trace data to find which IP addresses caused this traffic surge according to the time when the traffic surge occurred, so as to rapidly locate its source. In addition, the gateway traffic control feature provides bandwidth control at IP-gateway granularity, which can restrict the bandwidth from an IP address to the gateway and block abnormal traffic to safeguard key businesses.

What is a region?

Different regions of Tencent Cloud are completely isolated to ensure maximal stability and fault tolerance between regions. The South China, East China, and North China nodes cover China mainland. The Hong Kong (China) and Singapore nodes, which cover South East Asia, the Toronto node which covers North America, and the Silicon Valley node for the Western U.S, are also available. In the future, we will provide more available nodes to cover more regions. We recommend that you choose the region closest to your customers to minimize access latency and improve download speeds.

How do I select the most Suitable region?

Region selection abides by the following principles:

Be close to your users.

The region of a CVM should be selected 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 in the same region are interconnected with each other via the private network, but those in different regions cannot communicate with each other via the private network. Users who communicate with each other using multiple CVMs via a private network should choose the same region. CVMs in the same region can communicate with each other via a private network free of charge. CVMs in different regions cannot communicate with each other via a private network but only via a public network with a charge.

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?

Each VPC support 3 NAT gateways. For more information, please see [Use Limits](#). If you require a higher quota, please [submit a ticket](#).

Features

Last updated : 2024-01-04 21:49:21

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.